University of Sheffield

User Consent in IoMT System: A Case Study of Saudi Arabia

Hebah Albatati

Supervisors: Professor John Clark - TUoS

Dr Maysoon Abulkhair - KAU

A report submitted in partial fulfilment of the requirements
for the degree of Doctor of Philosophy

Faculty of Engineering
Department of Computer Science

November 6, 2024

Declaration

I, Hebah Ali Albatati, hereby declare that this PhD thesis titled "User Consent in IoMT System: A Case Study of Saudi Arabia" is the result of my original research work, and I have submitted it to the University of Sheffield to fulfil the requirements for the degree of Doctor of Philosophy. I am aware of the University's Guidance on the Use of Unfair Means (www.sheffield.ac.uk/ssid/unfair-means). All the ideas, concepts, and findings presented in this thesis are my own work, except where otherwise acknowledged. This work has not been previously presented for an award at this, or any other, university. Some parts of this thesis have been published in peer-reviewed conferences.

Name: Hebah Ali Albatati

Signature: Hebah

Date: 26-10-2023

Acknowledgements

I want to express my deepest gratitude and appreciation to all who have supported me throughout my doctoral studies and the completion of this thesis. The work in this study would not have been accomplished without the support of many people. First and foremost, I am immensely grateful to my supervisors, Professor John A. Clark (TUoS) and Dr. Maysoon F. Abulkhair (KAU), for their guidance, wisdom and unwavering support. Their expertise, patience and dedication have been invaluable in shaping this research and enhancing its quality. I am truly fortunate to have had their mentorship throughout this process.

I would like to express my sincere gratitude to the people who volunteered to participate in the survey and the experiment and who contributed their time, insights and experiences. Their valuable contributions were instrumental in completing this research, and I deeply appreciate their willingness to be involved. I would also like to acknowledge the professionals and experts who provided guidance during the research, especially Mrs Manal Binyameen, who helped us with her statistical expertise and advice.

My special gratitude goes to my parents, Ali and Zenah, whose love and affection have been a source of motivation and encouragement for my studies. I would also like to thank my sisters (Hadeel, Hanadi and Hanouf) and my brother (Faisal) for their unconditional support and for simply being there. They always supported and encouraged me with their best wishes. I would like to extend a special, heartfelt thank you to my loving husband, Khaled, for his unwavering support, patience and understanding throughout this entire journey. His belief in my abilities, his encouragement and his sacrifices have been the cornerstone of my success. I also want to express my deep appreciation to my three wonderful sons, Omar, Abdelelah and Ali. Their unconditional love, understanding and flexibility have been a constant source of inspiration and motivation. Their patience during my long hours of study and their understanding of the sacrifices required for this endeavour has touched my heart. I am grateful for their support and the joy you bring to my life.

Abstract

The legal and ethical frameworks that apply in many countries around the world require service providers to obtain users' agreement to the collection and further processing of their personal data. The healthcare sector has long-established foundations regarding consent processes for medical procedures, treatments and the use of patients' data. As it now seeks to provide many services online, it must refine its processes to maintain its current standards. Of particular interest, the Internet of Things (IoT) is emerging as an important means to deliver healthcare services. Such systems raise many issues regarding consent. For example, some users may not be familiar with their privacy rights, others may not read or understand the privacy policies of service providers, and many may not be familiar with the technical risks posed by IoT systems. This lack of awareness may lead users to give consent for the collection or processing of their sensitive data without being fully informed. Therefore, a consent tool is one of the important components of an IoT system that collects and processes user's personal data, particularly in the Internet of Medical Things (IoMT) services, where the required data is considered highly sensitive. The specific design and implementation of such tools may affect the users' decisions regarding consent. Thus, it must be considered whether online management of consent by users is actually reasonable. To do so, we must understand how aware users are of relevant issues and how online consent tools can facilitate the provision of informed consent.

To address the above, a case study that includes two main parts was conducted. The first part focused on a study that investigated the level of privacy awareness among users of healthcare services in Saudi Arabia. This used a quantitative survey method. Two types of assessments were used: a subjective assessment, which depended on the participants' self-assessment, and an objective assessment, wherein the questions had right and wrong answers (which do not depend on the participants' opinions). The second part focused on a study aimed to explore how users with different privacy awareness levels actually made personal data consent decisions when presented with various scenarios. Such consent was managed using two different smartphone-based applications. The experiment sought to establish how specific aspects of the consent mechanism design affect user-informedness and the actual decisions made. A within-subject experiment approach was used, incorporating both quantitative and qualitative methods. The results revealed that most participants have a medium level of privacy awareness, with no significant differences observed between the objective and the subjective assessments. The results show that users found some aspects of consent tool design helped them make more informed decisions. However, there is still a need to enhance users' privacy awareness levels regarding their data and to educate them about the privacy regulations that govern their data and the importance of understanding service providers' privacy policies.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The Internet of Things (IoT) is one of the most significant technologies in information and communications. Moreover, it is one of the leading technologies used to develop intelligent and sustainable innovations, and it is becoming increasingly important in the development of smart cities (Bellini et al. 2022). The IoT refers to a worldwide network of sensors, mobile devices and equipment that can function and communicate in real time (Rivadeneira et al. 2021). Various objects in the environment can interact through wireless and wired connections and special addressing schemes. These objects can work together to facilitate services and accomplish shared objectives (Patel et al. 2016). Sectors such as industry, transportation, agriculture and healthcare have developed IoT systems to improve the quality of their services. For example, IoT systems assist manufacturers in monitoring machines. Real-time sensors gather data such as cycle length, downtime, the number of components produced and other relevant parameters, which are then analysed to increase productivity and optimise machine utilisation (Javaid et al. 2021). Furthermore, IoT services and systems provide better experiences and make daily tasks easier. IoT systems in smart homes enable people to control energy consumption and manage appliances and home resources (Bellini et al. 2022) such as air conditioning systems (Neisse et al. 2015). IoT systems also make possible intelligent vehicles, such as self-driving cars, and help reduce road accidents and reckless driving (Fantin Irudaya Raj & Appadurai 2022). Connected cars with internet connections receive real-time data about city traffic and navigation details from cloud storage (Fantin Irudaya Raj & Appadurai 2022). Additional services and applications will develop as IoT technology evolves and becomes more widespread.

Healthcare is a critical area in which services depending on IoT systems are developing rapidly. The terms Internet of Medical Things (IoMT) and Internet of Healthcare Things (IoHT) are usually used to refer to the use of IoT technology and systems in healthcare. These systems comprise medical devices and software that use the internet to allow healthcare providers to collect, transmit and analyse patient information. In healthcare, the IoT often focuses on medical and fitness devices and applications that collect data from users. It then links them to healthcare IT systems via networks (De Michele & Furini 2019). Intelligent sensors on or near the body help to collect and transfer medical data (Scarpato et al. 2017, De Michele & Furini 2019). Medical professionals, such as doctors, nurses and others, can monitor patients' vital signs remotely in real time (Scarpato et al. 2017, Durán-Vega et al. 2019, Sun et al. 2019), allowing patients to receive treatment at home rather than making regular visits to hospitals or clinics (Al Bassam et al. 2021). This will reduce costs and save time (Pramanik et al. 2019). In addition, medical professionals can access a patient's data at any time (De Michele & Furini 2019). Patient data can be analysed to provide appropriate healthcare services, predict future health problems (De Michele & Furini 2019, Pramanik et al. 2019, Sun et al. 2019), and conduct medical research (Pramanik et al. 2019). The IoT can be used to manage patient information, emergency warning systems (Scarpato et al. 2017), medication management, and rehabilitation systems (Pradhan et al. 2021). It also facilitates remote patient monitoring systems, such as

those used to observe COVID-19 patients' vital signs (Al Bassam et al. 2021). Ensuring patients' information security, privacy and confidentiality are essential in healthcare to safeguard sensitive data against misuse (Pramanik et al. 2019). Moreover, the reliability and integrity of health data are crucial to ensure error-free diagnosis (Pramanik et al. 2019). Medical and health data are considered more sensitive than data in other sectors (Tanczer et al. 2017) such as transportation or industrial data. Therefore, IoMT systems must provide rigorous measures to protect the privacy of patient data.

1.1 IoT Privacy Issues and Users' Consent

IoT systems use technologies such as wireless networks (4G/5G) and cloud computing to connect devices, actuators, sensors and other equipment to form large-scale networks that automatically monitor and control collection, processing and communication activities without the need for human intervention (Ahmed et al. 2022). With the rapid increase in the number of connected IoT devices, a massive amount of data has been generated, and communication between these devices has become more complex. Data security and privacy are two of the most critical issues that have emerged with IoT technology (Zhou et al. 2018, Waheed et al. 2020, Babun et al. 2021). Strong measures need to be implemented in IoT systems to overcome security and privacy problems. Security measures usually focus on protecting systems and devices from viruses, external attacks and threats through the use of methods such as encryption and authentication (Abi Sen et al. 2018). Privacy measures focus on the data, especially highly personal or sensitive data; they concern authorisation, access control and trust, and the prevention of data misuse and data tracing (Abi Sen et al. 2018). Data privacy in IoT systems must be ensured in the collecting phase (Loukil et al. 2017) and during all other phases performed outside the user device, such as processing and storage (Sharma et al. 2018). Researchers have suggested different approaches and technologies to achieve users' privacy in IoT systems. However, many of the proposed privacy solutions are complex, which makes it challenging to ensure their reliability (Abouelmehdi et al. 2017). In addition, IoT privacy modelling is still in its infancy (Zhou et al. 2018); accordingly, IoT systems remain vulnerable to many types of privacy violations (De Michele & Furini 2019, Babun et al. 2021, Zhou et al. 2018).

Lopez et al. (2017) divided IoT privacy issues into two main types: network privacy problems and user privacy problems. In network privacy attacks, the content of the transferred packet, which may contain sensitive information, and the transmission information (e.g. the size and the number of messages being transmitted), are the targets (Lopez et al. 2017). In user privacy attacks, the targets are users' personal information and sensitive data (Lopez et al. 2017). Most user privacy violations occur in the IoT application layer (Babun et al. 2021). Some of these privacy violations can be performed without breaching the security measures in the system. It is easy for an attacker to infer what people are doing and determine when they are out of the house by surveilling IoT device behaviours in the wireless network (Babun et al. 2021). Users' identities and sensitive information may be exposed when data is collected via the sensors (Alkhatib et al. 2018). Malicious attackers can use this data to perform activities such as phishing. Moreover, user data collected by devices and the statistics generated from this data may be used to discover user behaviour patterns (Alhirabi et al. 2021). In some IoT services, data can be collected without users' knowledge, or users are not informed about the types of data that are collected (Babun et al. 2021). This collected data can be combined with other personal information to produce a profile of the user (Atlam & Wills 2020). Most of the time, users have no information about who will use their collected data and for what reasons (Loukil et al. 2017). IoT devices can track users' locations across space and time (Ogonji et al. 2020), and user data can be employed without the user's knowledge for purposes other than those for which they were collected (Alkhatib et al. 2018). This is referred to as *secondary usage*. For example, an IoT service provider may allow an advertising company to access and make use of

users' data without the users' consent (Zhou et al. 2018). Similarly, medical data can be utilised for research without the patient's permission (Pramanik et al. 2019). Insider attacks, involving an attacker who has authorised access to the system, are among the most dangerous attacks on data confidentiality and user privacy in IoT (Ahmed et al. 2018).

Many solutions have been proposed to overcome personal data privacy violations in IoT systems. One is the provision of control mechanisms that enable users to dictate when and how others acquire and utilise their personal information (Sengul 2017). In addition, solutions that allow users to customise their privacy based on their usage and privacy expectations are needed (Psychoula et al. 2020). A well-designed informed consent mechanism is crucial in IoT systems. It gives users control over their data and allows them to express their privacy preferences. Additionally, consent management technology should be employed to help users manage personal data not only during acquisition, but throughout the data's life cycle (Pesch et al. 2022).

User consent faces challenges in the legal, technological, sociological, privacy, security, User Interface/User Experience (UI/UX) and Human-Computer Interaction (HCI) domains (Pesch et al. 2022). In the coming years, consent will be a significant subject in the IoT arena because of the massive amount of personal data collected by IoT sensors and the implementation of regulations, such as the General Data Protection Regulation (GDPR) (Tanczer et al. 2017). Several studies have provided technical solutions for obtaining user consent in IoT systems. However, critical issues, such as the legal methods, user awareness level and the risks facing users and other actors, should be considered (Tanczer et al. 2017). Most users lack privacy awareness (Zhou et al. 2018); however, they need to have a suitable level of privacy awareness to make appropriate decisions regarding their data. In addition, they must understand how and why their data will be used and the benefits and consequences of that use before they give their consent (O'Connor et al. 2017). Consent mechanisms can help users enhance their privacy awareness by providing all the information they need to make appropriate decisions about their data.

1.2 Research Justification

IoMT systems are a promising field within the domain of IoT. Sensitive user data plays a critical role in these systems. The functionality of these systems relies on the collection, transfer and processing of users' personal information, especially medical information, to provide the necessary services (Zhou et al. 2018, Sharma et al. 2018, Sun et al. 2019). Physiological and sensitive information is collected through devices that can be placed on a person's body, such as wearable devices, and transferred to the cloud for further computing or analysis. Medical information and data are classified as *sensitive identifiable information* (PDPL 2023). Innovative IoT-enabled healthcare services process a massive amount of sensitive data. This type of data must be handled with the utmost care and discretion to ensure the privacy and security of healthcare users' personal information (Stallings 2019). Thus, data privacy is one of the most critical challenges that IoMT systems face (De Michele & Furini 2019, Sun et al. 2019, Miller et al. 2022). Violating health data privacy may cause direct harm to users, making them feel surveilled or cutting into their independence (Miller et al. 2022). Technical solutions alone are insufficient to protect sensitive data, as technological development is one of the primary causes of data privacy violations (Miller et al. 2022). Some types of privacy violations can be prevented by obtaining informed consent before the data is collected or processed (Miller et al. 2022). Users should have some control over their health data and the ability to determine who can access it (Pramanik et al. 2019). Hence, a well-designed consent mechanism that gives users a degree of control over their data and provides them with clear and easily comprehensible information for making informed decisions about their data when collected, used and shared is essential for the following reasons:

- Patients' informed consent is required before medical procedures and treatments as it is a fundamental step in healthcare. This process involves providing clear, comprehensive information about a medical intervention's risks, benefits and alternatives. Informed consent is also required when using patients' data for purposes beyond healthcare. For instance, patients' consent is required when using their data in research, such as using their medical data to improve specific treatment outcomes.

- Users' consent is required legally in many countries when collecting, transferring, using or performing any actions on users' personal and sensitive data. For instance, the GDPR in Europe and the Personal Data Protection Law (PDPL) in Saudi Arabia require obtaining such consent. Moreover, obtaining users' consent to collect and use their data is considered an ethical obligation.

- Health and medical data are classified as sensitive under regulations such as the GDPR in Europe (GDPR 2018) and the PDPL in Saudi Arabia PDPL (2023); thus, it is crucial to handle this data with the utmost care during collection, storage and usage. IoMT sensors collect health and medical data, including vital signs such as body temperature, oxygen saturation, heart rate, blood pressure, blood glucose level, etc. This information is then transmitted to servers for in-depth analysis (Vishnu et al. 2020). Additionally, IoMT sensors collect biometric data, such as heart rate variability (HRV), facial recognition and retinal scans, which are considered private and sensitive (Popoola et al. 2023). Furthermore, IoMT sensors also collect personal data, such as environmental information, activities and locations, which is then used to personalise or enhance healthcare services (Zhou et al. 2018). Users need to know and understand all relevant information before consenting to the collection, use and sharing of their data.

- Some studies in the literature aim to develop a generic user consent solution that can be used in different IoT services. However, this can be challenging for many reasons, including technical requirements (e.g. transmission protocols used across different devices) and factors influencing consent design, such as data sensitivity levels and the diversity of user characteristics. IoMT services collect medical and biometric data, which are highly sensitive compared to other services, such as home automation solutions that aim to enhance services without requiring the collection of sensitive data. Moreover, users of healthcare services vary in demographic characteristics, such as educational level and socioeconomic status, which can impact their understanding of privacy risks and their willingness to share their data. This level of data sensitivity and diversity in users' characteristics emphasises the need for well-designed consent mechanisms for IoMT that help these users make appropriate decisions regarding their sensitive data.

Soon, people will configure and use IoMT devices and sensors anywhere without professional assistance. Yet, if users are to have a role in protecting their data, they must think more like an administrator than an ordinary user (Zhou et al. 2018). However, many people are unaware of proper privacy protection and data management (Zhou et al. 2018). They may have difficulty managing their privacy preferences and settings or may not fully understand the consent process. There may also be issues related to interoperability and standardisation, as different healthcare providers may use different consent tools or have different consent policies. Thus, giving regular users a role in controlling their data in IoT systems, especially healthcare systems, cannot be achieved without increasing their privacy awareness to allow them to make appropriate decisions about their data. The consent mechanism can be used to enhance users' understanding and support their decision-making about their data (Cumyn et al. 2020). Most studies in the literature that investigate solutions for obtaining users' consent in IoT focus on security mechanisms, such as encryption and authorisation, or communication technology, such as Bluetooth. Moreover, most of these studies focus on meeting the privacy requirements

of the GDPR and principles such as Privacy by Design (PbD) when developing IoT consent mechanisms (Neisse et al. 2016, O'Connor et al. 2017, Sengul 2017, Castelluccia et al. 2018, Laurent et al. 2019, Morel et al. 2019, Lee et al. 2019, Rantos et al. 2019, Rhahla et al. 2019, Pathmabandu et al. 2023). A number of the proposed solutions in the literature depend on users' mobile devices, or, less commonly, computers, to assist the user in interacting with consent mechanisms and managing consent (Kouzinopoulos et al. 2018, Rhahla et al. 2019, Laurent et al. 2019, Morel et al. 2019, Rantos et al. 2019). A user-friendly solution to help users set their consent policies is required (Sengul 2017). Therefore, the involvement of experts in human-centred approaches, that is, UX and HCI, is required when designing and developing mechanisms to obtain user consent (Schraefel et al. 2017).

The literature reveals three main gaps in prior studies that address consent mechanisms in IoT systems.

- **First Gap:** Most of the literature stressed the significance of users' comprehension and awareness when engaging with a consent mechanism. However, there is a lack of studies investigating the state of privacy awareness of digital healthcare service users to determine whether they can make appropriate decisions when dealing with the consent mechanism in IoMT.
- **Second Gap:** Although the majority of the literature stressed the significance of consent mechanisms in IoT services, practical experiments are still lacking with regard to how users with different levels of privacy awareness make decisions and how specific mechanisms influence those decisions.
- **Third Gap:** Many studies in the literature emphasised the importance of obtaining users' informed consent. However, there is a lack of knowledge regarding the specific features of consent mechanisms and their influence on users' informedness in IoMT. No studies have involved users in assessing the features that contribute to their informedness of when using consent mechanisms in IoMT.

1.3 Contextual Motivation

Saudi Arabia is at the forefront of countries working on digital transformation and smart city development. According to the "Saudi Arabia 2030 Vision" the nation aims to transform cities into smart cities, beginning with Riyadh, Makkah, Jeddah, Al-Khobar and Madinah [1]. The nation aims to use the comprehensive adoption of new technologies, especially IoT, in industry, education and healthcare. Healthcare is one of the primary sectors the government is focusing on developing in these smart cities. The Saudi Data & AI Authority (SDAIA), in cooperation with the Ministry of Health in Saudi Arabia, is focusing on using AI, IoT and other technologies to improve the quality of its healthcare services and develop electronic health systems with increased patient involvement. However, many technical and non-technical challenges have emerged, and ongoing efforts are focused on devising solutions to address these challenges. The early adoption of technology, including IoT, in Saudi Arabia provides researchers and the research community with an opportunity to explore the implications of IoT technologies in a comprehensive, real-world context. This reflects the challenges and opportunities that other regions are likely to face in the near future and researchers have developed valuable insights into the available solutions to face these challenges.

One challenging area that needs to be addressed is users' informed consent in IoMT. Consent is required legally by the PDPL in Saudi Arabia; it is ethically required in this case. Users might configure the settings of devices that collect their personal and medical data, such as wearable

[1] https://sdaia.gov.sa/en/MediaCenter/News/Pages/NewsDetails.aspx?NewsID=285

devices, by themselves. It is essential to design consent mechanism that helps them understand the information needed to make informed decisions, such as the benefits and risks of sharing their data. Investigating users' privacy awareness and how they interact with the consent mechanism in the IoMT scenario can provide insights into consent design for regions with the same culture and opportunities to conduct comparative analyses with other regions and identify best practices in the design of informed consent for IoMT.

1.4 Research Aims and Objectives

This thesis has three main aims and objectives:

- **First:** To identify and assess privacy awareness among users of digital healthcare services in Saudi Arabia by examining their knowledge and understanding of it.
- **Second:** To investigate how users with varying levels of privacy awareness make decisions regarding their data when using consent mechanisms in IoMT services and examine the impact of the specific features of consent mechanisms on users' decision-making processes.
- **Third:** To identify the specific features of consent mechanisms in IoMT that contribute to users' informedness and awareness of their data and evaluate how these features assist them in providing informed consent.

1.5 Research Questions

The following research questions are addressed in this thesis:

- **RQ1 (User privacy awareness): How does the awareness of privacy issues relating to personal data vary among digital health system users?**
- **RQ2 (Decision-making): How does the enhanced design of consent mechanisms affect the decision-making of users with different privacy awareness levels on the collecting, processing, usage, and sharing of their data in IoMT systems?**
- **RQ3 (Informedness): To what extent do the features of the enhanced design of consent mechanisms in IoMT affect the informedness of users with different privacy awareness levels when they make decisions about their data?**

To support the RQ2 and RQ3 primary research questions, we developed the following sub-question:

- **SQ1 (User Perception): How do users with different privacy awareness levels perceive the specific features of the enhanced design of the consent mechanisms?**

As far as mechanisms are concerned, the work identifies and deploys both 'standard' mechanisms in its experiments and mechanisms with the potential to improve consent tools. The latter are referred to as 'enhanced' mechanisms in the research questions above and throughout the thesis.

1.6 Research Contributions

We have sought to gain new insights into users' privacy awareness, informed consent and the mechanisms by which such consent is obtained in the context of IoMT. In order to achieve this, we have in places to innovate methodologically. Thus, our contributions are not only related to what was achieved but also include innovative methods we employed. The contributions below include both methodological innovations and the contributions arising from their application.

- The development of a questionnaire which provides a foundational instrument for investigating privacy awareness of digital healthcare service users, focusing on five primary factors : privacy regulation, privacy policy, perceived benefits, potential risks and user experience. Moreover, this questionnaire can be modified and expanded to examine users' privacy awareness in diverse contexts, such as e-commerce platforms or across different geographical regions. Furthermore, the questionnaire's flexibility allows for the incorporation of additional factors, such as trust, enhancing its applicability and effectiveness in evaluating privacy awareness across various technological landscapes.

- The utilisation of two distinct assessment methods, subjective assessment and objective assessment, in the questionnaire. Subjective assessment, which depends on the participants' self-assessment, and an objective assessment, wherein the questions have right and wrong answers. The combination of these two distinct assessment methods was used to obtain the first understanding of privacy awareness in a sample population from both subjective and objective standpoints. This allowed the first comparison of subjective and objective assessment results for a more comprehensive analysis of privacy awareness, revealing the real alignment between users' perceived understanding and actual comprehension.

- The development and use of the empirical framework to conduct within-subjects experiments allowed the first practical assessment of a set of enhanced interfaces for consent mechanisms in the context of IoMT. The use of the framework provided insights that can inform the development of more effective and user-friendly consent mechanisms. In addition, the post-experiment questionnaire,provides the first user informed assessment of specific consent mechanisms. The framework is flexible and can incorporate other sets of features, allowing reuse in future experiments for different users or contexts. This design can be used as a model with the ability to add features and be reused in future experiments for different users or contexts.

- Two main studies were conducted: The development and use of the questionnaire to investigate privacy awareness (Study 1) and the development and use of the empirical framework, which includes a within-subjects experiment (Study 2) with the same participants. The integration of the results of these two studies allowed for an unprecedented evaluation of how privacy awareness aligns with actual behaviour. This comprehensive approach helped to examine the gap between users privacy awareness and how they behave in practice.

1.7 Publications

Some parts of this thesis have been published in peer-reviewed conferences

- Albatati, H. A., Clark, J. A., & Abulkhair, M. F. (2023, July). Privacy Awareness Among Users of Digital Healthcare Services in Saudi Arabia. In International Conference on Human-Computer Interaction (pp. 247-261). Cham: Springer Nature Switzerland. This work is reported and extended in Chapter 4. The URL for the electronic version of this publication is:

  `https://link.springer.com/chapter/10.1007/978-3-031-35822-7_17`

- Albatati, H. A., Abulkhair, M. F., & Clark, J. A. (2023, January). Toward a Design of User's Consent Tool for IoT-based Healthcare System. In 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC) (pp. 1-7). IEEE. This work is reported and extended in Chapter 5. The URL for the electronic version of this publication is:

  https://ieeexplore.ieee.org/abstract/document/10085034

The remainder of the thesis is not previously published.

1.8 Ethical Approvals

This thesis consists of two main studies involving human subjects. Both were ethically approved before data collection. The research protocol and procedures were reviewed to ensure compliance with ethical principles and guidelines for conducting research involving human participants. For the first study, ethical approvals were obtained from research committees of the University of Sheffield and the Ministry of Health in Saudi Arabia. Regarding the second study, ethical approval was obtained from the University of Sheffield research committee. The committees considered all related ethical considerations, such as participant informed consent, possible risks and benefits of the research to all persons involved in the research, and data confidentiality. The details of ethical approvals and considerations can be found in Section 3.6.

1.9 Thesis Structure

This thesis consists of six chapters. The first chapter serves as the introduction. Details of the remaining chapters are provided below:

- **Chapter 2: Background and Related Work**
  This chapter presents a comprehensive review of relevant theoretical concepts and literature. It is divided into two parts, each focusing on distinct aspects of the research. The first part focuses on privacy and privacy awareness. It begins by providing background on definitions of privacy, information privacy (IP), and information privacy awareness (IPA). It also discusses IP and IPA within the context of IoM (Internet of Medical Things). Next, it delves into the primary sources of privacy requirements, including privacy regulations, privacy principles and standards, and privacy best practices. Finally, it provides background on privacy measurement instruments. The second part focuses on user informed consent. It begins by establishing the significance of user consent as a privacy requirement. Then, an overview of informed consent is provided. After that, this chapter presents proposed solutions for obtaining user consent in an IoT environment, considering the unique challenges in this area. Then, it outlines the key consent features in both healthcare and IoT domains. It further gives a summary of the features of consent mechanisms for IoMT applications. Finally, it outlines the most important features of informed consent mechanism that need to be investigated in the IoMT context.

- **Chapter 3: Research Methodology and Design**
  This chapter introduces and justifies the research design and methodology used to investigate our research. It starts with a general overview of research paradigms and methodology. It defines the specific methodology utilised in this study. It provides a comprehensive description of the designs for Study 1, which is a survey focusing on privacy awareness among users of digital healthcare services in Saudi Arabia. This part includes a description of the methodology used to design and develop the questionnaire, including a literature review of factors shaping privacy awareness, validation and reliability of the questionnaire, and the sampling method and data collection. Then, the chapter presents and interprets the survey results. It provides a detailed explanation of the designs for Study 2, which is an experiment focused on investigating Informed Consent designed for IoMT Services. This chapter also describes the experiment design, hypotheses, measures, and experimental procedures. The chapter concludes with considerations of the ethical aspects of the project.

- **Chapter 4: Results Discussion**
  This chapter provides a comprehensive discussion of the key findings of the research. First, it discusses the results of Study 1 (the survey) in detail, demonstrating the results of the two types of assessment used in the survey to discover privacy awareness of the users of digital health services in Saudi Arabia: subjective and objective. Then, this chapter provides an exhaustive discussion of the findings from Study 2, explaining the results of the within-subject experiment, the post-experiment questionnaire, and the semi-structured interview. The significant findings of the research are identified, considering both the results of Study 1 and Study 2. This chapter evaluates how the results of the two studies provide insight into our research questions and identifies the significant findings of the results.

- **Chapter 5: Conclusion, Limitations and Future Work**
  This chapter summarises the main points covered in the thesis. It presents a comprehensive overview of the main findings and contributions, along with an exploration of their implications. It comprehensively examines the limitations encountered during the study and outlines potential avenues for future research. It begins by highlighting the limitations of Study 1 (the service), focusing on sampling bias and the number of factors investigated. Then, it illustrates the limitations of Study 2 (the experiment), including sampling size, hypothetical scenario and historical threat. In addition, the chapter provides valuable insights into potential areas for future research by identifying unanswered questions and suggesting paths for further investigation.

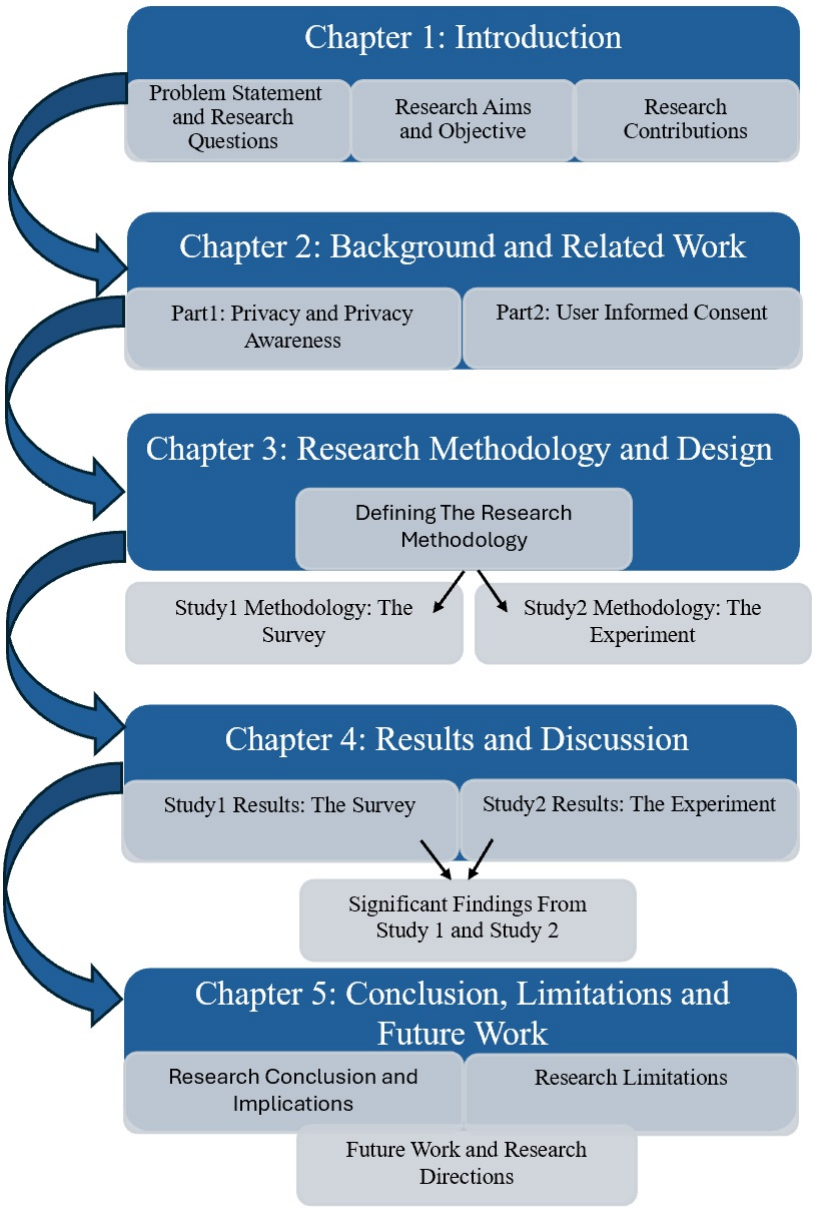

Figure 1.1: *Thesis structure with chapter titles and main sections*

Chapter 2

Background and Related Work

2.1 Introduction

This chapter has two main parts. The first part focuses on privacy and privacy awareness. It covers the key concepts relevant to this research and current practices and activities regarding personal data. It starts with an explanation of the meaning of privacy and information privacy (IP), because these concepts are essential. It then explains information privacy awareness (IPA) and the measurements in the literature that are used to assess IPA. Moreover, it discusses IP and IPA in relation to IoMT and the main strategies used to preserve IP in IoMT systems. Following that, the chapter presents the primary sources of privacy requirements, which include regulations, principles, standards and best practices. The second part focuses on informed consent. It starts by explaining the relationship between informed consent and privacy requirements. Then, it presents an overview of the notion of informed consent in different contexts. It gives an overview of the available solutions for obtaining users' consent in IoT systems and discusses the challenges and flaws in these solutions. This section also provides the background on the most important features that help in obtaining users' informed consent in healthcare systems using e-consent and the IoT. Finally, it illustrates the most important features that help in obtaining users' informed consent in IoMT systems.

Part1: Privacy and Privacy Awareness

2.2 Meaning of Privacy, Information Privacy (IP) and Information Privacy Awareness (IPA)

Privacy and IP are fundamental for people to protect and manage their personal and sensitive data. This section clarifies the meaning of privacy, IP and IPA.

2.2.1 The Meaning of Privacy

The term 'privacy' has always been challenging to define (Finn et al. 2013) as its meaning varies depending on the context. Privacy is a broad term that can include many things, such as privacy in one's home, control over one's body, the right to freedom of thought, control over personal information, freedom from surveillance, the preservation of one's reputation and immunity from searches and interrogation (Solove 2008). Therefore, different fields present privacy from their own perspective (Smith et al. 2011).

Many definitions of privacy have been proposed in the literature. Some of these definitions focus on freedom from interference and intrusion. For instance, one of the most frequently used definitions of privacy is that by Warren & Brandeis (1989), who define privacy in general as "the right to be let alone". Another definition is "the interest that individuals have in sustaining 'personal space', free from interference by other people and organisations" (Clarke 1997). From a different point of view, some definitions focus on the right of the person to control his or her information, such as the definition of privacy in the Cambridge Academic Dictionary (online) [1], in the business English section, which defines privacy as "the right that someone has to keep their personal life or personal information secret or known only to a small group of people". Smith et al. (2011) argues that privacy can be defined using two definitional approaches: value-based and cognate-based. According to the value-based approach, privacy may be viewed as either a human right essential to society's moral value system or as an object subject to trade-offs or a cost–benefit analysis at both the personal and social levels. In contrast, the cognate-based definition of privacy is related to the mind and perception of a person. Hence, from a cognate-based perspective, privacy may be described as a condition of restricted access to a person or as the person's ability to determine who has access to him/her.

Privacy is recognised as a fundamental human right, as clarified in the Universal Declaration of Human Rights (UDHR): [2] "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." Moreover, privacy can be seen as a subjective concept, and a person's perception plays a crucial role in determining what he/she considers as private. It is important to recognise that what is considered private by one person may not be perceived in the same way by another. People's perceptions of privacy vary because, in addition to being subjective, privacy is influenced by objective factors, such as cultural norms, ethical considerations, legal frameworks and public interest concerns (Moore 2003). Privacy is also an issue regarding what society considers appropriate to protect (Solove 2008). Moreover, users have the right to expect a certain level of privacy in terms of their personal information and activities. These rights are protected through legislation, regulations and organisational policies.

2.2.2 Information Privacy (IP)

IP, also known as data privacy, can be considered a part of general privacy (Smith et al. 2011). It focuses on people's data and information rather than on their physical space (Stallings 2019). Different fields of literature, such as marketing, law, management and psychology, have reported on IP (Bélanger & Crossler 2011). Clarke (1997) defined IP as "the interest an individual has in controlling or at least significantly influencing, the handling of data about themselves". Nowadays, when all data and information are being converted into digital formats, many studies have focused on IP from a technical point of view. IP is subjective to people; therefore, it can be categorised as cognate-based (see Section 2.2.1), where users have control over their personal data and information (Smith et al. 2011). Thus, most of the available definitions in the technology area focus on this idea. For example, in the Internet Security Glossary, privacy has been defined as "the right of an entity (normally a person), acting on its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others" (Shirey 2007). This definition highlights the importance of individual autonomy in privacy management. However, the practical implementation of this autonomy can be challenging, especially in environments where data collection is pervasive and often invisible to users. In addition, the Saudi Data & AI Authority (SDAIA) dictionary states that privacy is "a right to control access to and use of physical items and personal information" (SDAIA 2022).

[1] https://dictionary.cambridge.org/dictionary/english/privacy

[2] https://www.un.org/en/about-us/universal-declaration-of-human-rights

However, the individual's right to control data can conflict with the need for services that rely on collecting and processing personal data. This conflict arises due to the tension between an individual's privacy rights and the benefits of the services based on personal and sensitive data. For example, personalised services often collect data about users' behaviour, preferences and interactions to offer personalised experiences, such as targeted advertisements or content recommendations. While this can improve user satisfaction and service efficiency, it also involves extensive tracking and profiling, potentially compromising users' privacy. Two philosophical viewpoints have emerged: the rights-based perspective and the utilitarian perspective (Saxena 2020). The rights-based approach values individual privacy and argues for the importance of individual control over personal data and obtaining consent (Saxena 2020). On the other hand, the utilitarian perspective emphasises the advantages of data analytics and argues that societal benefits can override personal data concerns (Saxena 2020). Thus, it is important to maintain a balance between protecting and respecting an individual's dignity, freedom and privacy, and collecting and using that individual's data. Moreover, what is considered private can differ from person to person. Thus, the personalisation of privacy settings in systems and services can help to address the variations in what each person considers private (Ayci et al. 2023). This allows people to customise their privacy settings and preferences or enables systems to adapt to their specific needs and make appropriate decisions based on their expressed preferences. Therefore, balancing users' privacy expectations and service requirements is crucial. This can be achieved by implementing comprehensive strategies that adjust the necessity of data collection with robust privacy protection measures. These strategies, such as data minimisation, enhanced security measures and privacy-preserving technologies, should fit the user's privacy perceptions and needs within the bounds of legal, regulatory and ethical frameworks.

Both IP and information security (IS) aim to protect data and information. However, the difference between them is that IS is primarily focused on protecting data from attacks that benefit from system vulnerabilities (Pramanik et al. 2019). On the other hand, IP is more concerned with controlling the data and collecting, using and sharing personal data. However, both IP and IS are important, as both are critical to protecting sensitive data. A comprehensive approach that integrates both privacy and security measures is necessary to effectively address the complex landscape of data protection. Robust data governance frameworks and user-centric privacy controls are essential to mitigate these risks and enhance trust in digital services. The term 'IP' commonly focuses on personal data or personally identifiable information (PII), where the data can be used to identify a specific person or track that person down, such as through the individual's name, address information, contact information or information about a particular person that can lead to his or her identification, including, but not limited to, medical data (Stallings 2019). The General Data Protection Regulation (GDPR) identifies personal data as: "any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR 2018). The IP concept existed before information and communication technology rapidly developed (Bélanger & Crossler 2011).

In this current age, with the massive amount of data generated and collected from various sources, such as online systems, crowdsourcing platforms, social media, companies and IoT devices, open data has become widely used. Open data refers to data available in public repositories, which is freely accessible and can be used, shared and accessed by anyone (*Protecting data and opening data* 2018). The process of collecting and publishing open data starts with data collection, which includes gathering data using various methods (Kjærgaard et al. 2020). Following this, data integrity and completeness are ensured before the data are placed in a structured repository, and then cleaned and transformed into a usable format (Kjærgaard

et al. 2020). Then, the data are anonymised to protect privacy and stored in a repository with metadata, which can be a simple file system or a complex database (Kjærgaard et al. 2020). The repositories can be reliable, such as those maintained by governments or trustworthy organisations, with strict privacy considerations and policies, or unreliable repositories that lack privacy, which can pose risks Montori et al. (2020). The aim of open data is to promote transparency, and it has many benefits, such as enhancing the efficiency of services and supporting innovation. Although most of the open data sets do not include any personal or sensitive data, personal data may be included in some cases after rigorous anonymisation processes. However, data protection laws may not apply if the open data does not contain personal data or has been de-identified or anonymised using appropriate mechanisms to the extent that people cannot be identified [3].

Regarding privacy types, in 1997, Clarke (1997) categorised privacy into four distinct types to better understand it. The four types are: the privacy of the person, which is concerned with the probity of the person's body; the privacy of personal behaviour, which is concerned with all aspects of behaviour in public and private places, such as political, religious and media activities; the privacy of personal data, which is concerned with people's private data that must be protected against unauthorised access; and the privacy of personal communication, which is concerned with freedom from monitoring personal communication via various media. Later, he explained that communication privacy and data privacy together formed 'information privacy' (IP). Moreover, Clarke added personal experience privacy to the previous privacy types, which is concerned with the experience people gain from conversing with others, reading newspapers and books, watching videos, etc. However, Finn et al. (2013) argued that Clarke's four main categories needed to be extended because of technological developments. They added three more types: privacy of association, privacy of location and space, and privacy of thoughts and feelings. Privacy of association refers to the person's control over his or her social connections and affiliations, such as the right to keep social connections private and to control the disclosure of social networks or connections (Finn et al. 2013). For example, a social media platform monitors and analyses users' interactions to determine their social networks and affiliations. The privacy of location and space focuses on a person's control over his or her physical location and the ability to determine who has access to it (Finn et al. 2013). An example of this is the right to be free from surveillance or tracking without consent, such as when a smartphone's GPS is used to track movements without permission. However, privacy of thoughts and feelings involves protecting a person's inner mental and emotional life. Sensors and devices can gather and analyse emotional and physiological data that reveal thoughts and feelings (Finn et al. 2013). For example, sensor networks are used in semi-public areas, such as airports, to monitor stress levels and identify suspicious behaviour.

The total number of privacy types has thus become seven (see Figure 2.1). Finn et al. (2013) clarified that some of these seven forms of privacy overlap. However, in their article, they explored the possible impact of some technologies, such as drones, second-generation biometrics and RFID-enabled travel papers, on these seven forms of privacy.

From a different point of view, Solove (2006) provided an IP taxonomy consisting of four parts focusing on activities that create privacy problems and violations: information gathering, processing, distribution and invasion. In their comprehensive article, the authors explained the relationship between data subjects, data holders and privacy violations, and the harm that can occur in each of the four parts. The first part, information gathering, focused on two data collection methods, namely interrogation and surveillance. Interrogation uses various forms of questioning or probing for information, whereas surveillance concerns listening, watching and recording people's activities, which might be used to harm them in various ways . The second part concerns information processing, wherein Solove (2006) discussed five information-processing aspects that cause privacy violations: insecurity involves carelessness in protecting

[3] https://data.europa.eu/en/publications/datastories/protecting-data-and-opening-data

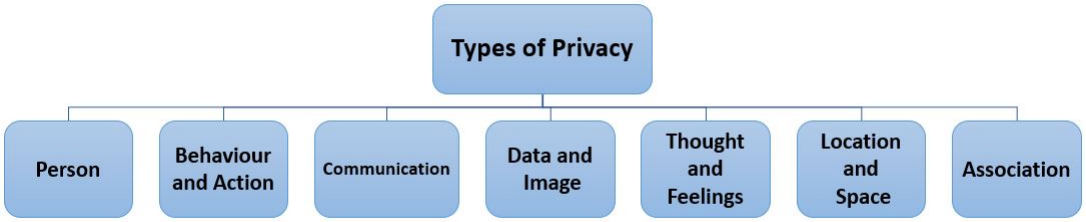

Figure 2.1: *Seven types of privacy by Finn et al. (2013)*

stored information from leaks and improper access; identification is linking information to particular individuals; secondary use is the use of information collected for one purpose for a different purpose without the data subject's consent; exclusion concerns the failure to inform people about the data others have about them and to involve them in its handling and use; and aggregation involves the combination of various pieces of data about a person. The third part focuses on information dissemination. In this part, the authors concentrate on disclosure, breaches of confidentiality, exposure, increased accessibility, distortion, blackmail and appropriation, all of which lead to privacy violations. Disclosure occurs when specific, accurate information about a person is released to others, impacting how others judge his/her character, such as the individual's reputation. Breaches of confidentiality, such as when a healthcare provider shares a patient's private details without consent, damage trust and lead to a breakdown of the relationship. Exposure involves the act of revealing someone else's confidential information. Increased accessibility amplifies the accessibility of information; it refers to making information currently available to the public more accessible, such as by putting data already available at a government office online so that the public can access the data more easily. Distortion involves publishing misleading or incorrect information about a person to adversely affect his/her reputation, bring down his/her status in society or dissuade others from associating or dealing with him/her or his/her constituents. Blackmail focuses on threatening a person to expose his/her personal data if he/she does not comply with the blackmailer's requests, such as requesting money for not disclosing the information. Appropriation involves using a person's identity to meet the goals and interests of another, such as using a person's login credentials to access restricted company information without their knowledge. Invasion is the last part discussed in this article Solove (2006), and it concentrates on decisional interference and intrusion. Decisional interference refers to the undesired intrusion of other entities into an individual's personal life decisions. The intrusion can be unpleasant, terrifying and disrupting, such as being gazed at for lengthy periods. Interrogation is also connected to intrusion, as individuals may perceive interrogation as an intrusion into their affairs. Solove's taxonomy provides a comprehensive framework for understanding privacy violations, but it also highlights the complex connections between various privacy-related activities. One of the important ideas stated by the author is that if a person consents to most of these activities, none of the above will cause privacy violations or harm. However, there is still some debate over what constitutes valid and informed consent. Although Solove (2006) presented a different way to categorise privacy, it is possible now, with the rapid development in technology, to add new parts to the four main parts and add new sub-types, addressing them from a purely technical point of view. For example, information transfer can be added to the main parts, and the privacy violations that can occur when transferring personal data can be discussed. Regarding the sub-parts, in the first part, information gathering, it is possible, for example, that the sensors used in smart homes or those connected to the body to collect personal data may affect the user's privacy.

2.3 Information Privacy Awareness (IPA)

People's awareness of their privacy is essential when dealing with any system that collects, uses and shares their sensitive and private information. The online Cambridge Dictionary defines awareness as "knowledge that something exists, or understanding of a situation or subject at the present time based on information or experience"[4]. However, there is ambiguity in using the terms 'knowledge' and 'understanding', with some studies using both of them with the same meaning. In general, it is commonly known that 'knowledge' is concerned with obtaining information by various means, such as education, while 'understanding' is focused more on recognising the intended meaning of information and the ability to absorb it. Researchers in the field of information technology (IT) have studied security awareness and privacy awareness. However, security awareness has acquired more focus in studies over time (Correia & Compeau 2017). Information security awareness (ISA) is defined as the degree to which users of organisational systems are aware of the importance of the IS policies, rules and guidelines adopted by their company, as well as the degree to which they follow these policies, rules and guidelines in their behaviour (Siponen 2000). ISA is different from IPA in a number of respects. The former involves being aware of attacks that take advantage of systems, programs and network vulnerabilities, as well as the measures taken to protect against these attacks. However, IPA is concerned with the information and data in a system or service, focusing on the use, access, disclosure and control of personal information and data. The term 'information privacy awareness' is still not well documented in the literature, as many studies define it differently (Correia & Compeau 2017, Soumelidou & Tsohou 2021). Emphasising the distinction between knowledge and understanding in IPA is crucial for developing effective privacy education programmes. Knowledge provides foundational information, while understanding enables individuals to apply this knowledge in real-world scenarios, thereby enhancing their ability to make informed privacy decisions and to give informed consent. It has been found that some studies in the literature define privacy awareness as the amount of knowledge, while other studies define it as understanding (Correia & Compeau 2017). For example, Ermakova et al. (2014) define privacy awareness as the amount of knowledge in their definition: "Privacy awareness refers to the degree to which an individual is informed about privacy issues". On the other hand, Malhotra et al. (2004) define it as understanding in their definition: "Awareness factor indicates understanding about established conditions and actual practices".

Endsley (1988) defines situational awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future". This definition divides situational awareness into three levels: perception, comprehension and projection. Perception deals with knowledge of the elements in the current situation, which involves gathering and perceiving relevant information about the environment. Comprehension consists of understanding the information that is presented. The final level of situational awareness involves projecting future developments and predicting potential outcomes based on the current understanding of the situation.

Depending on Endsley's definition of situational awareness, Correia & Compeau (2017) interpret IPA in such a way that they differentiate between knowledge and understanding. They define IPA as a combination of knowledge, understanding and projection of the three elements of technology, regulations and common practices (including privacy policies) in the context of IP. For each element (technology, regulations and common practices), knowledge involves knowing all of its elements and aspects, understanding involves comprehension of its components in the current environment and projection involves predicting how it can change or improve in the future. Even though they explain the term 'awareness' in a detailed way, predicting the future of technology, regulations and privacy policies can be challenging. Numerous factors, including the fast pace of technological advancements, a lack of regulation and policies, and

[4]https://dictionary.cambridge.org/dictionary/english/awareness

other factors, make it challenging. In addition, values and priorities also shift over time, and unexpected events can have a significant impact. However, based on the research conducted by Soumelidou & Tsohou (2021), IPA definitions in the literature can be classified into four distinct categories. First, the definitions focus on awareness of potential threats and their consequences. For instance, Deuker (2010) defines privacy awareness as "individual users' ability to identify and assess risks associated with the disclosure of personal information". Second, the definitions focus on the knowledge and understanding of privacy policies. An example of such a definition is provided by Bergmann (2008), who states that IPA is "the user's ability to reflect the communication partner's privacy policy statements regarding purpose binding, transfer assertion and retention period applied for a certain data disclosure", focusing on privacy policies. Third, the definitions focus on the ability to control and safeguard online privacy, such as the definition provided by Avgerou & Stamatiou (2015): "Privacy awareness's direct value is that it empowers people to protect their personal data". The final category focuses on the awareness of how service providers use personal data. An example of such a definition of IPA is provided by Pötzsch (2009), who explains that IPA is related to four main issues: first, whether or not others receive personal information about him/her, his/her presence and his/her actions; second, which personal information others receive; third, how these pieces of information are processed and used; and fourth, how much information others may access. Soumelidou & Tsohou (2021) find that the first and second categories, which focus on the knowledge of threats and their consequences and the knowledge of privacy policy content, are the most common in the literature. To achieve an extensive definition of IPA, Soumelidou & Tsohou (2021) combine all the aforementioned definition categories. They argue that IPA is concerned with knowing the threats and potential consequences of personal information disclosure, in addition to knowing the content of services' privacy policies. Moreover, IPA involves users' ability to handle and protect their online privacy, which can be achieved by reading and understanding services' privacy policies and taking appropriate action. Although they assume that service providers are concerned with laws and regulations and are obligated to comply with them, it is very important for users to be aware of the regulations and laws that guarantee the privacy of their data and help them take appropriate actions related to their personal and sensitive data. Thus, the definition would be more comprehensive if they clarified how users' awareness of regulations and laws is part of IPA.

2.4 Privacy Awareness Measurements

In general, studies focusing on users' security awareness have attracted more attention in the literature than studies focusing on users' privacy awareness. Employees' understanding of IS is critical because organisations and companies invest a large amount of money in technology to safeguard their systems and data, yet many security breaches result from human errors, whether directly or indirectly (Khando et al. 2021) such as an employee becoming a victim of social engineering. Thus, many of the available security questionnaires focus on employee security awareness. Moreover, many studies on security awareness have been undertaken in universities or colleges, with participants including students, academics and administrative employees (Rohan et al. 2023). Several non-academic questionnaires are available online that aim to assess users' security awareness, such as the Security Awareness Culture Assessment (SANS)[5]. Furthermore, many academic researchers have developed questionnaires to evaluate the level of ISA among different user groups. For example, the Human Aspects of Information Security Questionnaire (HAIS-Q) was developed by Parsons et al. (2013) with the aim of assessing ISA. It investigates the link between policy and procedure knowledge, the attitude towards them, and self-reported behaviour when using a work computer. During subsequent years, the HAIS-Q was developed, and several studies were conducted to verify its validity (Parsons et al. 2017).

[5]https://www.sans.org/security-awareness-training/products/cyber-risk-insight-suite/culture/

Several studies concerning IP have been presented in the literature. Most of these have focused on specific areas, such as privacy concerns, the privacy calculus and the privacy paradox (Correia & Compeau 2017). Usually, privacy concerns are considered when measuring privacy (Xu et al. 2008). Moreover, research on privacy concerns uses a survey method with self-assessment scales to discover and understand users' concerns and opinions. For instance, Smith et al. (1996) conducted one of the most important studies in the literature on privacy concerns, and many subsequent studies have relied on their research. They proposed a framework that outlines the components of people's concerns regarding organisational IP practices. Moreover, they carried out a number of investigations using a strict methodology to develop an instrument to measure privacy concerns regarding IP practices. Their instrument consists of only 15 items divided into four categories: collection, errors, unauthorised secondary use and unauthorised access to information. A seven-point Likert scale was used, where one indicated 'Strongly disagree' and seven denoted 'Strongly agree'. The users assessed themselves on these 15 items. It is important to note that, in the survey and questionnaire context, the term *item* refers to each component of the survey or questionnaire, which can be a direct question or a statement that respondents are asked to rate or agree with.

Malhotra et al. (2004) developed the internet users' information privacy concerns (IUIPC) scale, which is one of the commonly used questionnaires on users' privacy concerns. In addition to the IUIPC scale, Malhotra et al. (2004) proposed a causal model on the relationship between IP concerns and behavioural intention towards releasing personal information. The IUIPC scale focuses on three main dimensions of privacy practices: awareness, collection and control. Malhotra et al. (2004) conducted two empirical studies to develop and test a new scale for the IUIPC. The first study focused on measuring new dimensions of privacy concerns, and the second study focused on constructing second-order IUIPC factors using the new and existing scales. In their first study, they aimed to develop new privacy scales that were not found in Smith et al. (1996)'s scales. First, they reviewed the relevant literature to determine important privacy concerns. Then, they conducted qualitative interviews with experts and internet users to further elicit privacy concerns that might have been missed in the previous stage. As a result, items related to the IUIPC scale were developed. These included 7 awareness items, 15 control items and 21 items addressing online consumer privacy, such as security, honesty and social responsibility. They conducted a survey and collected data from 293 participants. Based on these results, the final IUIPC scale, which contained 10 items, was chosen for use in the second study. In their second study, they undertook a between-subjects experiment in which separate groups of participants were assigned to different experimental conditions to assess variations in their outcomes. Two scenarios were used: Type A, involving less sensitive information (personal shopping preferences), and Type B, involving more sensitive information (personal financial information). Each participant was assigned either to scenario Type A or scenario Type B. Later, Groß (2021) conducted comprehensive investigations on the validity and reliability of the IUIPC scale. They identified biases in questionnaire phrasing and some flaws, and suggested the IUIPC-8 scale, which is considered to be an improvement over the IUIPC scale. Unlike the IUIPC scale, which emphasises information collection and control, Dinev & Hart (2004) proposed using internet privacy concerns (IPC), which focuses on privacy concerns related to the misuse of information and specific private information being disclosed. They used a five-point Likert scale for 26 items. Later, Xu et al. (2012) proposed a theoretical framework for understanding mobile users' IP concerns (MUIPC). They referred to the communication privacy management (CPM) theory to understand mobile users' IP concerns. The MUIPC scale includes nine items with a seven-point Likert scale, measuring three dimensions: perceived surveillance, perceived intrusion and secondary use of personal information. The items related to the secondary use of personal information were derived from Smith et al. (1996). Items derived from Xu et al. (2008) were used to assess perceived intrusion. The researcher developed items for measuring surveillance based on a literature review and interviews.

Pelet & Taieb (2017) focused on understanding privacy policies. They developed a multidimensional privacy policy concern scale to measure users' attitudes towards social network privacy policies. The participants in their study were from France and the United States of America (USA), and most of them were students and employees. Their study had two parts. The first part was qualitative and exploratory. They conducted interviews with 15 respondents and found a connection between internet users' confidence in social networks and their online behaviour. The second part was a quantitative survey. This survey had eight items generated from the first study. They used a seven-point Likert scale. From the studies reviewed above, it was concluded that most of the studies that measured data privacy concerns among users in different contexts, such as online or mobile privacy, depended on the users' self-assessment of their feelings and opinions; thus, they used a Likert scale. However, self-assessment scales may lead the participants to portray themselves positively or over/underestimate themselves. Some studies have used different methods to measure user privacy concerns. For example, Braunstein et al. (2011) conducted a survey to measure privacy concerns by using indirect strategies, which means that they presented privacy warnings to the participants rather than asking direct questions about privacy. They concentrated on various online activities, such as email, news, online calendars, online images, online documents, online transactions, online bank data and browsing history. However, Braunstein et al. (2011) did not apply it to healthcare. They conducted three surveys with the same questions, while modifying the language used to examine its impact on users' responses. These questions depended on self-reported behaviours using a five-point Likert scale. Table 2.1 summarises the main measurements for privacy concerns.

Table 2.1: *The main studies that focus on measuring privacy concerns*

The Reference	The Tool	The Purpose	Dimensions	Items
Smith et al. (1996)	Concern for Information Privacy (CFIP)	Investigated the factors that impact users' concerns about organisational practices	Four dimensions: collection, errors, unauthorised secondary use, and unauthorised access to information	15 items, 7 point Likert scale
Malhotra et al. (2004)	Internet Users' Information Privacy Concerns (IUIPC)	Investigate the factors that influence users' privacy concerns when using the internet	Three dimensions: awareness, control and collection	10 items,7-point Likert scale
Dinev & Hart (2004)	Internet Privacy Concern (IPC)	Investigate privacy concerns related to misuse of information and specific private information being discovered in the internet	Privacy Concerns for Information Finding (PCIF) and Privacy Concerns for Information Abuse (PCIA)	26 items, 5-point Likert scale
Xu et al. (2012)	Mobile users' information privacy concerns (MUIPC)	Measure information privacy concerns of mobile users'	Three dimensions: secondary use of personal information, perceived surveillance and perceived intrusion	9 items, 7-point Likert scale
(Pelet & Taieb 2017)	Privacy Policy Concern	Measure users' attitudes towards social networks privacy policies	Focuses on privacy policies	8 items, 7-point Likert scale

Many survey studies have focused on the privacy calculus theory, which involves weighing the possible risks and potential benefits of disclosing personal information (Smith et al. 2011). For example, Krasnova et al. (2012) applied the privacy calculus perspective to analyse and examine culture's role in self-disclosure decisions on social networking sites (SNSs), such as Facebook, and to encourage users to share information about themselves. Self-disclosure is essential for user involvement and is in the interests of advertisers. However, understanding cultural differences is crucial for the sustainability of SNSs. Krasnova et al. (2012) integrated privacy concerns, anticipated benefits and trusting beliefs as critical predictors of self-disclosure into their model to explore the impact of these beliefs in a cross-cultural setting. They compared Facebook users from Germany and the USA because of their cultural differences. Krasnova et al. (2012) used pre-tested scales from previous studies wherever possible but had to modify or self-develop a significant portion of the scales to reflect the unique context of SNSs. They used a seven-point scale for the items that they developed. Furthermore, based on privacy calculus theory, Kim et al. (2019) investigated the factors influencing users' willingness to share personal information for IoT services. They surveyed three primary IoT services: intelligent transportation, smart homes and the IoMT. They developed the survey items based on previous studies. All of the survey items used a seven-point Likert scale.

Regarding studies investigating privacy awareness, some studies focused on privacy in general and included privacy awareness as one of the factors in the study, for example, Xu et al. (2008) and Zlatolas et al. (2015), while the other studies combined the concept of privacy awareness with security awareness, for example, Bellekens et al. (2016). Xu et al. (2008) designed a model based on information boundary theory (IBT). IBT suggests that users' IP management and disclosure are affected by personal characteristics, such as trust and privacy value. Their research model addressed many privacy issues, such as privacy concerns, privacy value, privacy control, privacy social norms, privacy risks, privacy policies and privacy awareness. The authors explained that privacy awareness reflects the extent to which an individual is informed about privacy practices and policies and how disclosed information is used, and is aware of their impact on the individual's ability to preserve his/her private space. Xu et al. (2008) clarified that privacy awareness refers to users' capability to protect their personal space by understanding privacy policies and practices and how their information is utilised. They considered privacy awareness to be an antecedent and discovered its relationship with the disposition to value privacy. The authors conducted a survey to test the research model on users of different types of websites. Their questionnaire consisted of 32 items, using a seven-point Likert scale. Xu et al. (2008) adopted the three items that focused on privacy awareness from Dinev & Hart (2005)'s study, who investigated how social awareness and internet literacy were related to privacy concerns and the intention to transact online in e-commerce settings. Zlatolas et al. (2015)) addressed privacy issues related to SNSs, namely Facebook. Their study explored the relationship between specific factors: privacy concerns, privacy policies, privacy social norms, privacy awareness, privacy control, privacy value and self-disclosure. They used an online questionnaire with 24 items, and only three of them were related to privacy awareness. All of the items were adopted from previous studies, such as from Dinev & Hart (2004), Xu et al. (2008) and Xu et al. (2012). Furthermore, a five-point Likert scale was used in the survey. However, privacy awareness was not the survey's main focus; it was one of the factors. Zlatolas et al. (2015) stated that privacy awareness refers to users' levels of cognition about SNS privacy procedures and problems. The authors found that privacy awareness was related to privacy concerns, privacy value and self-disclosure.

A comprehensive study conducted by Bellekens et al. (2016) focused on assessing both security and privacy awareness of users of wearable health devices. The study revolved around the concept of situational awareness and involved understanding the devices, the system environment, and related threats. They conducted a survey on cyber security and privacy, with questions ranging from requiring yes/no answers, rating security and privacy threats, evaluating

risk, to categorising threats as security or privacy threats. Their study participants were from different countries, including the UK, the USA, Belgium and Mauritius. Another study that focused on both security and privacy awareness was conducted by Kulyk et al. (2020). They investigated smart homes and health users' security and privacy awareness. According to Kulyk et al. (2020), smart homes refer to environments that connect home appliances, entertainment devices and smart health, including certain sensors and healthcare devices. Unlike all of the previously discussed studies that used quantitative methods, they used qualitative questionnaires with open-ended questions. Kulyk et al. (2020) claimed to have chosen a qualitative method to obtain comprehensive data without requiring further explanations from the participants. The survey was conducted with participants from Romania, Germany and Spain.

A limited number of survey-based studies in the literature have focused on users' privacy awareness. Bergmann (2008) conducted a study utilising both a survey and an experiment to collect the required data. Bergmann (2008) developed two questionnaires, completed before and after an experiment. Their study consisted of three steps. The first step used a pre-questionnaire to collect the participants' demographic information and privacy concerns using a Likert scale. The second step was the experiment, where they used a cross-sectional method. The authors utilised an online application called Foodie, which collects user recommendations for restaurants and requires registration and the acceptance of a privacy policy. The control group used a traditional interface, while the experimental group used an improved interface. The third step was the post-questionnaire, which assessed the participants' recall of privacy policy statements; it contained questions about the privacy policy that the user agreed to during the experiment, which focused on disclosing data. A study conducted by Sim et al. (2012) emphasised the importance of utilising situational awareness in privacy models. They also relied on Endsley's situational awareness definition. They presented the information privacy situation awareness (IPSA) scale, which focuses on users' data-sharing behaviours when using social networks. The IPSA scale concentrates on the users' knowledge of information related to their data privacy and the potential risks associated with it. To develop the IPSA scale, Sim et al. (2012) conducted a literature review on all of the related subjects, such as situational awareness and information privacy. The researchers then conducted qualitative focus group interviews to learn more about the IPSA assessment. Thereafter, based on the outcomes of the literature research and focus group interviews, an initial questionnaire item set was created. They used a seven-point Likert scale. The survey participants were Facebook users, but the authors clarified that the IPSA scale could be applied to other social networks. Alani (2017)'s study aimed to measure Android user privacy. He designed a survey to measure Android users' privacy awareness of application permissions. The survey consisted of 13 items, ranging from open questions to yes or no questions. Moreover, the survey uncovered what users considered their most private data. They found that photos and videos were considered the most private data, followed by passwords stored on their devices and in emails. Regarding IoT systems, Mugariri et al. (2022) investigated IoT users' concerns and their understanding of privacy. Furthermore, their study aimed to promote IPA among IoT users and identify privacy risks through a survey. They conducted online surveys to evaluate IoT users' awareness and concerns regarding information privacy and protection, as well as any shared beliefs and discrepancies. The research strategy chosen for this study was an open-ended survey. Most studies in the literature concerned with data privacy awareness focused on SNSs, applications, and mobile devices. However, there has been a significant shift towards developing IoT-based services and systems, including IoMT, which rely extensively on sensitive and personal data. Thus, understanding the privacy awareness of digital health service users is important to determine whether they can effectively control and manage their data when using IoMT services.

2.5 IP and IPA in IoMT Systems

IP and IPA are critical in IoMT services and systems for many reasons, such as the sensitive nature of health data, real-time data collection and stringent regulatory demands in the healthcare sector. Furthermore, the intricate nature of IoMT ecosystems involving numerous interconnected devices and sensors that continuously produce massive amounts of medical and health information increases the possibility of IP violations. Moreover, storing patients' sensitive data in electronic health records (EHRs) makes them more accessible and raises privacy and confidentiality issues (Keshta & Odeh 2021, Miller et al. 2022). However, these types of IoT services require collecting a large amount of data, which can conflict with users' privacy concerns (Al-Sharekh & Al-Shqeerat 2020). Given the sensitive nature of health data, robust privacy protection in IoMT systems is imperative. In addition, privacy protection measures and user privacy preferences must be balanced to safeguard users' data while respecting their preferences.

Health and sensitive data may be exposed to a breach of privacy at any stage when IoMT services are provided. Pramanik et al. (2019) explained how patients' data privacy can be breached in remote healthcare systems. For example, in the data collection phase, symmetric encryption protects the sensor nodes attached to the patient's body. Attackers can obtain the encryption key by physically seizing a sensor's node or travelling to the patient's location to take control of the sensor. This could breach the raw data's privacy and expose the patient's medical condition (Pramanik et al. 2019). Attackers can access sent data during the data transfer phase by taking advantage of security flaws in the network. Eavesdropping attacks can be passive or active. Passive eavesdropping involves the attacker silently monitoring and recording network traffic without altering it, often for later analysis. In contrast, active eavesdropping involves activities such as installing software or devices to intercept and manipulate the data being transferred (Pramanik et al. 2019). A remote healthcare server could be vulnerable to these types of attacks. Regarding data storage, healthcare service providers store encrypted patient data with an encryption key using third-party storage facilities, which poses a significant risk to the security and privacy of patient data (Pramanik et al. 2019). In addition, the availability of an encryption key means that the third party can decrypt the data or impart encryption keys to users other than authorised medical professionals (Pramanik et al. 2019). Additionally, the constant evolution of IoMT devices and increasing interconnectivity present ongoing challenges. Privacy frameworks need to continuously adapt to keep pace with technological advancements and emerging threats to ensure that there is comprehensive protection of sensitive health data.

IP violations in IoMT services may cause many complex problems. Miller et al. (2022) argue that some direct harms can affect people when their health data is exposed. The level of harm varies depending on the type of information and the recipients and their positions. For instance, people may feel ashamed or embarrassed when their health data is exposed (Miller et al. 2022). Additionally, they may lose trust in their service provider's ability to keep their information private (Miller et al. 2022). Users must have adequate knowledge and a reasonable understanding of certain factors in order to take on the role of protecting their data privacy and making appropriate decisions regarding collecting and processing their data in IoMT settings. Additionally, users need to be aware of their privacy rights to make informed decisions. Correia & Compeau (2017) conducted a review study of privacy awareness in information systems. They found the most addressed aspects were regulations, common practices and technology. User awareness of these three factors is important when using IoMT services. Moreover, regulations and common practices are sources of privacy requirements (Stallings 2019). In addition, according to privacy calculus theory, users disclose their personal information after assessing the possible benefits and risks (Smith et al. 2011). A study conducted by Cheng et al. (2021) has shown that users are willing to disclose their personal information when they obtain benefits. In contrast, risks negatively affect the disclosure of personal information. Informed consent, therefore, requires users to be fully aware of the benefits and risks, and a process must be developed to ensure this informedness and awareness.

2.6 Preserving IP in IoMT

IoMT systems use different techniques to ensure and protect data, information privacy and confidentiality, including, but not limited to, encryption techniques, access control mechanisms and differential privacy techniques. These techniques are crucial for protecting data during their collection, transmission, processing and storage. Additionally, data must be protected from unauthorised access, use or disclosure of personal information. Multiple techniques must be combined to achieve comprehensive privacy protection. But, in this section, we will discuss only those techniques mentioned above.

The two main types of cryptography algorithms that are commonly used in secure communication and data protection are symmetric and asymmetric. Symmetric techniques depend on a single key that the sender uses to encrypt messages, and the receiver uses to decrypt them (Ghubaish et al. 2020). This technique is considered fast to perform. However, it is less secure if the key is compromised. Asymmetric techniques depend on using a public key for encryption and a private key for decryption, where messages encrypted with the public key can only be decrypted with the corresponding private key (Ghubaish et al. 2020). This enhances confidentiality and authentication. However, the cost of computational resources is higher. Different cryptographic techniques can be used in IoMT systems, including symmetric and asymmetric algorithms (Ghubaish et al. 2020). Symmetric algorithms are commonly used in IoMT services when a large amount of data needs to be decrypted and encrypted quickly and efficiently. The hierarchical access technique allows for role-based authorisation and enables hierarchical access to patients' data (Bhushan et al. 2023). Asymmetric elliptic curve cryptography (ECC) and homomorphic encryption (HE) are commonly used in IoMT solutions. ECC offers robust security with shorter key lengths and lightweight characteristics (Bhushan et al. 2023). HE is a developed cryptographic technique that allows computations and mathematical operations to be performed directly on encrypted data (Salim et al. 2021).

However, traditional cryptographic techniques have many limitations due to their high computational and power requirements. Lightweight cryptographic (LWC) techniques have been developed that are more suitable for the IoT and IoMT. Moreover, a combination of lightweight cryptographic protocols and hybrid encryption techniques, along with advanced ECC implementations, provides a robust framework for securing IoMT systems. For example, Sowjanya et al. (2021) proposed a lightweight authentication protocol for IoMT systems using ECC that aims to ensure safe communication between patients and medical care providers while being computationally efficient. Another example is a novel hybrid deep-learning-based HE model for the industrial IoMT proposed by (Ali et al. 2023). They developed access control algorithms using HE to secure electronic medical records (EMRs). Using HE enables complex mathematical and statistical operations, ensuring end-to-end security and privacy of healthcare data. They integrated HE with blockchain technology to allow data encryption on the user's side and cloud outsourcing. This method supports keyword searches in the distributed ledger while maintaining user anonymity.

Access control is a security measure that regulates who can access which resources in a system and under what conditions, ensuring that only authorised users have permission to access resources. There are three main elements in access control mechanisms: access subjects are users or entities requesting access to data, access objects are protected resources or data and access policy rules dictate who can access resources (Liu et al. 2023). Discretionary access control (DAC) and mandatory access control (MAC) are considered to be the fundamental models of access control (Qiu et al. 2020). DAC enables resource owners to determine access rights. There are two types of DAC: strict DAC, which focuses on only the owner having access rights, and liberal DAC, which allows the owner to transfer access rights to other users (Aftab et al. 2022). In MAC, a hierarchical model manages access rights, and security labels are utilised to regulate and control access. MAC is used in highly sensitive environments, e.g. government systems. MAC systems can be challenging to manage due to their reliance on trusted components and high installation and operational costs (Aftab et al. 2022).

The Bell-LaPadula (BLP) model is a type of MAC that associates subjects and objects with different security labels (Zhang et al. 2021). For objects the label represents the sensitivity of that object's data. For subjects the label reflects the highest sensitivity of data they are trusted to read. The subject's label is referred to as their *clearance*. The labels are hierarchically ordered in terms of sensitivity. For example, (Top_Secret, Secret, Confidential, Restricted and Unclassified) forms a common set of so-called classification markings with Top_Secret being the most sensitive and Unclassified being the least sensitive. The BLP model depends on two principles. The first one is 'No Read Up', where it is not possible for the subject or user to access data that has classification higher than their clearance. The second is 'No Write Down', where a subject or user cannot write information to an object with a lower classification than their clearance (Zhang et al. 2021). Several modified BLP models have been developed to overcome its limitations. These models include fine-grained access control and the introduction of concepts such as 'break the glass' for emergency situations. The 'break the glass' model allows users to temporarily override access restrictions to access data in emergency situations Yang et al. (2018). This override is monitored and logged to ensure system security Yang et al. (2018).

With the continued development of new technologies and complex systems like IoT, new models such as role-based access control (RBAC) and attribute-based access control (ABAC) have been developed. These new models aim to address DAC and MAC challenges, including scalability, flexibility and resource constraints. RBAC is a widely adopted access control method that assigns and manages user permissions based on their roles and responsibilities within a system (Liu et al. 2023). It makes management easier by allowing administrators to change user access through role assignment, audits and management rather than individually assigning permissions (Liu et al. 2023). ABAC's ability to make decisions based on a wide range of attributes makes it particularly suited to such environments, offering fine-grained control over access decisions (Qiu et al. 2020). ABAC determines whether access requests to perform operations on objects should be granted or denied based on attributes. These attributes can be related to the user (subject), the object being accessed, environmental conditions and the policies defined in terms of these attributes (Qiu et al. 2020).

Access control is a critical aspect of IoMT systems. A sufficient access control mechanism must be applied in IoMT systems so that they adhere to privacy requirements, preserve patient confidentiality and ensure that only authorised users can access sensitive medical and personal data. However, new access control solutions are needed for IoMT systems to solve the limitations of traditional access control methods, such as flexibility and scalability limitations, while ensuring appropriate access privileges for healthcare professionals, patients and other authorised users. For example, Chaudhry et al. (2021) proposed a solution focused on a certificate-based direct device-to-device access control mechanism (D2DAC-IoMT). The device-specific certificates are digital certificates uniquely assigned to individual devices within a network. In this solution, they employed ECC to ensure secure communication between devices. Moreover, they used the real-or-random (ROR) cryptographic model to analyse and validate their solution and ensure its resistance to some attacks, such as impersonation and the physical capture of a device. Their solution involves concealing device identities and using dynamic parameters to achieve anonymity.

Solutions using decentralised methods, such as blockchain technology, have been adopted for IoMT systems. For example, a triple-subject purpose-based access control (TS-PBAC) for the IoMT was proposed by Wu et al. (2021). Their model comprises three sub-models deployed at the data owner's site (the patient's site), blockchain site and data requester's site. The authors also designed a hierarchical purposes tree (HPT) to depict the classification and relationships between different purposes in the TS-PBAC. Moreover, they designed different purpose computation, matching and PBAC decisions based on the proposed HPT. They introduced a time-based authority revocation mechanism into the control decision, such that the data

can only be accessed in a period that the owner specifies. The TS-PBAC model allows users to update privacy policies and perform operations such as removing, adding, and merging policies efficiently, with minimal disruption to the existing system. Additionally, to secure communication between sensors, personal servers and cloud servers in IoMT applications, Wazid & Gope (2023) presented BACKM-EHA, which is a blockchain-enabled access control and key management protocol. BACKM-EHA utilises collision-resistant cryptographic one-way hash functions and the elliptic curve decisional Diffie–Hellman problem (ECDDHP) to provide a robust security framework, ROR model and informal mathematical methods to validate BACKM-EHA. Popoola et al. (2023) proposed a combination of lightweight solutions, including ECC and advanced encryption scheme (AES), and a proof-of-authority (PoA) based permission blockchain to enhance data security and privacy in smart home healthcare solutions based on the IoT. They described the smart contracts model for fine-grained access control and evaluated various threat models to preserve privacy. They provided three types of smart contracts. First, the publisher contract contains the data subject's consent and manages the requests for sharing the data. Second, the subscriber contract specifies the sensors to subscribe to and filters the data accordingly. Finally, the client contract maps normal nodes to their respective subscriber contracts and enables data retrieval.

The differential privacy (DP) concept has emerged with the development of statistics, artificial intelligence and machine learning. DP can defined as "a mathematical definition of privacy in machine learning that allows collecting, analysing, and sharing statistics about a data set based on personal data while protecting individuals' privacy" SDAIA (2022). DP ensures privacy without compromising the accuracy of query results by limiting the amount of information that can be disclosed by introducing random noise (Yan et al. 2024). Many studies focusing on privacy in machine learning have employed DP for privacy protection. However, many challenges arise. For example, when this technique is used to protect users' data from training machine-learning models, the accuracy of these models might reduce over time because DP relies on adding noise at each training session (Blanco-Justicia et al. 2022). DP was introduced in 2006 by Dwork (2006) as a mathematical framework that involves anonymising the results of interactive queries to a database. The basic DP model is epsilon DP (ε-DP), where ε is a parameter that measures privacy loss (Yan et al. 2024, Dwork et al. 2014). A smaller ε indicates more robust privacy protection. ε-DP adds random noise to the data, ensuring that the presence or absence of user data does not affect the outcome or result of the computation and analysis (Yan et al. 2024, Dwork et al. 2014). There are two main types of DP: (ε,0)-DP and (ε,δ)-DP. The (ε,0)-differential has a strong level of privacy protection, with no exceptions. This ensures that data are secure and that the privacy of the data is protected when data analysis is performed. This type of DP ensures that the presence or absence of a single user's data does not significantly affect the analytical outcome. This strong guarantee helps protect users' privacy by making it difficult to infer their personal information from the published data. This type of DP can be useful when absolute privacy guarantees are difficult to obtain without considerably reducing the usefulness of the data (Dwork et al. 2014). (ε,δ)-DP is a more flexible version of DP, incorporating an additional privacy parameter, δ. This parameter acknowledges that there may be a minimal probability of error, which means that a small number of privacy breaches or violations beyond the specified ε level can occur. It provides a probabilistic privacy guarantee with controlled privacy breaches. It accommodates statistical analyses that might not be feasible under stricter conditions (Dwork et al. 2014). However, with technological developments, different types of DP have been developed that aim to fit different systems and address their challenges. One of the most common DP techniques employed to balance privacy and data utility in IoMT systems is federated learning DP (FL-DP). Federated DP comprises DP principles with federated learning—a distributed machine-learning approach that enables training models across multiple decentralised devices or edge devices. Both ε-DP or (ε,δ)-DP can be used in FL-DP (Farooqi et al. 2024). There are several main steps required when implementing DP,

including FL-DP. First, a sensitivity analysis needs to be undertaken to understand the stability and reliability of the data and to determine the level of noise necessary to protect privacy. In addition, to determine the privacy budget, which limits how much privacy can be compromised in this step, the maximum allowable privacy loss when using DP is calculated. A smaller budget means more robust privacy, but this could lower model accuracy due to noise injection. On the other hand, a larger budget may improve the model's utility at the cost of privacy. It is crucial to recognise and manage the complexities associated with undertaking sensitivity analyses and allocating a privacy budget to execute FL-DP effectively (Farooqi et al. 2024).

2.7 Primary Sources of Privacy Requirements

To ensure the protection of IP in any system, it is essential to adhere to the privacy requirements of the three main classifications: privacy regulations, privacy standards (principles) and privacy best practices (policies) (Stallings 2019). These requirements aim to mitigate privacy issues, such as unauthorised access to the data or using the data for purposes other than those for which the data were collected.

2.7.1 Privacy Regulations

Laws and regulations are created by a nation's government, and everyone in the nation is required to abide by them. The law clearly outlines what one must and may not do, and it is upheld by enforcing penalties, punishments or both (Tzafestas 2018). Data privacy laws and regulations are essential for several reasons. First and foremost, they safeguard people's rights by enabling them to control their personal information and make informed decisions about how it is used. Regulations also stop unauthorised access to, sharing of or misuse of personal data. They also provide companies and organisations with a clear framework to follow, promoting compliance and ensuring that they take the necessary measures to safeguard personal information (Stallings 2019). Various regulations regarding personal data privacy have been enforced around the world in different countries and regions. Some regions have a single law, such as the GDPR, which applies to all countries within the European Union (EU). Some countries have a single law, such as the Personal Data Protection Law (PDPL) in Saudi Arabia, while other countries, such as the USA, have a combination of federal and state laws and industry-specific regulations. Some of the most important regulations in the USA are: The Health Insurance Portability and Accountability Act (HIPAA)[6], The Children's Online Privacy Protection Act (COPPA)[7] and the California Consumer Privacy Act (CCPA)[8]. Figure 2.2 illustrates the status of the countries in terms of data protection regulations around the world. This thesis will focus on the GDPR in Europe and the PDPL in Saudi Arabia.

.

General Data Protection Regulation (GDPR)

The GDPR is a comprehensive data protection law enacted by the EU. It was enacted in 2016 and came into force in 2018 (GDPR 2018). It provides individuals with data privacy rights. These rights include, but are not limited to, being informed about data usage, having access to it, fixing it, deleting it, restricting its processing, porting it to another company, opposing processing and not being subject to automated decision-making (*The EPSU guide on GDPR* 2019). The GDPR applies to all personal and identifiable data. Moreover, the GDPR requires organisations and businesses that handle personal information to comply with a number of fundamental requirements. These include obtaining a lawful basis for processing

[6]https://www.cdc.gov/phlp/publications/topic/hipaa.html
[7]https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
[8]https://oag.ca.gov/privacy/ccpa
[9]https://securiti.ai/privacy-laws/

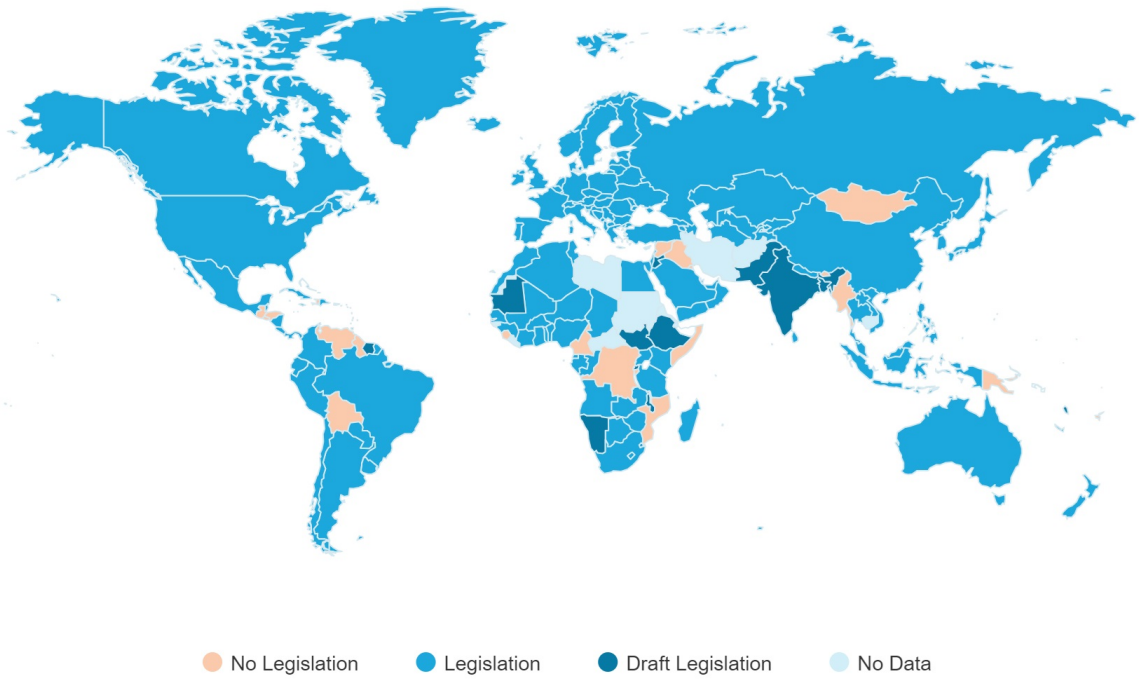

Figure 2.2: *Data privacy laws and regulations around the world* [9]

data, limiting data processing to specific purposes and ensuring that data are accurate and kept up to date (*The EPSU guide on GDPR* 2019). Additionally, the GDPR requires companies and organisations to implement appropriate security and privacy measures to protect personal data, requiring privacy to be included in systems and processes by design (*The EPSU guide on GDPR* 2019). Additionally, the GDPR mandates data protection impact assessments, requires organisations to report data breaches to the local data protection authority within 72 hours and introduces the right to be forgotten (*The EPSU guide on GDPR* 2019).

The Personal Data Protection Law (PDPL)

The PDPL was issued in Saudi Arabia via a royal decree on 16 September 2021 and took effect on 23 March 2022. This comprehensive law is designed to protect individual personal data by implementing strict guidelines for data collection, usage and storage. The PDPL law shares many similarities with the GDPR. Both require organisations that collect, use or store personal data to follow specific rules, using data only for legal purposes, protecting data from unauthorised access and deleting data when no longer needed (PDPL 2023). Additionally, the PDPL, like the GDPR, grants individuals several rights, including the right to access, correct inaccuracies, request deletion and object to processing. These guidelines are designed to safeguard the privacy and confidentiality of personal data (PDPL 2023). Although the PDPL shares several similarities with the GDPR, there are some key differences between them. For example, the GDPR is a comprehensive data regulation that applies to the EU and European Economic Area countries, establishing high data protection standards on a global scale. In contrast, the PDPL is a relatively new law that focuses only on regulating data protection within Saudi Arabia. The PDPL is designed to meet Saudi Arabia's specific requirements and aims to improve privacy practices within the country.

2.7.2 Privacy Principles and Standards

The term 'principles' typically refers to general rules or guidelines that are not legally enforced (they may, of course, motivate legally enforced regulations). 'Privacy principles' aim to assist service providers in managing personal information and upholding people's privacy rights. Within the IT industry, some well-established privacy principles seek to safeguard personal information and promote responsible data handling by organisations. Fair Information Practice Principles (FIPPs) and Privacy by Design (PbD) are two well-known principles that have gained significant attention in the IoT field. For example, a study conducted by Feng et al. (2021) proposed user-centred designs that enable meaningful choices in IoT systems based on the FIPPs' privacy notice principle. Similarly, Scarpato et al. (2017) emphasised the importance of incorporating PbD principles when developing IoT systems. Additionally, O'Connor et al. (2017)'s study suggested practical ways in which to apply PbD principles in IoMT systems. Obtaining user consent is crucial when dealing with personal information. Thus, both FIPPs and PbD approaches highlight the importance of obtaining user consent when collecting, processing, storing, maintaining or disclosing personal information. PbD also acknowledges users' right to withdraw consent at any time.

Fair Information Practice Principles (FIPPs)

FIPPs are a collection of guidelines for assessing information systems and procedures in order to achieve users' information and data privacy. It was initially proposed in 1973 in the USA by the US Department of Health, Education, and Welfare (HEW), and it is not a legal requirement. According to the official website of FIPPs [10], these principles contain the following:

- **Access and Amendment:** Users should be able to access and amend their personal data.
- **Accountability:** Service providers should take responsibility for adhering to privacy requirements, and they should define roles and responsibilities for all employees who have access to users' personal information.
- **Authority:** Service providers must have the authority to create, collect, use, process, store, maintain, disseminate or disclose users' personal data. They should not do so without such authority.
- **Minimisation:** Service providers should use personal data only for its intended purpose and avoid any unnecessary collection or disclosure. They should keep the data only as long as needed to achieve its purpose.
- **Quality and Integrity:** Service providers should ensure the accuracy, relevance, timeliness and completeness of personal data to ensure fairness to users.
- **Individual Participation:** Service providers must obtain users' consent. Additionally, providers should establish procedures to handle any privacy-related complaints.
- **Purpose Specification and Use Limitation:** Service providers should inform individuals of the reason for collecting data. They should only use, process, store, maintain, share or disclose the data for a purpose that aligns with the original reason.
- **Security:** Service providers should establish safeguards to protect personal data from unauthorised access, use, modification, loss, destruction, dissemination or disclosure.
- **Transparency:** Service providers should be transparent about personal data policies and practices and provide clear and accessible privacy policy notices.

[10] https://www.fpc.gov/resources/fipps/

Privacy by Design (PbD)

PbD is an approach to systems engineering developed by Cavoukian (2009). The author clarifies how PbD principles are based on FIPPs; however, PbD goes beyond them by stressing the need to incorporate privacy into systems, procedures and technologies from the outset. It contains seven foundational principles that aim to integrate privacy requirements at each stage of an IT system's development, including its design, implementation and operation phases (Stallings 2019). The seven foundational principles of PbD are summarised in Table 2.2. PbD principles can be implemented in systems using various methods, such as privacy-enhancing technologies (PETs). PETs, such as K-anonymity, DP, and pseudonymisation, protect users' identities and sensitive information. Moreover, it is essential for systems and technologies to have privacy as the default setting (Cavoukian 2009).

International Organization for Standardization (ISO)

Although several organisations create standards around the world, the International Organization for Standardization (ISO) is considered the most important. The ISO is a global organisation that develops voluntary standards on various topics, particularly in the field of IT, with a focus on software. The ISO partners with the International Electrotechnical Commission (IEC) to create standards that prioritise security and data communication (Stallings 2019). The ISO/IEC 29100 Privacy Framework provides comprehensive privacy guidelines for protecting PII within an information and communications technology (ICT) environment. It gives clear definitions for key terms, identifies the various actors and their roles, specifies the privacy requirements and references key principles. The framework satisfies the existing legal requirements in most regions around the world (*ISO/IEC 29100* 2011). The eleven principles of ISO/IEC 29100 and their descriptions as mentioned in Morales-Trujillo et al. (2019)'s paper are:

1. **Consent and Choice** : Users consent to PII processing based on privacy policies and notifications, and they can withdraw.
2. **Purpose Legitimacy and Specification**: Data processing complies with laws, individuals understand the purpose, and organisations communicate PII management clearly.
3. **Collection Limitation**: An organisation collects necessary information for specific purposes, documenting and justifying the PII type.
4. **Data Minimisation**: An organisation minimises PII processing, restricts access, reduces identification and disposes of outdated data.
5. **Use, Retention and Disclosure Limitation**: PII processing, maintenance and transfer are for legitimate purposes. Data should be securely destroyed or anonymised internationally.
6. **Accuracy and Quality**: PII must be accurate, complete and relevant, with proper procedures and control mechanisms in place to ensure its accuracy and quality.
7. **Openness, Transparency and Notice**: An organisation must provide accessible, easily accessible information on PII processing, public access and notifications.
8. **Individual Participation and Access**: Authenticated individuals can access, review and modify personal information in software systems.
9. **Accountability**: An organisation must document, communicate privacy policies, assign responsibility, provide training and inform stakeholders of privacy breaches and the measures taken.

10. **Information Security**: An organisation must maintain PII integrity, confidentiality and security through legal requirements, standards and regular reviews.

11. **Privacy Compliance**: An organisation must ensure data protection and privacy by conducting audits, complying with relevant laws, policies and procedures, and maintaining privacy risk assessments.

Moreover, the ISO/IEC 29151 Code of Practice for the Protection of Personally Identifiable Information guides organisations on commonly used PII protection and information security measures in various organisations (*ISO/IEC 29151* 2017). In addition, with an emphasis on privacy choices and management, the ISO/IEC 27556 user-centric framework offers guidelines for handling PII in ICT systems. It includes components designed to manage privacy preference information but does not specify the content and format of such privacy preference information. The framework enables organisations to implement PII processing based on privacy choices and includes user-centric PII handling methods in their systems while adhering to PbD principles. This document may be used to build and implement ICT systems that deal with PII, create PII exchange platforms based on privacy preferences and offer services for managing privacy preferences (*ISO/IEC 27556* 2022).

Self-Sovereign Identity (SSI)

The self-sovereign identity (SSI) concept offers promising solutions for enhancing security, privacy and user empowerment. It aims to give users complete control over their digital identity, data and information while ensuring their privacy and rights are protected (Schardong & Custódio 2022). Traditional systems are centralised, federated models that rely on external entities for user identity provisioning and management, where users are required to create accounts with service providers (SPs) or identity providers (IdPs), and store identifiers and attributes centrally (Čučko et al. 2022). Moreover, SP and IdP internal policies affect the privacy and security of users' data (Čučko et al. 2022). On the other hand, users' SSI allows them to generate, manage, store and control their identity without external intervention, preventing third parties from acquiring data directly from SPs and eliminating middlemen while enabling secure and interoperable identity management (Schardong & Custódio 2022, Čučko et al. 2022). Two main standards, which are defined by the World Wide Web Consortium (W3C)[11], form the foundation of SSI: decentralised identifiers (DIDs) and verifiable credentials (VCs) (Čučko et al. 2022). DIDs [12] are a new type of identifier that is global, unique and verifiable—a decentralised digital identity. DIDs are types of uniform resource identifiers (URIs) that allow trustable digital interactions. They are associated with a DID user and a DID document that describes the DID user, which includes cryptographic public keys, biometrics and other authentication mechanisms. The design of DIDs allows them to perform independently of centralised registries, identity providers and certificate authorities, empowering the controller to demonstrate control without obtaining permission from any other entity. VCs [13] seek to balance users' privacy with ease of use and the sharing of digital credentials. VCs have the ability to represent the user's credentials' information that is used in physical life, for example, user-related information (such as an identification number or a photo) and credential-type information (such as a health insurance card, passport or driving licence). VCs provide a way to represent credentials on the web that are verifiable by devices, compliant with privacy and securely encrypted.

One of the technologies used in the SSI system is blockchain. Blockchain provides a decentralised, secure platform for managing digital identities (Schardong & Custódio 2022). It enables secure data sharing between users and SPs (Schardong & Custódio 2022). Blockchain

[11] https://www.w3.org/

[12] https://www.w3.org/TR/did-core/#dfn-decentralized-identi_ers

[13] https://www.w3.org/TR/vc-data-model/

Table 2.2: *Privacy by design (PbD) foundational principles by Cavoukian (2009)*

	PbD principle	Summary
1	Proactive Not Reactive; Preventative Not Remedial	The PbD approach is proactive and aims to prevent privacy risks before they occur. This involves setting high privacy standards, involving stakeholders and correcting negative impacts before they happen.
2	Privacy as the Default	PbD aims to automatically protect personal data in any system without requiring any action from users. This is achieved through some methods declared by fair information practices, such as purpose specification, collection limitation, data minimisation and use, retention, disclosure and limitation.
3	Privacy Embedded into Design	PbD should be integrated into systems to ensure privacy while preserving full functionality. The approach to integrating privacy should rely on recognised standards and frameworks, and all fair information practices should be followed. In addition, approaches such as privacy risk assessments should be adopted to minimise privacy impacts and risks.
4	Full Functionality – Positive-Sum, Not Zero-Sum	PbD aims to enable all parties involved to achieve their goals while maintaining privacy and other objectives. It involves integrating privacy measures into technology, processes and systems to ensure full functionality for all users. This approach eliminates unnecessary compromises between privacy and other goals.
5	End-to-End Security – Lifecycle Protection	PbD guarantees that information is kept secure throughout its entire lifecycle. Strong security measures, such as encryption and access control, are crucial for maintaining personal data's confidentiality, integrity and availability.
6	Visibility and Transparency	PbD aims to enable transparency and accountability in technology, which can be independently verified. This is consistent with FIPPs, which stress responsibility, transparency and compliance in protecting personal information.
7	Respect for User Privacy	PbD focuses on users' interests through solid privacy defaults, clear notice and user-friendly options, focusing on empowering users to manage their data. It aims to give users more control over their data by obtaining their consent, ensuring accuracy, providing access, setting up complaint procedures and creating human-centred interfaces and architectures.

improves the privacy and security of SSI systems by allowing users to control their identities and data, ensuring tamper-proof transactions and verifying VCs (Schardong & Custódio 2022). Christopher Allen is considered the first author to have proposed a comprehensive set of SSI principles to guide SSI development and execution (Schardong & Custódio 2022). These principles include user control, privacy, consent, minimal disclosure, a decentralised architecture, interoperability and verifiability (Allen 2016). The ten SSI principles are listed below:

- **Existence:** Users should have their independent and actual existence outside the digital domain. User identity (self-sovereignty) operates by selectively sharing users' preferred digital attributes.
- **Control:** Users should have complete control over their identities, including the ability to create, manage and revoke them and to be able to choose publicity or privacy. Algorithms ensure the continued legitimacy and validity of an identity and its claims.
- **Access:** Users should have access to their data and personal information and easily obtain any claims and other data linked to their identification.
- **Transparency:** Systems should be transparent. Furthermore, algorithms in these systems should be open source, allowing anyone to understand their workings.
- **Persistence:** A user's digital identity should last forever, or at least for as long as the user wishes. However, this should be aligned with the 'right to be forgotten', and any claims should be removed or modified as needed, over time.
- **Portability:** Users' digital identities should be able to move across different systems and technologies, giving users control of their data. Trusted third-party entities should not store users' identities for many reasons, such as when the regulations that govern them change or if the third-party entity no longer exists.
- **Interoperability:** Systems should be interoperable with each other, achieving easy digital identity transfer between various platforms and services while ensuring that users maintain control over their identities.
- **Consent:** Users should give their consent when their data and identity are collected, used and shared. This consent must be informed, deliberate and well understood to be valid.
- **Minimisation:** The minimum amount of data should be disclosed when users' data are needed to provide a service or complete a task.
- **Protection:** Users' rights should be protected, and their independence should be prioritised over network needs through independent, censorship-resistant and decentralised identity authentication algorithms.

2.7.3 Privacy Best Practices

Experts in various fields work to develop best practice guidelines to be followed by designers and developers in order to promote the security and privacy of users and other entities involved (Stallings 2019). These guidelines are based on regulations and standards outlined in previous sections. Many non-profit organisations around the world focus on best practices for security and privacy. For example, the Cloud Security Alliance (CSA)[14] organisation promotes best practices in cloud computing, emphasising security, privacy and reliability. It was originally established in the USA. However, it has some branches worldwide, such as its branch in Saudi Arabia [15]. Another example is the IoT Security Foundation (IoTSF)[16], a not-for-profit organisation

[14]https://cloudsecurityalliance.org
[15]https://circle.cloudsecurityalliance.org/saudi/home
[16]https://iotsecurityfoundation.org

addressing security challenges, and promoting collaboration, best practices and advice.

Regarding data and IP, there are many organisations, such as the International Association of Privacy Professionals (IAPP) [17] and the Future of Privacy Forum (FPF) [18]. The IAPP is considered a leading global community and resource for data and IP. It is a non-profit organisation established in 2000. The IAPP works to define, advance and strengthen the privacy profession worldwide. It supports privacy experts to share best practices, advancing privacy management concerns and tracking trends. An example of one of the guidelines provided by the IAPP on its official website is the 'EU–US Data Privacy Framework: Guidance and Resources', [19] which is always updated with the most recent guidelines and resources explaining what these new rules say, how they work and what should happen next. The FPF supports privacy leadership and research by promoting ethical data practices that align with cutting-edge technology. For example, the FPF provides the 'Best Practices' page [20], which is considered a comprehensive repository for privacy-related guidelines, documents, reports and other resources.

[17] https://iapp.org
[18] https://fpf.org
[19] https://iapp.org/resources/article/eu-us-data-privacy-framework-guidance-and-resources
[20] https://fpf.org/best-practices/

Part2: User Informed Consent

2.8 User Consent as a Privacy Requirement

All systems that use personal and identifiable data must comply with privacy requirements of regulations, principles, standards, and best practices guidelines. Transparency, accountability, data protection, data minimisation, data access, data modification, consent, and consent withdrawal are some of the essential privacy requirements mentioned in the previous section. Other specific requirements may apply depending on the system's sector and services.

Transparency and choice are considered part of the main concepts on which privacy laws and principles are focused. These concepts are commonly referred to as "notice and consent" or "informed consent" (Okoyomon et al. 2019). GDPR tightens the rules for obtaining consent to collect and use personal information. The definition of consent can be found in Article 4, point 11, which states that " consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (GDPR 2018). Moreover, the conditions for consent outlined in GDPR Article 7 require that the user's clear and distinguishable consent be obtained before processing personal data and that users have the right to withdraw their consent at any time. Moreover, GDPR requires institutions to comply with specific requirements, such as informing users about how their personal information will be used, with financial penalties for non-compliance (Duckert & Barkhuus 2022). The PDPL in Saudi Arabia also complies with the GDPR in requiring the users' consent before processing their personal data and when changing the processing purpose (PDPL 2023). The PDPL document explains that processing personal data involves various actions, such as collecting, recording, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing, and destroying. It sets out guidelines for obtaining consent, explicit consent, and obtaining consent from a legal guardian if the Data Subject is unable to provide it themselves (PDPL 2023). It also requires "Implementing appropriate measures to verify that the Data Subject has given their explicit consent to the Collection of the Personal Data, changing the purpose of the Collection, or Disclosure or Publishing of the Personal Data in accordance with the provisions of this Law and the Credit Information Law" (PDPL 2023). However, in certain situations, obtaining users' consent is not necessary. According to the GDPR and PDPL, processing personal data may not require consent in specific cases, such as for security or legal requirements or when it is necessary for legitimate interests under the law. Moreover, data protection regulations do not apply to unidentified or anonymous data, which can be used for research purposes without consent (GDPR 2018). Also, in the United States, it is allowed to use anonymous data without the user's consent if the data will be used for research after competent authorities approve and the requester signs an agreement that prohibits re-identification of the data (Cumyn et al. 2020).

The principles and standards discussed in the previous section clarify that user consent and choice are crucial privacy requirements. According to the Fair Information Practice Principles (FIPPs) (see Section 2.7.2), under the "Individual Participation" principles, user consent is required for the collection, processing, or disclosure of personally identifiable information except where permitted by law. Also, PbD's seven foundational principles include "Respect for User Privacy - Keep it User-Centric," which emphasises the importance of user consent and free and specific consent is required for collecting, using or disclosing personal information, except where otherwise permitted by law (Cavoukian 2009). The greater the sensitivity of the data, the clearer and more specific the quality of the consent required, and it can be withdrawn later.

Some ISO/IEC standards provide guidance on obtaining and managing consent for personal information collection, use, and disclosure. The ISO/IEC 29100:2011 (*ISO/IEC 29100* 2011) privacy framework requires organisations to obtain users' consent and communicate all information for collecting, using, and disclosing personal data to the users. ISO/IEC 29151:2017 (*ISO/IEC 29151* 2017) emphasises obtaining informed consent from individuals for PII collection, use, and disclosure by cloud service providers (CSPs). CSPs must provide clear information about the purpose and scope of the consent request, allow individuals to withdraw consent at any time, and use plain language while avoiding pre-ticked boxes. ISO/IEC 27556:2021 (*ISO/IEC 27556* 2022) stresses the importance of obtaining free, specific, informed, and unambiguous consent for collecting, using, and disclosing personal information. It provides guidelines for clear requests, users' right to withdraw consent, and compliance with ethical practices. In addition, organisations that focus on privacy best practices have provided many documents, guidelines, and resources that emphasise the importance of user consent. For example, the Future of Privacy Forum's Best Practices website provides documents to guide companies on how to protect consumers' data, emphasising the importance of consumers' consent. Some examples of these documents are "Best Practices for Consumer Wearables and Wellness Apps and Devices"[21] and "Guiding Principles on the Privacy and Security of Personal Wellness Data"[22].

2.9 An Overview of Informed Consent

The concept of informed consent originated in the medical field as a procedure before undertaking any medical procedures. It is a legal and ethical obligation that refers to obtaining a patient's permission before any medical procedure is carried out (*Consent to treatment* 2022). In order for consent to be considered valid, specific requirements must be met. Firstly, it is necessary to provide complete and clear information about patients' condition, potential risks, benefits, and alternative treatments to enable them to make informed decisions (*Consent to treatment* 2022). Secondly, consent must be given voluntarily, without any influence from the medical team, family, or friends (*Consent to treatment* 2022). Lastly, the individual must be capable of comprehending the information provided and making an informed decision (*Consent to treatment* 2022). Also, informed consent usually includes a conversation between a doctor and a patient, allowing them to make the best decision regarding their health services. Furthermore, informed consent is considered a fundamental legal and ethical requirement for any research or study that involves human subjects, such as clinical trials and social sciences. It is essential to ensure that participants have all the information they need to make a decision regarding participation in a study (Nijhawan et al. 2013, Ferreira & Serpa 2018). This includes understanding the objectives, duration, procedures, potential risks, benefits, and incentives (Ferreira & Serpa 2018). Participants should be made aware of how their data will be used and why, as well as their rights to access, correct, and communicate their personal information (Ferreira & Serpa 2018). Moreover, informed consent includes the communication between participants and researchers, from the start of recruitment to the end of the study (Nijhawan et al. 2013). Informed consent must be obtained before the research study or treatment begins. An Institutional Review Board (IRB) must approve the study and the consent form (Nijhawan et al. 2013). Then, participants will receive a personalised consent form. The study's purpose, potential risks, and possible benefits are explained, and questions can be asked (Nijhawan et al. 2013). If the patient decides to participate, they sign and date the form, a copy will be given to the patient, and the study or treatment procedures can begin (Nijhawan et al. 2013).

According to Coiera & Clarke (2004), the consent form has four levels: (i) general consent;

[21] https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf

[22] https://fpf.org/wp-content/uploads/2015/10/CEA-Guiding-Principles-on-the-Privacy-and-Security-of-Personal-Wellness-Data-102215.pdf

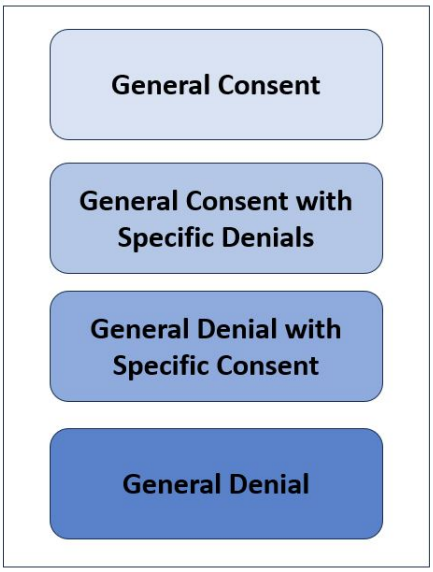

Figure 2.3: *The consent form levels according to Coiera & Clarke (2004)*

(ii) general consent with specific denials; (iii) general denial with specific consent; and (iv) general denial (see Figure 2.3). The general consent represents the opt-in consent, which allows any worker in the healthcare institute to access the patient data at any time. The patient can revoke the consent whenever he or she desires. In general consent with specific denials, the patient gives general consent but can refuse access in some cases. For example, the patient refuses access to specific data, to specific users, or for specific purposes. In general denial with specific consent, the patient gives general denial but gives access in some cases. For example, the patient gives access to specific data, to specific users, or for specific purposes. In general denial, which is equivalent to the opt-out model, the patient is asked for consent to access information each time a new request is made by a clinician.

Traditionally, paper-based forms have been used to obtain informed consent from patients for medical procedures, treatments, and research. However, paper-based informed consent processes have several challenges and limitations. For example, storing and accessing paper-based informed consent can be time-consuming. Also, obtaining informed consent from individuals can be difficult due to complex language, which consequently affects participants understanding (Nijhawan et al. 2013, Budin-Ljøsne et al. 2017). Moreover, Communicating the potential risks and perceived benefits to participants can be difficult (Nusbaum et al. 2017). In addition, collecting additional data if new research needs arise and need new consent from participants can be expensive and time-consuming (Budin-Ljøsne et al. 2017). With current advances in technology, electronic consent, also known as e-consent, has the potential to address several issues in both medical and non-medical fields. The use of e-consent to obtain research participants' permissions has become widespread (Skelton et al. 2020). Furthermore, the development of e-consent in the medical field has gained significance as telemedicine continues to evolve. According to Wilbanks (2018), electronic informed consent is a consent that is designed and developed in a digital form where it can be carried out via a computer screen, tablet or phone with no interaction with a human specialist before or during the process. However, developing general consent with specific denials and the general denial with specific consent might face some technical challenges (Pruski 2010). However, although e-consent offers solutions to the limitations of paper-based consent methods, still, there are concerns about its privacy and security (Verreydt et al. 2021).

In fact, informed consent applies beyond the domains of healthcare and research. As mentioned in the previous section (see Section 2.8), obtaining users' informed consent is ethically

and legally necessary before collecting, using, and sharing their personal and identifiable data. Thus, information systems, online services, social networks, IoT services and any system that relies on users' personal and sensitive data are required to obtain users' consent. Consent can be obtained via various methods, including pop-up boxes, checkboxes, and online forms. In software systems, End User License Agreements (EULAs) used to be a standard method to obtain user consent. Sometimes EULAs are very general, which makes them unsuitable for the different types of users, or they are too long, which makes them difficult to read for most users (Neisse et al. 2015). Consequently, people may give consent without reading the terms and conditions or they may not understand them if they do (Schraefel et al. 2017). Moreover, most EULAs must be accepted by the user to access relevant services, and with his/her acceptance, they give full access to their data (Neisse et al. 2015). Also, the EULA mechanism is not suitable for IoT systems because the user must be aware of all running processes that are performed on his data (Neisse et al. 2015).

In online services such as mobile applications, social networks and websites, the privacy policy is essential to obtain users' consent (Okoyomon et al. 2019, Kurtz et al. 2020). Through privacy policy, service providers inform users about operations on their data, including collection, use, sharing, and use (Okoyomon et al. 2019, Kurtz et al. 2020). This privacy policy should cover other important aspects of user data, like security measures and policy updates. All information provided in the privacy policy aims to support users in making a decision about their consent regarding a service's activities. Nevertheless, most users do not read the privacy policies documents before they give their consent (Mulder & Tudorica 2019, Steinfeld 2016). In addition, a lot of users who read the privacy policy can find it difficult to understand due to the complex language and confusing legal terminology (O'Connor et al. 2017, Steinfeld 2016, Sebastian 2021). Consequently, the privacy policy can be confusing and incomprehensible to users, which makes it useless (Sebastian 2021). However, the latest regulations on privacy demand that when collecting and processing users' personal data, the process should be transparent, user-friendly, accountable and according to privacy by design principles (Pesch et al. 2022). Thus, it is crucial to ensure that the design of these mechanisms is clear and accessible to users, facilitating their comprehension of the terms and conditions. This requires new recommendations on consent for research, policy and industry to comply with the regulations (Pesch et al. 2022).

2.10 Proposed Solutions for Users Consent in IoT

The consent mechanism is crucial in IoT systems that collect, use, analyse and share users' personal and sensitive data. As stated earlier, users' consent is required legally and ethically when handling their personal and identifiable data. Additionally, the consent tool serves as a way to address potential privacy concerns that users may have with IoT technology (Wakenshaw et al. 2018). Numerous studies in the literature concerning IoT privacy focus on finding solutions for obtaining user consent, particularly for IoT systems that provide medical services. Obtaining informed consent in IoT systems can be challenging due to various factors. IoT faces several challenges associated with consent and managing authorisation. One of these challenges is the heterogeneous environment, which includes different wireless technologies, computational power, and I/O capabilities.(Sengul 2017).

The existence of privacy regulations such as GDPR, which emphasise the principle of transparency and choice, is the primary motivation for many researchers to find solutions for obtaining user consent in IoT systems (O'Connor et al. 2017, Tanczer et al. 2017, Castelluccia et al. 2018, Rantos et al. 2019, Lee et al. 2019, Rhahla et al. 2019, Pathmabandu et al. 2023). However, implementing GDPR in IoT systems can be difficult due to the unique characteristics of IoT, such as its scalability and distributed big data (Rhahla et al. 2019). A study conducted by Wakenshaw et al. (2018) suggests a framework of meaningful consent using "apparency-

semantic/pragmatic transparency" design to achieve transparency in IoT systems. The framework consists of three components: pragmatic transparency, which focuses on the consequences of user consent and activities such as risks and potential harms; semantic transparency, which focuses on the language used to describe these consequences in a clear, understandable and accessible way; and apparency, which focuses on making the interaction, data flows, and data processing clear for the users. The authors believe that their approach assists users in making appropriate decisions regarding their data. However, they did not test it on real IoT environments.

Consent solutions for IoT services were actually proposed before the enforcement of GDPR in Europe. For example, Neisse et al. (2015) presents a technical solution for informed consent in IoT smart spaces. The authors suggest an agent-based, policy-based, and privacy-enabling framework. When the user is subscribing to services and logging in, he/she can give consent by selecting profiles linked to an alias. The profile contains policy rules based on "Event-Condition-Action" structure where events are triggered, conditions are assessed, then actions performed. The authors also consider if users may access smart spaces that are not owned by them. Their framework entities are a user who owns the data, a service provider who consumes the data, a smart space that generates the data and a security gateway. First, the user will use his mobile phone to subscribe to a service by the service provider. The service provider may ask for some information, such as user location. Second, the user will identify the policies that will be used to declare the data that will be collected when he enters the smart space. There will be two types of policies: "a smart space disclosure policy" and "an IoT data policy". Third, the user will enter the smart space. The "IoT data policy" will be loaded from the security gateway to the smart space. Fourth, the service provider will be notified about the IoT devices available for the user by the smart space and it will respond with data subscription information and loads "IoT data policies" for the particular user. The Smart Space uses "Event-Condition-Action" rules to enforce the "IoT data policies" to ensure applying informed consent rules before sending the data to the service providers. The authors use the following tools: Security Toolkit (SecKit) to define "Event-Condition-Action" rules and Idemix for authentication. The authors claim their solution can be applied in many scenarios. Still, the situation maybe different in healthcare IoT where most devices are attached to the user's body, e.g. insulin pumps. Also, in health care, there are other actors who have important roles, e.g. doctors and researchers. Another solution proposed by Neisse et al. (2016) is less complicated for the user than the previous one. The authors combined different existing approaches to develop a semi-autonomous policy-based system. First, the user defines his policies via a graphical interface, which may positively enhance usability. Then, according to the IoT context elements (cars, home, etc.), third-party reputations and behaviour of the user, the semi-autonomous agent evaluates the policies defined and chosen by the user. Next, on behalf of the user, the semi-autonomous agent takes the decision to accept or deny any action regarding user data.

In order to adhere to GDPR regulations, numerous technical solutions have been proposed. However, a significant number of these studies neglected to evaluate how users perceive and interact with these solutions. Lee et al. (2019) argue that their solution meets the "freely given" and "transparency" consent requirements of GDPR. Their solution contains three components: the user device, the user agent, and the data collecting server. The main idea is to send PII (Personally Identifiable Information) from the user device to the data collection server. The IoT device will be set up by the user agent using a smartphone or PC and encryption techniques are specified. Then, the IoT devices will generate personal information and produce PII messages. A PII message will contain information collected from the user's device. This information will be encrypted. One of the elements in the PII is contact information, such as a social network service account or email address. Data collection servers will receive (one or more) PII messages and then send the consent request to the user via the method specified in the contact information. The consent request will include components such as a privacy policy and a data collection

certificate. The user agent will authenticate the certificate and verify the PII message, then send them to the data collection server. Only data approved by the user will be decrypted by the data collecting server. Using the social network account or email address as a method to manage consent requests may help achieve usability as most people use them in their daily lives. The authors claim that even though this solution collects the PII messages and sends them encrypted to the data server before obtaining the user consent, the GDPR "freely given" consent requirement will be achieved. Yet, it seems that there are some risks involved in using this method, where attackers or a third party may find some way to decrypt the data.

Morel et al. (2019) propose a framework for IoT consent in smart spaces. In their design, when any user enters the smart area each device collecting data must send a declaration about its information. This information includes the device location, the data type it collects, and privacy policies. The user will receive the information via a smartphone and give consent if he willing to share his data. Providing information about the IoT sensors could help users feel more confident in sharing their data, which could have positive implications. In their solution, there are two types of communication between users and devices. In the first type, where there is no previous relationship between the user and the firm that owns sensors, a direct connection will be used. The firm that owns the sensors will send the information message via a Bluetooth beacon to the user gateway device, which may be a smartphone. The user gateway device will contain an application called "Personal Data Custodian". This application will check if this data controller privacy policy satisfies the user privacy policy. Then, an automatic consent including the MAC address will be sent. The data controller receives the permissions through Privacy Beacons. When consent is not received, personal user data is immediately deleted. The second type is indirect communications using registries. All device information will be stored in a registry database accessible through the internet and viewable in a human-readable format. The authors argue that using Bluetooth has many advantages, e.g., the risk of tracking by an attacker will be decreased because the communications are local. Later, drawing upon this work, Cunche et al. (2020) introduced a prototype called CoIoT in a new paper titled "CoIoT: A Consent and Information Assistant for the IoT". CoIoT consists of an Android mobile application called a Personal Data Custodian (PDC) and BLE Privacy Beacons to automatically share information about personal data collection and consent management in the Internet of Things (IoT) setting. Privacy Beacons declare devices for data controllers, ensuring data subjects receive declarations. The prototype enables data subjects to define, modify, and delete privacy policy rules. The application securely communicates and stores consent on a central server using Merkle Hash Trees (see Figure 2.4). They declared that the prototype they presented was fully functional and addressed the issues raised. The developers of CoIoT argued that it addresses challenges such as the transparency and accountability of personal data collection in IoT devices. However, the paper lacks a detailed description of the interface of the CoIoT application. Additionally, it is important to note that only the data collection stage is focused on, neglecting other phases of the data life cycle in IoT systems.

In a recent study Pathmabandu et al. (2023) proposed the Informed Consent Management Engine (ICME) model for managing consent in smart buildings. This aims to enhance privacy controls, informed decision-making, and transparency. ICME allows users to interact via a mobile app with IoT devices and IoT dashboards. Pathmabandu et al. (2023) conduct the study in three stages: modelling, prototyping, and interviewing. In the modelling stage, the authors conducted a literature review to identify the essential elements required for obtaining informed consent in IoT-based smart buildings. Based on these requirements, they developed an Informed Consent Model (ICM) for smart buildings. Additionally, they created a dependable methodology for privacy and consent management. To examine the feasibility of the proposed solution, a prototype was created and tested in a simulated environment with various technologies. In the final stages, 15 experts in the area of smart buildings and IoT conducted interviews to evaluate the ICME prototype. The proposed approach involves five phases. These include

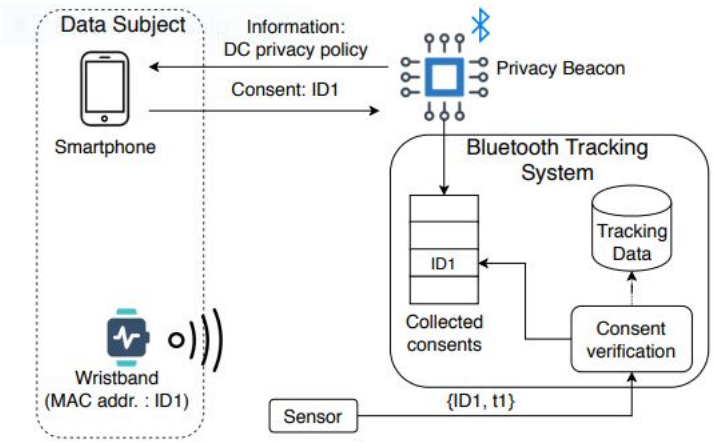

Figure 2.4: *IoT consent solution proposed by Cunche et al. (2020)*

extracting privacy policies, maintaining a list of risky permissions, checking for privacy breaches, tracking and logging events associated with these breaches and recommending corrective actions using nudges. Privacy policies, permissions, events, and nudge details are stored in a document database.

Rivadeneira et al. (2021) proposed a framework named "PACHA", a privacy-aware component for a human-in-the-loop IoT approach to address privacy concerns in human-centric IoT systems. This framework aims to meet GDPR requirements and ensure users' privacy. PACHA enables users to control their dataflows through a model called Human-in-the-Loop "HiTL", which takes into account human emotions, intents, psychological states, and actions inferred through sensory data (Nunes et al. 2015). The PACHA is composed of two primary components: the PACHA Privacy Orchestrator "PPO", located in the cloud, and the PACHA Privacy Interagent "PPI", installed on the user's mobile device. The PPO establishes connections between IoT service providers and users, facilitating requests, notifications, and responses. The PPI serves as the interface that allows users to set their privacy preferences, grant consent, encrypt data, receive notifications for consent requests, subscribe to IoT services, and discover location-based services. Subsequently, drawing on PACHA, Rivadeneira et al. (2023) presented an improved privacy-preserving model framework that includes a more comprehensive approach to consent management. This framework utilises blockchain technology to address the challenges of consent management and transparency in human-centred IoT environments.

All the above studies focus on giving control over the data to the user because he or she is the owner of it. Other actors in the systems cannot collect or access user data without his or her consent. However, in healthcare IoT systems, some emergencies require access to user data to be allowed. Yang et al. (2018) propose a lightweight 'break-glass' access control (LiBAC) system for healthcare IoT. Their proposed system has two parts: attribute-based access and break-glass access for emergency contact persons only. All files are encrypted. The access control policy will be defined by the patient to encrypt his files (see Figure 2.5). Despite the fact that the access control over the data is in the user's hands, there is no explicit consent from the user about using his data. For example, if a researcher is authorised to access the patient data, he can use it for more than one purpose without user consent. That may not satisfy the GDPR "Consent must be specific and must be informed" consent requirement. While some of the previous studies included a prototype with a user interface, the authors were more focused on functionality and performance rather than addressing the user's needs and level of awareness.

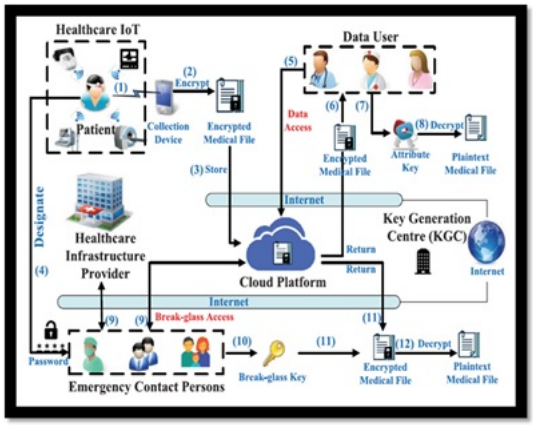

Figure 2.5: *IoT consent solution proposed by Yang et al. (2018)*

2.11 Background on the Components of Consent Mechanisms

There is a need to extract the crucial characteristics that should be developed in the consent mechanism to overcome the lack of users' privacy awareness, enhance users' privacy awareness, overcome some of the users' privacy concerns, and help users provide their informed, meaningful consent. Thus, the current consent mechanisms used in two areas that rely on users' personal data and identifiable data have been surveyed: consent in healthcare (e-consent and paper form) and consent in IoT systems. Scopus and Google Scholar were used to find the most relevant papers from 2015 onwards. However, the health sector is a vast sector and contains a large number of studies focusing on user consent. Therefore, the most closely related studies based on the abstract were selected for this short review. Regarding studies focusing on consent in IoT, we looked for papers with titles having the keywords (Consent AND IoT) and (Consent AND "Internet of Things"); then, we chose the most relevant papers depending on the abstract.

2.11.1 Overview of Electronic Consent (E-Consent) Mechanism Components in Healthcare Studies

Most of the current studies on e-consent in the medical sector focus on the techniques for obtaining consent, such as dynamic consent and meta consent, the consent contents, and the methods used to present the consent. Yet, few studies focus on assessing user comprehension, withdrawal procedure, and functional requirements, such as policy configuration and consent management.

Consent Purpose, Types, and Mechanisms

Health data and medical data are collected to provide medical care to patients. However, these data can be used for secondary purposes, such as scientific or educational purposes (Kotsenas et al. 2021). Most of the studies in the healthcare field, which concern e-consent approaches, focus on obtaining the user's consent to use their medical and health data for research purposes. At present, the user's general consent or refusal regarding the use of their data in research is obtained when providing initial care by using paper forms or via an electronic portal before an appointment (Kotsenas et al. 2021). Another way to obtain users' approval for using their data for research purposes is through an e-consent tool by providing the potential participants with a tablet in the healthcare organisations in order to interact with the e-consent system (Harle et al. 2019). However, with the rapid development of healthcare systems and the use of new technologies such as big data and the IoT, developing new approaches for e-consent is becoming a necessity. Moreover, after the spread of coronavirus around the world, which led

to the imposition of restrictions on visitors' entry to healthcare institutions and the prevention of face-to-face contact, the need to develop and use an e-consent mechanism to obtain patient approval to participate in clinical research has increased (Jaton et al. 2020).

Many studies have focused on meta consent and dynamic consent techniques to enhance the consent process in the medical field (Kotsenas et al. 2021). Meta consent concerns having users' approval for using their personal and health data and biological material for future use by expressing user preference for how and when to provide consent (Ploug & Holm 2016). It can be performed by using checkboxes where the participants tick their preference, and it can be delivered in a paper form or an electronic form such as applications and websites (Ploug & Holm 2016). Furthermore, the information that the participants might need, such as how the data would be utilised in research and the research outcomes, can be provided with meta consent (Cumyn et al. 2020). Ploug & Holm (2016) explained that the differences between people in values, vulnerabilities, and trust affect their preference on when, how, and why they provide their consent. However, this study argues that user privacy awareness also affects this decision if this consent is performed using online services or applications. Some studies mentioned tiered consent. According to Ivanova & Katsaounis (2021), participants may partially modify their preference choices in tiered consent but only for certain study types. In fact, as mentioned earlier, meta consent participants can select their consent options for specific categories of data within different types of research tiers. Thus, meta consent may be viewed as a type of tiered consent. Dynamic consent is online consent obtained using interactive, user-friendly platforms that allow two-way communication between participants and researchers (Budin-Ljøsne et al. 2017). In addition, dynamic consent improves the consent process in medical research by providing transparent access to all of the related information and giving users a role to play by controlling their data (Ivanova & Katsaounis 2021). Thus, many difficulties associated with medical research participants, such as obtaining informed permission and managing consent, can be addressed using dynamic consent (Budin-Ljøsne et al. 2017).

Consent Content and its Presentation

Most of the studies in the healthcare area focus on obtaining user consent for research purposes. The consent content must specify the data type that will be used, such as electronic records, genomic data, health databases, or non-health databases, and the context of the research, such as private or public, national or international, or commercial or non-commercial (Ploug & Holm 2016). Furthermore, there is some information that the participants seek when using e-consent. These are research purpose, research duration, research benefits, research potential risks, research administration processes, their rights as participants, and the measures taken for data protection and privacy (Harle et al. 2018); information about sharing data with third parties, such as who the third party is, when the data will be used and why; participants' future relationships with the involved entities (Ivanova & Katsaounis 2021); and information about researcher expertise and researcher contact information (Harle et al. 2018). Clinical concepts that the participants should be aware of before providing their consent are considered one of the important elements in e-consent (Wilbanks 2018). Regarding withdrawal or revoking consent procedure, some studies, for instance, Ivanova & Katsaounis (2021), mention that informing the users about their right to withdraw is one of the consent contents. However, most studies have not mentioned that the details of the withdrawal procedure must also be a part of the consent information provided to the user. Most agree that the language used in the consent form must be plain and unambiguous (Nusbaum et al. 2017, Rowan et al. 2017, Wilbanks 2018). Some suggest the use of standardised iconography (Wilbanks 2018). In addition, e-consent must be an interactive process using a variety of presentation tools, such as text, graphs, audio, and video, to provide adequate information to the participants and increase their comprehension (Ivanova & Katsaounis 2021).

In their study, Nusbaum et al. (2017) focused on communicating the research's potential

risks and benefits for the potential participants by using traditional consent procedures (paper form) from a professional's point of view. However, they clarified some of the points that would be effective if considered when representing potential risks and benefits and other information in an e-consent mechanism. For example, they suggested the use of numbers and statistics and tables or pictures to display this information. They have also mentioned that reading-aloud methods can be effective when communicating information such as potential risks and benefits.

Assessing User Comprehension

User comprehension is a critical issue in obtaining informed, meaningful consent. Thus, one of the elements that need to be developed in e-consent is the measurement of participant understanding where possible (Skelton et al. 2020). However, comprehension evaluation has rarely been documented as part of informed consent, except in some studies that tested the knowledge of informed consent processes (Wilbanks 2018). For example, Ploug & Holm (2016) argued that the information provided in the consent system should be designed to assist users' comprehension, while Ivanova & Katsaounis (2021) suggested that a dynamic real-time consent tool can help in enhancing users' comprehension. Yet, they did not develop any methods to evaluate user comprehension within the consent mechanism. Suggestions have been given in certain studies to assess user comprehension, such as using specific related questions or a teach-back strategy where potential research participants are asked to relay the information provided in their own words (Nusbaum et al. 2017). Wilbanks (2018) suggested a 'formative' evaluation in which each erroneous response leads to further instruction and assistance, with a summary score at the end. Participants who do not get a perfect score can still participate in the study and have the option to redo the consent process as many times as they would like to. However, Wilbanks stated that such a method may not be suitable for higher-risk observational research.

Additional Functionality

The consent mechanism must allow the users to manage their consent and data. For example, besides obtaining user approval for requests, the users must be able to manage the authorisation to use the data and withdraw consent (Ivanova & Katsaounis 2021). In addition, the mechanism must have a feature to inform all the entities of a change in the consent status in real-time (Ivanova & Katsaounis 2021). Moreover, the consent mechanism must allow the involved entities to communicate with the participants (Ivanova & Katsaounis 2021). However, to avoid strain on the users, the number of actions must be limited, and the participants should be allowed to go backward, move forward, or cancel actions (Wilbanks 2018). One of the functions suggested by Ploug & Holm (2016) is that the consent system provides the users with feedback according to the user choices. According to this feedback, the user can then either confirm or modify the choices. For example, after the user selects their preferences, the system can provide them with the potential number of consent requests in the future and the potential extent of use of their data for research. Furthermore, the consent documents can be viewed and downloaded by the participants as a PDF (Harle et al. 2019).

2.11.2 Overview of Consent Mechanism Components in IoT Studies

Most current studies on developing consent mechanisms for IoT systems aim to investigate technical solutions such as encryption/decryption techniques and Bluetooth. While these solutions effectively address the technical challenges of consent mechanisms in IoT systems, they do not necessarily account for the needs and preferences of users. Few studies explore the interface design for consent mechanisms and its effects on obtaining the informed consent of users in IoT systems.

Consent Purpose, Types and Mechanisms

The primary purpose for developing a consent mechanism in IoT systems is to obtain users' approval to collect, process, store, and use their personal and sensitive data to provide them with the required services. In addition, these data are used for secondary purposes, such as improving the quality of the provided services. Moreover, because of the reliance of IoT systems on sensors to collect data in real-time, most studies in the literature have proposed and discussed dynamic consent mechanisms (Neisse et al. 2016, Tanczer et al. 2017, Sengul 2017, Wakenshaw et al. 2018). Consent mechanisms that can be applied to different types of IoT services have been proposed. For example, Rantos et al. (2019) proposed a general consent mechanism that can be applied to different types of services such as smart homes and healthcare. Cunche et al. (2020) focused on a consent solution for smart spaces. O'Connor et al. (2017) proposed consent mechanisms for IoMT.

Wi-Fi is the most popular medium used in most studies for the transmission of privacy policies and consent information. Some studies have proposed other types of wireless communication, such as a study conducted by Cunche et al. (2020) that proposed using Bluetooth (BLE Privacy Beacons) to communicate the device information, data controller privacy policies, and consent information to the users. Smartphones play a significant role in the IoT systems. They are used as a gateway to connect devices (such as sensors) to the Internet. Furthermore, smartphones allow users to interact with the systems and manage their consent regarding the devices owned by them or the devices owned by the service provider. Moreover, the use of smartphones enables users to define their privacy policies.

Consent Content and Its Presentation

The main content that all studies have focused on is the privacy policy for both the data controller (usually, the service providers or any entity using the collected data) and the data subject (users). This privacy policy should cover information about: the data collection process, which includes what types of data are collected, how much data and what behaviour are tracked; data processing and usages such as aggregation, identification, secondary use and exclusion; and information about the devices collecting data, such as device ID number, the device position, and types of data collected (Morel et al. 2019). Furthermore, showing data flows is one of the critical components of the consent mechanism (Tanczer et al. 2017, Rhahla et al. 2019). Also, illustrating privacy risks and their implications to the user is essential to achieving transparency (O'Connor et al. 2017, Wakenshaw et al. 2018). Wakenshaw et al. (2018) argued that different types of potential risks need to be clarified to users. For example, the users must be aware of privacy threats that might affect their control over their data, such as unauthorised access to their health information, identity threats, and unauthorised disclosure of personal health information. Users must also be aware of potential attacks that the system might face, such as spoofing, tampering, and denial of service. In addition, a risk analysis system must be used along with a consent mechanism to notify the users about potential risks. As in the healthcare field, studies in the IoT field emphasise the importance of using simple, plain, and unambiguous language to display consent information (Morel et al. 2019, Wakenshaw et al. 2018, O'Connor et al. 2017). More importantly, the users must be able to easily access the privacy policy (O'Connor et al. 2017).

O'Connor et al. (2017) investigated the design aspect of obtaining informed consent in the context of IoT smart health and explored how to apply "privacy by design" principles. They proposed employing visual approaches with voiceover capabilities. The authors also emphasised the importance of presenting privacy policies and terms and conditions in a comprehensible way and making them easily accessible. Moreover, visual or graphical means of presentation with voiceover are critical for obtaining electronic consent and should be preferred to a complex document with challenging text.

Assessing User Comprehension

Although most studies have mentioned that user awareness and understanding of the policies and potential risks is an essential part, such as Wakenshaw et al. (2018), no study in the IoT field has used any methods to assess user compensation in the same consent procedure. However, O'Connor et al. (2017) suggested measuring users' understanding of privacy policies and terms and conditions by asking them questions about them. They suggested the use of a quiz to overcome the gaps in user knowledge. To enhance user privacy awareness, Neisse et al. (2016) suggested using a friendly questionnaire that introduces the user to the privacy issue in IoT systems. The authors also recommended the development of a rule suggestion engine to automatically propose rules to the users, which helps the users easily define their policy rules.

Additional Functionality

Most of the studies on IoT have given the users the ability to manage their consent and control over their data (Rantos et al. 2019, Laurent et al. 2019, Cunche et al. 2020). Furthermore, the users can set and manage the policies of their consent (Neisse et al. 2016, Rantos et al. 2019). They should be able to set the level of privacy that best suits their needs (O'Connor et al. 2017). However, these policies need to be easy to set but sufficiently expressive to represent the context of permissions and consent (Sengul 2017). Lee et al. (2019) suggested that using contact information such as a social network service account or email address to send consent request messages may help to achieve usability. The consent mechanism can decide on the user's behalf such as in the Neisse et al. (2016) solution, where the user can define their policies. Then, the semi-autonomous agent evaluates the policies denied and chosen by the user on the basis of the IoT context elements (cars, home, etc.), third-party reputations, and the user's behaviour. The semi-autonomous agent then determines whether to approve or reject any activity involving user data on behalf of the user.

2.12 Informed Consent Features for IoMT

As clarified in the previous section, most proposed solutions in the IoT area focus on the technical components of the consent mechanism, such as providing secure communication and using cryptography methods to accomplish security and privacy requirements. In contrast, the healthcare area focuses on ensuring that all of the information that the user needs to decide on is available and delivered to the participants in an appropriate manner. Moreover, there is a significant difference in the purposes of obtaining users' consent, where the IoT studies focus on the consent for collecting data with consideration to the processing, use, and storage. In contrast, healthcare and medical studies focus on obtaining users' consent for using the data for secondary purposes, specifically research. IoMT services have both IoT system features and some of the healthcare system features.

Therefore, the research in this thesis aims to develop and evaluate a user-centric design for obtaining consent in IoMT systems. This enhanced design combines consent features found in both the healthcare and the IoT fields, and it aims to fill the gaps in these two areas by focusing on the users. The proposed features of the enhanced consent design focus on improving users' privacy awareness and assisting their understanding of the consent process, thereby addressing the gaps in these two areas. Furthermore, the consent process will be sufficiently simple for most users to understand. This enhanced design of consent will be used to achieve the study's goal of ascertaining whether e-consent can actually help users with different privacy awareness levels to make appropriate decisions regarding the collection, processing, use, and sharing of their personal health data in IoMT. These aspects will be illustrated in the next parts.

2.12.1 Language, Audio, and Visual Components

Misunderstandings can occur when people sign consent forms without fully understanding them (Nijhawan et al. 2013). Thus, as stated in the previous section, it is important to use plain, simple, and easy-to-understand language when communicating privacy policy information to users. This practice will improve users' comprehension. Steinfeld (2016) found that users tend to read the privacy policy when it is presented to them by default. However, if users are given the option to click a link or button to open the policy, the majority of them tend to skip it and do not read it. Thus, in our study, we suggest that displaying the privacy policies should be mandatory when requesting to collect, use, or share users' medical and personal data.

One approach used in the traditional (paper) consent procedure involves having a specialist read the information aloud to the participant to avoid the participant granting approval without reading the consent form. This procedure is also used to satisfy the condition that participants must be informed (Nusbaum et al. 2017). Nusbaum et al. (2017) reported that the read-aloud technique in the on-paper process has some disadvantages. For instance, the expert might read the form verbatim without pausing to allow for comments or clarifying questions. There is also the risk of participants becoming passive listeners. However, these disadvantages can be avoided in the e-consent mechanism because the user can stop and repeat the audio as many times as they wish. In addition, instant chat with a specialist can be added if a specific question arises, or an AI question-answering system can be used, depending on the data available from previous users' questions. Furthermore, as it is important to include visual methods to support users' understanding, videos, pictures, and graphics can be added as required. For example, short videos can be used to illustrate the benefits of sharing health data in research or graphs to illustrate the possibility of the occurrence of some types of privacy risks. Data flows are an important component (Tanczer et al. 2017), and visual approaches such as graphs or diagrams can be used to illustrate them. However, Tanczer et al. (2017) argued that it is a challenge to keep users tracking their data and informed of all the operations performed on their data in an IoT environment. Wilbanks (2018) has suggested the use of standardised icons in e-consent design, such as using the lock icon to illustrate security and privacy measures.

2.12.2 Perceived Benefits and Potential Risks

Most studies that examined users' willingness to provide their data in different types of healthcare systems confirmed that knowledge of the benefits provided to the users and the community are factors which positively affect the users' acceptance to share their data (Rowan et al. 2017, Esmaeilzadeh 2019, Kim et al. 2019). Furthermore, users' behaviour towards the e-consent process can be affected by potential risk (Harle et al. 2018). For example, users are less likely to consent to data disclosure in any system when informed of potential risks. Moreover, many studies in the literature have emphasised the importance of users' privacy risk awareness with regard to IoT and wearable devices (Udoh & Alkharashi 2016, Psychoula et al. 2020). Moon (2017) conducted a review study to identify the factors that affect users' decisions when sharing their personal health data. The author classified the factors that affect users' willingness to share their healthcare data into five main sections. One set of factors related to balancing risks and benefits, such as allowing an entity to share medical data in return for improving medical care. Thus, the perceived benefits and potential risks of collecting and using user data should be clearly communicated to ensure their informed consent.

2.12.3 Privacy and Security Measures and Withdrawal Procedures

Transparency is an important aspect of both Privacy by Default and Privacy by Design (PbD) principles. Scarpato et al. (2017) argued that both Privacy by Default and Privacy by Design (PbD) principles are essential in the design of IoT architectures. Also, system transparency is an important factor in enhancing user awareness. Many users are unaware of the privacy protection of IoT systems (Zhou et al. 2018). Thus, it is vital to help the users become aware of how their data will be processed in the system (Cha et al. 2018) and how their data privacy will be protected in the IoT system.

Harle et al. (2018) found that users' behaviour when interacting with e-consent can be affected by many factors, including the service provider's data protection methods. Moon (2017) clarifies that healthcare providers understand that robust data protection measures and system transparency are essential to build trust with the users. Gupta et al. (2023) argue that users are more likely to share their health information when specific privacy protections are provided. Therefore, in addition to obtaining users' consent, providing transparent information about the privacy and security measures the service provider uses to safeguard users' data is essential. However, such information must be enough to gain the user's trust without revealing details that could lead to cyberattacks.

The consent specification of the GDPR states that "the withdrawal must be as easy as giving consent" (GDPR 2018). However, despite the significance of this requirement, most research studies have primarily focused on the process of obtaining user consent without providing adequate details on the withdrawal procedure. Therefore, it is crucial to provide users with detailed information on how to withdraw their consent. This information should be easily accessible and clearly explained to ensure that users can exercise their right to withdraw their consent effectively. This will help users to have control over their personal data and ensure that their privacy is protected.

2.12.4 Regulations and Polices

In a study conducted by Duckert & Barkhuus (2022), participants indicated that managing privacy rules and consent for digital health information was time-consuming and difficult. They also expressed uncertainty and misunderstanding regarding GDPR requirements. Thus, it is important to provide users with access to related regulations, such as by providing a link to the necessary regulation documents. Furthermore, the participants experienced privacy fatigue when managing their privacy settings, leading to a lack of concern about who had access to their data. Many other technical solutions have been proposed for achieving user consent in the IoT and for maintaining user privacy. However, most of those that help users set their policies are not user-friendly (Sengul 2017). Sebastian (2021) argued that well-designed interfaces can increase user understanding and retention of privacy policies and regulations, which can result in higher click and read-through rates. Wakenshaw et al. (2018) argued that the language used in consent agreements to describe privacy and risk must be understandable. Moreover, O'Connor et al. (2017) argued that privacy policies that consent depends on must be presented in an easy and understandable manner and be displayed in multiple languages where applicable. Also, third-party involvement in online services increases the challenges, such as incongruity in privacy policies and actual practices (Kurtz et al. 2020). However, obtaining users' consent is a formal process that must comply with local and international personal data protection regulations, laws, and required ethics guidelines (Skelton et al. 2020). Furthermore, as concluded in the first part of the research, users' knowledge of laws and regulations is one of the factors affecting their privacy awareness. Using methods such as notifications with updates regarding the related regulations and policies or adding 'news' on the consent interface's main screen may help educate the users about the related regulations and laws. Also, a clear and comprehensive privacy policy is one of the most important best practices for organisations that collect and use personal data.

The privacy policy should explain how the organisation collects, uses, and stores personal data. It should also include information about the rights of individuals concerning their data, such as the right to access, correct, and delete their data. Organisations and companies can create their privacy policies, but these policies must comply with applicable legal and regulatory standards. An organisation's information collection, usage, and disclosure practices should be outlined in a privacy policy. Because it educates people about how their personal information will be treated, this policy is a crucial component of privacy best practices.

2.12.5 Methods for Ensuring Users' Comprehension

User comprehension of the factors including regulations, privacy policies, potential risks, and benefits, is essential for achieving informed user consent. Among the elements that must be developed in e-consent are online tools and methods to measure participant understanding where possible (Skelton et al. 2020). Although many of the relevant studies emphasise their importance, few studies in the healthcare arena have combined methods to ensure user understanding as a part of the consent mechanism, and, as far as we know, no prior study on the subject of IoT has combined such methods in the design. Cognitive friction refers to the difficulty people may face while attempting to comprehend or engage with a particular task or system. It can appear as mental effort or difficulties in cognitive processes such as learning, memory, and solving problems. According to Wilbanks (2018), while it is essential to minimise cognitive friction when designing and developing digital systems, some activities in the system, such as informed consent, require cognitive effort to complete. Therefore, some questions related to the content must be added at some point in the consent process to ensure the users' understanding. When users respond to these questions, the correct answer provides additional explanatory sentences, and the wrong answer leads to an explanation of the reason.

2.12.6 The Most Important Features for Informed Consent Mechanisms

Guided by the background presented in the previous sections and by reviewing studies that focused on electronic consent mechanisms (e-consent) in healthcare and consent mechanisms, the most important features that need to be investigated in IoMT consent mechanisms were extracted. The aim of incorporating these features in the enhanced design of the IoMT consent approach is to obtain users' informed consent. However, obtaining users' informed consent in any system is highly connected to system transparency and user comprehension. System transparency refers to how a system's processes and decision-making are visible and accessible to users. It provides clear information about the system's operation, data processing, and decision-making. User comprehension refers to users' ability to understand information provided in a way that facilitates effective interaction and decision-making. Thus, some of these features help to achieve transparency, while others help to enhance user comprehension.

The specific features of the enhanced consent mechanisms that will be be investigated in this research are given below.

1. Links to data protection laws and regulations that govern personal data in Saudi Arabia – achieve transparency;
2. Dividing the privacy policy into small sections instead of one long text on one page (focusing only on the service or request) - achieve user comprehension;
3. Mandatory access to privacy policy instead of having optional links – achieve user comprehension;
4. Explaining the benefits which will be gained from accepting a service or request – achieve transparency;

5. Explaining the potential risk that could occur from accepting a service or request – achieve transparency;
6. Clarification of the withdrawal procedures and updates (not only mentioning that it is possible to withdraw) – achieve transparency;
7. Using icons (especially privacy icons) to visually represent parts and sections – enhance user comprehension;
8. Using videos to explain some points such as service or request information - enhance user comprehension;
9. Explicit indication of privacy and security measures used to protect the data - achieve transparency and enhance user comprehension;
10. Questions to assess user understanding – achieve user comprehension.

2.13 Chapter Summary

This chapter starts by comprehensively explaining the main concepts related to this thesis. It clarifies the meaning of privacy, information privacy and privacy awareness. Then, it offers a summary of the primary sources for privacy requirements, focusing on regulations, principles, standards, and best practices guidelines. It explains how primary sources of privacy requirements agree about the significance of obtaining user-informed consent in order to achieve transparency. It provides background on some of the privacy awareness measurement instruments. Then, it provides an overview of informed consent, its origin and how it applies in different contexts that involve the collection, processing, and sharing of users' personal data. It demonstrates that most IoT studies focused on consent concentrate on technical solutions, whereas most of these studies concentrate on consent mechanisms that can be applied in different contexts. Then, the consent tool features which help to obtain user consent in IoMT were extracted from the literature after examining studies that focus on the e-consent mechanism in healthcare systems and the consent mechanism in IoT systems.

In this thesis, the term **privacy** is used to refer to **information and data privacy**, which refers to users' right to control their data and make decisions about their data, including collection, storage, use, and sharing. Moreover, in the context of this study, users' privacy awareness refers to a combination of the users' knowledge and understanding of specific factors, in addition to users' previous experience. However, projection, which involves predicting the situation and the impact of certain factors in the future, was excluded from this study because projection can be a complex task as many factors can influence the prediction process (e.g. social, economic and technological changes). In Section 3.4.2, the factors that shaped users' privacy awareness are discussed in detail. Also, the work presented in this thesis considers information privacy in IoMT from the cognate-based point of view (as described earlier). It concentrates on the states that users might face when using these systems and how they can control their medical and personal data. The following chapter will describe in detail the methodology that was used to conduct the research.

Table 2.3: *Summary of the studies that proposed consent solutions for the IoT systems*

The reference	The main aim	The proposed solution
Neisse et al. (2015)	Addressing the limitations of using EULA	The proposed solution focuses on a policy-based, agent-based, and privacy-enabling framework for informed consent in IoT. Users can consent by selecting profiles linked to the alias "Event-Condition-Action" when subscribing to services and checking in.
Neisse et al. (2016)	Addressing the limitations of using EULA	The proposed solution focuses on a policy-based framework approach to informed consent. The researchers combined different existing approaches, including a dynamic and context-aware approach, a semiautonomous agent, reputation systems, behaviour modelling, and analysis of the EULA.
Lee et al. (2019)	Complying with GDPR	The proposed solution focuses on encryption and decryption methods. Encrypted PII messages from IoT devices can only be sent to a data-collecting server if the user provides the decryption key for each personal information.
Morel et al. (2019)	Addressing privacy concerns	The proposed framework focuses on obtaining consent and protecting information using direct (BLE privacy beacon) and indirect (registries) communication modes.
Cunche et al. (2020)	Complying with GDPR	The proposed solution focuses CoIoT, a prototype designed to manage user consent and information in IoT. It includes an Android app that works as a Personal Data Custodian (PDC) to automate communication for information and consent management for personal data collection.
Rivadeneira et al. (2021)	Addressing privacy concerns and Complying with GDPR	The proposed solution focuses on a framework that protects privacy and can be incorporated into user-centric IoT systems. They introduced the architecture of the PACHA framework.
Pathmabandu et al. (2023)	Increasing Privacy visibility, users awareness, and informed decision-making	The proposed solution focuses on a user-centric Informed Consent Model (ICM) for smart buildings. Based on critical requirements from a literature review, the ICM redefines data flow structure and provides a methodology for managing privacy and consent.

Chapter 3

Research Methodology and Design

3.1 Introduction

Chapter 1 clarified the research aims, and questions, and Chapter 2 provided an in-depth analysis of the background and related work. This chapter explains and describes the research methodology, beginning with an introduction to research paradigms and methodologies to serve as a foundation for a better understanding of the selected methodology. Then, the methodology of Study 1 (The Survey) is explained in detail, followed by the methodology of Study 2 (The Experiment). Finally, this chapter outlines the ethical considerations associated with this research.

3.2 Research Paradigms and Methodologies

Research paradigms vary according to the nature of the problem and the research questions with each paradigm having different philosophical assumptions and practical implications (Kankam 2019). Positivism, interpretivism, pragmatism and post-positivism paradigms are commonly used in information research (Kankam 2019). The positivism paradigm focuses on quantitative research methods and is measurable, objective, and solid (Kumatongo & Muzata 2021), whereas the interpretivism paradigm uses qualitative research methods to investigate human behaviour, perspectives, and interactions (Kumatongo & Muzata 2021). The pragmatism paradigm employs a framework combining both qualitative and quantitative techniques (Kumatongo & Muzata 2021) and is considered the most suitable method to effectively address research problems. Post-positivism is considered an amended positivism paradigm (Kumatongo & Muzata 2021) focusing on the fact that research can never be completely objective, as a researcher's worldview and biases inevitably influence the results (Kankam 2019).

The main types of research methodology are: qualitative, quantitative and mixed methods. Qualitative research concentrates on exploring a research topic in-depth, and it mainly evolved in social sciences (Creswell & Creswell 2017). Various approaches are used in qualitative research, such as phenomenology, ethnography, case studies, and grounded theory. Qualitative data collection can include interviews, observations, documents, and records (Creswell & Creswell 2017). The quantitative design focuses on measuring variables and examining the relationships between and among variables to answer questions and hypotheses (Creswell & Creswell 2017). Approaches such as surveys and experiments can be used. Quantitative data collection can include instrument data, checklists, or numeric records (Creswell & Creswell 2017). The mixed methods approach integrates qualitative and quantitative techniques to provide a more comprehensive understanding of research problems and overcome the limitations of using a single approach (Creswell & Clark 2017). Utilising mixed methods design in research offers many benefits over working with a single approach. It addresses the limitations of single research methods. For example, quantitative methods can be used to test hypotheses and identify rela-

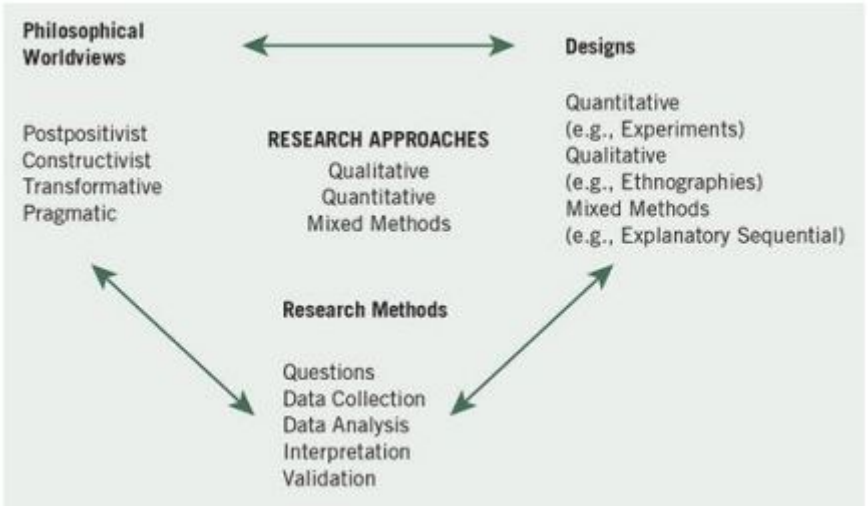

Figure 3.1: *The interconnection of worldviews, design, and research methods (Creswell & Creswell 2017).*

tionships, while qualitative methods can explore underlying reasons. Moreover, it helps to gain a comprehensive understanding of the research problem. It involves collecting both qualitative and quantitative data, using strict methods for data collection, analysis, and interpretation (Creswell & Clark 2017).

The mixed methods approach is appropriate for explaining quantitative results, incorporating individual perspectives, and evaluating programmes and policies (Creswell & Clark 2017, Creswell & Creswell 2017). Moreover, there are three distinct types of mixed methods designs: the convergent, the explanatory sequential, and the exploratory sequential (Creswell & Clark 2017, Creswell & Creswell 2017). In their book, Creswell & Clark (2017) explain the difference between these types. The convergent design (also known as parallel design) depends on collecting and analysing quantitative and qualitative data independently to obtain a more comprehensive understanding of the problem. The goal is to link themes with statistical data using the same variables. Explanatory sequential design has two phases: the first phase is gathering and analysing quantitative data and the second is collecting and analysing qualitative data to support the findings from the quantitative analysis or to provide extra explanation. The latter is an exploratory sequential design involving three phases. Unlike explanatory sequential design, the exploratory sequential starts with collecting and analysing qualitative data before the results are used to develop quantitative features and variables. Finally, these variables are tested and interpreted considering the first qualitative findings. Figure 3.1 illustrates the relation between the research paradigms, methods and design.

3.3 Defining The Research Methodology

A case study involves an in-depth examination and analysis of a specific entity, such as an individual, group, organisation, or community (Yin 2018). Case studies can be exploratory, descriptive, or explanatory (Yin 2018). Different data collection methods, such as surveys, observation and interviews, can be utilised to collect data in case studies (Runeson & Höst 2009). Case studies have been criticised because they are limited in their generalisability (Runeson & Höst 2009); however, they have significant value in research because of the comprehensive understanding of each case obtained by examining its various aspects within a real-life context.

This thesis aims to investigate the current privacy awareness of digital health service users in Saudi Arabia and how the enhanced consent design for IoMT helps users with different privacy awareness levels provide their informed consent. Thus, this research is a case study focused

on the users of digital health services in Saudi Arabia. The reasons for choosing Saudi Arabia for this case study were explained in Section 1.3. In this research, two studies were conducted using the most appropriate research methods and tools for each study. Study 1 involved a quantitative survey, while Study 2 was a mixed-method experiment to collect data within the case study allowing for a comprehensive investigation of the research subject. A survey enables the description of people's opinions and attitudes or helps to test relationships among variables (Creswell & Creswell 2017), thus it can be used to answer the descriptive research questions, determine correlations between variables and forecast associations over time (Creswell & Creswell 2017). A quantitative survey design can help researchers investigate relationship, predictive, and descriptive questions by studying a sample of a population (Creswell & Creswell 2017). The use of mixed approaches can provide researchers with a deeper understanding of a subject, overcoming the limitations of relying solely on one type of data source (Creswell & Creswell 2017). Thus, this study adopted a mixed-method experimental design to combine quantitative and qualitative data collection, analysis, and integration within an experimental quantitative research design (Creswell & Clark 2017). Integrating qualitative methods alongside quantitative research assists in comprehending participants' experiences and interpreting experimental outcomes (Creswell & Clark 2017). Moreover, mixed-methods experimental designs are highly versatile and can be used in many types of experiments including quasi-experiments, between-subjects, single-subject, and within-subject experiments.

The two studies are strongly connected. Study 1 aims to determine the current situation of users' privacy awareness regarding their personal data when using digital health services to categorise users according to their privacy awareness level. The understanding gained in Study 1 informs the interpretation of the behaviours exhibited in the subsequent Study 2 to determine if users with different privacy awareness respond differently to the proposed consent mechanisms. Also, categorising the users helps to understand if the proposed features of the consent mechanism have a different effect when making decisions regarding their data if they use IoMT services. An experimental smartphone-based framework was developed in Study 2 to investigate how users with different privacy awareness levels provide informed consent and make decisions in IoMT.

3.4 Study 1 (The Survey): Privacy Awareness among the Users of Digital Healthcare Services in Saudi Arabia

This study was designed to determine the current state of privacy awareness among the users of digital health services in Saudi Arabia, specifically to address RQ1 (see Section 1.5). A descriptive research design using a quantitative survey method was applied to understand the study population's current situation of privacy awareness. First, the factors affecting users' privacy awareness were identified from previous studies, and then a quantitative questionnaire was designed to measure users' privacy awareness. The survey questions were designed to measure user knowledge and understanding of each factor. A pilot study was conducted before the questionnaire was distributed to collect data.

3.4.1 Identifying Factors that Affect Users' Privacy Awareness

Correia & Compeau (2017) reviewed privacy awareness in information systems to determine the factors that affect users reporting that privacy awareness consists of three factors: regulation, common practice and technology. Moreover, as stated in Section 2.7, there are three primary sources of privacy requirements: privacy regulations, principles and standards, and best practices.

Information privacy regulations are the laws that govern the obtaining, processing, and sharing of a user's personal data between users, service providers and third parties (Correia & Compeau 2017). These regulations provide a clear framework for companies and organisations to protect personal information security and privacy (Stallings 2019). The details about privacy regulations were discussed in section 2.7.1 highlighting that the awareness of data privacy regulations is an important issue for privacy awareness (Varkonyi et al. 2019). Users need to know and understand the regulations that aim to protect their personal and sensitive data. For example, users in Europe not only need to know that the GDPR exists but also understand what their rights are and how this law protects their data. Thus, the supervisory authority must promote "public awareness and understanding of the risks, rules, safeguards and rights in relation to processing" (GDPR 2018). Some studies focus on investigating user awareness of the regulations used in their area. For example, Varkonyi et al. (2019) conducted a survey concentrating on GDPR knowledge and awareness among EU and non-EU students. Moreover, the Antecedents, Privacy Concerns, Outcomes Model (APCO Macro Model) illustrates that regulations affect users' privacy concerns, consequently affecting their data-disclosing behaviour (Smith et al. 2011). Thus, users' awareness of data privacy regulation is a crucial issue that enables them to make informed decisions about their personal data when using healthcare services.

According to Correia & Compeau (2017), common practices awareness means that users must know the policies and techniques service providers use to collect, manage, integrate, analyse and share their personal information. Also, they define technology awareness as meaning that users must know what devices are used to collect, transfer, and use their personal data and how they work; what types of software process and use the data; and the security and privacy measures to protect personal user data. Noticeably, user awareness about common practices and the technology used in the system is associated with system transparency. The privacy policy is the most appropriate means to inform users about how their personal information is managed (Kuznetsov et al. 2022) and what security and privacy measures are used to protect their personal data. However, service provider's privacy policies are based on several factors, including the three main sources of privacy requirements: the privacy laws and regulations in their country or region, the principles and standards in the area, and industry best practices (see Section 2.7. Privacy policy statements must be easily located by the user (O'Connor et al. 2017). Privacy policies support users in making decisions about their engagement and consent regarding a service's activities. Nevertheless, some users do not read the privacy policies and terms and conditions documents before they give their consent (Steinfeld 2016, Mulder & Tudorica 2019). Other users may read them, but not fully understand the content (O'Connor et al. 2017, Mulder & Tudorica 2019, Sebastian 2021) as most privacy policies are difficult to understand because they are presented using complex text (O'Connor et al. 2017, Sebastian 2021). These issues are affect users' privacy awareness and lead them to make inappropriate decisions. Many studies about users' privacy, such as Pelet & Taieb (2017), focus on privacy policies due to their importance in users' decisions about their data. Therefore, users' knowledge and understanding of service providers' privacy policies is one factor that affects their privacy awareness.

Privacy calculus theory suggests that people's behavioural responses, including disclosing their data, are determined by trade-offs between costs (risks) and benefits (Smith et al. 2011). Some scholars, such as Malhotra et al. (2004), define privacy risk as the potential loss of personal information when shared with a company. However, technological developments have led to new privacy risks, such as creating user profiles using data mining or identity theft. Many studies have found that privacy risk negatively affects users' willingness to share their information (Smith et al. 2011) with people disclosing information based on the perceived benefits. Financial rewards, personalisation and social adjustment can encourage users to disclose their data (Smith et al. 2011). Some studies have investigated privacy calculus theory in IoT, for example, Kim

et al. (2019) concluded that most users benefit from IoT services regardless of their privacy concerns, especially younger users familiar with the technology. They found that the perceived risk did not affect users' intentions to disclose their data for IoT personalised services. Similarly, Menard & Bott (2020) argued that users' future IoT purchase intentions are not significantly affected by risk with users being open to purchasing smart home devices in certain instances despite the perceived risks. However, the potential risk can affect the user's decisions in IoT services that involve sensitive data. Kim et al. (2019) found that in IoT healthcare services, perceived privacy risk affects users' decisions to disclose their data. Also, they found that in the IoT context, the network externality variables, such as service usage and the number of users, have no significant effect on perceived benefit, except in smart homes where the number of services (e.g. energy meters, lighting control and air quality system) affects perceived benefit. Service providers should focus on the users' benefits to attract them to use the services and reveal their information (Kim et al. 2019). Thus, understanding potential risks like data breaches can motivate users to take privacy precautions. Nevertheless, recognising the benefits of responsible data use, such as personalised services, encourages users to share their data. Thus, users' privacy awareness about the risks and benefits of personal data collection and disclosure is essential to balancing risks and benefits, which helps users make the appropriate decisions regarding their data.

When users are familiar with technology and how to use it to secure personal data, they feel more confident using IoT healthcare services (Alraja et al. 2019). Also, according to the APCO Macro Model, privacy experience affects users' privacy concerns, consequently affecting users' data disclosure decisions (Smith et al. 2011). Users who have been exposed to or have been the victims of personal information violations have more concerns about information privacy (Smith et al. 1996). For example, mobile users with privacy issues, such as personal information misuse without their knowledge, are more concerned about privacy (Kusyanti et al. 2022). Udoh & Alkharashi (2016) conducted an exploratory study to determine the level of privacy risk awareness among smartwatch users in Indiana (USA), showing that users prefer Apple smartwatches over other brands because Apple does not have serious privacy violation issues. In an experimental study by Aleisa et al. (2020), user privacy awareness was enhanced by observing some privacy violations in network traffic analysis reports when using IoT services that collect non-personal data. Aleisa et al. (2020) examined the level of participants' trust and their privacy concerns before and after an experiment aiming to raise their privacy awareness, reporting that users' trust levels were reduced while privacy concerns were raised. A month later, they re-examined user trust and privacy concerns and found that both returned to nearly the same level observed before the experiment. Therefore, it can be concluded that knowledge of or experience with privacy violations is a factor affecting users' privacy awareness.

According to what has been discussed in this section, the factors that shape user privacy awareness are privacy regulation, privacy policy (common practices), perceived benefits, potential risks, user experience with previous privacy violations and user experience with technology (see Figure 3.2). An instrument to measure user privacy awareness was developed in light of these factors. Other factors that may influence users' awareness of privacy, such as privacy concerns, have been extensively investigated in the literature. The next section describes the design and development of the privacy awareness questionnaire.

3.4.2 Designing and Developing the Questions

As explained in Chapter 2, users' privacy awareness is defined in this study as a combination of the user's knowledge and their understanding of specific factors. These factors include privacy regulation, privacy policy (common practices), perceived benefits, potential risks, and user experience. A set of questions was designed to assess users' knowledge and their understanding together with experience questions focused on users' experience with related applications, such as "Sehhaty", home healthcare devices, and privacy violations (see Figure 3.3).

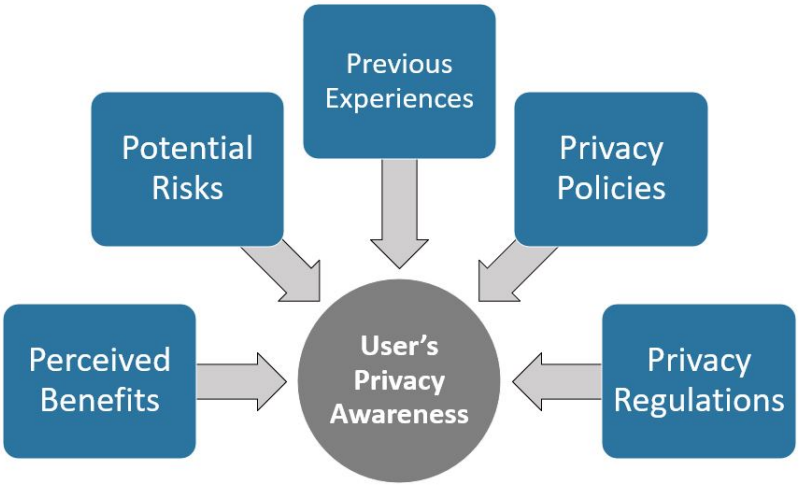

Figure 3.2: *Factors that affect users' privacy awareness (identified by previous studies)*

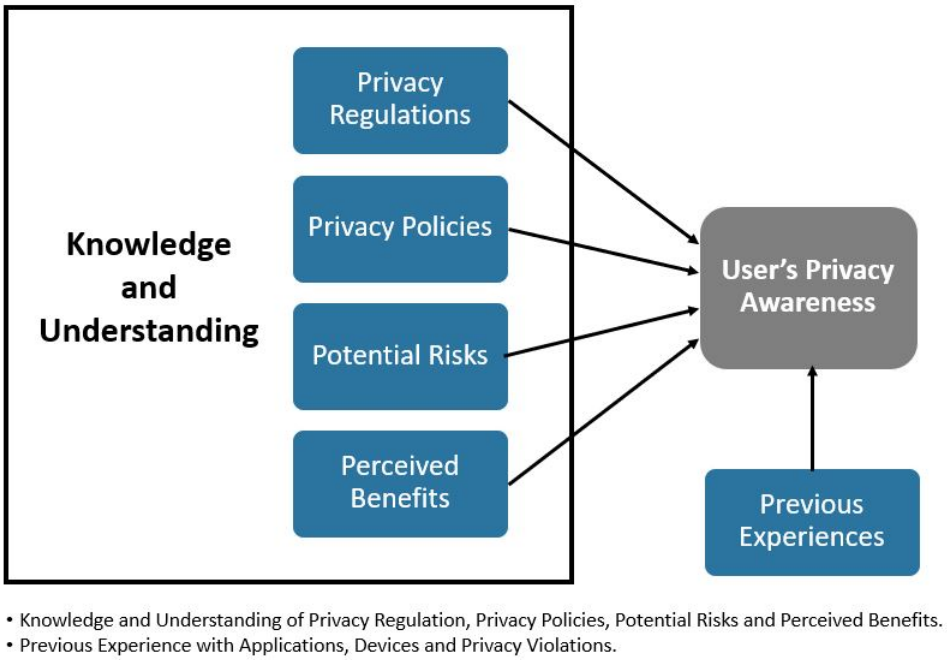

Figure 3.3: *Privacy awareness factors investigated through questionnaire questions in Study 1*

According to the investigation conducted in Section 2.11, most studies that focus on measuring privacy used self-assessment strategies, particularly the Likert scale. Braunstein et al. (2011) argued that self-reporting behaviours could produce inaccurate outcomes as participants may unintentionally make mistakes, such as having an inaccurate memory when evaluating themselves or wanting to seem to engage in society-respected behaviours (Braunstein et al. 2011, Brace 2018). According to Sim et al. (2012), situation awareness measures can be subjective or objective. Subjective measures rely on users' self-assessment of their knowledge or skills whereas objective measures usually rely on the observer's judgment to assess a subject's abilities by comparing their responses to an actual situation. Therefore, to avoid the limitation of using self-assessment and self-reported behaviours and to obtain more accurate results, two types of assessment, subjective and objective, were used in this study. The Likert scale for self-assessment questions and score scaling with right and wrong answers for objective assessment were utilised.

The questions were formulated after the development of the study framework and the question types and this process took several months due to the need to review all related sources and documents. Before March 2022, there was no single law in Saudi Arabia regulating the handling of users' data and privacy by service providers with laws such as Shari'a, Anti-Cyber Crime Law and Electronic Commerce Law protecting users' data and information. Saudi Arabia's new Personal Data Protection Law (PDPL 2023) was announced by Royal Decree on 16 September 2021 and came into effect in March 2022. Service providers had approximately a year to modify their arrangements to ensure compliance, therefore, developing questions about privacy regulations in Saudi Arabia at that time was challenging. The available Personal Data Protection Law (PDPL 2023) documents were reviewed in detail to design the questions on privacy regulations.

Published studies have proven that most users agree to online service terms and conditions and privacy policies without reading them (Schraefel et al. 2017, Wakenshaw et al. 2018) or users may read them but not fully understand the content (O'Connor et al. 2017, Wakenshaw et al. 2018). Thus, the privacy policies section started with general questions including whether participants read privacy policies when using applications and what topics privacy policies cover. However, although the terms of use and the privacy policy are always located in the same place in any application or website, the terms of use were excluded from this research because of their content which focuses more on the agreement between users and service providers on the rules and guidelines of using the application or website. Next, some questions were raised regarding general practice in healthcare in Saudi Arabia and were formulated based on the Ministry of Health's 'Acceptable Use Policy' document, now updated under 'Cybersecurity Policy for Acceptable Use' [1]. In addition, the design of the "Sehhaty" application was studied, and its privacy policy [2] was carefully read to design the related questions.

Regarding the questions focused on the potential risks and perceived benefits associated with data disclosure, the question design was based on previous studies that highlighted these factors. For instance, Fox & James (2021) study demonstrated that users are concerned about risks that may compromise their health data such as unauthorised access, sale of data to third parties, and use of data without consent for secondary purposes. Additionally, Fox & James (2021) highlighted some benefits of sharing health data such as increased efficiency in health services and improved diagnoses and treatments. Moreover, personalised services have been identified as an additional benefit by Smith et al. (2011). Thus, the questions centred around these risks and benefits. Also, The Ministry of Health's page on the benefits of new health systems for patients [3] was reviewed. Regarding the questions that focus on users' previous experiences, questions related to using medical devices and healthcare applications and privacy violations were developed. Table 3.1 illustrates the questions designed for the regulation factor.

[1] https://www.moh.gov.sa/en/Ministry/Rules/Documents/Acceptable-Use-Policy.pdf
[2] https://api.sehhaty.sa/services/individuals/privacy-policy/?lang=en
[3] https://www.moh.gov.sa/en/Ministry/nehs/Overview-of-eHealth/Pages/Benefits-to-Patients.aspx

Table 3.1: *Samples of the questions (privacy regulation)*

Regulation		Knowledge	Understanding
subjective (Self-assessment)	Likert scale 5 points	On a scale from 1 to 5, with 1 being a "no knowledge of" and 5 being "an excellent knowledge of", how would you describe your knowledge of the laws and regulations related to data privacy in Saudi Arabia?	On a scale from 1 to 5, with 1 being a "no understanding" and 5 being "an excellent understanding", how would you describe your level of understanding of the regulations that you know regulate users' personal data in Saudi Arabia?
Objective assessment	Yes/no or multiple choice	Which of the following sentences describes the current state of personal data protection in Saudi Arabia: 1. The personal data protection regulation has been approved by the government and will come into force by March 2022. 2. There is no personal data protection regulation in Saudi Arabia.	It is allowed for a service provider whose application or service you have used and shared your personal data with to further process and use this data if: 1- the reason was stated (implicitly/explicitly) in the privacy policy, which you approved when using the application. 2- the reason was not stated in the privacy policy, which you approved, and they need the data. 3- the reason was not stated in the privacy policy which you approved, and they gained your approval (by other means) for its use before processing the data.

It is important to carefully formulate questions using simple, clear, and neutral language to obtain reliable data and reduce bias (Brace 2018). Moreover, technical terminology must be avoided and specific and concrete language should be used to ensure clarity and minimise interpretation (Brace 2018) and to avoid ambiguity and misinterpretation (Brace 2018). In addition, it is important to provide balanced response options, such as adding an "I don't know" option when applicable. Also, each question must address only one idea. The questionnaire was developed in English and then translated into Arabic to be suitable with the survey participants. All the points above were considered when designing the questions in English and translating them into Arabic. In addition, we have organised each section of the questionnaire by starting with general questions and then moving towards more specific topics. We have avoided questions which combine multiple issues into a single question. As per ethical considerations, we have included an information sheet at the beginning of the questionnaire. This sheet provides clear and concise instructions, explains the purpose of our study, and includes contact information in case the users have any questions or want to withdraw or escalate any concerns.

The first part of the questionnaire included demographic questions and contact information (e-mail and/or mobile number) to be provided if the participant agrees to participate in Study 2 (The Experiment). Different types of questions were used according to the question's aim. A five-point Likert scale and Yes/No questions were employed for the self-assessment questions, whereas Yes/No, three scales (Yes/No/I don't know), multiple-answer multiple-choice and single-answer multiple-choice questions were used for the objective assessment questions. Two questions were open-ended. The questionnaire was divided into four categories: privacy regulations (6 questions), privacy policies (16 questions), risks and benefits (19 questions) and user experience (16 questions) and had a total of 57 questions not including demographic ques-

tions. This instrument focused on users' privacy awareness in the healthcare context. However, most questions could be used to assess the privacy awareness of Saudi Arabian citizens in other contexts, with some modifications relating to privacy policies and user experiences. The final version of the questionnaire is provided in Appendix A.

3.4.3 Questionnaire Validity and Reliability

Research is considered rigorous when an effort is made to improve the research quality through validity and reliability tests (Heale & Twycross 2015). Validity and reliability tests of the data collection instrument are fundamental to ensure the accuracy and consistency of the data collected, thereby enhancing the quality and credibility of the study findings. This study employed a questionnaire to collect the survey data and conducted content and face validity tests, followed by a reliability test to ensure the questionnaire's validity and reliability before conducting the main study. Figure 3.4 illustrates the validity and reliability tests conducted in this study.

Validity Test

The validity of a questionnaire refers to ensuring that all of its items measure what they aim to measure (Taherdoost 2016). Validity tests can be classified into two main types depending on the methods used to conduct the test: criterion-related validity and judgment validity (Sarmah & Hazarika 2012). Judgment validity includes content validity and face validity (Sarmah & Hazarika 2012). Depending on their objectives, researchers can use various types of validity tests. Content validity is used to evaluate how well the survey covers the study subjects (Sarmah & Hazarika 2012) with professional judges or panels assessing the survey items (Taherdoost 2016) to provide feedback on the relevance and comprehensiveness of the survey items. Content validity and face validity tests are commonly used in studies that use questionnaires due to their relevance and suitability for assessing different aspects of the instrument.

In this study, the content and face validity tests were conducted using the judgment method. Content validity is crucial in a questionnaire as it ensures the instrument accurately represents the measured construct, demonstrating its comprehensiveness and relevance to the research objectives by covering all relevant aspects of the intended construct. In this case, the focus was on evaluating how each question was relevant to its privacy awareness factor and ensuring that all essential aspects needed for assessment were included. An expert statistician from the Ministry of Health in Saudi Arabia, a supervisor from King Abdulaziz University, and a supervisor from the University of Sheffield (who also holds a Master's in Applied Statistics) were chosen to conduct the content validity test. These professionals, with their extensive experience in survey design and development, were instrumental in ensuring the quality and relevance of the questionnaire. The questionnaire was prepared in an Excel spreadsheet and we ensured that the items were clear, concise, and aligned with the evaluated concept. A clear explanation of the purpose of each question was also provided before the questionnaire was sent via email to the experts for evaluation. As a result of the expert feedback, some questions were removed for reasons such as they might be confusing to the participants. For example, questions related to the 'terms of use' were excluded after the discussions because they were not related to the study's main objectives. Other questions were modified to be clearer with many discussions between the researcher and supervisors to review the items, the questions, and the related changes until the final questionnaire was achieved. This process helped ensure the questionnaire items were relevant, comprehensive, and aligned with the intended construct. In contrast, face validity can be assessed by non-experts, mainly the participants, to evaluate some factors such as the readability and clarity of the language and identify any ambiguity (Taherdoost 2016). Face validity is crucial for comprehensible and relevant questionnaire items, ensuring that the questionnaire is user-friendly and enhancing the likelihood of accurate responses from participants. To conduct the face validity test, all survey items were translated into Arabic and then reviewed by

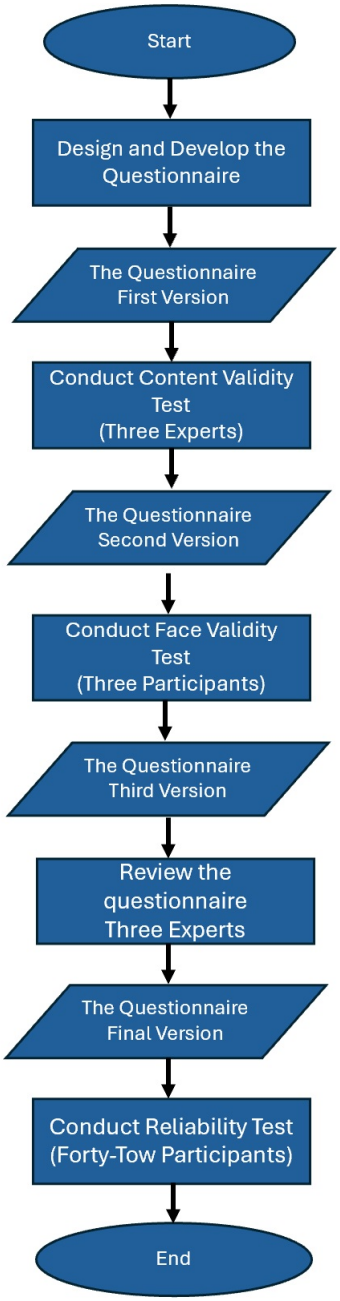

Figure 3.4: *Key Steps of Validity and Reliability Testing of the Questionnaire.*

the experts involved in content validity (the statistician and the supervisor from KAU) before the first version of the questionnaire was developed using Microsoft Forms. Volunteers were recruited to evaluate the questionnaire via WhatsApp with different characteristics and ages: adults (18–35 years), middle-aged adults (36–60 years), and older adults (above 60 years). The volunteers were contacted via their mobile phones and provided with clear instructions explaining the purpose of the survey and their role in evaluating the questionnaire, emphasising that their feedback would help improve the questionnaire's clarity and relevance. The participants had the option to receive the questionnaire via email or WhatsApp with feedback collected received via WhatsApp and phone calls. Then, some parts of the questionnaire were modified accordingly and the participants' opinions and feedback were collected over the phone to clarify any vague questions and ensure that the users understood the questions. Furthermore, spelling errors and ambiguous words were modified. All modifications were made to the survey in Microsoft Forms for the reliability test. The same three experts who conducted content validity reevaluated the questionnaire before proceeding with the reliability test to ensure its quality.

Reliability Test

The reliability test determines the extent to which the survey produces consistent results over time and across different respondents (Heale & Twycross 2015). It ensures that the data collected is consistent and representative of the target population (Heale & Twycross 2015). Cronbach's alpha is the most common measure used to examine internal consistency in surveys (Johanson & Brooks 2010) and is commonly used when testing Likert scale questions. Taber (2018) argued that Cronbach's alpha measures instrument quality when preparing knowledge and understanding examinations for the students. A pilot study to evaluate the instrument's reliability is considered an essential step before conducting the actual experiment. According to Van Teijlingen & Hundley (2001), performing a pilot study may provide an early warning about areas where the research may fail or indicate whether the instruments are unsuitable or very complicated. However, only a few studies in the literature discuss acceptable sample sizes for pilot studies (Johanson & Brooks 2010). Johanson & Brooks (2010) suggested that 30 participants would be appropriate when conducting a pilot study. Moreover, it has been suggested that 10% of the target number of participants is sufficient for the pilot study. The questionnaire was reviewed to ensure that the new version developed in Microsoft Forms incorporated all the modifications and then ethical approval was sought from both the University of Sheffield and the Ministry of Health in the Kingdom of Saudi Arabia. The reliability test was then conducted by participants recruited via messages sent to people in the contact list, WhatsApp groups, and e-mail lists. Everyone who received the message was asked to resend it to all their contacts and e-mails. This message included the survey's title, a brief explanation of the survey's purpose, a short description of the survey and the information confidentiality measures, a link to the survey (Microsoft forms), and the contact information of the main researcher. The survey was closed after 42 participants filled out the questionnaire, which was the appropriate number for conducting the reliability test. The pilot study started on 21 October 2021 and lasted for a month. Of the total participants, 54.8% were females and 45.2% were males aged 18 to 72 years. Most participants (83.3%) were from Jeddah, possibly due to the study location's accessibility. Regarding their educational background, 92.9% of participants held a bachelor's degree or higher (e.g., a Master's or PhD), while 7% had a high school diploma or equivalent. However, the primary purpose of the pilot study was to assess the questionnaire's reliability rather than draw conclusions based on the results. First, the questionnaire data was downloaded in an Excel sheet and then prepared for reliability analysis by properly coding, cleaning, and organising it for statistical analysis. For the data analysis, each choice in the multiple-choice questions was converted into a separate variable with two values, 0 representing not selected and 1 indicating selected, thus, the number of items considered to be on a two-point scale increased. The conditional questions that were not displayed to all participants and the

open-ended questions were excluded from the reliability test. Then, the data was imported into IBM SPSS (v.28) to perform the tests. Cronbach's alpha was used to test each type of question independently and was 0.867 for the five-scale items, 0.648 for the three-scale items and 0.820 for the two-scale items. The acceptable range for the Cronbach's alpha reliability test is above 0.70 (Taber 2018). However, some studies found a value of 0.60 and above to be acceptable for an exploratory or pilot study (Straub et al. 2004). Thus, the questionnaire was considered reliable and had reasonable internal consistency.

3.4.4 Sampling Method and Data Collection

The target population was adults (18 years old or older) who live in Saudi Arabia and use the "Sehhaty" application. According to the reports of the General Authority for Statistics, the population of Saudi Arabia in 2021 (mid-year) was 34.1 million[4]. There were approximately 24 million adults over the age of 18 and all people in Saudi Arabia were required to register on "Sehhaty" because of the COVID-19 pandemic. Thus, based on the formula for calculating sample size with a confidence level of 95% and a margin of error of 5%, this study required 385 participants (Taherdoost 2017). Snowball sampling is a technique in which additional participants are recruited by the initial participants chosen through probability or non-probability methods (Acharya et al. 2013). Snowball sampling was used in this study to recruit users of the "Sehhaty" application via WhatsApp and email. They were asked to forward the service to other "Sehhaty" users and so on. However, snowball sampling is a non-probability sampling technique which may cause selection bias (Alvi 2016).

The online survey was conducted to collect the data from December 2021 to February 2022. The online questionnaire was developed using Microsoft Forms, a user-friendly online survey tool and the survey link was sent to the participants via channels such as WhatsApp and e-mail. The target population was any user over 18 years of age living in Saudi Arabia who used "Sehhaty". The "Sehhaty" application was chosen for this investigation because it is a unified platform provided by the Ministry of Health in Saudi Arabia that allows users to access their health information and medical e-services, offering a variety of services, such as vital sign updates and medication tracking. Also, following the COVID-19 crisis, most people in Saudi Arabia have used this application regularly. The total number of respondents was 418, of which, 28 did not complete the survey, so the final number of participants was 390, of which, 152 were male and 238 were female.

3.5 Study 2 (The Experiment): An Empirical Investigation of Informed Consent for IoMT Services

This study investigated the proposed features for obtaining informed consent in IoMT systems, exploring how users with different privacy awareness provide informed consent and decisions regarding their data when using IoMT systems. Thus, a mixed methods experimental design emphasising the quantitative approach combined with a qualitative approach was chosen according to the second study's aims. First, informed by the literature review that has been conducted in Sections 2.11 and 2.12, the most important factors that need to be addressed in the IoMT consent mechanism were determined. Then, a prototype was developed, followed by a mixed methods experimental approach (qualitative and quantitative). A secondary qualitative method was embedded within the larger design (Creswell & Clark 2017) to collect qualitative before, during, or after the quantitative experiment (Creswell & Clark 2017). Thus, the experiment was followed by a short semi-structured interview to provide more comprehensive answers to the research questions RQ2 and RQ3, and sub-question SQ1 (see Section 1.5).

[4]https://www.stats.gov.sa/sites/default/files/POP%20SEM2021E.pdf

3.5.1 The Experiment Design

A within-subject experiment design with two conditions was adopted to investigate the effect of the enhanced consent mechanisms design on users' informedness and their actual decisions when their sensitive data is collected, used, and shared in IoMT systems. Participants performed specific tasks using consent 'A' (the control design) and then consent 'B' (the experimental design with the enhanced features). Many studies that are concerned with studying users' behaviour have used within-subject designs (Barkley & Lepp 2021, Knutzen et al. 2021), also known as a repeated measures design, comparing variables for the same participants but under different conditions (Budiu 2023). Each participant in a within-subject study experiences multiple conditions (Charness et al. 2012, Budiu 2023) and observing changes in participant behaviour as experimental settings change allows for the generation of causal estimates (Charness et al. 2012). The within-subjects design was chosen in this study for many reasons. First, it requires fewer participants than the between-subjects design (Budiu 2023). Second, it is less affected by the individual differences that exist in the between-subjects experiments, and it is statistically robust (Charness et al. 2012). Thus, two consent mechanisms were developed to conduct the within-subject experiment. The first design, 'A', which represents features of most applications used, was used as a baseline condition in the experiment (control condition) to record the participants' responses in specific situations before any intervention. The second design, 'B', was used as the intervention condition (the experimental condition) and contained the features for the enhanced design of the consent mechanism in IoMT systems, as outlined in Section 2.12. Table 3.2 illustrates the features and how they will be represented. For example, in design 'B' (experimental condition), a link to personal data protection regulations was placed on the home screen with the privacy policy texts divided into eight small sections. The first four sections, namely data collection and use, data access, perceived benefits and potential risks, and the withdrawal procedure were customised according to the service or request the participants were dealing with. The remaining four sections, including data disclosure, external links, data protection, and data storage and processing, remained the same across all services and requests. Moreover, in design 'B', opening all eight sections in the first task was mandatory, while in subsequent tasks, only the first four mandatory sections, which varied according to the service or request, needed to be opened. However, it is important to acknowledge that within-subject experimental designs have been criticised for the learning effects that they generate. To mitigate these effects, a counterbalance strategy was used (MacKenzie 2012) whereby the participants were divided into two groups: the first group started with the first condition 'A' and then the second condition 'B', while the second group started with 'B' and then 'A'. Moreover, to reduce the impact of the other factors and noise, the applications designed and developed for both conditions, 'A' and 'B', were identical in terms of all of the other characteristics (except the features), such as text, screen flows, buttons, colours, and font types.

Table 3.2: *Within-subjects experiment conditions: 'A' the control condition, and 'B' the experimental condition*

The Feature	**The way it is represented in condition 'A', the control design**	**The way it is represented condition 'B', the experiment design**
1- Privacy regulations.	Nothing about personal data regulations or regulations updates.	Links to personal data regulations.
2-Privacy policy text.	Presented by long text on one page.	Divided into smaller parts.
3-Access to privacy policy.	Optional access, links to the privacy policy in regular places (login page, main menu, footer of pages).	Force to access the privacy policy when interacting with each request.
4- Perceived benefits processes on data.	Not explained in the privacy policy.	Explained in a separate section.
5- Potential risks of processes on data.	Not explained in the privacy policy.	Explained in a separate section.
6- Withdrawal procedures.	Mentioned in the privacy policies, most of the time, without explaining the procedures.	Explained, with a clarification of the required steps.
7- Use of icons.	Text is the main component with some icons sometimes.	Use of icons to illustrate sections and ideas beside text.
8- Use of videos.	No videos.	Use of videos to explain some points such as service or request information.
9- Privacy and security measures.	Mentioned in general.	Explicitly identifying the privacy and security measures that are used to protect the data.
10-User understanding assessment.	Use of general sentences with which the user can agree or disagree, such as "By clicking register or login, you are agreeing to ..etc.".	Use of specific questions to assess user understanding.

Experiment hypothetical Scenario

For the purpose of this study, a hypothetical IoMT service scenario was designed comprising tasks that users may face in real life to conduct the within-subjects experiment. The scenario depends on two facts: first, wearable medical devices have received greater attention than other medical devices (Sun et al. 2019, Durán-Vega et al. 2019) and second, obesity, diabetes, and high blood pressure (hypertension) are common chronic diseases in Saudi Arabia, posing significant health risks to the Saudi population [5]. Therefore, it was assumed that participants wanted to subscribe to a service that focused on monitoring their vital signs. Vital signs, such as blood pressure and heart rate, were collected using a wristband equipped with IoT sensors. The entities involved in the proposed scenario are as follows:

- The user or the patient: The individual who subscribes to the healthcare service and owns the data generated by the monitoring of their vital signs.
- The healthcare institute or hospital (service provider): They use the data for main purposes, such as providing a service, and secondary purposes, such as research or enhancing service quality.
- The Ministry of Health (MOH): The MOH supervises proceedings to ensure regulatory and legal compliance. It also possesses the authority to use data in high-level emergency cases without user consent.
- Third parties: These entities request data for secondary purposes, such as academic research, education, and commercial use.
- IT and IoT service provider (third-party): In this scenario, it was assumed that one service provider provides the IT and IoT services under the supervision of the MOH. This service provider is responsible for the ecosystem, network, infrastructure, and communication required for healthcare services and for developing IoT applications and portals. It also provides IoT hardware, including sensors (wearables).

The scenario was as follows:

1. The hospital (service provider) provides the patient with a wearable device in the form of a wristband equipped with sensors to enable the patient to collect their data and thereby monitor their health.
2. The development and operation of this wearable device, encompassing both the hardware and its accompanying application and system (software), has been entrusted to an IT development company (third-party) working under the supervision of the MOH.
3. The patient or user (participant) manages the devices and data, and consents to the research via their mobile phone using a consent management system.
4. The patient's or user's (participant's) mobile phone functions as a gateway that connects IoT sensors to the internet.
5. In addition to the data collected via the sensors, each user has a Unified Health File (UHF), as per the directive of the Saudi MOH [6], which contains personal and medical information in storage units under the control and management of the MOH.

[5] https://www.healthdata.org/sites/default/files/files/Projects/KSA/Saudi-Health-Interview-Survey-Results.pdf

[6] https://www.moh.gov.sa/en/Ministry/Unified-Health-File/Pages/default.aspx

The data involved in this scenario can be categorised into three types: personal data, medical data and information, and data collected via the sensors. The UHF consists of two types: personal data and medical data. Personal data includes ID, full name, addresses (home and work), and contact information (mobile number, phone, email), while medical data and information include allergy, blood type, chronic diseases, height, weight, body mass, patient appointment, lab tests, radiology tests, prescriptions, sick leaves, medical reports, vaccinations, medical referrals, user's previous visits, and other medical information via the 'Sehhaty' application. The data collected by the sensors are heart rate (HR), body temperature, arterial oxygen saturation (SpO2), blood pressure (BP), location, and motion activities. The sensors must collect the minimum amount of data needed according to the required services to comply with regulations. The data in the UHF and the data collected by the sensors are linked to the patient ID. Personally identifiable information (PII) can be highly sensitive, depending on the context in which it is used (Stallings 2019). Moreover, disclosing such data can cause harm, even if it is not categorised as sensitive information. Thus, in this scenario, all data involved in the experimental scenario is considered sensitive taking into account the possibility of linking it to the health condition and location of the person and deducing more accurate information. Moreover, in this scenario, the focus is only on the medical data collected via IoT sensors and personal data and health data in the UHF which is related to the research aim. All other collected data is excluded, such as the device information, because such data lies outside this study's scope.

The Cases and Tasks

The experiment comprised five distinct cases and corresponding tasks, all designed to align with the scenario outlined in the previous section (Section 3.5.1). Each participant was required to complete these tasks under two conditions: the control condition 'A' and the intervention condition 'B', as per the experimental design discussed in Section 3.5.1. In order to design the experiment cases and tasks, the principles and guidelines discussed in Section 2.7 (Primary Sources of Privacy Requirements) have been taken into consideration. In addition, the following references were reviewed to verify the data and details required for the cases identified in the following research: 'GDPR consent'[7], 'National Data Governance Interim Regulations'[8], and 'What information must be given to individuals whose data is collected?'[9].

For example, as GDPR (General Data Protection Regulation in Europe) and PDPL (Personal Data Protection Law in Saudi Arabia) state, individuals have 'the right to be informed about the legal basis and the purpose of the Collection of their Personal Data'. Fair Information Practice Principles (FIPPs) further underscore this point through principles such as 'Purpose Specification and Use Limitation'. Moreover, the 'National Data Governance Interim Regulations' define many principles of using personal data, such as 'Principle 4: Limiting Data Collection' and 'Principle 5: Use, Retention, and Destruction'. Thus, users must be informed about why their data is collected. Also, the 'GDPR consent' article mentions that 'the data subject must at least be notified about the controller's identity, what kind of data will be processed, how it will be used and the purpose of the processing operations'. Hence, users must be informed about who is requesting to collect and use their data. Moreover, the 'National Data Governance Interim Regulations' define many principles of using personal data, such as 'Principle 5: Use, Retention and Destruction'; thus, users need to know for how long their data will be kept. Furthermore, the article 'What information must be given to individuals whose data is collected?', which depends on GDPR, clarifies the information that users must be made aware of when their data is collected, such as what sort of process will be performed on the data.

[7]https://gdpr-info.eu/issues/consent/

[8]https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf

[9]https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected

Hence, in line with these regulations and guidelines, it is imperative that users are informed about the following:

- Who is requesting the data?
- What type of data needs to be used?
- What are the processes involved?
- Where will the data be stored?
- Why will the data be used?
- For how long will the data be retained?

Tasks 1 and 2 revolve around the services provided by the service provider but they differ in terms of the type of service, process, and data used. Task 1 focuses on collecting medical data to provide the main service to the participant, whereas Task 2 focuses on obtaining participants' consent to use the collected data for other purposes (another service). Next, Task 3 focuses on a request from the service provider to use participants' data for secondary purposes (educational). Tasks 4 and 5 are scenarios where medical and personal data are required for research by two different third parties, one of which offers public benefits (non-commercial purpose), while the other offers personal benefits (commercial purpose). Table 3.3 provides an overview of each case, its related tasks, and the information provided to obtain participants' informed decisions. The tasks are designed to have varying purposes for collecting and utilising participant data and other details.

The primary focus is on cases that the user may encounter when using IoMT systems. Also, it should be acknowledged that there may be other sub-cases that were not covered in this experiment because of the need to manage participants' time effectively and the requirement for more extensive investigations into these cases. However, these aspects will be taken into consideration in future studies.

In a study conducted by Duckert & Barkhuus (2022), participants were anxious about the lack of transparency regarding the healthcare personnel that had access to their health information and the sorts of health data they could access. As a result, these participants voiced their concerns about their consent provisions. Therefore, written informed consent documents for research studies should include information about the research purpose and the expected duration of participation, and should also describe the procedures involved including any experimental procedures (Nijhawan et al. 2013). Any risks posed to the subjects or any discomfort they may experience should be described, along with the steps taken to prevent or minimise them. Plus, any potential benefits should also be mentioned, excluding monetary compensation. Lastly, any document should provide information on the confidentiality of records, compensation and medical treatments available in case of injury, remuneration for subjects, contact information for questions, and a statement emphasising voluntary participation.

Table 3.3: *Experiment cases and the related tasks to be performed by the participants*

The Case	The Information Provided	The Required Task
Case1 Purposes: Main. Processes: Collect, transfer, analyse and use. Type of data: Data collected by the sensors and personal data in the UHF.	• Who: Service provider. • What is the required process: requests to start collection (via sensors), transfer (via mobile phone (gateway)) and analysis. • What type of data are involved: data collected by the sensors (BP), location, motion activities) and personal data in the application: ID, full name, addresses (home and work), and contact information (mobile number, phone, email). • Where: storage units that are managed and supervised by the Ministry of Health inside Saudi Arabia. • Why (purpose): to start to provide the user with the main service. • For how long: until he/she withdraws from the service.	Subscribe to the Basic Vital Signs Monitoring service provided by the Remote Patient Services department in the hospital from which you received the wristband. After subscription, the service will start by transferring the data collected by sensors via your mobile phone to the storage units and use a real-time system to monitor and analyse your general health status and check symptoms to detect some of the early diseases, such as heart attacks, before they occur. If the system detects any health problems or indicates that you may have a specific disease, our team will contact you to set a date for you to visit the clinic or to come to your location to perform necessary tests and examinations.
Case2 Purposes: Another main purpose. Processes: Integrate, analyse and use. Type of data: Data collected via the sensors, personal data and medical information.	• Who: Service provider. • What is the required process: requests to integrate and analyse. • What type of data is involved: the data is collected data via sensors (which are in the storage units) with UHF (which is in the storage units). • Where: storage units that are managed and supervised by the Ministry of Health inside Saudi Arabia. • Why (purpose): to provide the user with a new main service. • For how long: until he/she withdraws from the service	Assume that you have to subscribe in Task 1. Now, you are required to decide on an offer from the Remote Patient Services department in the hospital, which already provides you with the main service. This offer is to use and integrate your collected data with medical information in the Unified Health File (collected data + personal data+ medical data) to provide you with an Advanced Early Disease Detection Service which can predict many types of diseases. If the system detects any health problems, our team will contact you to set a date for you to visit the clinic and perform other necessary examinations. Your unified health file (UHF) contains your medical information, such as lab tests, radiology tests, prescriptions and others.

Case3 Purposes: Secondary purposes (educational, social). Processes: access, analyse and use. Type of data: Data collected by the sensors and personal data.	• Who: Service provider. • What is the required process: requests to access, use and analyse. • What type of data are involved: the data collected via sensors and personal data. • Where: storage units that are managed and supervised by the Ministry of Health inside Saudi Arabia. • Why (purpose): to use the data for secondary purposes (educational, social). • For how long: for a specific period.	Decide on a request from the team in the Remote Patient Services department, which already provides you with Basic Vital Signs Monitoring (case1), to use your collected and personal data that is stored for educational and training purposes concerned with training new employees on how to deal with specific situations and the procedure of contacting the patients for two months. This training will include how to help patients to properly use these devices. The patients might be contacted by the employees to arrange a visit or to assist the patients with using the medical devices.
Case4 Purposes: Secondary purposes (research, Public health). Requester: Third-party. Processes: access, analyse and use. Type of data: Data collected by the sensors, personal data and medical information.	• Who: Third-party. • What is the required process: requests to access, use and analyse. • Copying data is not allowed. • What type of data are involved: the data collected via sensors, medical information and personal data. • Where: storage units that are managed and supervised by the Ministry of Health inside Saudi Arabia. • Why (purpose): to use the data and results for secondary purposes (research, social). The results of the research will be published without any identifiable data • For how long: for a specific period.	Decide on a request from the Research Centre at King Abdulaziz University (KAU) to access and use your collected vital signs, personal information in UHF, and results of the Basic Vital Signs Monitoring service to be used in research. This research concerns the effect of dietary habits on the results of monitoring vital signs. The research team will contact you to ask questions about your dietary habits. All personal and identifiable data will be removed when the search results are published.

Case5 Purposes: Secondary purposes (commercial). Requester: Third-party. Processes: access, analyse and use . Type of data: Data collected by the sensors and medical information.	• Who: Third-party. • What is the required process: requests to access, use and analyse. • What type of data are involved: the data that collected via sensors, medical information and personal data. • Where: storage units that are managed and supervised by the Ministry of Health inside Saudi Arabia. • Why (purpose): to use the data and results for secondary purposes (commercial). • For how long: for a specific period.	Decide on a request from the Research Centre in Alpha Pharmaceutical company to access and use the collected data, personal information, and results used in the Basic Vital Signs Monitoring service to be used in research. This research concerns the relationship between the changes in vital sign readings and specific types of medicines. The research team will contact you to ask some questions related to the research. All of the personal and identifiable data will be removed once the search results are obtained.

Experimental Framework Design and Development

An experimental framework was constructed in order to evaluate the enhanced design of the consent mechanism. The framework contained two mobile applications representing conditions 'A' and 'B'. First, **Adobe XD** was used to design the prototypes for its components and features, enabling the creation of high-quality user interfaces. Adobe XD also allowed to illustrate the screen flow efficiently, aiding discussions with supervisors during meetings. Initially, four mobile application prototypes to represent the experiment conditions 'A' and 'B' in English and Arabic languages were designed (condition A-English, condition A-Arabic, condition B-English, condition B-Arabic). After the basic design was determined, we focused only on the versions in Arabic because Arabic was the primary language of the target sample. Figure 3.5 illustrates the use of Adobe XD to design the condition A-English prototype. The colours of the applications designed for the experiment were carefully chosen based on a comparative analysis of official Saudi Arabian applications and the 'Sehhaty' application. The aim was to use colours that participants widely recognised, thereby enhancing the application's credibility and reliability. Given that the experiment's primary focus was on obtaining consent for using medical and personal data in different situations, the design of the buttons was crucial, as they are used by the participants to make choices, such as accepting or rejecting a request. Therefore, the design button guidelines were reviewed, namely the Apple Developer[10] and UX plant[11,12] websites. According to these guidelines, the buttons' position in the two applications aligned with user expectations and the screen layout in an accessible location. All buttons were clearly labelled to communicate their purpose and make them easily recognisable. A consistent button design and placement were maintained across the applications to create a friendly user interface. Also, positive buttons were placed on the right after completion and negative buttons on the left for left-to-right languages, while this arrangement was reversed for right-to-left languages like Arabic. One of the buttons' design principles is visual weight, which involves creating a clear distinction between two buttons with different options, such as using different colours (usually green and red) for 'accept' and 'reject' buttons. However, this principle was not followed to rule out any external influence on the user in making the decision which may have affected the results. Thus, a black and white colour scheme was used for all buttons (black for the background and white for the font) to prevent user selection bias and achieve a clean and simple look.

[10]https://developer.apple.com/design/human-interface-guidelines/buttons
[11]https://uxplanet.org/primary-secondary-action-buttons-c16df9b36150
[12]https://uxplanet.org/7-basic-rules-for-button-design-63dcdf5676b4

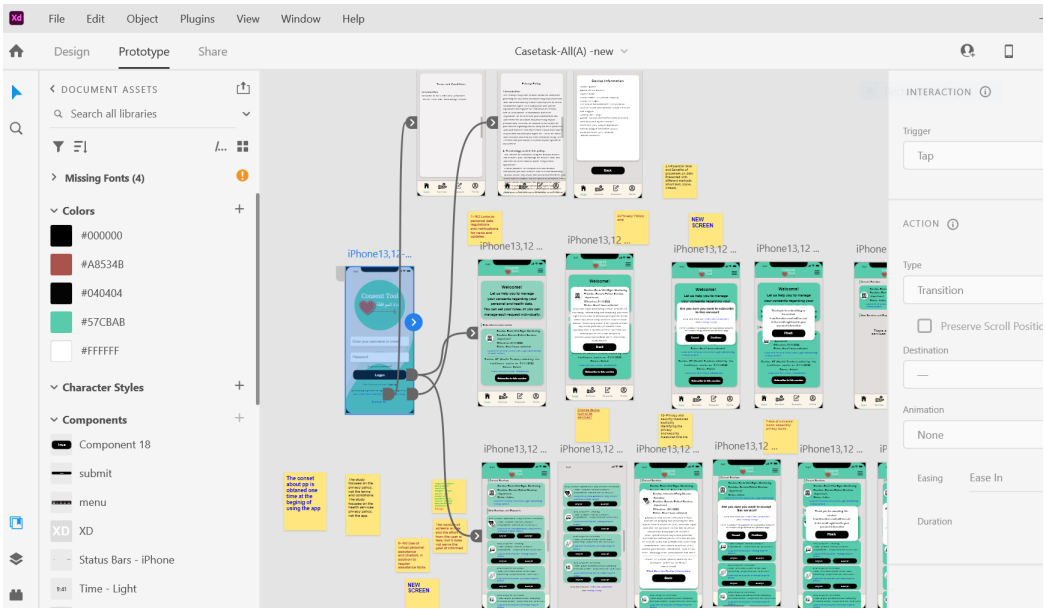

Figure 3.5: *Example of the use of Adobe XD (Condition A-English).*

In reference to the icons used in the designs, we sourced icons from plugins in Adobe XD and the iconfinder[13] website, carefully selecting freely available icons without any cost or licensing restrictions. Some of these free icons were combined to create new ones that conveyed the intended meaning effectively. In addition, for the application representing condition 'B', we designed five videos (one for each task). To do this, we created animated presentations using Powtoon[14], a web-based animation application that offers premade pictures, music, objects, and voice-overs (see Figure 3.6).

Regarding the content of the applications, texts created during the development of the tasks were used to provide information about each service and request (see Table 3.3). In addition, we relied on the 'Sehhaty' application's privacy policy [15] as a reference to develop the privacy policies for applications 'A' and 'B'. Initially, the privacy policy for applications 'A' and 'B' was written in English, then translated into Arabic after review with the supervisors. However, in application 'A', the privacy policy was one piece of text, while in application 'B', the privacy policies were divided into sections, as mentioned earlier on page 64. In application 'B', the section on perceived benefits and potential risks describes different benefits that participants can gain from accepting a service or request and the consequences that participants may face. The withdrawal procedure section explains, step by step, how to withdraw from each request and service. Each task featured a video explaining the request, available within the service or request information. Moreover, the privacy and security measures section outlines the measures that are used to protect users' data, thereby making them feel comfortable and secure. Specific software details were not disclosed to avoid providing information to potential attackers. Before accepting any service or request, a question in the form of true or false was presented to the participants in order to assess their understanding. If the participant answered the question incorrectly, the system would provide the correct answer and an explanation of it.

[13] https://www.iconfinder.com/
[14] https://www.powtoon.com
[15] https://api.sehhaty.sa/services/individuals/privacy-policy/?lang=en

Figure 3.6: *Example of the designing video using Powtoon (Condition B).*

After that, **Flutter** (an open-source SDK that helps build native mobile applications for iOS and Android, provided by Google) was used to build and develop mobile application prototypes for the 'A' and 'B' conditions. Both **Visual Studio Code** and **Android Studio**, which are Integrated Development Environments (IDEs), were used to build Flutter projects and to write and edit the codes. Both code editors were used interchangeably to develop our Flutter application based on our requirements. Visual Studio Code served as our primary code editor for writing Flutter code, while Android Studio was used for its specific features and specialised interface for managing platform-specific code resources and optimising the Flutter application. Figure 3.7 illustrates the use of Android Studio for developing and running condition 'B' in the emulator. Given that all participants' primary language was Arabic and there were time limitations, we focused on developing the applications for conditions 'A' and 'B' in Arabic. Figure 3.8 and 3.9 illustrate examples of the first three screens of applications 'A' and 'B', respectively. For more details about these screens and other screens, see Appendix C.

Moreover, **Firebase** (a Backend-as-a-Service (BaaS) web development platform provided by Google) was integrated into the application development process as it offers a range of cloud-based services and tools that help developers build, deploy, and manage applications more efficiently. These services and tools include a real-time database, authentication analytics tools, and cloud storage. First, the Firebase Authentication SDK feature was utilised that offers methods for creating and managing user authentication in mobile applications to create participant accounts. Firebase Authentication SDK offers many authentication methods, including email, phone number, social media account, and multi-factor authentication. An email address was selected where the username and password of the participant can be created and managed easily in the Firebase console, the Authentication section. For each participant, an account was created by the main researcher for the experiment to log in to the application and collect the interaction data. The username of this account takes the format of Gmail addresses, such as user2@gmail.com and was securely stored in Firebase's user management system. The same account was used in applications 'A' and 'B'. When any participant downloads and installs applications 'A' and 'B' (from the Google Play Store or Apple App Store), the login screen is displayed and the participant is required to enter their account credentials. Firebase's authentication feature handles the user authentication securely, verifying the provided credentials. Once authenticated, the user gains access to the applications and starts performing the tasks required for the experiment.

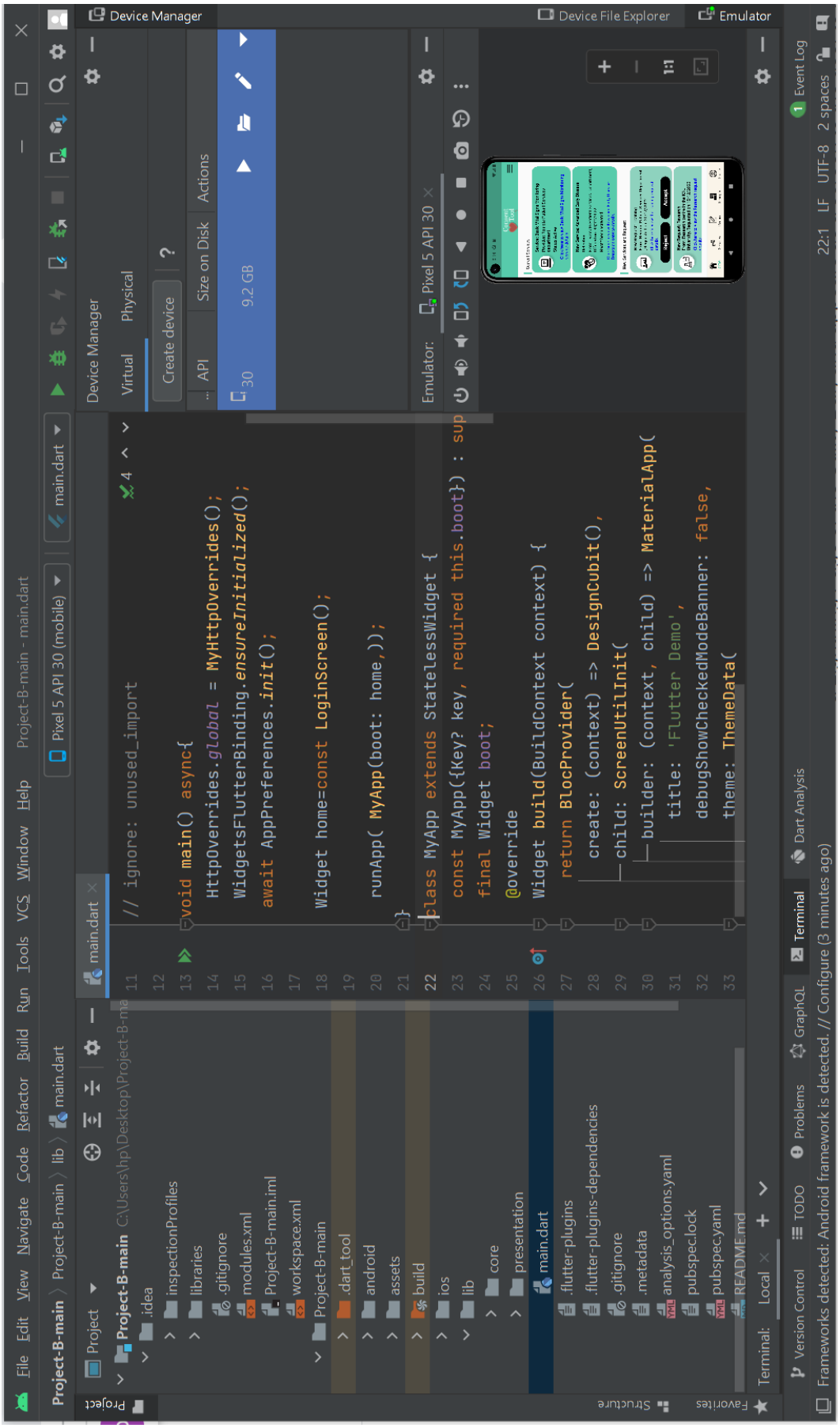

Figure 3.7: *Example of the use of Andriod Studio*

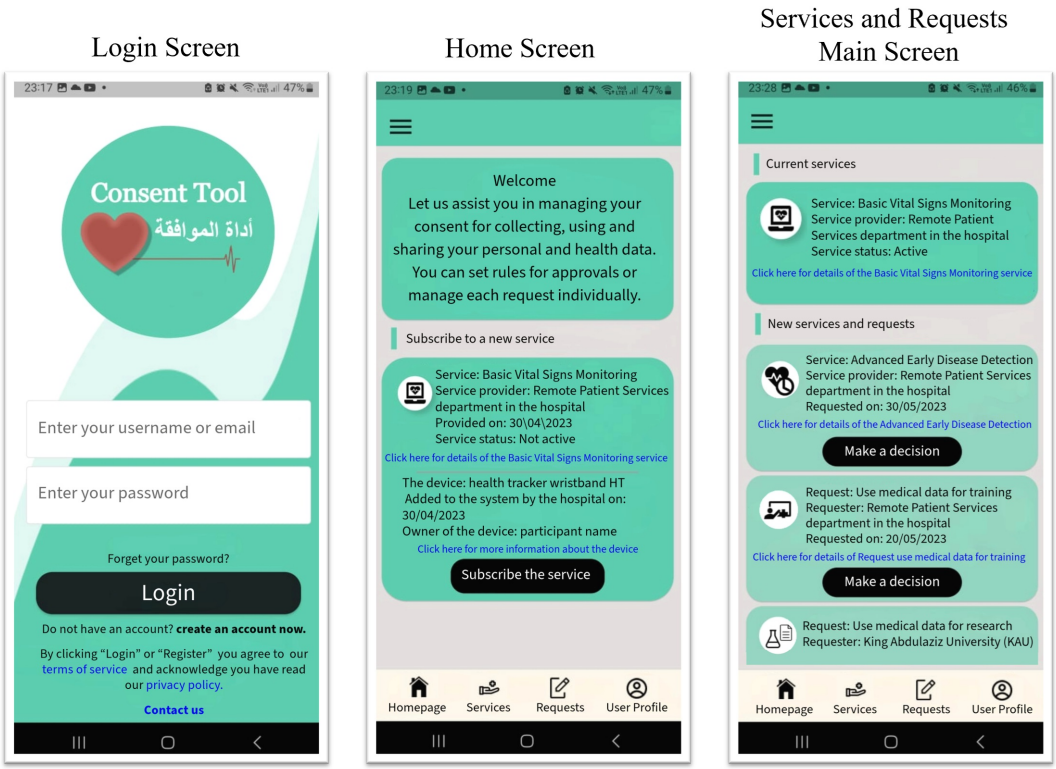

Figure 3.8: *Example of screens from Application 'A' that represent the control condition.*

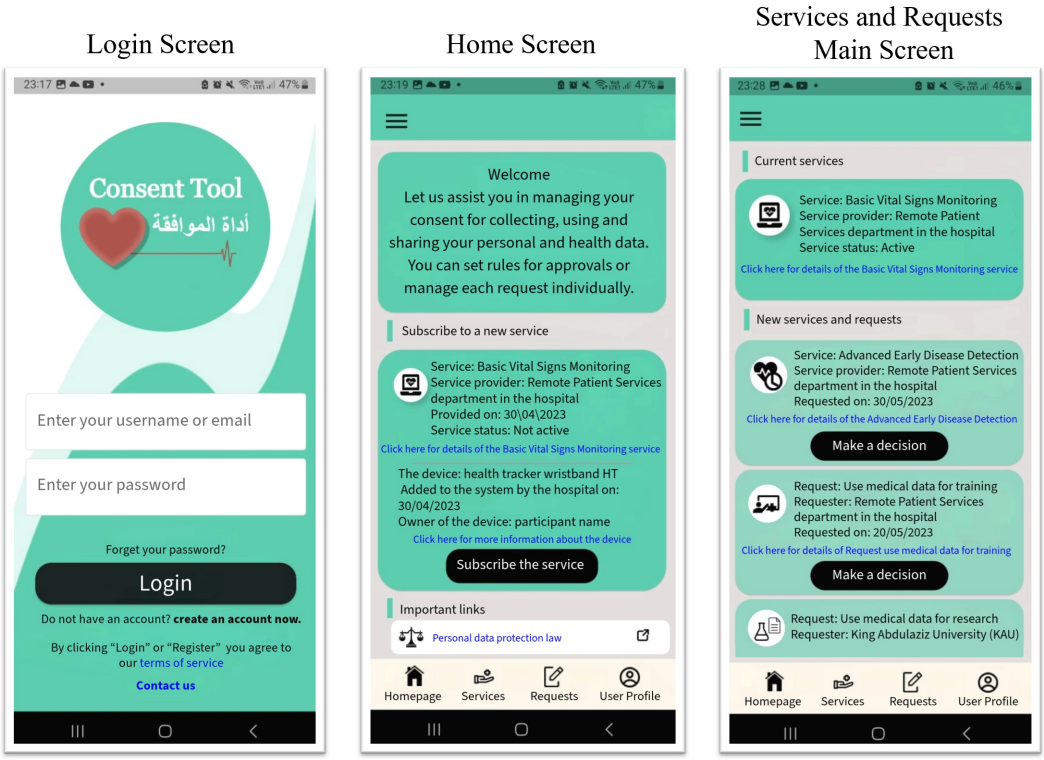

Figure 3.9: *Example of screens from Application 'B' that represent the experiment condition.*

The main method for collecting data is Firebase's client-side SDK, which is integrated into the mobile application. It has event-logging capabilities that automatically record user actions and interactions within the application. When the participants start to perform the experimental tasks in 'A' or 'B', Firebase's client-side SDK captures button clicks, which pages are opened, and the time spent on each page, providing valuable insights into user behaviour and engagement. All of this collected data were transferred in real time to the Firebase database, which acts as a central storage and synchronisation point for the information. The Firebase real-time database (Cloud Storage) is a NoSQL cloud-hosted database that provides real-time synchronisation of data across connected clients. Data is organised in a JSON-like structure, which allows for efficient storage and retrieval. This type of database offers flexibility, scalability, performance, cost-effectiveness, and developer friendliness, making it an ideal choice for mobile applications. Moreover, the real-time database ensures that any changes made to the data are instantly pushed to all connected clients, guaranteeing up-to-date information for all participants. Figure 3.10 illustrates an example of the variables captured when the user (U2) performs tasks in application 'A'.

Many security measures employed in Firebase ensure the security of user data during transmission and storage. Transport Layer Security (TLS) was used to secure data from being intercepted or altered during transmission. It is a cryptographic protocol designed to provide communications security over a computer network to establish a secure connection between the client-side SDK and Firebase backend services. Furthermore, Firebase employs encryption algorithms to encrypt data during storage. This robust encryption ensures that unauthorised individuals cannot access user data. Firebase also offers fine-grained access control mechanisms, empowering developers to specify who can access and modify data within the real-time database, thereby preventing unauthorised access to sensitive user information. The Firebase team emphasises the importance of data privacy and describes all the implemented measures on its website[16]. For example, Firebase adheres to GDPR and CCPA data protection regulations, ensuring that data controllers and processors are responsible for their data. The GDPR and CCPA/CPRA impose obligations on data controllers, processors, businesses, and service providers. Firebase clients act as the "data controller" (GDPR) or "business" (CCPA/CPRA), while Google operates as a "data processor" (GDPR) or "service provider" (CCPA/CPRA). Clients are responsible for fulfilling obligations regarding their end-users data. Also, Firebase is certified under major privacy and security standards, including ISO and SOC compliance. Thus, all measures were taken to protect participants' data privacy. Also, the experiment was based on a hypothetical scenario, so no personal or sensitive data were collected via the developed applications. Firebase's DebugView feature was employed during the development stage to monitor application actions and events, ensuring that the required actions were captured. See Figure 3.11. However, we did not use this feature in the experiment because it could not function after the applications were published in the Apple and Google stores.

[16]https://firebase.google.com/support/privacy

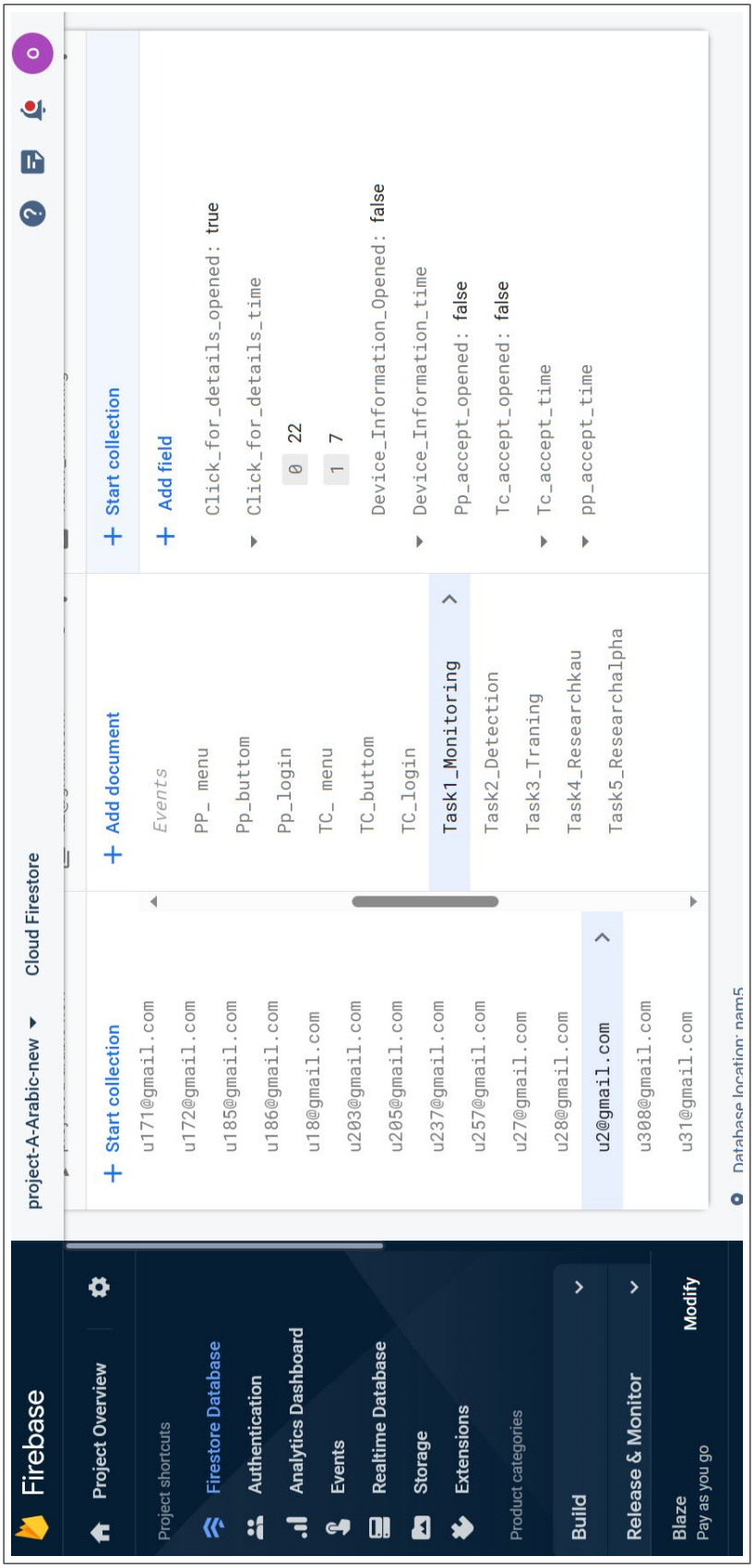

Figure 3.10: *Example of Firebase database*

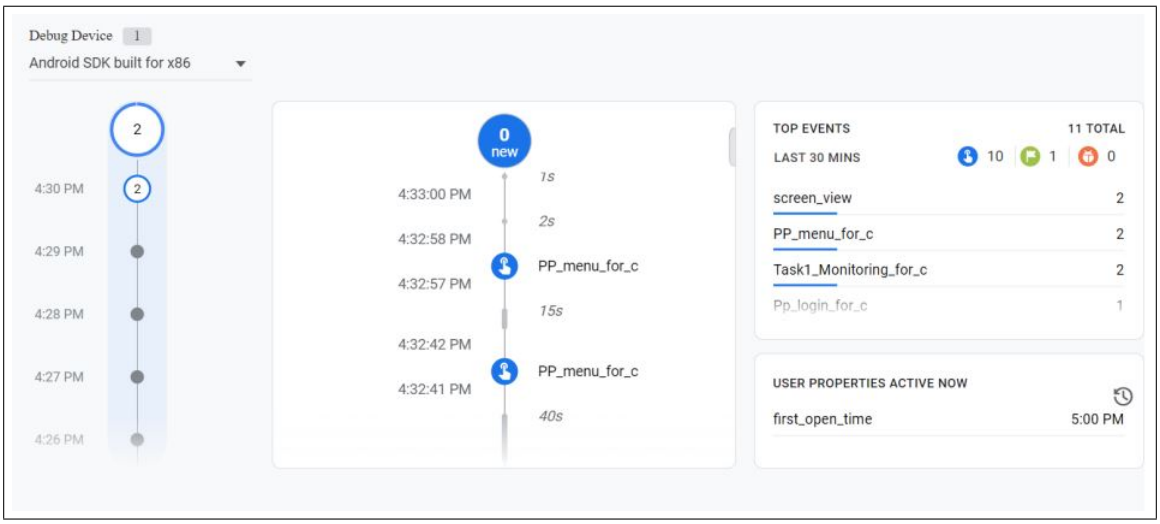

Figure 3.11: *Example of DebugView Screen where a user interact with Condition 'A'*

To prepare the applications for the experiment, developer accounts were created on the Google Play Developer and Apple Developer websites – a process that took several days as our IDs needed to be verified. After that, applications 'A' and 'B' were configured for release using specific settings and options. APK files for A and B applications were generated to be uploaded to the Google Play Store and IPA files for 'A' and 'B' applications to be uploaded to the Apple Store. Then each of them were uploaded to its respective consoles (Google Play Store and Apple Store). For research purposes, applications 'A' and 'B' were developed to perform only five designated tasks (as noted in section 3.5.1) rather than for full functionality, thus the Apple Store and the Google Play Store administrations did not accept our request to publish the applications. However, they did assist us with other testing solutions. The Apple store administration accepted our request to use external testing, which involved generating external links for each application to invite participants (see Figure 3.12 and 3.13) . When the participants clicked on these links, they were directed to the 'Test Flight' application, an official Apple application designed to help participants download and test applications. However, it should be noted that such applications only remained available for up to 90 days. For the Google Play Store, the conditions were less complicated. The 'internal test' method involved adding each participant's email address (the same one they use to log in and download apps from the Google Play Store) to a testing list and then, the participants were sent a link to download the applications directly (see Figure 3.14 and 3.15. There was no expiration date for this type of testing.

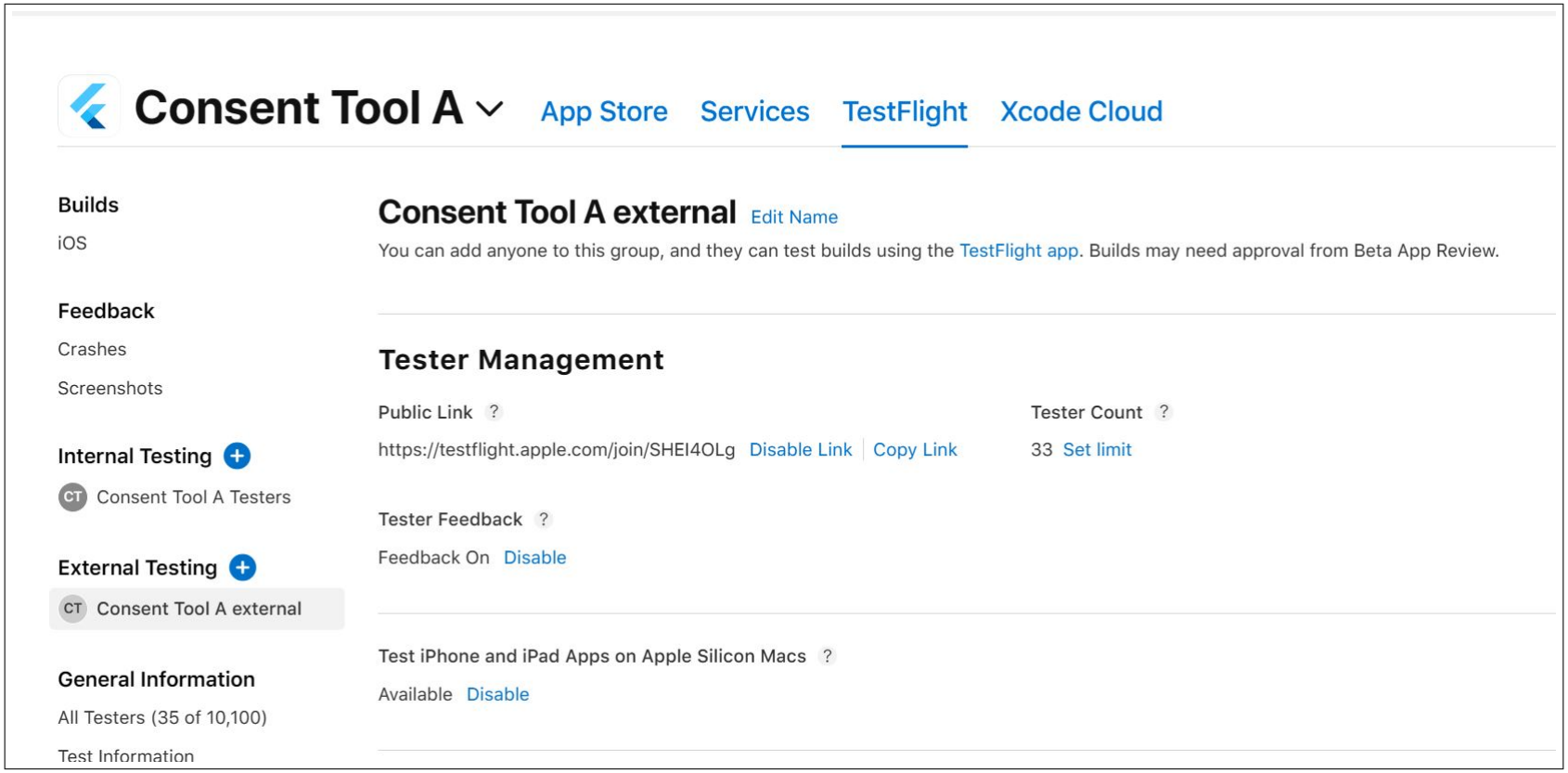

Figure 3.12: *Apple Store external test screen for application 'A'*

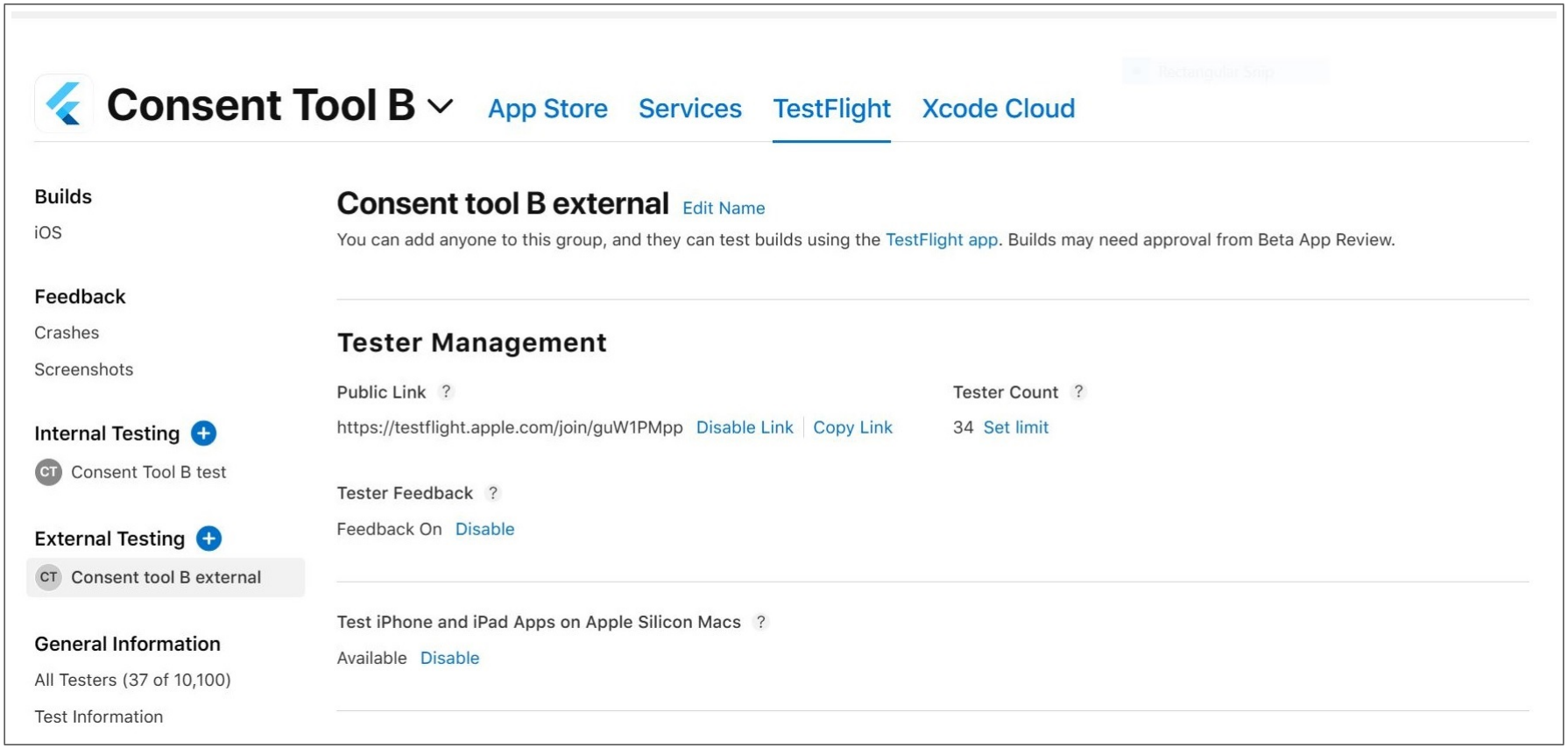

Figure 3.13: *Apple Store external test screen for application 'B'*

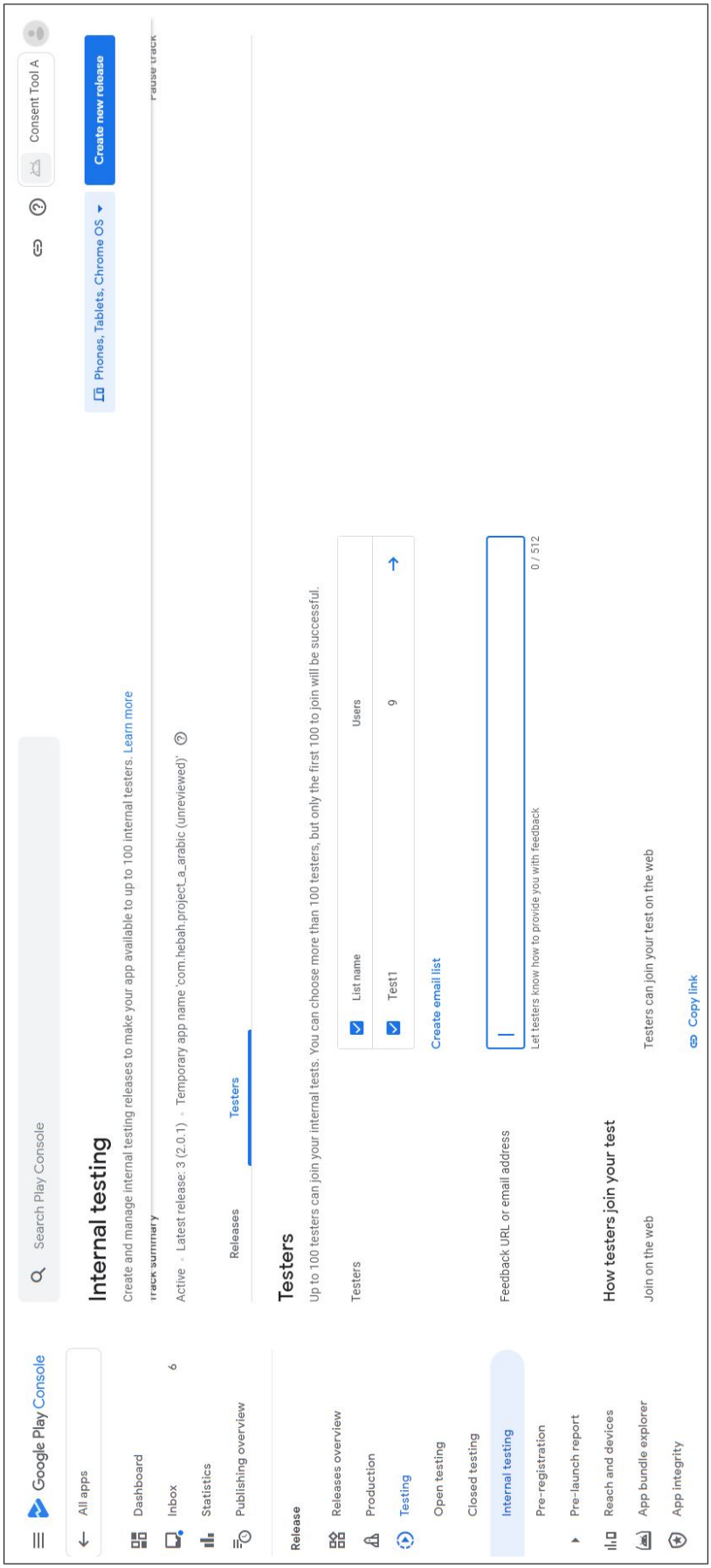

Figure 3.14: *Google Play Store internal test screen for application 'A'*

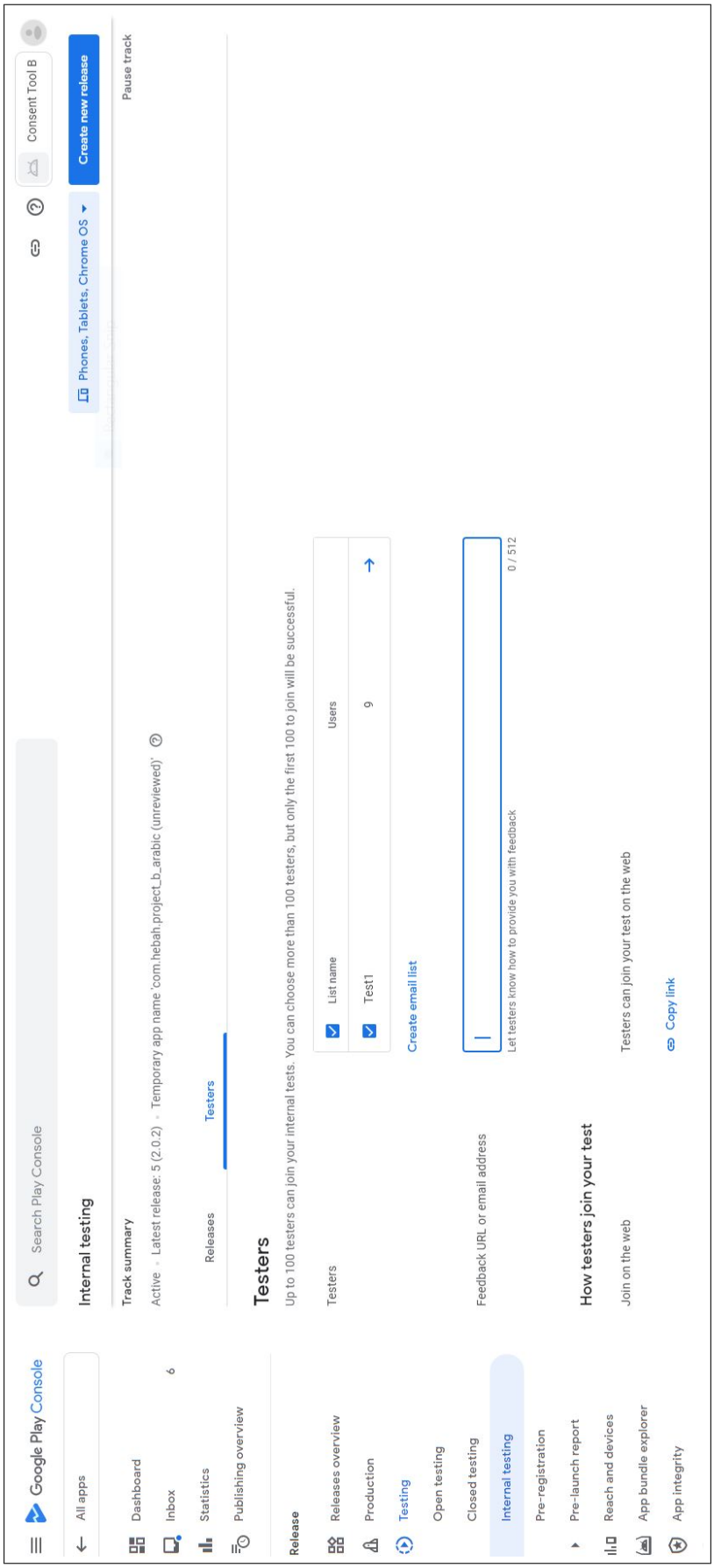

Figure 3.15: *Google Play Store internal test screen for application 'B'*

3.5.2 Hypotheses and Measures

The measures employed in the experiment were crucial for quantifying variables, capturing data, and investigating hypotheses, all of which aided in answering the research questions. In light of this, we have outlined hypotheses and described measures for the second and third research questions (RQ2 and RQ3), as well as a qualitative measure in relation to the sub-question (SQ1).

Within-subjects Experiment

This part of the experiment focused on addressing the second research question (see Section 1.5) with the hypotheses formulated according to the study cases and tasks discussed in Section 3.5.1. The hypotheses were developed to investigate the impact of the enhanced design of the consent mechanism in IoMT on participant decisions by determining whether there was a significant difference in participants' decisions between application 'A' and application 'B'. As previously explained in Section 3.5.1, a within-subject experiment was conducted with the participants performing the required tasks using consent 'A' (the control design) and consent 'B' (the experimental design). During the experiment, each participant's decision was recorded for each task, with an accept value represented by 1 and a rejection value represented by 0. Then, the participant's decisions for each task in conditions 'A' and 'B' were compared. However, it should be noted that based on the scenario and task design, the participants' initial task in both conditions 'A' and 'B' was to subscribe to the IoMT system, thus, there was no specific hypothesis focused on the decision made during Task 1, rather, we assessed their level of informedness when they subscribed.

- **Ha:** There is (Ha0) no difference, (Ha1) a significant difference, in the participants' decision regarding the request in Task 2 between conditions 'A' and 'B'.
- **Hb:** There is (Hb0) no difference, (Hb1) a significant difference, in the participants' decision regarding the request in Task 3 between conditions 'A' and 'B'.
- **Hc:** There is (Hc0) no difference, (Hc1) a significant difference, in the participants' decision regarding the request in Task 4 between conditions 'A' and 'B'.
- **Hd:** There is (Hd0) no difference, (Hd1) a significant difference, in the participants' decision regarding the request in Task 5 between conditions 'A' and 'B'.

Moreover, this part of the experiment also investigated the correlation between participants' objective privacy awareness, which was explored in Study 1 (the survey), and their changing decisions between conditions 'A' and 'B'. Thus, the following hypotheses were developed:

- **He:** There is (He0) no relation, (He1) a significant relation, between objective privacy awareness level and changing participants' decision of the requests between conditions 'A' and 'B'.

Participants' interactions and decisions were captured and stored in predefined variables. Once a participant started using either application 'A' or application 'B', every click on an object (links and buttons) from the homepage screen until the end of the experiment was recorded. Each screen had two values: one for when the user opened it (represented by 1) and one for when the user did not open it (represented by 0). Additionally, the time that each participant spent on each screen was calculated. The time spent on each page in the applications might indicate the participant's effort in reading and understanding the content. For example, spending more time on the page enhances the likelihood that participants have read and understood the content, improving their awareness of privacy issues and leading to more informed decisions. However, individual differences, cognitive abilities, and personal motivations can also influence the time

users spend on each page; however, these factors were beyond the focus of our research. This experiment was designed to determine if there is any relationship between the privacy awareness level, which was discovered in the first study, and the time spent on each page. All user actions were then logged in the Firebase database in real-time and chronological order. The data collected were quantitative with no sensitive or private data collected. All the captured data were saved in the main researcher's KAU account (halbatati@kau.edu.sa) provided by Google. The results of the two conditions, 'A' and 'B', were then compared to evaluate the effect of each user's privacy awareness level on their decision-making and the effectiveness of the features in enhancing the users' informedness. Figure 3.16 illustrates the events captured in Firebase for user 'U2' when interacting with application 'A'.

Post-experiment Questionnaire

Post-experiment questionnaires were used to answer the third research question (see Section 1.5) and to determine whether the enhanced design of the consent mechanisms for IoMT systems assisted users in making informed decisions. First, a specific hypothesis was designed for each feature and integrated into the enhanced consent mechanism design (10 features) to examine the relationship between each feature and users' informed decision-making. Then, a statement that reflects each hypothesis was developed. The responses were scored using a 5-point Likert scale (1=Strongly Disagree to 5=Strongly Agree) to measure the level of perceived informedness. In addition, the statements were reviewed to ensure that they were clear, concise and focused on a single idea. Then, the questions were translated into Arabic. The Arabic version was revised to ensure its clarity and meaning remained unchanged. Finally, an electronic survey was created using Google Forms with clear instructions provided to participants at the beginning of the questionnaire. The participants answered questionnaire questions after finishing the tasks in conditions 'A' and 'B'. Table 3.4 provides an overview of the hypotheses and their related measures.

Semi-structured Interview

A semi-structured interview was conducted to address Sub-Question SQ1 (see Section 1.5). This is a qualitative approach in which certain questions are predetermined while others arise based on the participant's responses. A semi-structured interview approach was selected as the qualitative component of the mixed-method study at the end of the experiment to gain a deeper understanding of the within-subject experiment and post-experiment results. First, we determined the aspects of users' perceptions to support the within-subject experiment and the post-experiment questionnaire results which were the preference, achieving informed consent, privacy awareness enhancement, and general questions. Then, seven fixed questions were developed to cover these aspects. All interviews started with warm-up questions and general questions about the participant's overall experience with the design or their initial impressions such as, "How was your overall experience using the applications?" We asked for clarification when needed and encouraged participants to expand on their thoughts. Table 3.5 illustrates the predefined questions related to the measure.

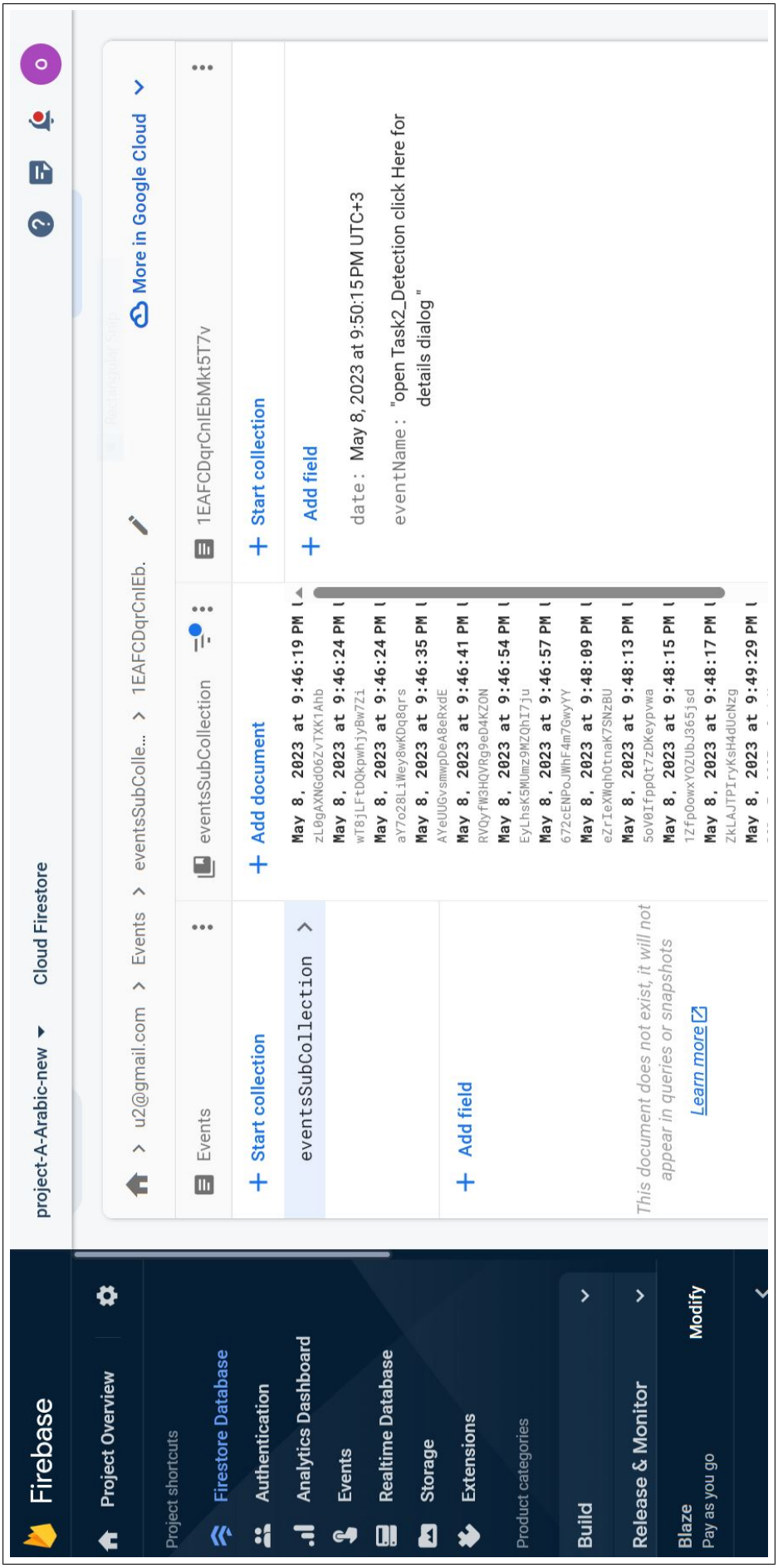

Figure 3.16: *Example of Firebase screen where events captured for user 'U2' when interacting with application 'A'*

Table 3.4: *The features, hypotheses, and the measurement questions*

The Feature	The Measurement Factor	The Hypothesis	Likert Scale Question (1=Strongly Disagree to 5=Strongly Agree)
1- The presence of data protection laws link.	Privacy regulations (display)	**Ha:** link to data protection laws and regulations that govern personal data in Saudi Arabia **(Ha0)** have no role, **(Ha1)** have a role in helping the user to provide his/her informed decision.	The existence of a link to data protection laws and regulations that govern personal data in Saudi Arabia helps me make an informed decision.
2- Mandatory access to privacy policy.	Privacy policy (location and how to access it)	**Hb:** The mandatory access to privacy policy instead of using optional links **Hb0** has no role **Hb1** has a role in helping the user to provide his/her informed decision.	The mandatory display of the privacy policy sections before making any decision makes me read them, which consequently helps me make an informed decision.
3- Dividing privacy policy into small parts which contain only the information related to the specific request or service.	Privacy policy (length)	**Hc:** Dividing the privacy policy into small parts instead of one long text on one page **(Hc0)** has no role **(Hc1)** has a role in helping the user to provide his/her informed decision.	Displaying privacy policy in sections focusing only on the service or request that I deal with instead of one piece of long text makes it easier to read, which consequently helps me make an informed decision.
4- Displaying and clarifying the perceived benefits users will get from accepting the request or service in a separate section.	Benefits (display and clarification or declaration)	**Hd:** displaying and clarifying the benefits that users will gain from accepting a request or service in a separate section **(Hd0)** has no role **(Hd1)** has a role in helping the user provide his/her informed decision.	The explanation of the benefits which I will gain from accepting a service or request helps me make an informed decision.
5-Displaying and clarifying the potential risk that could occur when accepting the request or service in a separate section.	Potential Risk (declaration)	**He:** displaying and clarifying the potential risk that could occur when accepting a request or service in a separate section **(He0)** has no role **(He1)** has a role in helping the user provide his/her informed decision.	Explaining the potential risk that could occur from accepting a service or request helps me make an informed decision.
6- Clarification of the withdrawal procedure in an a separate section.	Withdrawal procedure (Clarification)	**Hf:** Clarification of the withdrawal procedure in an explicit section Hf: Withdrawal procedure clarification **(Hf0)** has no role **(Hf1)** has a role in helping the user to provide his/her informed decision.	Clarifying the withdrawal procedure in an explicit section helps me make an informed decision.
7-Explicit indication of privacy and security measures that are used to protect users' data in a separate section.	Privacy and security measures	**Hg:** Explicit indication of privacy and security measure **(Hg0)** has no role **(Hg1)** has a role in helping the user to provide his/her informed decision	Explicit indication of security and privacy measures that are used to protect my data helps me make an informed decision.
8- Using icons (especially private icons) to illustrate subjects and some points.	Icons (especially private icons)	**Hh:** using icons (especially private icons) to visually represent parts and sections **(Hh0)** has no role **(Hh1)** has a role in helping the user to provide his/her informed decision.	Icons that illustrate titles and sections help me visually understand the general idea, which consequently helps me make an informed decision.
9- Using videos to explain some points such as service or request information.	Videos (Explain and illustrate some points)	**Hi:** using videos to explain some points such as service or request information **(Hi0)** has no role **(Hi1)** has a role in helping the user to provide his/her informed decision.	Videos that explain services and requests help me make an informed decision.
10- Assessing user understanding.	Questions to assess user understanding	**Hj:** Questions to assess user understanding **(Hj0)** has no role **(Hj1)** has a role in helping the user to provide his/her informed decision.	Questions that assess my understanding before accepting a service or request help me make an informed decision

Table 3.5: *Semi-structured interview questions and the specific aspects that they emphasise*

Aspects	**The Questions**
Preference	Which consent mechanism do you prefer 'A' or 'B' ? and why?
Achieving informed decisions	• In your opinion, what are the three most important factors that helped you make an informed decision? why? • Are there any factors that did not help you make the decision? why?
Privacy awareness enhancement (consent B)	• In your opinion, do the consent mechanism features help to increase privacy awareness? • If yes, name the top three and how? • Are there any other factors you believe, from your point of view, that help increase privacy awareness.
General	Would you like to add anything else?

3.5.3 The Experiment

The initial plan was to conduct the within-subject experiment in the KAU (King Abdulaziz University) computer labs. However, the Covid-19 pandemic caused difficulties working directly with end-users due to lockdown restrictions. Instead, we had to design a within-subject experiment that could be conducted remotely. This actually offers many advantages. For instance, Urbano et al. (2017) clarified that the remote experiments are flexible and allow participants to access the experiment tool from anywhere at a convenient time, which reduces the consumption of time and resources. Furthermore, Urbano et al. (2017) argues that remote experiments minimise potential risks that affect the participants. For example, participants' stress associated with conducting the experiments in a lab can be reduced when the experiment is conducted remotely. Additionally, conducting the experiment in the participant's preferred environment instead of controlled laboratory settings enabled us to obtain more accurate results regarding their behaviours and interactions. This section describes the procedure followed to experiment remotely and the specific instructions given to the participants.

The Experimental Procedure

As explained in Section 3.4.2, participants who were willing to participate in the experiment provided their contact information, including their email and/or mobile number. We then initiated contact with these participants to confirm their continued interest in participating in the experiment. For individuals who declined to participate, their contact information was promptly removed from the research database. However, those who remained interested were given an overview of the experiment's requirements and allowed to schedule their participation at a convenient time. The participants were primarily contacted through email, phone calls, and WhatsApp. The following steps were taken:

1. Before each appointment, the participant was sent two links via email or WhatsApp. The first link led to the experiment's 'Information Sheet', which was stored on the main researcher's Google Drive as a PDF file. The second link directed the participant to the consent form in Google Forms.

2. The participant read the 'Information Sheet' and then filled out the 'Consent Form'. The participant was provided with the contact information for the main researcher in case they had any questions or required further clarification.

3. In the experiment appointment, the participant was sent two links, one for mobile application 'A' and the other for mobile application 'B', via email or WhatsApp. The links were sent based on the participant's mobile phone type, either the Google Play Store links or the Apple Store links.

4. The participant was provided with the download instructions.

5. After downloading the applications, a link to the 'Tasks Form', which was stored on the main researcher's Google Drive as a PDF file, was sent to the participant.

6. An account for each participant was created in Firebase (solely for the experiment's purposes), which the participants then used to log in to the applications to perform the required tasks. The account username follows the format of Gmail addresses, such as user2@gmail.com (not an actual email). The number next to the word "user" corresponds to the participant's unique record number generated during Study 1 (The Survey). This enabled us to link the results after deleting the contact information (see Figures 3.17 and 3.18).

7. The user account and the password were sent to the participant to log in and perform the tasks.

8. The participant performed the tasks in the first application ('A' or 'B' according to participant ordering) and then performed the tasks in the second application.

9. After the participant completed all tasks in the two applications and logged out, they were sent a link to a post-questionnaire Google form. In this form, the participant was required to provide the username that they used to log in to the applications.

10. After that, the semi-structured interview was conducted via phone call or WhatsApp messages, depending on the participant's personal preference.

11. As per the consent form, the researcher recorded voice notes for participants who consented to this process and took written notes for those who declined.

The experiment procedure includes using the following:

- Experiment information sheet (PDF)
- Experiment consent form (Google Forms)
- Experiment tasks form (PDF)
- Post-experiment questionnaire (Google Forms)

After completing the experiment, we verified that the data was correctly saved. Then, we ensured that all the data was linked and attributed to the correct participant's ID number for simple accessibility and management. After that, all participants' contact information and identifiable data were deleted. The use of WhatsApp to communicate with participants and share links and forms was approved (See Section 3.6). During the experiment, the data was saved in Firebase, Google Forms, and Google Drive.

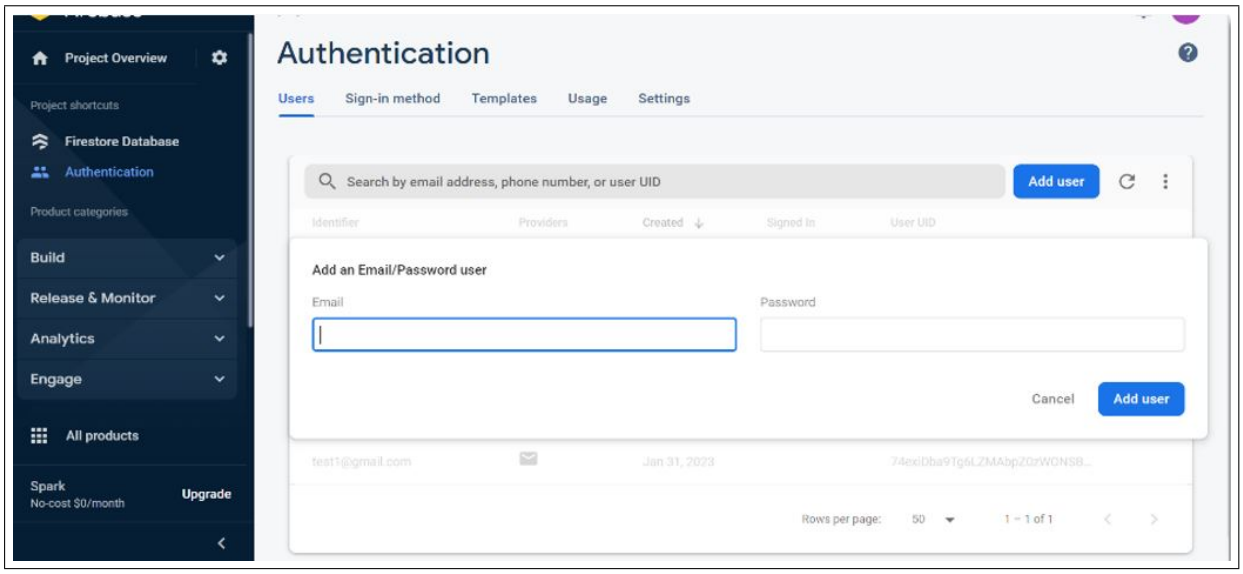

Figure 3.17: *Account creation process for participants*

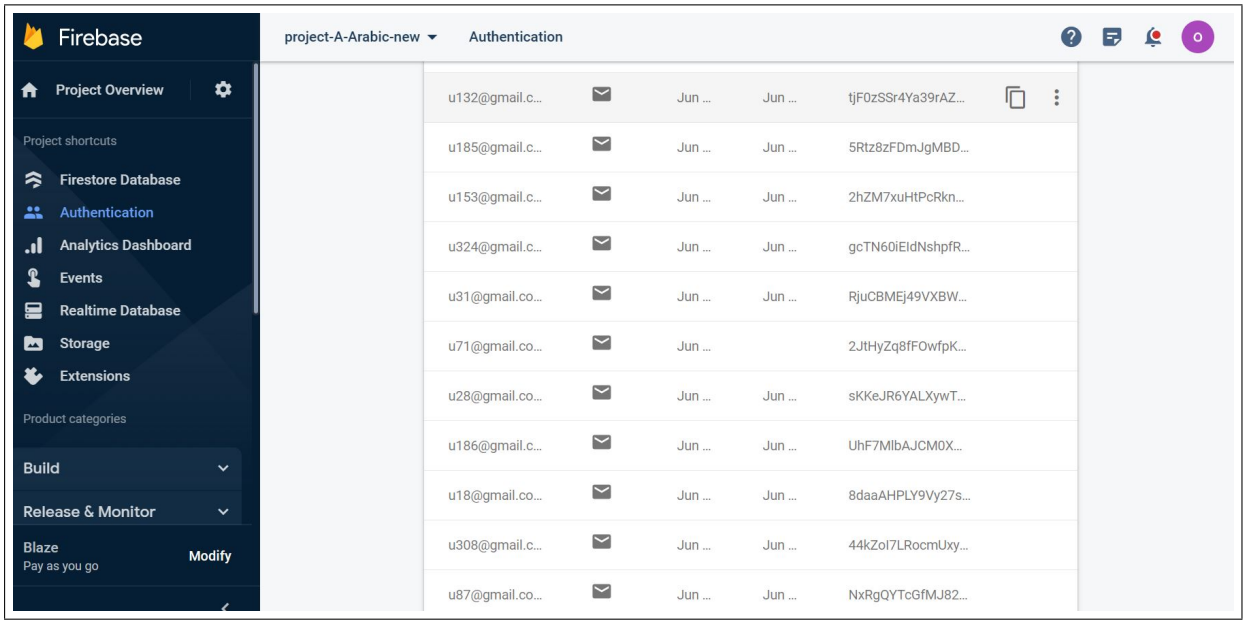

Figure 3.18: *Users accounts to login into the applications*

Pilot study

A pilot study was conducted to validate the experimental framework. In Study 1 (The Survey), 42 participants filled out the questionnaire for the reliability test, of which, 27 expressed their willingness to participate in Study 2 (the experiment) and provided their contact information accordingly. These participants were contacted in order from the top to bottom of the list and recruitment was stopped after receiving responses from five (four females and one male). However, of these four females, two (a 64-year-old and a 28-year-old) agreed to conduct the experiment, while the one male participant was just 18 years old. These age differences provide a diverse range of opinions across different age groups. They were contacted via phone to clarify the reasons for our contact and explain the experimental procedure (see Section 3.5.3) and that their main task was to check the experiment's content, language, and design and provide us with any feedback on how to improve the applications. All three owned an iPhone and they chose to take part in the experiment over the weekend. The 28-year-old female (with a higher education degree) and the 18-year-old male (undergraduate) downloaded the applications via the test flight application using the link provided. Meanwhile, the 64-year-old participant (with a bachelor's degree) had difficulty downloading the application and had to seek help from a family member, indicating that older participants may have difficulty using the necessary technology to access our experiment. Usernames (in the form of Google email addresses) were then created for each participant, with the username containing the participant's record number from the survey results. Communication with participants during the experiment was conducted via phone calls and WhatsApp, as online meetings were not necessary. After completing the tasks, the participants provided feedback on the applications. Other notes were taken after the questionnaire and semi-structured interview. The following changes were made according to the participants' feedback: the experiment consent form (Google Forms) had a field for participants to enter the date but this was removed as the date and time were automatically saved in Google Forms upon form submission. Some typos in applications 'A' and 'B' were fixed and some text was modified to be clearer. Also, some buttons and their labels were modified in application 'B' because participants found them confusing. Regarding the semi-structured interview, participants found the question 'Please rank the following factors from most helpful to least helpful for helping you reach an informed decision' difficult to answer orally, hence, it was removed.

Sampling and Recruitment

Several factors influence the determination of an experiment's sample size, such as study design, analysis method, objectives, and research context. Moreover, practical limitations like time, budget, and participant availability can also play a crucial role in determining the sample size. Other factors like significance level, effect size, and type of test also determine the required sample size for a statistical test (Brysbaert 2019). For example, to achieve a power of 80% when using a repeated measures t-test, a sample size of 52 participants is required (Brysbaert 2019). For a properly powered reaction time experiment with repeated measures, it has been suggested that having at least 1,600-word observations per condition and a sample size of 40 participants for a balanced design is recommended, allowing each participant to experience each condition equally (Brysbaert & Stevens 2018). The sample size in this study was influenced by several factors, including the target population, which consisted of only 185 questionnaire participants who provided their contact information. Additionally, the experiment utilised a tightly controlled within-subject design. Moreover, the experiment procedure is considered complex and lengthy because it involves three methods to collect data: user interaction logging when performing five tasks with two applications, post-experiment questionnaires and semi-structured interviews. As a result, the number of participants was limited to 40.

Study 1 involved 390 participants, of which, 185 provided their contact information and agreed to participate in Study 2. The participants were contacted in the order they participated in Study 1. Regarding the participants who provided their email addresses, mailing lists with ten addresses each were created and an email was sent using the BCC (Blind Carbon Copy) field to ensure privacy containing a brief explanation of the experiment, our contact information, and a request for a response if the participant still agreed to participate in the experiment. However, seven supplied email addresses were invalid. Once we received an email with the initial agreement, we contacted the participants to provide more explanation and set the appointment. For those who provided only their mobile numbers, we sent a text message containing the same content as the email and only those participants who responded to this message were contacted. The number of those who responded was 44 but one participant was excluded from the experiment due to a poor internet connection. Additionally, scheduling a face-to-face appointment was impossible because the participant lived out of the city. Moreover, three participants gave us an appointment after our deadline, thus, the experiment was performed with 40 participants. The first participants engaged in the experiment on 29/04/2023, while the last engaged on 16/06/2023. We attempted to contact the remaining participants who had provided their contact information but many did not respond or requested a significant delay beyond the set deadline. It was observed that females were more willing to participate in the experiment compared to males and individuals with higher education levels were more inclined to participate. Unfortunately, we were unable to perform the experiment on a larger sample size due to time constraints.

3.6 Ethical Considerations

Both the Study 1 (The Survey) and Study 2 (The Experiment) involve human subjects. For Study 1, which focuses on the questionnaire to measure users' privacy awareness in Saudi Arabia, ethical approval was obtained from the University of Sheffield Research Ethics Committee, with Reference Number 039692. Another ethical approval was obtained from the central institutional review board of the Ministry of Health in Saudi Arabia under the number 21-82 E. Regarding Study 2, which is focused on an experiment to investigate the proposed consent mechanisms, approval from the University of Sheffield Research Ethics Committee has been obtained with Reference Number 050879.

Informed consent was obtained from participants of both Study 1 (The Survey) and Study 2 (The Experiment). In Study 1, participants' consent was obtained electronically before answering the questionnaire (Microsoft Forms). A clear description of the research, all the information participants needed, and the primary researcher's contact information were provided for clarification enquiries, together with information on how to escalate concerns. Regarding Study 2, the researcher contacted the participants who provided their contact information in Study 1. The contact information of the participants who became unwilling to participate was deleted directly from the research database. Regarding the participants who were still willing to participate, we sent them two links through email or WhatsApp. The first link directed them to the experiment information sheet in PDF format. This sheet had all the necessary details and information they needed to contact the researcher if they had any questions or needed further clarification. The second link directed them to the consent form, which was in the form of a Google Form. Participants were welcome to ask any questions during and after the experiment. They were allowed to withdraw at any stage. Contact information was provided for participants to escalate any concerns.

All ethical criteria for conducting research were followed before, during and after the study. Moreover, it is crucial to maintain confidentiality and anonymity during research. Therefore, all personal and contact information was deleted after the experiment directly. Data management plans were created according to the University of Sheffield's requirements.

3.7 Chapter Summary

This chapter explains the methodology adopted in this research and the methods and design of two studies conducted in this research. It begins with an overview of research paradigms and methodologies. Then, it describes the process of determining this research methodology and outlines the rationale behind selecting a quantitative survey for Study 1 and a mixed methods approach for the experiment for Study 2. Each study methodology is described in detail.

The first study aims to investigate the current state of users' awareness regarding the privacy of their personal data when using digital health services. This study addresses RQ1 (Section 1.5). A quantitative method was selected to conduct the study. The study starts by surveying the literature to extract the factors that affect users' privacy awareness. A questionnaire based on privacy awareness factors extracted from the literature was designed and developed. After that, the survey was developed using Microsoft Forms. The validity and reliability of the questionnaire were examined. The survey was launched to collect the data.

The second study aims to investigate the important features of the consent mechanism in IoMT systems that help to obtain users' informed consent. Mixed-method designs that combine quantitative and qualitative approaches were chosen. This study addresses RQ2 and RQ3 and sub-question SQ1 (Section 1.5). First, an experimental framework has been designed depending on the important features of informed consent in IoMT that have been identified in Section 2.12. This experimental framework includes two mobile applications (referred to as 'Condition A' and 'Condition B' in this thesis) to allow a comparative within-subject experiment followed by post-experiment questionnaires and semi-structured Interviews. Then, a pilot experiment was conducted. After that, a full experiment was conducted to collect the data. The participants who took part in this study were originally part of the first study. At the end of this chapter, the ethical approvals issued for each study and the ethical considerations in this research were discussed.

Figure 3.19 illustrates the main steps conducted in Study 1 (The Survey) and Figure 3.20 illustrates the main steps conducted in Study 2.

Study 1 (The Survey): Privacy Awareness among Users of Digital Healthcare Services in Saudi Arabia

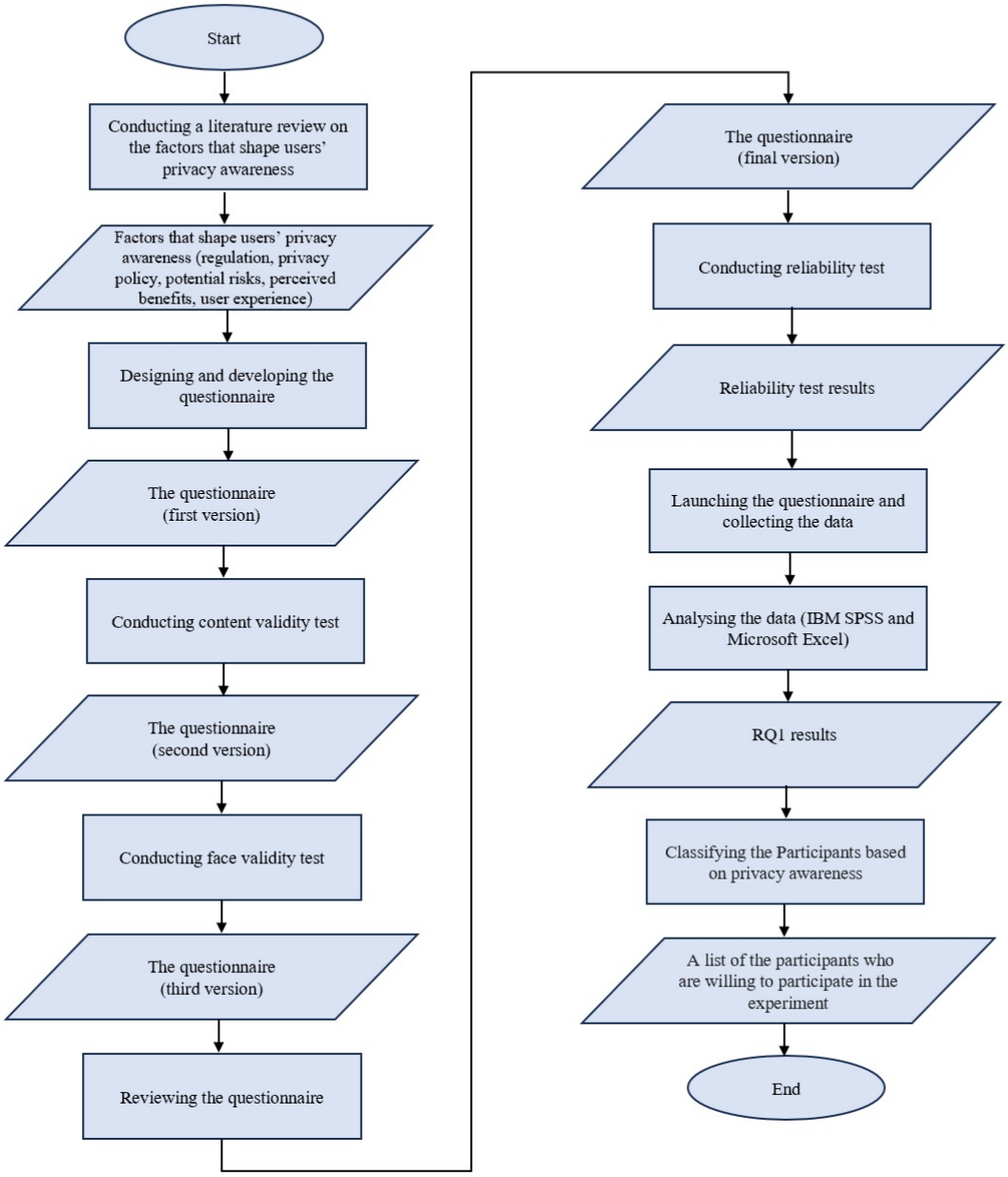

Figure 3.19: *The main steps involved in Study 1 (The Survey)*

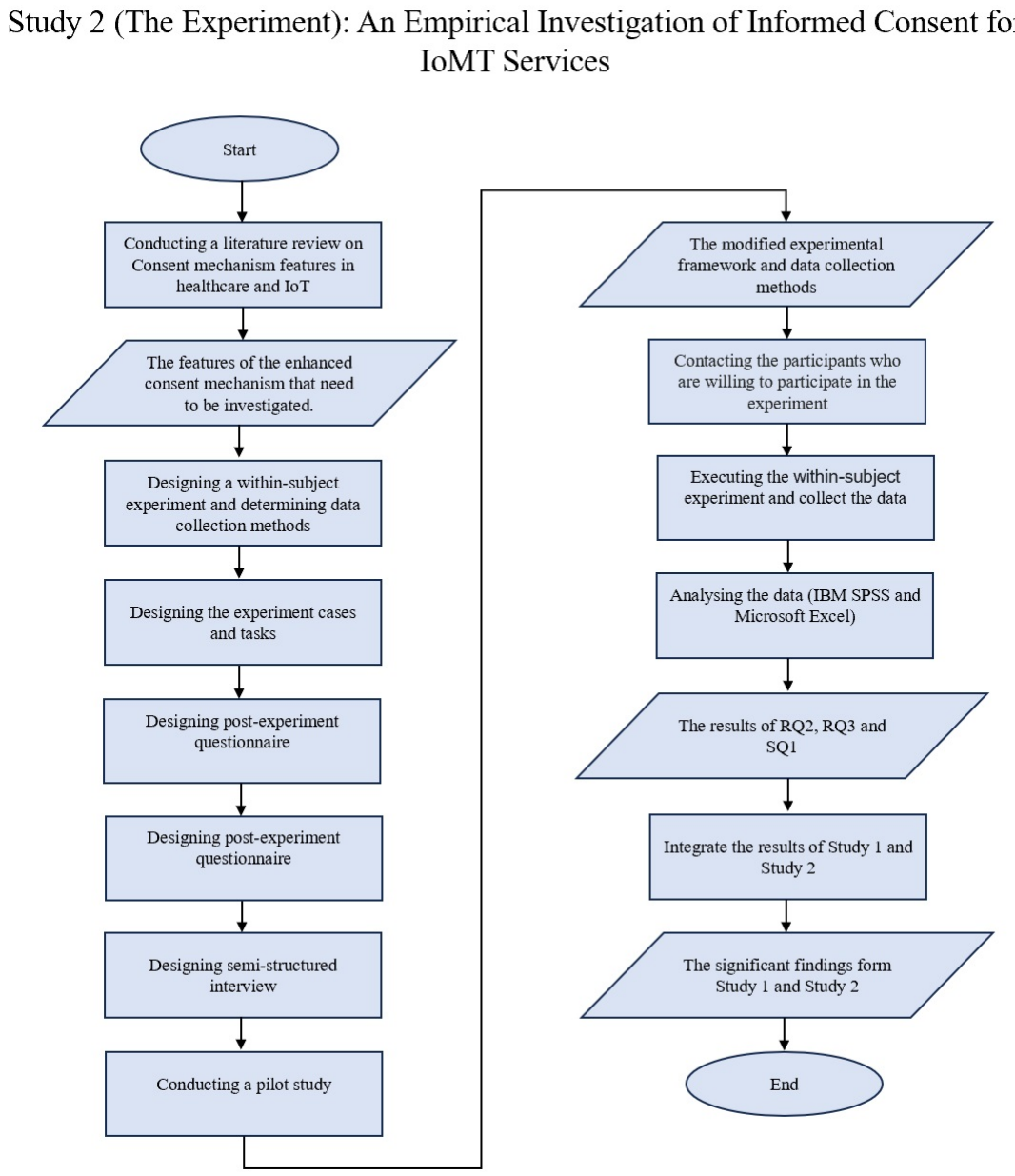

Figure 3.20: *The main steps involved in Study 2 (The Experiment)*

Chapter 4

Results and Discussion

4.1 Introduction

In this thesis, we conducted two studies: Study 1 (The Survey) and Study 2 (The Experiment). In the previous chapter, Chapter 3, we discussed the methodology that has been used to conduct these studies. In this chapter, the results of these studies are presented and discussed. First, the results of Study 1 are exhaustively discussed, followed by a comprehensive discussion of the results of Study 2. Finally, this chapter discusses integrating and analysing the results from both Study 1 and Study 2 to provide a more comprehensive understanding.

4.2 Study 1 (The Survey): Privacy Awareness among the Users of Digital Healthcare Services in Saudi Arabia

Before starting the data analysis, the data was encoded in Microsoft Excel and then imported into an SPSS file (IBM SPSS (v.28)). Both Microsoft Excel and SPSS IBM SPSS (v.28) were used for the data analysis. As mentioned before in Section 3.4.1, the survey was designed to focus on five main factors that shape users' privacy awareness: privacy regulation, privacy policy, perceived benefits, potential risks, and user experience. For each of these factors, two types of questions were designed: subjective assessment (self-assessment) and objective assessment (see Section 3.4.2).

The self-assessment questions used a 5-point Likert scale. The corresponding calculations are straightforward (with results between 1 and 5). For the objective assessment, the questions could have raw scores other than 5. In such cases, the individual question scores were normalised (to a top score of 5) to calculate the factor and overall scores. For each participant, the mean score on each factor was calculated (a simple average of the constituent question scores for that factor). The overall score for the participant was the simple average (i.e. mean) of the factor scores. This holds for both self-assessment and objective assessment.

For the last factor, which is user experience, there were no right or wrong answers because it focused on user experience and concerns in using healthcare applications and if they have faced any privacy breaching situation before. In addition, some questions on the potential risks and perceived benefits section have no right or wrong answers. These questions focus on participants' viewpoints about their privacy concerns, the risks associated with disclosing their data, and the benefits they hope to gain when sharing their data.

4.2.1 Demographic Profile

A total of 390 participants completed the questionnaire, 61.0% females and 39.0% males, ages from 18 to 70 years, with an average age of 39.03. The majority (66.4%) of the sample is from Jeddah, with the next largest group (12%) being from Riyadh. Regarding education level, 53.6% hold at least a Bachelor's degree, while 32.3% hold a Master's or PhD. For more details, see Figure 4.1.

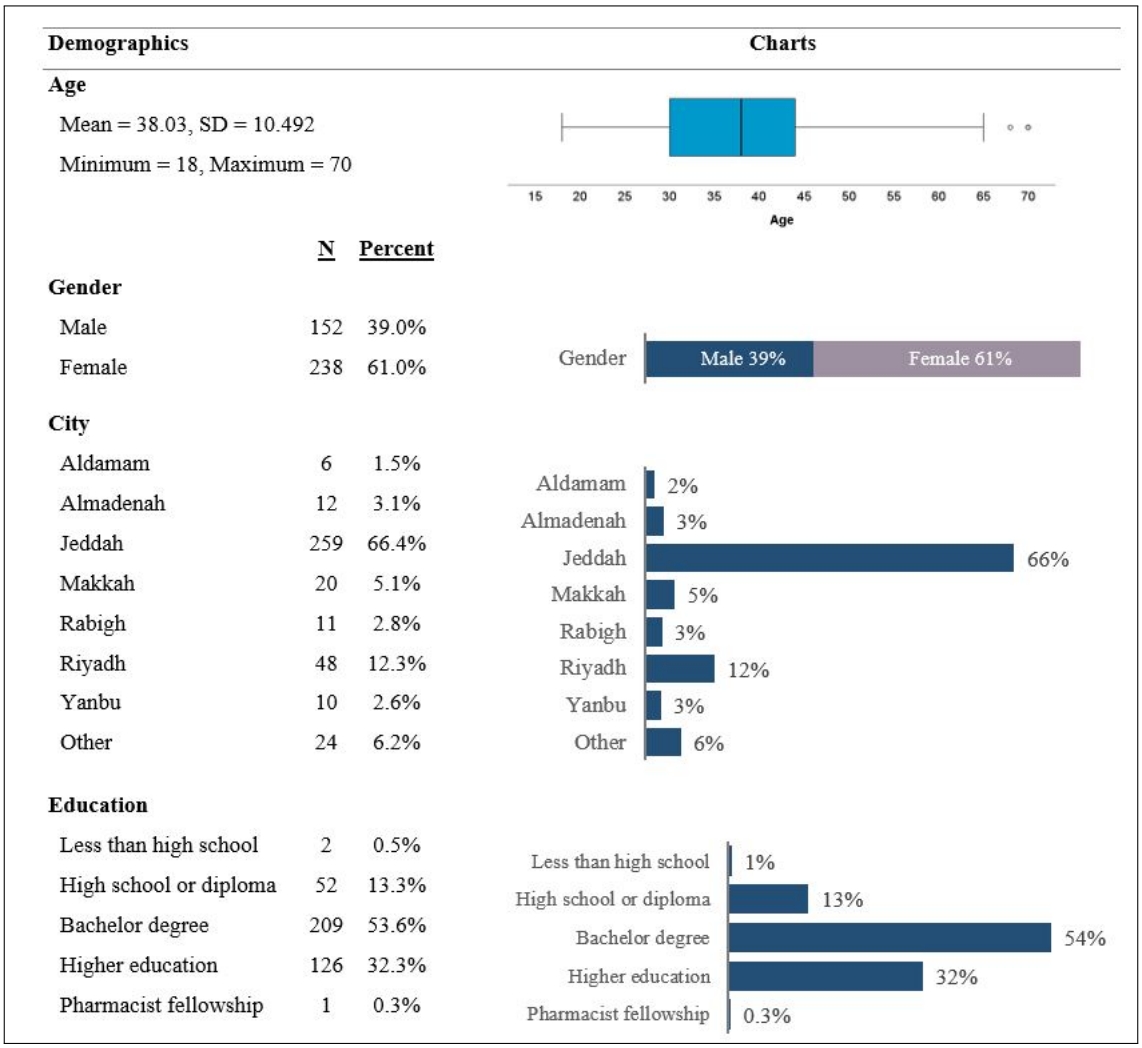

Figure 4.1: *Sample demographics*

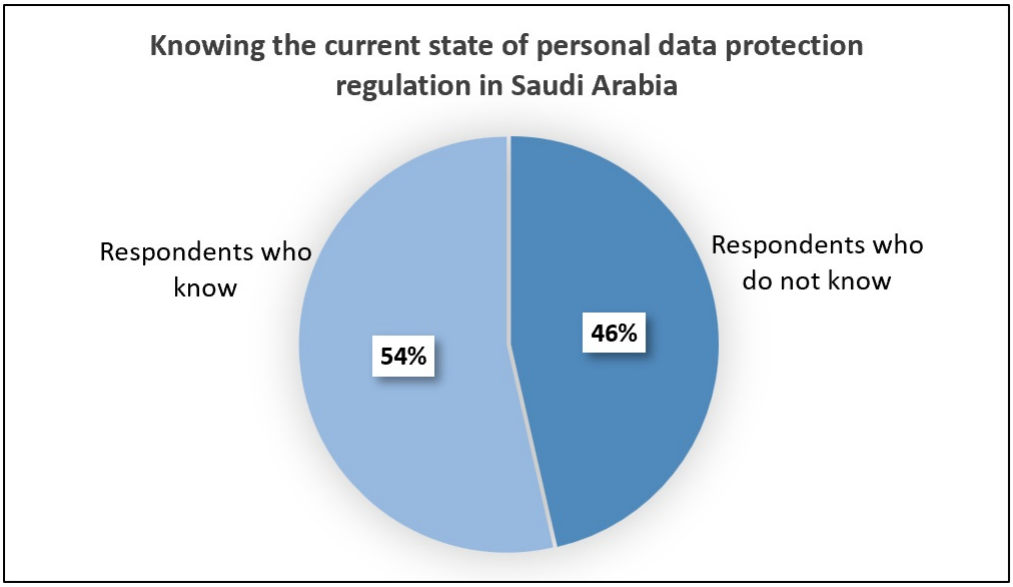

Figure 4.2: *Respondents who knew the current state of personal data protection regulation in Saudi Arabia*

4.2.2 Privacy Regulation

The respondents self-assessed their knowledge of the laws and regulations relating to data privacy in Saudi Arabia with a mean score of 3.07 out of 5 (equivalent to 61.4%) and a standard deviation (SD) of 1.102. However, when they were asked about the current state of personal data protection regulation in Saudi Arabia (see Appendix A, part 2 for the question), 46.4% selected that there is no specific personal data protection regulation in Saudi Arabia, while 53.6% of respondents knew the current state which is that the government has approved personal data protection regulation and will come into force by March 2022 (see Figure 4.2). However, at the time of conducting the survey, the regulation that protects personal data in Saudi Arabia was in a transitional stage, which could have impacted these findings. Varkonyi et al. (2019) conducted a study of regulatory awareness, particularly focused on GDPR. They reported that 61% of participants knew of the existence of GDPR. Participants in their survey were all students. Thus, our results seem broadly comparable.

The following questions were intended to assess the understanding of the respondents who **knew the current state of personal data protection regulations in Saudi Arabia**. These respondents self-assessed their level of understanding of personal data protection law with a mean score of 3.21 out of 5 (equivalent to 64.2%) and a standard deviation of 1.007. Then, to objectively assess these respondents' understanding, they were asked some questions about the cases where the service provider is allowed to collect, process, use, and share their personal data according to regulations (see Appendix A, part 2 for the questions). Regarding the cases in which the service provider can **collect** users' data, the results show that the majority (72.2%) of respondents have a high to very high level of understanding. As for the cases that allow service providers to **further process and use the data that they collected for specific purposes after user approval**, most respondents (71.8%) have a medium understanding. Finally, regarding the cases that allow the service provider to share user data with a third party, 30.8 % have medium, while nearly half of the participants (48.3%) respondents have a high level of understanding.

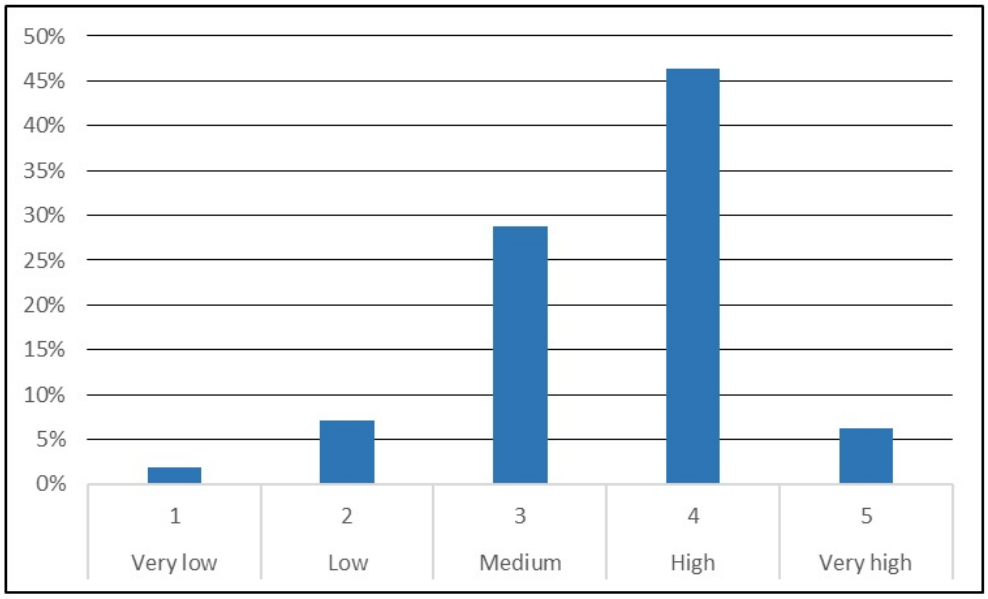

Figure 4.3: *Respondents' results on cases where the service provider is allowed to collect, process, use, and share their personal data under regulations (objective assessments).*

The respondents' overall result on questions about the cases where the service provider is allowed to collect, process, use, and share their personal data in accordance with regulations (objective assessments) is illustrated in Figure 4.3. It demonstrates that most respondents who knew the current state of personal data protection regulations in Saudi Arabia have a high understanding of when service providers can collect, use, and share their data. The finding indicates that respondents who are knowledgeable of the existence of PDPL in Saudi Arabia are aware of when it allows service providers to collect, use, and share their data. This implies these respondents are likely to be more aware of their rights concerning personal data and how to make appropriate choices regarding their data compared to those who are unaware of the existence of PDPL.

4.2.3 Privacy Policy

The first part of the privacy policies questions addresses whether participants read privacy policies when using new applications or systems (see Appendix A, part 3 for the questions). Only 5% of the survey respondents claimed that they always read them, 11% claimed that they often read them, and 33% said they read them sometimes. On the other hand, 25% of users said they rarely read the privacy policy, and 27% said they never read it (see Figure 4.4). That aligns with the results of a survey study conducted by Alghamdi et al. (2023) in Saudi Arabia, where they asked computer science students if they read the privacy policy before installing the new applications, and they found that most of them do not read privacy policy documents. The respondents who reported that they read the privacy policies provided their motivations for doing so. Their motivations can be summarised in five categories, illustrated in Figure 4.5. Half the participants (50.6%) read the privacy policy because they have concerns regarding the privacy and security of their personal and sensitive data. This indicates their need to understand how the service provider will protect their data. For example, they wanted to know how their

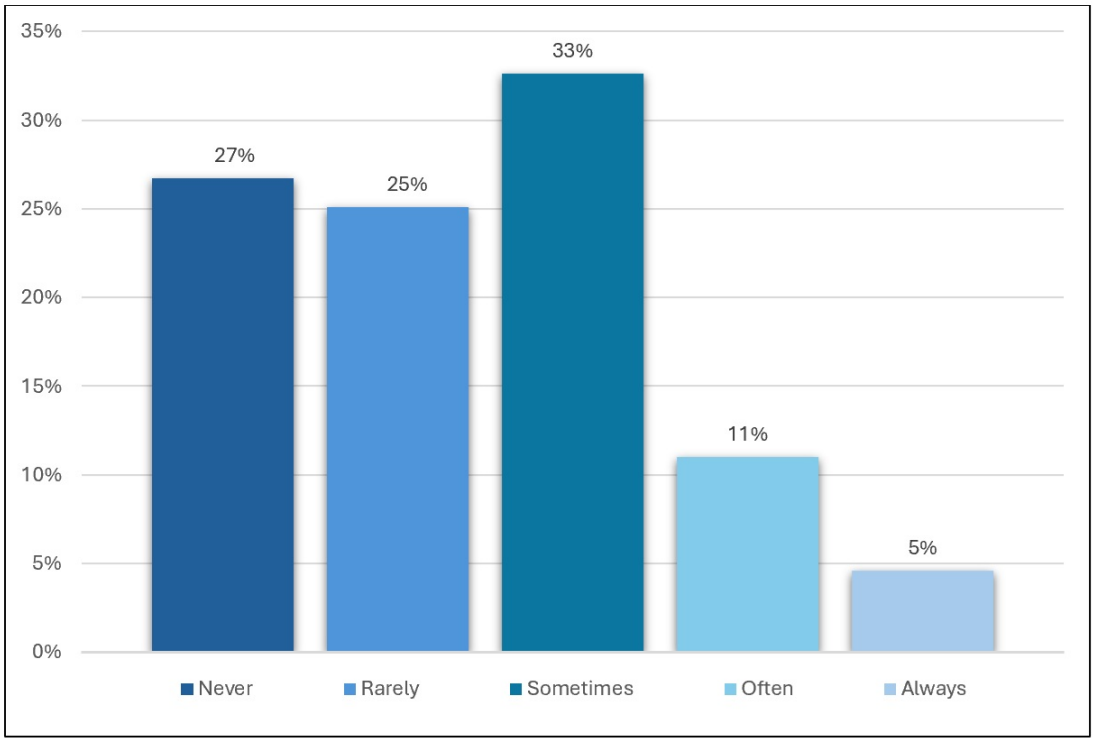

Figure 4.4: *Frequency of reading privacy policy*

data would be protected, why their data would be used, the possibility of their data being shared with a third party, and the potential risks. Thus, service providers should have a transparent privacy policy that describes how users' data privacy and security will be maintained, addressing users' concerns. Of the respondents, 25.3% were interested in acquiring general information about the application or service. This information included details about how the application works, as well as its features. Of survey respondents, 12.0% read the privacy policy because they wanted to learn about their rights and obligations. Moreover, all the participants of the survey were asked about the topics are defined in a privacy policy for any application. The majority of respondents (71.3%) have a medium level of knowledge of what these topics are. Regarding the Ministry of Health's (MOH) "Acceptable Use Policy" 74.9% of respondents stated that they did not know about its existence. The result is reasonable because the "Acceptable Use Policy" is primarily directed at employees, even though it is publicly available. It governs employees' use of resources, including patient information, ensuring security and compliance with legal standards. In contrast, privacy policies and terms of service are aimed at users.

All respondents were "Sehhaty" application users. Out of all participants, 54.1 % claimed that they had not read the privacy policy, and 20.3 % claimed that they were unaware of its existence. Consequently, that means a total of 74.4% were unaware of the "Sehhaty" application privacy policy, and they agreed to it without reading it. This result agrees with previous studies that confirm that most users agreed to the privacy policy without reading it. For example, Steinfeld (2016) conducted an experiment and found that 79.7% of their participants agreed to the privacy policy without clicking the link to read it. These results indicate a significant gap in respondents' engagement with critical information about their data privacy and their rights. Thus, strategies to make the privacy policy more accessible, understandable, and engaging are needed when designing and developing services that deal with users' sensitive and personal data can help bridge this gap.

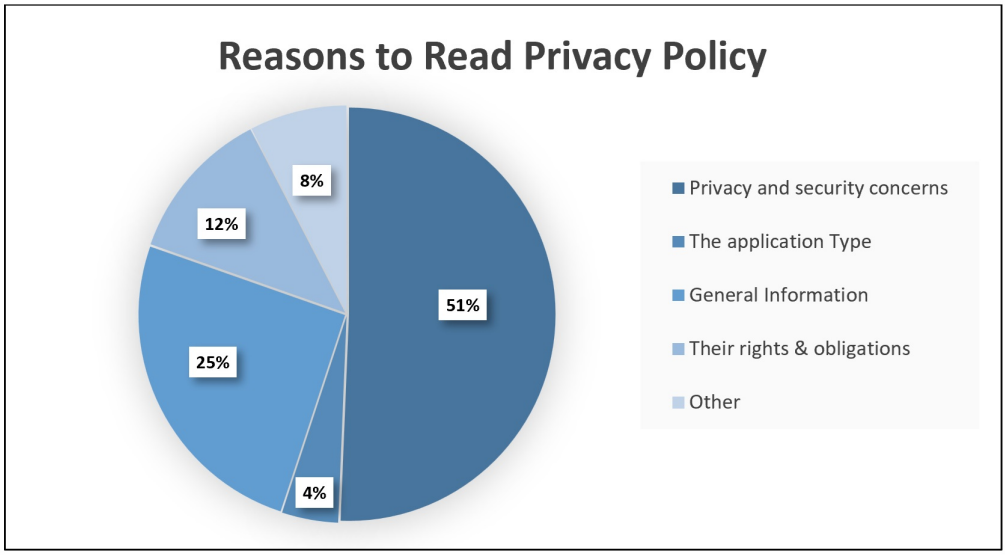

Figure 4.5: *Participants' motivations for reading privacy policies when using new a application or service*

The majority of users tend to skip the "Sehhaty" application privacy policy, but 25.6% of respondents claimed to have read it. These respondents demonstrated high engagement in three locations where the policy can be accessed (see Figure 4.6). 83% claimed to have read the privacy policy before registering in the application, while 17% did not. Regarding the privacy policy link on the login page, 75% claimed that they had used it to read the privacy policy, while 25 % did not. Lastly, regarding the privacy policy link in the main menu, 63% claimed that they used it to read the privacy policy while using the application, while 37% did not.

A significant proportion claimed that they read the privacy policy before registering for the service, suggesting they may have concerns about their personal and medical data privacy. Also, many of these participants used the link on the login page, which suggests that they might not read it while registering, or they had read it and they wanted to go back and remember some points. Moreover, using the link in the main menu after the registration and login phases indicates that these participants wanted to know and understand the privacy policy at a specific point while using the service or remind themselves of some points that they have read before. However, further investigation is needed to understand users' behaviour better.

Moreover, these participants were subsequently questioned about three aspects to measure their satisfaction: ease of access, the clarity of the language and length of text (see Appendix A, part 3 for the questions). Respondents were most satisfied with the clarity of the language used in the privacy policy, with 75.6% of them rating the language used from good to excellent. Also, respondents were satisfied with how they accessed the privacy policy, with 73.4% assessing it as good to excellent. Finally, 70.6% respondents were satisfied (good to excellent) with the length of the privacy policy text (see Figure 4.7). To assess their understanding of the privacy policy they have read, they were asked about what type of data the administration of the "Sehhaty" application collects, and the results show that 61.4% of the respondents had a medium understanding of this. Also, the respondents were asked about cases where the administration of "Sehhaty" can disclose users' data. Again, the results show that the majority of respondents (63.4%) have a medium understanding of these cases.

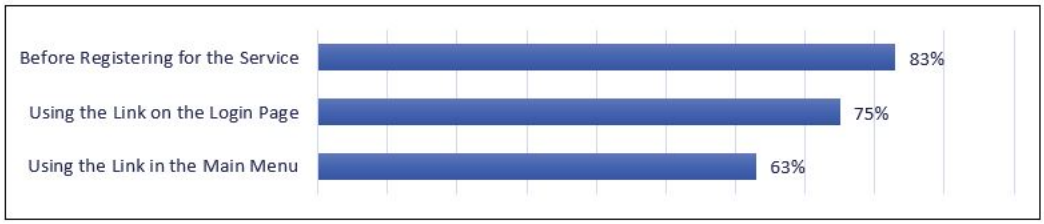

Figure 4.6: *How participants access and read the "Sehhaty" application privacy policy*

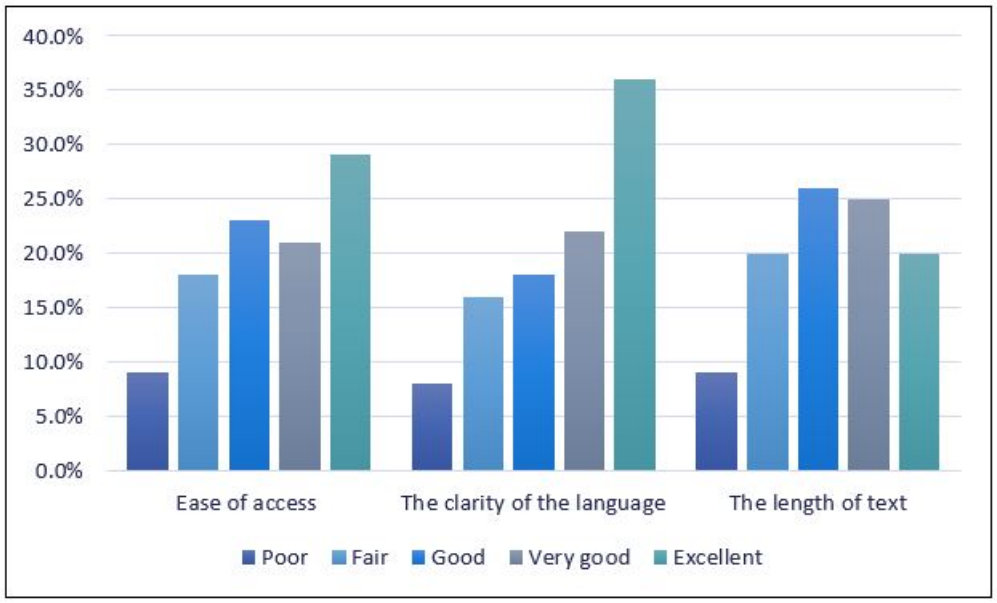

Figure 4.7: *Participants' overall satisfaction with "Sehhaty" privacy policy*

4.2.4 Perceived Benefits and Potential Risk

Respondents self-assessed their knowledge of the benefits they could receive when they allow service providers to collect and use their personal information. 19.2% of the respondents stated that they do not know what benefit they can gain when they allow service providers to collect their data, 19.7% stated that they have a low level of knowledge, while 41.8% stated that they have a medium level of knowledge. On the other hand, 12.3% stated they have good knowledge, and 6.9% stated they have excellent knowledge about benefits they can receive. Moreover, respondents self-assessed their knowledge of the additional benefits that may be gained if they agree to the service provider's use of their personal information for purposes other than the service they agree about. The results found that 23.3% of respondents have no knowledge about the benefits that they may get by allowing the service provider to use their personal information for purposes other than the service they agreed upon, while 21% have a low level of knowledge. Of the respondents, 38.2% have a medium level of knowledge. Also, respondents self-assessed their knowledge of the additional benefits that may be gained if they agree that the service provider shares their personal data with a third party for a specific reason. Of the

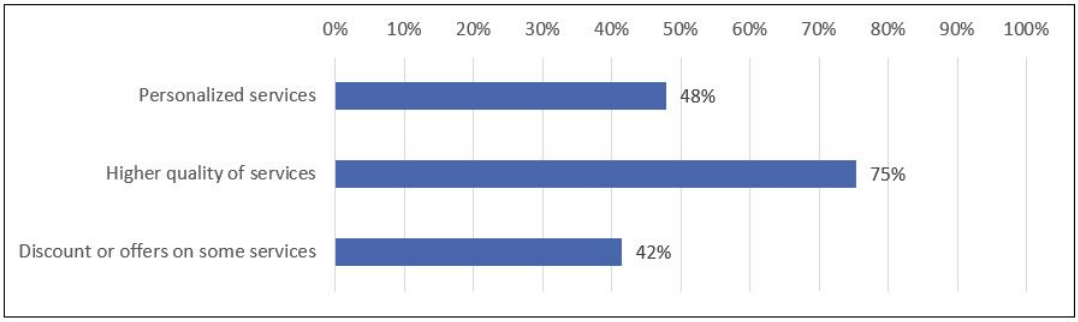

Figure 4.8: *The benefits preferred by participants when giving their approval for data collection and use*

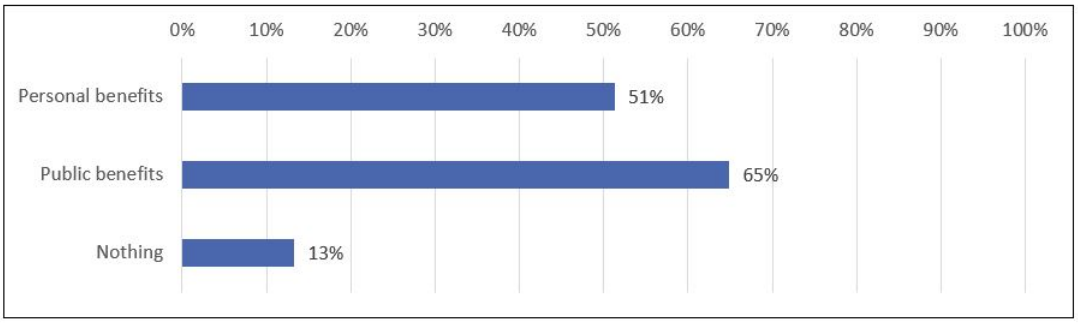

Figure 4.9: *The benefits preferred by participants when giving their approval to service providers to use their data for secondary purposes*

respondents, 27.7% have no knowledge, 19.7% have a low level of knowledge, and 36.4% have medium knowledge, while 10.8% have good knowledge and 5.4% have excellent knowledge.

The participants were asked about the benefits they prefer to receive from the service provider if they agreed to the collection and use of their personal information (see Appendix A, part 4 for the questions). The results show that 75.4% of respondents prefer to gain a higher quality of services, 47.9% prefer to gain personalised services, and 41.5% prefer to gain discounts or offers on some services (see Figure 4.8). In return for giving their approval to an application or service provider to use their personal information and data for purposes other than the main service, 64.9% of respondents prefer to have public benefits, e.g. improve the application design, improve the application or service efficiency, and improve the outcomes of services. 51.8% prefer personal benefits, e.g., priority in services and discounts or offers. On the other hand, 13.3% do not expect any additional benefits (see Figure 4.9). As compensation for giving their approval to an application or service provider to share their data with a third party for a specific reason, 64.4% of respondents would like to have public benefits, e.g. improve the application design, improve the application or service efficiency, and improve the outcomes of services. However, 57.7% would like to have personal benefits, e.g., priority in services and discounts or offers. On the other hand, 11.3% did not want any benefits, while 2.3% preferred not to share their data even if there were benefits (see Figure 4.10.)

Respondents self-assessed their knowledge regarding the potential risks that might occur when an application or service provider collects and uses their personal information and data associated with them (see Appendix A, part 4 for the questions). The results show that 35.6% of respondents felt they have good to excellent knowledge of these potential risks, and 36.9%

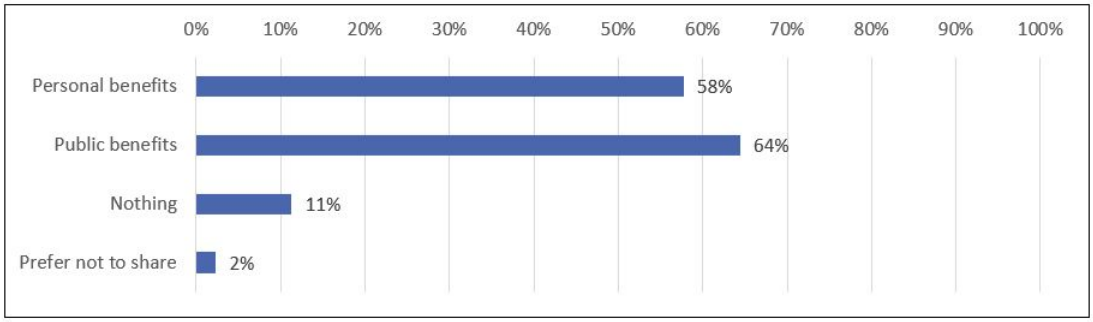

Figure 4.10: *The benefits preferred by participants when giving their approval for data sharing*

have a medium level of knowledge. Also, participants self-assessed their knowledge regarding the risks that might occur if they approved a service provider to share their personal information and data associated with them with a specific third party. The results show that the largest proportion of respondents (42.3%) indicated a medium level of knowledge, followed by 19.0% with a good level, 10.8% with an excellent level, 18.2% with a low level, and 9.7% with no knowledge. Moreover, the survey evaluates respondents' understanding of the service provider's responsibility regarding protecting their data from potential risks. The majority of respondents, 74.9%, understand that the service provider must provide sufficient privacy measures to protect personal and identifiable data. Similarly, 75.1% of respondents understand that any service provider collecting, processing, and using personal information and data associated with users must prepare and document procedures necessary to manage and address privacy violations. Finally, 66.7% of respondents understand that the service provider must assess system activities' potential risks and impacts.

Respondents explained their concerns if they accept collecting their personal information and data from the service provider to provide a specific service for them. The survey found that 64.6% of respondents were concerned about using the collected data for other purposes without their approval and 62.3% of respondents were concerned about sharing the collected data with a third party without their approval. Also, 52.8% of respondents were concerned about insecure data transmission, such as unencrypted data transmission, and 50.3% of respondents were concerned about collecting unnecessary personal data. Finally, 23.8% of respondents were concerned about data corruption or loss. However, only 18.7% of respondents did not have any concerns (see Figure 4.11).

Moreover, participants were questioned about their concerns regarding accepting the service provider using their personal information and data associated with them (which have been collected after their approval to provide them with a main service) to provide them with a new service. Of respondents, 74.6% were concerned about data leakage or breach where the data could be used for phishing or identity theft, 63.8% of respondents were concerned about unauthorised access by employees, where the data could be sold or used without permission, 59.0% of respondents were concerned about sharing data with a third party without user permission, and finally, 16.4% of respondents have no concerns (see Figure 4.12). Participants who agree to the service provider sharing their personal information with a third party are mostly concerned about data leakage or breach (74.4%). 64.6% of respondents are concerned about security and privacy measures used by the third party to protect the data. 51.8% are concerned about third-party privacy policies. 16.4% of respondents had no concerns (see Figure 4.13).

Participants were asked whether they knew if the E-health systems in Saudi Arabia provide benefits for patients (see Appendix A, part 4 for the questions). 48.7% said yes, they know.

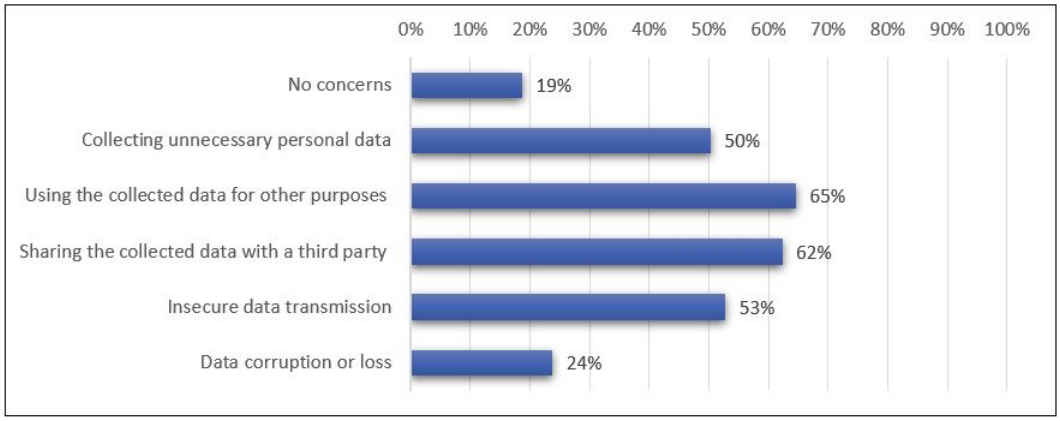

Figure 4.11: *Participants' concerns regarding personal data collection*

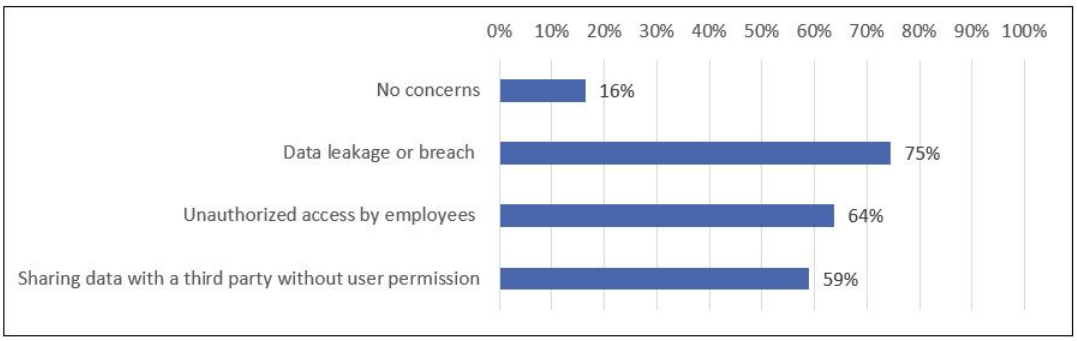

Figure 4.12: *Participants' concerns regarding using their personal data for a new purpose (new service)*

These positive respondents were asked about the type of these benefits. The results found that 60.5% of the respondents have a medium level of knowledge of these benefits where these benefits include ease of finding health services requested through the internet services, reducing the need to revisit service providers resulting from lack of correct information or difficulties resulting from setting appointments, and the ability to view the patient's health information at any time and the information about who can access it and for what purpose. Moreover, participants were asked whether they knew that new E-health systems in Saudi Arabia are designed to reduce potential privacy risks. It was found that 34.6% of the respondents knew. Those who knew that new E-health systems in Saudi Arabia are designed to reduce potential privacy risks were asked about some of the potential privacy risks that they expect the new E-health systems will reduce, such as unauthorised access, collecting unnecessary data, and personal data leakage. It was found that 44.4% have medium level of knowledge. Regarding the "Sehhaty" application, 45.4% of respondents said they know that the application administration collects some personal information, such as the user device's language and the type of operating system, in order to improve the user's experience. Also, 63.1% of the respondents have a medium level of understanding of the benefits that will be achieved when the "Sehhaty" application administration shares users' information with partners and all related entities, including the Ministry of Health.

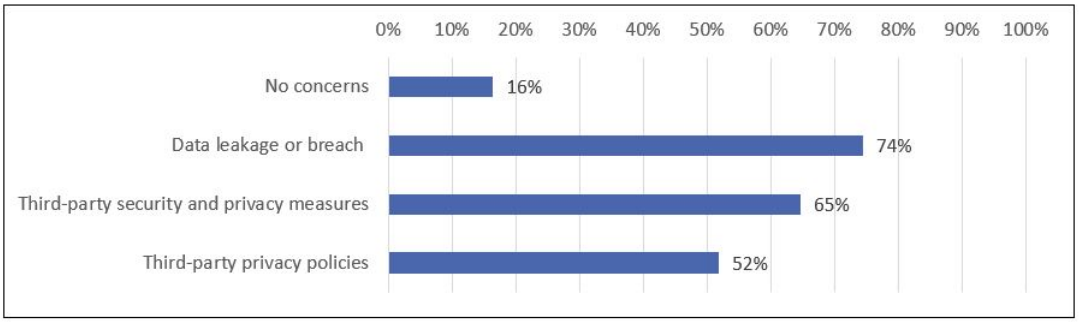

Figure 4.13: *Participants' concerns regarding personal data sharing*

4.2.5 User Experience

According to the results, 38.5% of the respondents use medical devices at home (see Figure 4.14). The most commonly used medical device at home is the blood glucose monitor, used by 31.3% of the respondents. Following that were digital thermometers (21.9%) and blood pressure monitors (22%), while weighing scales were used by 20.7% of the respondents. Finally, only 2% of the respondents used a nebuliser at home. Moreover, 27.3% of respondents, that use medical devices at home use a mobile application related to the device. The majority of them (51.3%) had no concern at all about privacy when using their devices. However, the respondents who were concerned about their privacy when they used the medical devices were asked about the types of concerns they had. The results show that the most common types of privacy concerns were using users' data to steal their identity (48.7%) and collecting unnecessary data, such as your location, without your knowledge (46.0%). All respondents' concerns are illustrated in Figure 4.15.

The "Sehhaty" application was primarily used to book COVID-19 tests (81%) and vaccine appointments (80%). Also, 34.4% of respondents used the "Sehhaty" application to book an appointment in the primary healthcare centre. However, it is important to note that the questionnaire was conducted during the period of December 2021 to February 2022, when vaccination was mandatory and Coronavirus restrictions and measures were imposed around the world. Therefore, there may be a significant change in the result of this question if the questionnaire is repeated now. As shown in Figure 4.16, 32.3% of respondents do not have any privacy concerns when using the "Sehhaty" application, while 21.0% have little concern. However, 46.7% have at least a medium level of concern. The most common types of privacy concerns respondents have when using the "Sehhaty" application are: using their data to steal their identity (42.6%) and collecting unnecessary data, such as their location, without their knowledge (42.1%). see Appendix A, part 5 for the questions.

According to the survey, 26.2% of the respondents use healthcare applications other than "Sehhaty". Of these respondents, the majority (57.6%) use other healthcare applications for booking clinic appointments. The second most common reason for using these applications is to obtain remote medical advice (41.4%), followed by monitoring general health (39%) and getting general medical advice (36%). Regarding privacy concerns, 20.6% of respondents have no user privacy concerns at all when using the other healthcare applications. Only 3.9% are very concerned, 19.6% are somewhat concerned, 35.3% are moderately concerned, and 20.6% are concerned a little. Respondents indicated their privacy concerns when using the other healthcare applications. The most common concern was using their data to steal their identity, indicated by 48.5% of respondents. The second concern was collecting unnecessary data, such as their location, without their knowledge, indicated by 43.6% of respondents.

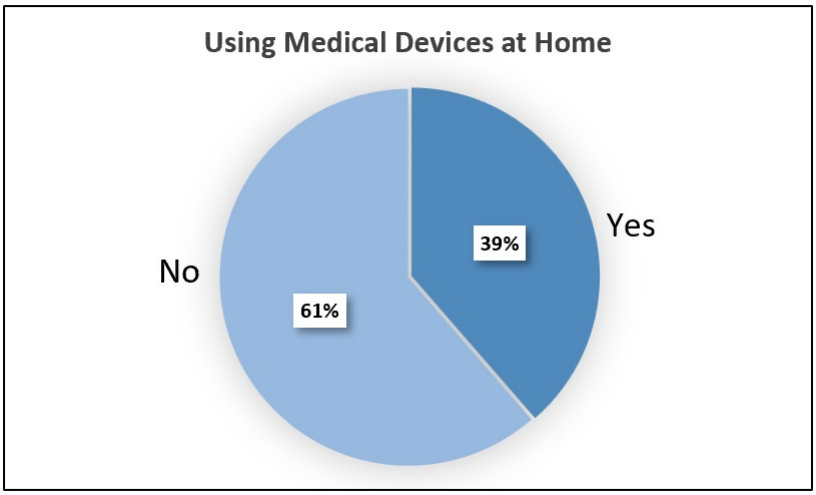

Figure 4.14: *The Participants' who use medical devices at home*

According to the survey results, a very low percentage of respondents, specifically 9.5%, reported experiencing data privacy breaches. However, the percentage of participants whose privacy was violated might be higher, but they were unaware of the violations; thus, they did not report them. Of those respondents who had their data privacy breached, almost half of them (45.9%) did not take any action. This result indicates a lack of privacy awareness among these respondents. They might be unaware or unsure of the appropriate actions to take after a data breach and how to report this incident, or they are to take or lack confidence in the efficacy of the responses. On the other hand, 16.2% solved the problem by themselves. For example, they contacted the person or entity who exposed their data and asked them to stop. 37.8% reported the breach to the authorities, which indicates that these participants have a good level of privacy awareness and knowledge of their rights (see Figure 4.17).

4.2.6 Overall Subjective Privacy Awareness

Based on the level of self-assessed awareness on the topics of Data Regulations, Privacy Policy, Risks and Benefits, and User Experience, an overall level of awareness was calculated using the mean of all these aspects and performing the Visual Binning procedure in SPSS to create a new variable that represents the three levels of awareness: (1) low, (2) moderate, and (3) high. First, these four scores were averaged and a new variable was created, as summarised in Table 4.1 and in Figure 4.18. Then, three bins (classes) were created using the Visual Binning procedure to create three levels of awareness. The bin size was calculated by dividing the range (1.00-5.00) by 3 to reflect three levels of awareness, yielding a bin size of 1.33. To calculate the bin size, the range of values is divided by the desired number of bins. In this case, the range is determined by subtracting the minimum value (1.00) from the maximum value (5.00), resulting in a range of 4.00. Next, the range is divided by the desired number of levels or bins, which in this case is three. Dividing the range of 4.00 by 3 results in a bin size of 1.33. The first bin starts at 1.00 to 2.33, the second bin starts at 2.34 to 3.67, and the third bin starts at 3.68 to 5.00. The results show that the majority (61.8%) of respondents assessed their awareness as medium, 27.7% as low, and 10.5% as high.

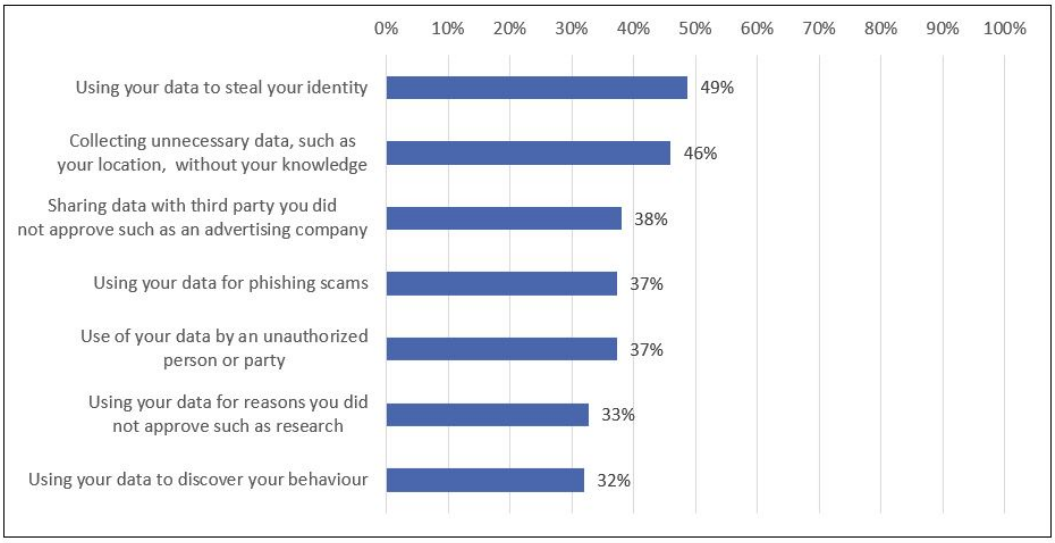

Figure 4.15: *Participants' privacy concerns when using medical devices*

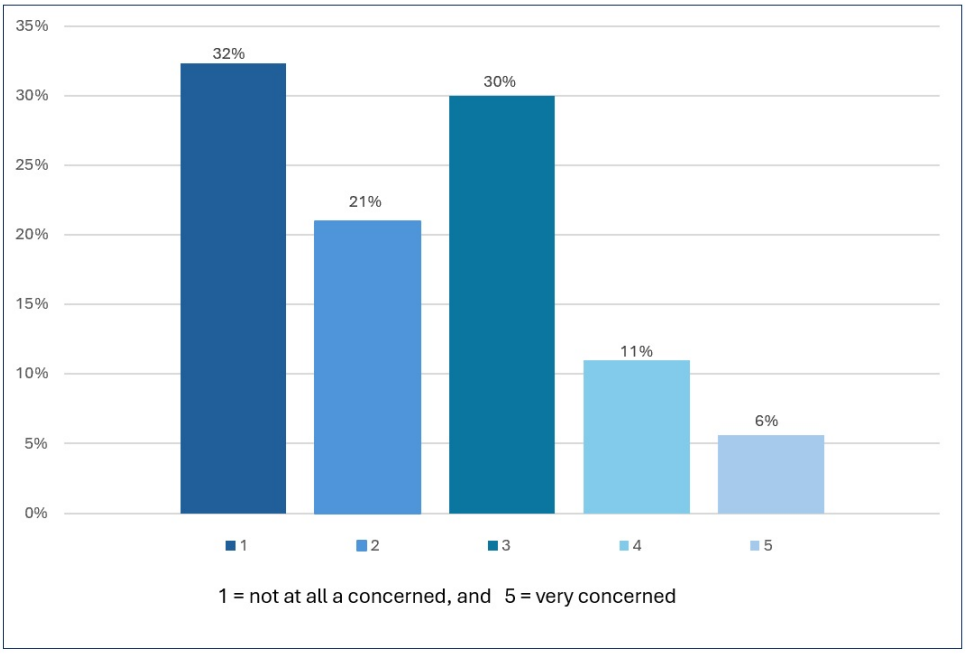

Figure 4.16: *Participants' privacy concerns when using "Sehhaty" application*

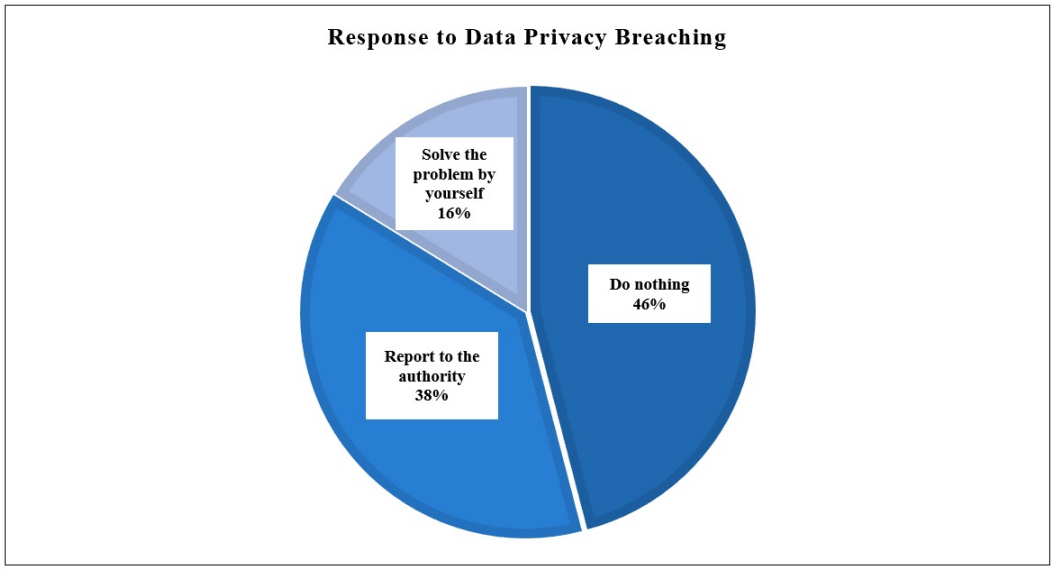

Figure 4.17: *Participants' responses to data privacy breaches*

Table 4.1: *Descriptive statistics for self-assessed awareness calculated mean score*

Mean	Median	SD	Skewness	Kurtosis	Minimum	Maximum	Bin Size
2.73	2.68	.802	.229	.302	1.00	5.00	1.33

4.2.7 Overall Objective Privacy Awareness

Based on the level of awareness (objective assessment) on the topics of Privacy Regulations, Privacy Policy, and Risks and Benefits, an overall level of awareness was calculated using the mean of all these aspects and performing the Visual Binning procedure in SPSS to create a new variable that represents the three levels of awareness: (1) low, (2) moderate, and (3) high. First, these four scores were averaged, and a new variable was created, as summarised in Table 4.2 and the histogram in Figure 4.19. Then, three bins (classes) were created using the Visual Binning procedure to create three levels of awareness. The bin size was calculated by dividing the range (1.57-5.07) by 3 to represent three levels of awareness, yielding a bin size of 1.17. The first bin ranges from 1.57 to 2.74, the second ranges from 2.75 to 3.90, and the third ranges from 3.91 to 5.07. The majority (72.3%) of respondents have medium awareness, 23.1% have low awareness, and only 4.6% have high awareness.

4.2.8 The Relationship Between Subjective and Objective Privacy Awareness

In order to determine if there is a difference between participants' subjective and objective privacy awareness assessment results, we performed a paired-sample t-test. The results showed a p-value of 0.681, indicating that there is no significant difference between the two. Figure 4.20 illustrates the results.

Table 4.2: *Descriptive statistics for objective awareness calculated mean score*

Mean	Median	SD	Skewness	Kurtosis	Minimum	Maximum	Bin Size
3.06	3.05	.508	.120	.446	1.57	5.07	1.17

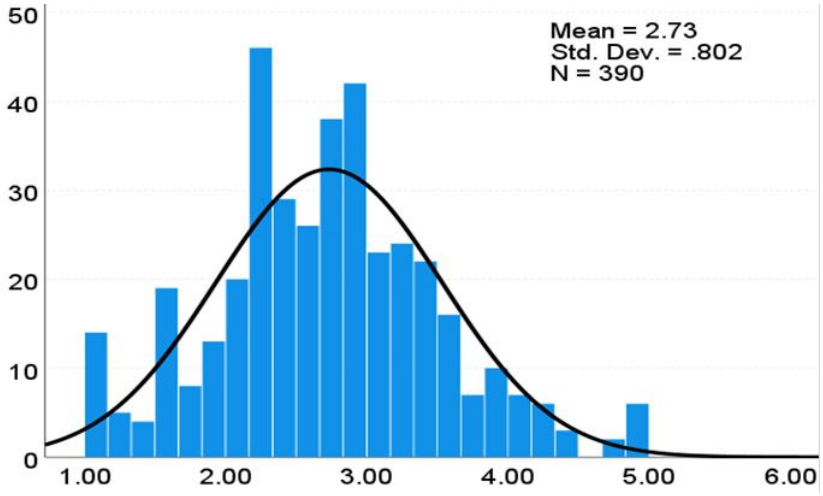

Figure 4.18: *Self-assessed privacy awareness*

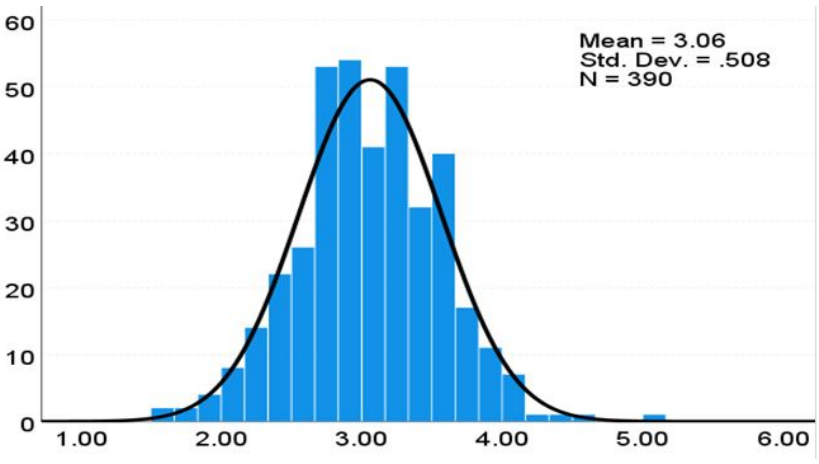

Figure 4.19: *Objective privacy awareness*

Paired Samples Test

		Paired Differences					t	df	Significance	
					95% Confidence Interval of the Difference					
		Mean	Std. Deviation	Std. Error Mean	Lower	Upper			One-Sided p	Two-Sided p
Pair 1	Objective - Subjective	-.0128205128	.61459518609	.03112123699	-.0740073876	.04836636191	-.412	389	.340	.681

Figure 4.20: *Paired Samples T-test for participants' subjective and objective privacy awareness*

4.2.9 The Relationship Between Objective Privacy Awareness and Ages

Spearman's rho correlation coefficient was used to measure the relationship between participant age and privacy awareness, as shown in Table 4.3. The Spearman's rho values indicate that there is no significant relationship between overall objective privacy awareness level and age, r = -0.054, p = 0.283. However, there was a negative, weak relationship between age and the awareness of the general benefits and risks when using any application, r = -0.116, p-value = 0.022. There was also a positive weak relationship between age and awareness about benefits and risks awareness when using healthcare systems, r = 0.133, p = 0.009. The results indicate that older participants are more aware of the benefits and risks of using healthcare systems and applications than younger participants.

Table 4.3: *Spearman's rho correlation coefficients for objective awareness vs. age*

Awareness Criteria	Age
Privacy Regulation Awareness	-.093
Privacy Policy Awareness	-.024
Risk and Benefits Awareness	-.116*
Risk and Benefits in Healthcare Awareness	.133**
Objective Awareness	-.054

*. Correlation is significant at the 0.05 level (2-tailed)
**. Correlation is significant at the 0.01 level (2-tailed)

4.2.10 The Relationship Between Objective Privacy Awareness and Gender

As the awareness variables are measured on an ordinal scale, a Mann-Whitney test was used to find significant differences between males and females in terms of their levels of awareness. The test results are presented in Table 4.4, showing a significant difference between males and females in the levels of privacy policy awareness and risk and benefits in healthcare awareness, p-value$<$0.05. As shown in the results females have a higher level of awareness about privacy policy. Similarly, females are more aware of the benefits and risks of healthcare services.

4.2.11 The Relationship Between Objective Privacy Awareness and Education

Kruskal-Wallis tests were conducted to find significant differences in awareness levels between the different education groups of users. The results are reported in Table 4.5, showing that there were significant differences between user education groups in terms of privacy policy, benefits and risks in healthcare, and overall objective awareness. Post hoc multiple comparisons Mann-Whitney tests were used to determine which groups have significant differences in privacy policy, risk and benefits in healthcare awareness, and overall objective awareness levels, and the results

Table 4.4: *Mann-Whitney test results for awareness vs. gender*

	Mean Rank		Test Statistics[a]	
Awareness Criteria	Male	Female	Mann-Whitney U	Sig.
Personal Data Regulation Awareness	104.18	105.50	5070.50	.871
Privacy Policy Awareness	179.79	205.53	15700.00	.012*
Risk and Benefit Awareness	205.79	188.93	16523.50	.128
Risk and Benefits in Healthcare Awareness	181.97	204.14	16031.50	.036*
Objective Awareness	188.71	199.84	17056.00	.223
a. Grouping Variable: Gender *. Significant at 0.05				

are presented in Table 4.6. The results revealed that for privacy policy, benefits and risks in healthcare, and overall objective awareness, users with higher education (Master's degree or PhD) significantly had higher mean rank than users with High school or diploma, p-value<0.005 (the Bonferroni corrected significance level, calculated as alpha level divided by the number of Mann-Whitney tests conducted; i.e., 0.05/10). That is, users with higher education had higher awareness of privacy policy, benefits and risks in healthcare, and overall objective awareness than users holding high school or diploma level qualifications. Post hoc analysis also revealed that for privacy policy, benefits and risks in healthcare, and overall objective awareness, users with higher education (Master's degree or PhD) significantly had higher mean rank than users with bachelor's degree, p-value<0.005. Thus, users with higher education degrees had a better understanding of privacy policies, benefits, and risks related to healthcare services than those with a bachelor's degree.

Table 4.5: *Kruskal-Wallis test results for awareness vs. education*

	Mean Rank					Test Statistics[a]	
	Less than high school	High school or diploma	Bachelor degree	Higher education	Pharmacist fellowship	K-W	Sig.
Privacy Regulation	182.25	89.48	108.86	101.24	159.50	7.584	.108
Privacy Policy	167.00	153.12	188.29	224.42	320.00	23.060	<.001**
Benefit and Risk	288.75	199.61	201.32	183.46	97.50	4.664	.324
Benefit and Risk in Healthcare	217.75	156.63	187.92	224.25	132.50	19.276	<.001**
Objective Awareness	231.50	159.27	194.70	210.93	231.50	13.204	.010*
a. Kruskal Wallis Test b. Grouping Variable: Education *. Significant at 0.05 **. Significant at 0.01							

Table 4.6: *Post hoc multiple comparisons Mann-Whitney tests [education]*

Awareness	Category (J)	Category (Y)	Mean Rank Difference (J-Y)	M-W U	Sig.
Privacy Policy	Higher education	High school or diploma	31.12	2130.50	< .001*
		Bachelor degree	31.62	10681.50	.001*
Benefit and Risk in Healthcare	Higher education	High school or diploma	31.26	2125.00	< .001*
		Bachelor degree	30.97	10732.50	.002*
Objective Awareness	Higher education	High school or diploma	23.20	2422.00	< .001*
*. Significant at 0.005 [Bonferroni Corrected]					

4.3 Study 2 (The Experiment): An Empirical Investigation of Informed Consent for IoMT Services

Before starting the data analysis, the experimental data from the applications 'A' and 'B', the post-questionnaire and the semi-structured interview were collated. The data from the applications 'A' and 'B' were collected in Firebase and each participant's data had to be downloaded in a separate Excel file. Forty separate Excel files were downloaded and merged into one Excel file for import into an SPSS file for analysis. Also, the post-questionnaire results from Google Forms were downloaded in an Excel file for analysis. The semi-structured interview data from the audio recordings and notes taken when interviewing participants who did not consent to the voice recording were transcribed and filtered. Then, key themes were identified after carefully reading the interview texts. The data were categorised and organised in an Excel file because the number of participants was small and the interviews were short. Quantitative coding and analysis were performed for some questions that were considered quantitative, such as "Which consent mechanism do you prefer, 'A' or 'B' ?". The data from Firebase, post-questionnaire and semi-structured interviews, and data from Study 1 (objective and subjective privacy awareness level) were collected into a single Excel file and concatenated with the participant's ID recorded in Study 1. Then, the data was organised and coded to prepare it for analysis in Microsoft Excel and IBM SPSS (v.28).

4.3.1 Demographic Profile

A total of 40 participants completed the experiment, including 29 females (73.0%) and 11 males (28.0%) with an average age of 37.07 (with ages ranging from 19 to 62) years. Most participants (36; 90%) were from Jeddah, two (5%) were from Almadenah, one (3%) from Abha and one (3%) from Riyadh. Regarding their educational level, 48% of the participants held a Master's degree or PhD, 43% of them held a Bachelor's degree, and 10% were educated to high school or diploma level. These participants were recruited from Study 1 (The Survey) participants, and we used their data from Study 1 (The Survey) to examine and analyse the correlation between their privacy awareness situation and their decision-making and interactions when using the enhanced consent design. Table 4.7 illustrates the privacy awareness of each participant from Study 1 (The Survey). The Participant ID column contains the ID used to link the survey results to the experimental results. Figure 4.21 summarises the results from Study 1 (The Survey), displaying participants' subjective and objective privacy awareness, in which one represents low awareness, two represents medium awareness, and three represents high awareness. Approximately 40% of the participants in this study had low subjective privacy, 52.5% medium, and 7.5% high, whereas 25% of the participants had low objective privacy awareness, and 75% had medium privacy awareness. However, none had high objective awareness. Moreover, a paired-sample t-test was conducted to examine whether there were significant differences between the subjective and the objective assessment of participants' privacy awareness, indicating that there was no significant difference between the subjective ($M = 1.675$, $SD = 0.615$) and the objective ($M = 1.75$, $SD = 0.439$) assessment of the participants' privacy awareness ($t(39) = 0.771$, $p = .446$).

Table 4.7: *Participants' awareness situation that results from Study 1 (The Survey)*

	Participant ID	Subjective Awareness Level	Objective Awareness Level
1	U2	Medium	Medium
2	U4	Low	Low
3	U75	Low	Low
4	U65	Medium	Medium
5	U146	Medium	Medium
6	U44	Low	Low
7	U203	Low	Low
8	U11	Medium	Medium
9	U15	Low	Medium
10	U27	Low	Medium
11	U13	Medium	Medium
12	U171	Low	Medium
13	U48	Medium	Medium
14	U257	Low	Medium
15	U166	Medium	Low
16	U92	Medium	Medium
17	U93	Medium	Medium
18	U237	Medium	Low
19	U66	Low	Medium
20	U96	Medium	Medium
21	U147	Medium	Medium
22	U352	High	Medium
23	U130	Medium	Medium
24	U67	Low	Low
25	U52	High	Medium
26	U425	Low	Low
27	U40	Low	Medium
28	U205	Medium	Low
29	U172	Medium	Medium
30	U90	Medium	Medium
31	U308	Medium	Medium
32	U18	Medium	Medium
33	U87	Medium	Medium
34	U186	Low	Low
35	U28	Low	Medium
36	U31	Low	Medium
37	U324	Medium	Medium
38	U153	High	Medium
39	U185	Low	Medium
40	U132	Medium	Medium

Subjective_awareness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	16	40.0	40.0	40.0
	2.00	21	52.5	52.5	92.5
	3.00	3	7.5	7.5	100.0
	Total	40	100.0	100.0	

Objective Awareness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	10	25.0	25.0	25.0
	2	30	75.0	75.0	100.0
	Total	40	100.0	100.0	

Figure 4.21: *Participants' subjective and objective privacy awareness results from Study 1 (1=low, 2= medium, and 3=high)*

4.3.2 Within-subjects Experiment Results

In application 'A' (the control condition), which represents the control condition, the privacy policy can be accessed via links on the login page, main menu, and bottom of the main page. The privacy policy page is not mandatory for the participants to display. The application is designed to collect and register these links, click action, register the time spent on the page, and store this data on Firebase in real-time. The data collected indicated that none of the participants opened the privacy policy link on the login page, with only one participant opening the privacy policy link in the main menu and spending just 4 seconds there. Another participant opened the privacy policy link at the bottom of the main page and spent only 9 seconds. However, according to the read-o-meter online tool [1], the time estimated for reading the content of privacy policy page is 4 minutes, 50 seconds, which means that these participants did not read it. Thus, it can be concluded that none of the participants read the privacy policy when using the application 'A'. The participants spent an average time of 4 minutes and 29.25 seconds (SD = 05:47.57) in application 'A' to perform the tasks.

In application 'B' (the experimental condition), the privacy policy was designed differently from the traditional method. It was divided into eight sections that appeared to the participants in each task before they made a decision. Also, application 'B' was designed to collect and store data on user interactions, including click actions, time spent on each page, and time spent on each section of the privacy policy, all in real-time using Firebase.

In Task 1, the participants had to open and view all eight sections before being able to click on the agreement button to start the main healthcare service. Figure 4.22 illustrates the time spent by each participant in each section while performing Task 1. The top of the table includes the name of each section and the time needed to read it based on the read-o-meter online tool. As demonstrated in the table, mandatory opening and displaying of these sections enhances the chance of some participants to spend reasonable time reading the page content. However, some participants, such as U2, U4, U205, U172 and U153, spent only between 0 to 2 seconds in each section, indicating that they opened and clicked these sections to proceed to the next and finally start the healthcare service. During the semi-structured interview, participants U4 and U153 said they preferred application A because the tasks were performed in a shorter time compared

[1] https://niram.org/read/

to B. This was because B required opening the privacy policy sections in each task, which was considered time-wasting. Additionally, U4 articulated the view that the privacy policy sections should be optional for users to mitigate stress and fatigue. Conversely, U205 and U172 preferred the design and features of application 'B', but they disliked the necessity of individually opening each section, suggesting instead that the section buttons be visible before consent and made optional for opening. This explains why they navigated the sections very quickly. In the rest of the tasks (Task 2, Task 3, Task 4, and Task 5), the content of the sections 'Data Collection and Use', 'Data Access', 'Perceived Benefits and Potential Risks', and 'Withdrawal Procedure' differed based on the specific task case; thus each section had to be opened and viewed by participants to activate the decision buttons (accept and reject). However, the content of the sections, including 'Data Disclosure', 'External Links', 'Data Protection', and 'Data Storage and Processing', remained the same in all the tasks because these sections focus on aspects that apply to all cases. The average time in seconds needed to read each section was calculated using a read-o-meter. Figures 4.23,4.24,4.25 and 4.26 illustrate the time spent by each participant in each section while performing Task 2, Task 3, Task 4, and Task 5. Almost all participants did not open the section on data disclosure, external links, data protection, and data storage and processing because it was not mandatory, or they opened and skipped the sections when they found that they had the same content.

Table 4.8 presents an overview of the descriptive statistics for the time spent across the eight sections in all tasks from 1 to 5. 'Data Collection and Use' and 'Data Access', which were mandatory to be opened by the participants in all tasks and 'Data Disclosure', 'Data Protection' and 'External Links', which were mandatory to be opened only in Task 1 have a high SD (27.21, 17.93, 27.69, 23.91 and 9.96 respectively) compared to their means (23.62, 12.07, 25.05, 21.48 and 9.43 respectively), suggesting significant variability in the time participants spent in these sections and indicating variety in user behaviour when dealing with these sections. However, the 'Withdrawal Procedure', 'Data Storage and Processing' and 'Perceived Benefits and Potential Risks'sections have lower SD (7.30, 5.75, and 15.23 respectively) compared to their means (8.45, 5.85 and 15.60), indicating less variability in the time participants spent in these sections.

Task 1

	Sections	Data collection and use	Data access	Perceived benefits and potential risks	Withdrawal procedure	Data disclosure	External links	Data protection	Data storage and processing
	Estimated reading time in seconds	24	10	16	11	36	10	57	5
1	U2	2	0	2	1	2	1	2	1
2	U4	1	1	1	1	2	1	1	1
3	U75	25	6	33	10	45	33	65	8
4	U65	18	102	72	24	16	18	52	2
5	U146	10	2	9	1	20	32	56	5
6	U44	90	18	34	21	28	5	11	5
7	U203	45	9	21	17	23	23	30	5
8	U11	16	3	2	1	42	1	6	2
9	U15	23	16	14	10	13	2	4	3
10	U27	56	37	16	13	31	5	26	5
11	U13	33	25	37	12	82	21	56	9
12	U171	10	2	2	2	2	2	4	2
13	U48	5	5	4	5	7	3	8	2
14	U257	6	6	5	2	3	2	4	2
15	U166	12	6	12	11	8	2	7	3
16	U92	9	5	4	2	3	1	2	3
17	U93	3	2	4	1	9	1	4	2
18	U237	7	15	20	27	7	15	6	28
19	U66	47	54	16	24	31	21	22	14
20	U96	8	4	10	4	27	13	24	7
21	U147	58	13	25	11	87	36	51	15
22	U352	5	8	2	5	8	3	11	4
23	U130	62	18	10	12	31	14	7	3
24	U67	10	7	7	4	3	1	4	2
25	U52	135	6	13	5	18	5	16	15
26	U425	13	10	2	1	1	3	4	1
27	U40	14	8	15	11	20	9	7	4
28	U205	1	2	1	1	2	1	2	1
29	U172	1	1	1	1	1	1	2	1
30	U90	31	9	40	15	74	13	51	13
31	U308	3	3	11	2	2	7	3	8
32	U18	21	17	19	14	53	10	53	12
33	U87	45	22	31	16	127	26	105	14
34	U186	35	5	25	7	22	11	29	7
35	U28	3	4	12	2	20	1	10	1
36	U31	14	4	10	7	44	11	50	4
37	U324	16	8	13	13	44	1	10	5
38	U153	2	1	1	1	1	1	2	1
39	U185	24	11	49	9	20	14	20	13
40	U132	26	8	19	12	23	7	32	1
	Average time in seconds	23.625	12.075	15.6	8.45	25.05	9.425	21.475	5.85

Figure 4.22: *The time spent by each participant in each section of the privacy policy for Task 1 in application 'B'*

Task 2

	Sections	Data collection and use	Data access	Perceived benefits and potential risks	Withdrawal procedure	Data disclosure	External links	Data protection	Data storage and processing
	Estimated reading time in seconds	33	8	17	14	36	10	57	5
1	U2	2	1	1	9	5	1	2	1
2	U4	2	1	1	1	0	0	0	0
3	U75	2	1	1	1	7	0	3	1
4	U65	3	2	2	1	0	0	0	0
5	U146	9	1	5	1	1	1	3	1
6	U44	10	9	21	3	1	0	2	0
7	U203	4	4	3	5	10	0	2	0
8	U11	2	3	2	1	0	0	0	0
9	U15	2	1	2	1	5	0	0	0
10	U27	11	1	3	2	0	0	3	0
11	U13	31	9	12	7	0	0	0	0
12	U171	1	1	3	1	0	0	0	0
13	U48	2	1	3	1	6	0	2	0
14	U257	6	4	5	4	0	0	0	0
15	U166	13	6	13	3	4	0	7	0
16	U92	2	1	2	1	1	0	0	0
17	U93	20	16	24	13	46	0	0	0
18	U237	10	6	13	7	0	0	0	0
19	U66	3	1	2	1	14	0	0	0
20	U96	17	4	4	5	0	0	0	0
21	U147	42	8	8	7	42	0	16	3
22	U352	2	1	3	2	3	0	0	0
23	U130	4	1	4	16	1	0	0	0
24	U67	1	3	3	14	0	0	0	0
25	U52	13	5	4	5	9	0	8	0
26	U425	1	1	2	1	0	0	0	0
27	U40	3	1	1	30	5	0	0	0
28	U205	1	3	3	1	3	4	2	2
29	U172	1	1	3	1	1	1	2	1
30	U90	43	8	42	23	21	13	19	15
31	U308	1	3	6	2	6	2	8	2
32	U18	4	6	13	5	30	2	0	0
33	U87	36	12	98	15	14	0	29	2
34	U186	7	2	7	6	1	0	0	0
35	U28	9	5	8	43	2	0	2	1
36	U31	7	2	2	3	9	1	6	1
37	U324	5	1	2	2	3	0	0	0
38	U153	1	1	1	1	1	0	0	0
39	U185	5	14	7	11	3	2	4	0
40	U132	24	1	14	13	0	0	0	0
	Average time in seconds	9.05	3.8	8.825	6.725	6.35	0.675	3	0.75

Figure 4.23: *The time spent by each participant in each section of the privacy policy for Task 2 in application 'B'*

Task 3

Sections		Data collection and use	Data access	Perceived benefits and potential risks	Withdrawal procedure	Data disclosure	External links	Data protection	Data storage and processing
Estimated reading time in seconds		30	9	15	11	36	10	57	5
1	U2	5	9	10	5	2	1	4	1
2	U4	1	1	2	1	0	0	0	0
3	U75	2	7	3	2	0	0	0	0
4	U65	1	1	0	1	1	0	0	0
5	U146	5	1	67	1	0	0	0	0
6	U44	39	72	25	23	0	0	0	0
7	U203	2	1	4	2	0	0	0	0
8	U11	1	11	5	6	0	0	2	1
9	U15	4	1	1	1	0	0	0	0
10	U27	28	17	10	9	0	0	0	0
11	U13	9	17	17	7	0	0	0	0
12	U171	6	6	5	5	0	0	0	0
13	U48	2	1	1	2	0	0	0	0
14	U257	6	3	5	8	0	0	0	0
15	U166	3	6	1	4	0	0	0	0
16	U92	0	0	1	0	0	0	0	0
17	U93	4	1	3	5	4	0	0	0
18	U237	7	4	10	6	0	0	0	0
19	U66	1	21	1	1	0	0	0	0
20	U96	8	9	8	5	0	0	0	0
21	U147	8	9	19	11	0	0	0	0
22	U352	2	1	2	2	0	0	0	0
23	U130	6	1	3	3	0	0	0	0
24	U67	7	5	5	1	0	0	0	0
25	U52	6	10	13	6	0	0	0	0
26	U425	6	1	1	5	0	0	0	0
27	U40	1	1	1	1	0	0	0	0
28	U205	2	1	1	1	1	1	2	1
29	U172	1	1	1	1	0	1	2	1
30	U90	56	10	92	14	49	7	19	1
31	U308	7	8	44	3	4	0	0	0
32	U18	22	23	13	7	0	0	0	0
33	U87	15	154	9	30	0	0	0	0
34	U186	2	2	2	7	0	0	0	0
35	U28	2	1	8	6	0	0	0	0
36	U31	2	13	4	1	2	0	3	0
37	U324	23	8	10	7	0	0	0	0
38	U153	1	1	1	1	0	0	0	0
39	U185	5	6	0	1	0	0	0	0
40	U132	33	2	1	2	0	0	0	0
	Average time in seconds	8.525	11.175	10.225	5.1	1.575	0.25	0.8	0.125

Figure 4.24: *The time spent by each participant in each section of the privacy policy for Task 3 in application 'B'*

Task 4

	Sections	Data collection and use	Data access	Perceived benefits and potential risks	Withdrawal procedure	Data disclosure	External links	Data protection	Data storage and processing
	Estimated reading time in seconds	36	7	13	15	36	10	57	5
1	U2	2	1	1	2	0	0	0	0
2	U4	2	2	1	2	0	0	0	0
3	U75	4	6	1	1	0	0	0	0
4	U65	3	1	1	1	0	0	0	0
5	U146	3	1	4	2	0	0	0	0
6	U44	24	9	9	16	0	0	0	0
7	U203	2	11	9	5	0	0	0	0
8	U11	3	1	2	1	0	0	0	0
9	U15	1	1	1	1	0	0	0	0
10	U27	16	11	3	2	0	0	0	0
11	U13	17	9	5	25	0	0	2	0
12	U171	17	7	6	11	0	0	0	0
13	U48	3	1	1	3	0	0	0	0
14	U257	2	1	8	2	0	0	0	0
15	U166	3	8	4	3	0	0	0	0
16	U92	9	10	6	1	0	0	0	0
17	U93	14	11	19	9	0	0	0	0
18	U237	11	2	26	6	0	0	0	0
19	U66	1	1	1	1	0	0	0	0
20	U96	14	5	4	9	0	0	0	0
21	U147	24	12	8	12	0	0	0	0
22	U352	5	1	2	4	0	0	0	0
23	U130	2	4	3	2	8	0	4	13
24	U67	2	2	2	1	0	0	0	0
25	U52	7	10	10	9	0	0	4	0
26	U425	2	1	0	1	0	0	0	0
27	U40	1	1	2	3	0	0	0	0
28	U205	1	1	1	1	1	1	3	1
29	U172	1	1	1	2	0	1	2	1
30	U90	21	16	18	20	3	1	4	2
31	U308	40	10	6	8	0	0	0	0
32	U18	20	7	7	4	0	0	0	0
33	U87	3	8	5	11	0	0	0	0
34	U186	7	2	2	1	0	0	0	0
35	U28	12	5	3	3	0	0	0	0
36	U31	4	8	2	1	0	0	0	0
37	U324	7	8	5	1	0	0	0	0
38	U153	1	1	0	1	0	0	0	0
39	U185	2	1	0	1	0	0	0	0
40	U132	24	45	1	13	0	0	2	0
	Average time in seconds	8.425	6.075	4.75	5.05	0.3	0.075	0.525	0.425

Figure 4.25: *The time spent by each participant in each section of the privacy policy for Task 4 in application 'B'*

Task 5

	Sections	Data collection and use	Data access	Perceived benefits and potential risks	Withdrawal procedure	Data disclosure	External links	Data protection	Data storage and processing
	Estimated reading time in seconds	44	7	10	16	36	10	57	5
1	U2	1	1	1	2	0	0	0	0
2	U4	1	1	1	2	0	0	0	0
3	U75	3	1	1	1	0	0	0	0
4	U65	1	1	0	0	0	0	0	0
5	U146	1	1	3	1	0	0	0	0
6	U44	6	23	12	21	0	0	0	0
7	U203	4	8	2	5	0	0	0	0
8	U11	2	1	2	2	0	0	0	0
9	U15	1	1	1	1	0	0	0	0
10	U27	14	8	2	2	0	0	0	0
11	U13	15	11	33	13	0	0	0	0
12	U171	1	1	2	2	0	0	0	0
13	U48	1	1	1	1	0	0	0	0
14	U257	2	2	1	1	0	0	0	0
15	U166	7	6	8	3	0	0	0	0
16	U92	1	1	0	1	0	0	0	0
17	U93	24	18	51	18	0	2	0	0
18	U237	38	1	4	3	0	0	0	0
19	U66	1	1	2	1	0	0	0	0
20	U96	15	3	6	3	0	0	0	0
21	U147	6	6	11	10	0	0	0	0
22	U352	3	1	2	2	0	0	0	0
23	U130	5	11	8	25	0	0	0	0
24	U67	4	0	1	1	0	0	0	0
25	U52	7	6	19	19	0	0	0	0
26	U425	0	1	0	1	0	0	0	0
27	U40	1	1	1	1	0	0	0	0
28	U205	1	1	1	1	1	1	2	1
29	U172	1	1	1	1	0	1	2	1
30	U90	7	8	23	14	4	3	5	2
31	U308	14	10	7	1	0	0	0	0
32	U18	11	7	16	7	0	0	0	0
33	U87	62	1	4	2	0	0	0	0
34	U186	4	8	4	4	0	0	0	0
35	U28	1	1	3	3	0	0	0	0
36	U31	1	4	11	2	0	0	0	0
37	U324	2	7	14	3	0	0	0	0
38	U153	3	5	1	7	0	0	0	0
39	U185	2	1	1	2	1	0	0	0
40	U132	1	2	1	1	0	0	0	0
	Average time in seconds	6.875	4.325	6.55	4.75	0.15	0.175	0.225	0.1

Figure 4.26: *The time spent by each participant in each section of the privacy policy for Task 5 in application 'B'*

Table 4.8: *Descriptive statistics for the time spent on each section in application 'B'*

Section	Count	Mean	Std Dev	Min	25%	50%	75%	Max	Range	Variance
Data collection and use	40.00	23.62	27.21	1.00	5.75	14.00	31.50	135.00	134.00	740.60
Data access	40.00	12.07	17.93	0.00	3.75	6.50	13.50	102.00	102.00	321.66
Perceived benefits and potential risks	40.00	15.60	15.23	1.00	4.00	12.00	20.25	72.00	71.00	231.94
Withdrawal procedure	40.00	8.45	7.30	1.00	2.00	7.00	12.25	27.00	26.00	53.33
Data disclosure	40.00	25.05	27.69	1.00	3.00	20.00	31.00	127.00	126.00	766.97
External links	40.00	9.43	9.96	1.00	1.00	5.00	14.00	36.00	35.00	99.28
Data protection	40.00	21.48	23.91	1.00	4.00	10.00	30.50	105.00	104.00	571.74
Data storage and processing	40.00	5.85	5.75	1.00	2.00	4.00	8.00	28.00	27.00	33.11

However, in application 'B', the participants spent an average of 18 minutes and 41.20 seconds (SD = 19:08.91) throughout using the mechanism. The difference in time spent on the two mechanisms, 'A' and 'B', was statistically significant, as determined by a paired-sample t-test (t (39) = -5.118). Only 27.% (11) of the participants opened the external link that directs the participants to the personal data regulation in Saudi Arabia in application 'B'. The average time spent on the page was 31.8 seconds but the text in the personal data regulation web page is too long (16 pages). Thus, these results indicate that none of the participants read the content.

In application 'A' (the control condition), most participants accepted most requests when performing the tasks, although they spent little time on them. Task 2 and Task 4 had the highest rate of requests acceptance, with 92.5% of participants accepting, followed by Task 3 request with 80% acceptance, and Task 5 request with 70% acceptance. In application 'B' (the experimental condition), the request of Task 2 had the highest rate of acceptance, with 97.5% of participants accepting it, followed by Task 4 request with a 92.5% acceptance rate, Task 3 request with 87.5% acceptance rate, and Task 5 request with a 75% acceptance rate. As the results show, the most accepted request by the participants in both 'A' and 'B' conditions was the request in Task 2, which focused on a new main service from the service provider (offer from the Remote Patient Services department in the hospital to provide you with an Advanced Early Disease Detection Service to predict many types of diseases). This was followed by the request in Task 4, which focuses on a request from a third party to use the data for secondary purposes, that is, research to benefit public health (a request from the Research Centre at King Abdulaziz University (KAU) to use collected data in research). There are several reasons why participants may accept these two requests more than the others, such as the perceived benefits. The request in Task 2 offers personal benefit, a new service of advanced health monitoring that can be convenient and efficient, while the request in Task 4 benefits society's public health.

Hypotheses Testing Results

According to the experimental scenario (Section 3.5.1), all participants were required to accept the request in Task 1 and subscribe to the IoMT main service in both 'A' (the control condition) and 'B' (the experimental condition). This task focused on measuring the level of informedness, i.e., whether the participants agreed to the service with full knowledge and comprehension of all pertinent information. A variable was created for each of the tasks to test the hypotheses developed in Section 3.5.2, which indicates whether the user displayed the same behaviour in applications 'A' and 'B' (marked with 0) or if they changed their behaviour (marked with 1). The mean of those variables was then used to indicate the proportion of participants who changed their behaviour between the two conditions, and those proportions were tested against 0 using a one-sample t-test. The results were as follows:

- **Ha:** There is (Ha0) no difference, (Ha1) a significant difference, in the participants' decision regarding the request in Task 2 between conditions 'A' and 'B'. The one-sample t-test showed that the proportion of participants who changed their decision regarding the request in Task 2 between conditions 'A' and 'B' ($M = 0.05$, $SD = 0.221$) is not significantly different from 0, $t\ (39) = 1.433$, $p = 0.16$. Therefore, the null hypothesis could not be rejected and the study hypothesis was not supported. The findings indicate that there is no significant difference in the proportion of participants who changed their decision regarding the request in Task 2 between conditions 'A' and 'B'.

- **Hb:** There is (Hb0) no difference, (Hb1) a significant difference, in the participants' decision regarding the request in Task 3 between conditions 'A' and 'B'. The one-sample t-test showed that the proportion of participants who changed their decision regarding the request in Task 3 between conditions 'A' and 'B' ($M = 0.18$, $SD = 0.385$) is significantly different from 0, $t\ (39) = 2.876$, $p = 0.006$. Therefore, the null hypothesis was rejected, and the study hypothesis was supported. The findings indicate that there is a significant difference in the proportion of participants who changed their decision regarding the request in Task 3 between conditions 'A' and 'B'.

- **Hc:** There is (Hc0) no difference, (Hc1) a significant difference, in the participants' decision regarding the request in Task 4 between conditions 'A' and 'B'. The one-sample t-test showed that the proportion of participants who changed their decision regarding the request in Task 4 between conditions 'A' and 'B' ($M = 0.05$, $SD = 0.221$) is not significantly different from 0, $t\ (39) = 1.433$, $p = 0.16$. Therefore, the null hypothesis could not be rejected and the study the hypothesis was not supported. The findings indicate that there is no significant difference in the proportion of participants who changed their decision regarding the request in Task 4 between conditions 'A' and 'B'..

- **Hd:** There is (Hd0) no difference, (Hd1) a significant difference, in the participants' decision regarding the request in Task 5 between conditions 'A' and 'B'. The one-sample t-test showed that the proportion of participants who changed their decision regarding the request in Task 5 between conditions 'A' and 'B' ($M = 0.2$, $SD = 0.405$) is significantly different from 0, $t\ (39) = 3.122$, $p = 0.003$. Therefore, the null hypothesis was rejected, and the study hypothesis was supported. The findings indicate that there is a significant difference in the proportion of participants who changed their decision regarding the request in Task 5 between conditions 'A' and 'B'.

The results suggest that the features of the enhanced design of the consent mechanism for IoMT services, which were represented in application 'B', significantly affected participants' decisions regarding the requests in Task 3 and Task 5. Moreover, it can be observed that the acceptance rates for requests in Tasks 3 and 5 are higher in 'B' compared to 'A', suggesting that the enhanced design of the application 'B' has affected participants' decisions. In Task 3, the same service provider who offered the participant the main service, basic vital signs monitoring service, requested to use his/her data for secondary purposes with an educational aim. Regarding Task 5, the requester was a third party (pharmaceutical company), and their purpose for using the data was a secondary but with a commercial aim. Thus, based on the findings, it can be concluded that most of the participants tend not to share their data for secondary purposes, as evidenced by condition 'A' results. However, once the participants read and understood the provided information on how their data will be used, for how long, and the associated benefits, risks, and withdrawal procedures in the privacy policy sections, they became more willing to accept such requests, as evidenced by the results of condition 'B'. These results highlight the importance of systems transparency. Providing comprehensive information about data collection and sharing practices assists users in making informed decisions about their data privacy and increases their engagement.

In order to test hypothesis (**He**), a new variable was calculated. This new variable indicated the number of tasks on which a participant changed their behaviour from the application 'A' to 'B'. Then, an independent sample t-test was utilised to determine if there was a difference in the average number of tasks on which a user changed their behaviour, depending on each participant's objective privacy awareness level.

- **He:** There is (He0) no relation (He1) a significant relation between objective privacy awareness level and changing participants' decision of the requests between conditions 'A' and 'B'. The independent samples t-test showed that there were no significant differences in the number of tasks on which participants changed their decisions between the low objective awareness (M = 0.3, SD = 0.68) and the medium objective awareness (M = 0.53, SD = 0.92) group, t (38) = -0.811, p = 0.422.

Therefore, the null hypothesis cannot be rejected, and the study hypothesis was not supported. The results revealed that participants' privacy awareness level (objective) had no relation with changing their decisions regarding the requests between conditions 'A' and 'B'. This means that the features of the enhanced design of the consent mechanism have the same effect on participants with low and medium privacy awareness.

4.3.3 Post-experiment Questionnaire Results

The post-questionnaire designed to test the hypotheses regarding how each factor assesses participants in making informed decisions included questions that were answered on a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) (see Section 3.5.2). Almost all participants agreed or strongly agreed that most features of the consent tool for IoMT services assisted them in making informed decisions, except the link to data protection laws and regulations, which only 22 participants saw and assessed. Moreover, only five evaluated the video.

The results indicate that 97.5% of the respondents found it helpful to display the privacy policy sections before making any decision, enabling them to make informed decisions. Similarly, 97.5% of the respondents found it helpful to explicitly indicate the security and privacy measures used to protect their data. Furthermore, an explicit section on the withdrawal procedure was found to be helpful for 97.5% of the respondents to make an informed decision. Also, 95% of the respondents agreed that explaining the benefits and potential risks of accepting a service or request helped them make informed decisions. Similarly, 92.5% of the respondents agreed that displaying a privacy policy in sections focusing only on the service or request that they are dealing with helped them make an informed decision. Lastly, 90% of the respondents agreed

that questions assessing their understanding before accepting a service or request helped them make an informed decision (see Figure 4.27). Since the Likert scale ranged from 1 to 5, a cut-off value of 4 was used to determine the importance of a factor. If an item had an average answer of four or higher, it was concluded that the participants considered the factor to be significant. A series of one-sample t-tests were performed to assess how useful the participants found each of the factors in helping them make an informed decision. The results of these tests are presented in Table 4.9. However, only 22 participants evaluated the link to data protection laws and regulations that govern personal data in Saudi Arabia, and they did not find it significantly informative. Regarding using icons (especially private icons) to visually represent parts and sections, the results suggest some level of supporting the hypothesis and further investigation is required to determine its efficacy. Only five participants watched the videos explaining some points, such as service or request information, and they all found them helpful. However, 35 participants did not engage with the video links; thus, the result is not statistically significant.

4.3.4 Semi-structured Interview Results

Participants were asked about which consent mechanism they prefer, 'A' or 'B'. Out of all the participants, only 12.5% (five) chose mechanism 'A', while 87.5% of the participants opted for mechanism 'B'. When we asked them why they preferred 'A', all five participants stated that they liked 'A' because the process of performing the tasks consumed less time. However, according to the results of the within-subject experiment, none of them read the privacy policy in 'A'. Additionally, two participants said that 'A' not only took a short time but was easy to use. This behaviour can be attributed to various factors, one of which is their level of awareness of privacy as three of them have low objective privacy awareness, while two have medium objective privacy awareness. (These participants were part of Study 1 (The Survey), and their data was extracted.)

Regarding mechanism 'B', most participants (65%) preferred it because the information they needed to decide on their data (privacy policy) was well organised and divided into sections rather than one piece of text. Most of these participants found that dividing the privacy policy into smaller sections makes its structure clear and logical, enhances its readability and accessibility and helps users navigate and understand the information more easily. Also, one participant said it allowed him to select and read first the sections that were of particular interest to him. Also, some participants (32.5%) found that mechanism 'B' was visually clear and comfortable for the eyes because the privacy policy was divided into sections where each section button had an icon that illustrated the section content. Some participants (27.5%) stated that they liked that the privacy policy information provided directly before making a decision makes it more manageable to read and understand. One of them said, "I can make a decision with all the necessary information still in mind". Displaying the mandatory privacy policy helps achieve system transparency and enhances users' chance to read it and make informed choices. Few participants (10%) found that the process of mandatory opening each section in the privacy policy to be able to click on the decisions buttons motivated them to read and make informed decisions. The reasons for mechanism 'B' being the most preferred are outlined in Figure 4.28.

The participants, including those who preferred mechanism 'A', were asked to choose the top three features that helped them make informed decisions about their data when they used mechanism 'B'. The results show that the top feature was to have the privacy policy divided into small sections instead of one long text on one page (57.5%). The second most preferred feature was a clear explanation of the benefits that they would gain from accepting a service or request (52.5%). The third most preferred feature was a clear explanation of the potential risks that could occur from accepting such a service or request (47.5%). The next most preferred feature was mandatory access to the privacy policy section instead of having optional links (30.0%), followed by questions that assess the understanding of the policy, explaining the withdrawal

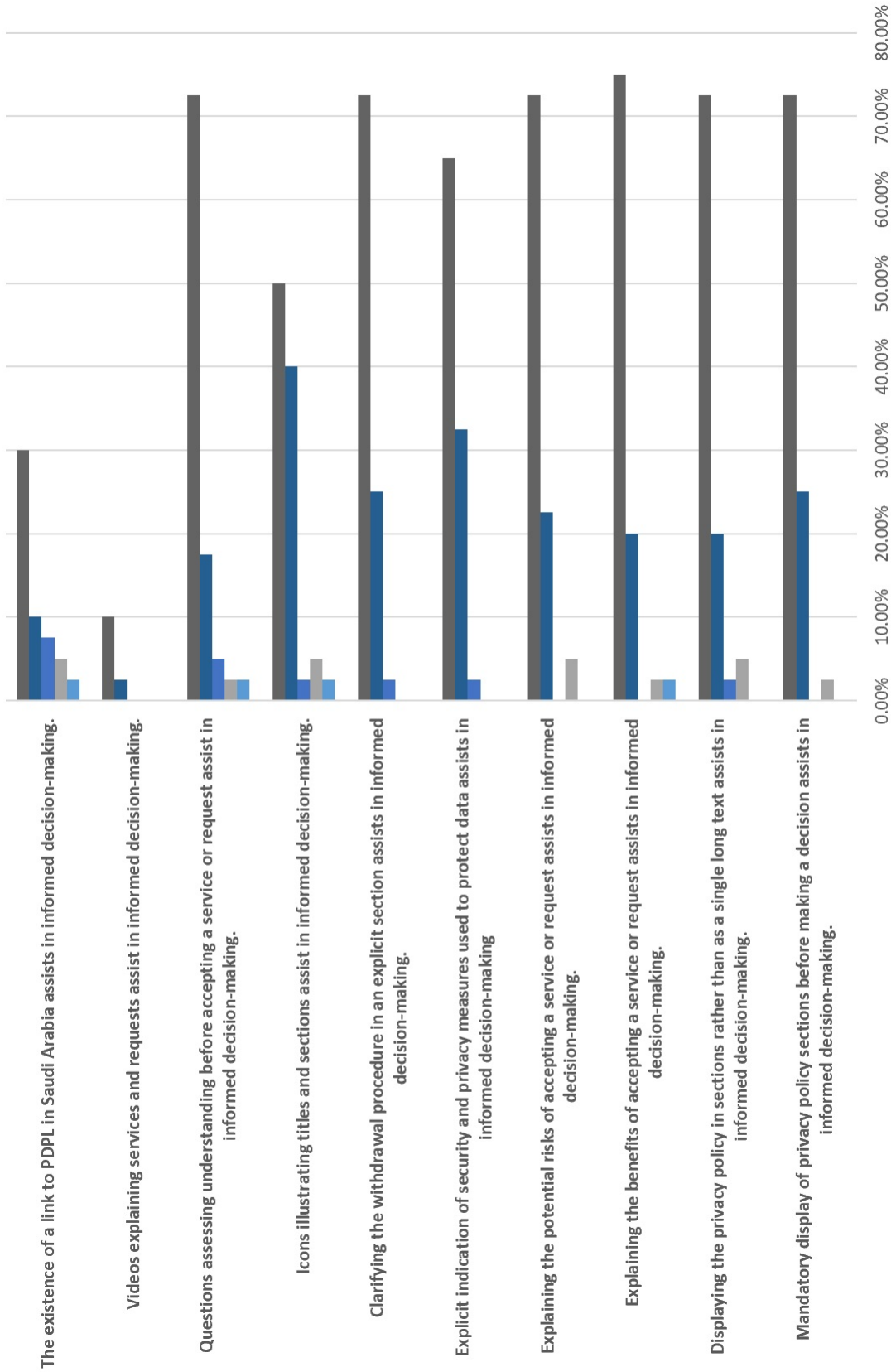

Figure 4.27: *Participants' evaluation of consent tool features for IoMT services in assisting informed decision making*

Table 4.9: *Post-experiment questionnaire hypothesis testing results*

The Hypothesis	N	M	SD	t	df	p	Result
Ha: link to data protection laws and regulations that govern personal data in Saudi Arabia **(Ha0)** have no role, **(Ha1)** have a role in helping the user to provide his/her informed decision.	22	4.09	1.23	0.346	21	0.732	-
Hb: The Mandatory access to privacy policy instead of depend having optional links **Hb0** has no role **Hb1** has a role in helping the user to provide his/her informed decision.	40	4.68	0.62	6.936	39	0.000	+
Hc: Dividing the privacy policy into small parts instead of one long text on one page **(Hc0)** has no role **(Hc1)** has a role in helping the user to provide his/her informed decision.	40	4.60	0.78	4.878	39	0.000	+
Hd: displaying and clarifying the benefits that users will gain from accepting a request or service in a separate section **(Hd0)** has no role **(Hd1)** has a role in helping the user provide his/her informed decision.	40	4.63	0.84	4.718	39	0.000	+
He: displaying and clarifying the potential risk that could occur when accepting a request or service in a separate section **(He0)** has no role **(He1)** has a role in helping the user provide his/her informed decision.	40	4.63	0.74	5.339	39	0.000	+
Hf: Clarification of the withdrawal procedure in an explicit section Hf: Withdrawal procedure clarification **(Hf0)** has no role **(Hf1)** has a role in helping the user to provide his/her informed decision.	40	4.70	0.52	8.573	39	0.000	+
Hg: Explicit indication of privacy and security measure **(Hg0)** has no role **(Hg1)** has a role in helping the user to provide his/her informed decision.	40	4.63	0.54	7.319	39	0.000	+
Hh: using icons (especially private icons) to visually represent parts and sections **(Hh0)** has no role **(Hh1)** has a role in helping the user to provide his/her informed decision.	40	4.30	0.94	2.020	39	0.050	∼
Hi: using videos to explain some points such as service or request information **(Hi0)** has no role **(Hi1)** has a role in helping the user to provide his/her informed decision.	5	4.80	0.45	4.000	4	0.016	+ (The responses number is too small for statistical significance)
Hj: Questions to assess user understanding **(Hj0)** has no role **(Hj1)** has a role in helping the user to provide his/her informed decision.	40	4.55	0.90	3.846	39	0.000	+
N = number of participants, M = mean, SD = standard deviation, t = t statistic, df = degrees of freedom, p = probability of type I error, + = hypothesis supported, ∼ = hypothesis marginally supported, - = hypothesis not supported.							

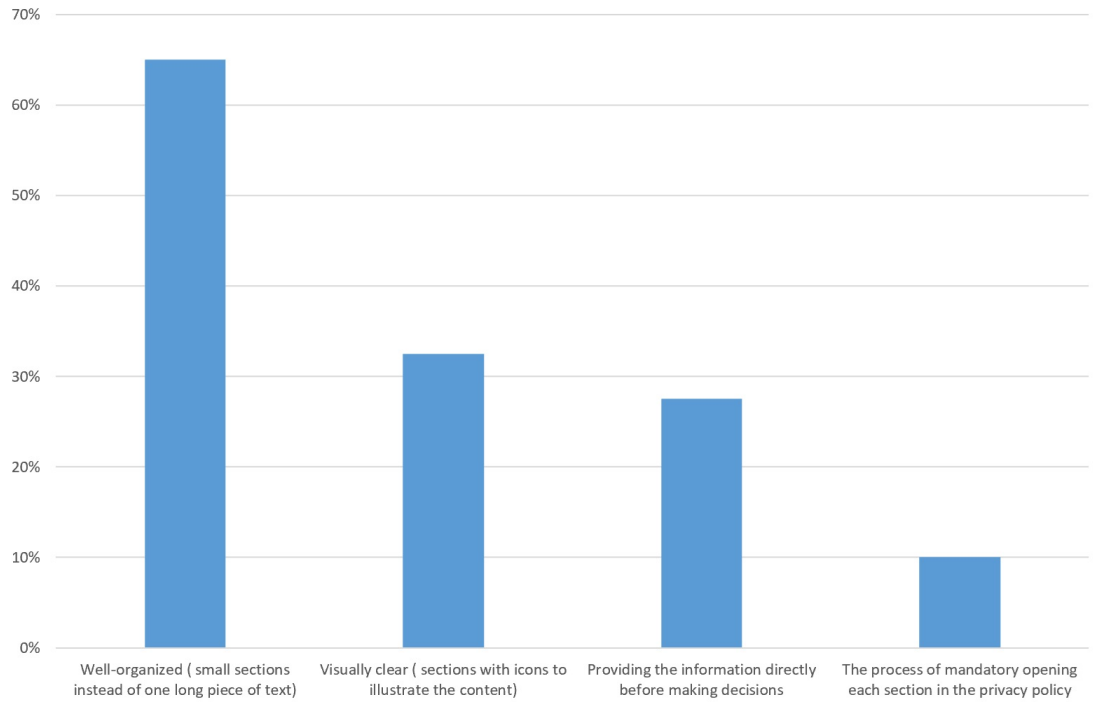

Figure 4.28: *Participants' reasons for 'B' being the most preferred*

procedure and the explicit indication of security and privacy measures (25.0%). After that, the link to data protection laws and regulations that govern personal data in Saudi Arabia (22.5%). Then, the icons that illustrate titles and sections (12.5%). The videos (2.5%) were considered the least important feature as many participants did not see these video links as they stated in the interview. Table 4.10 shows features that assist users in making an informed decision ranked by their importance.

Most participants preferred to have the privacy policy divided into smaller sections instead of one long text on a single page. When asked why, most agreed that this technique, where each section addresses specific aspects such as data collection, data usage, benefits and risk, makes the information well-organised and easy to read, helping them to understand one aspect at a time. This improves their comprehension, allows them to make informed decisions, and enhances their awareness regarding their data. Some participants say that explaining the benefits they may gain if they accept a service or a request can positively impact their decision, mainly if they are uncertain about their decision. Participants suggest that focusing on the positive aspects of accepting the request can help them be more confident about their decision. Additionally, clarifying the risks can make them more aware of the potential consequences. Most participants who choose these two factors together believe that explaining the benefits and risks can provide a more balanced and informed understanding of the situation and enable individuals to make better decisions.

When the participants were asked about the factors that were not useful in helping them make informed decisions, most participants (67.5%) responded that the videos that explained services and requests were not helpful. Many participants did not see the video links, while some saw them but did not watch the videos because it was time-consuming. One participant said she/he was not interested in watching the video because the text was clear enough. Moreover, 32.5% of participants found the questions that assessed their understanding were not helpful. Some of these participants believed understanding information does not necessarily mean remembering it to answer questions. Others found it time-consuming, while some participants said they would select answers randomly, possibly hitting upon the correct ones by coincidence. Some participants (27.5%) found that a link to data protection laws and regulations governing

Table 4.10: *Features that assist users in making an informed decision ranked by percentage*

The Features	The Percentage
Dividing the privacy policy into small sections instead of one long text on one page (focusing only on the service or request)	57.5%
Explaining the benefits which I will be gained from accepting a service or request	52.5%
Explaining the potential risk that could occur from accepting a service or request	47.5%
Mandatory access to privacy policy instead of having optional links	30.0%
Questions that assess the understanding	25.0%
Clarifying the withdrawal procedure in an explicit section	25.0%
Explicit indication of security and privacy measures	25.0%
The existence of a link to data protection laws and regulations that govern personal data in Saudi Arabia	22.0%
Icons that illustrate titles and sections	12.5%
Videos that explain services and requests	2.5%

personal data in Saudi Arabia did not help make informed decisions. Some of them mentioned that the text was too long and complicated, while two participants believed that the existence of a link to the protection law had a negative impact. Furthermore, one participant stated that external links are usually ignored. Some participants (20.0%) said that they found the mandatory display of privacy policy sections not helpful in making informed decisions. Most of them suggested that just making the privacy policy easily accessible, dividing it into sections, and appearing before making a decision is sufficient. They believed that forcing engagement by design was unnecessary. A few participants (12.5%) found the icons illustrating titles and sections not useful, and they did not attract their attention. These participants were asked if they think the features of the enhanced design of the consent mechanism help to increase privacy awareness. Of the participants, 87.5 % believe that if most of these features are present together, they could improve their privacy awareness and help promote public privacy awareness in the future.

Many participants agreed that most features assist them in reading and understanding all the information they need before making a decision, which raises their privacy awareness. Most participants found that dividing the privacy policy into smaller sections focusing only on the service or the request helps deliver the information more effectively and enhances privacy awareness. A participant reported that having sections instead of one long text encourages them to read, which can help raise their awareness, especially if they do not have technical experience. Another participant stated, “Explaining the potential risk that could occur from accepting a service or request makes me aware of the privacy problems that I and other users may face when disclosing such data, which increases privacy awareness”. Moreover, repeating the process of reading the privacy policies sections every time they need to make a decision helps to increase privacy awareness. One participant expressed a different opinion that these factors may help to raise awareness among certain groups, such as people who like to read, but for people who are not accustomed to technology, such as the elderly, it may be tiring for them and not useful. On the other hand, one participant did not agree that these factors can help to enhance privacy awareness and said, “People who used to not read privacy policy will still skip pages and sections without reading or understanding them”. Another participant stated, “These factors cannot enhance privacy awareness alone. They must be integrated with other strategies such as such as campaigns”.

A participant discussed the fact that many people don't take the time to read privacy policies and terms and conditions when using various applications, even if the data being used is sensitive, and it is important to start finding solutions. However, three participants found it beneficial to display the sections and information before making a decision directly. There is no need to make it mandatory for these sections to be opened and viewed. The questions that assess users' understanding can demonstrate that they have understood.

4.4 Significant Findings Form Study 1 and Study 2

This section discusses the significant findings and insights obtained from Study 1 and Study 2.

4.4.1 Subjective and Objective Medium Level of Privacy Awareness

As discussed in Study 1 (The Survey), two types of assessments, subjective and objective, were used to investigate the privacy awareness of digital healthcare service users. Subjective assessments typically involve self-reported measures, where individuals rate their privacy awareness or knowledge. In contrast, objective assessments may involve questions or tests of individuals' actual knowledge and understanding. The results show no significant difference between subjective and objective assessments, with most participants exhibiting a medium level of privacy in both. This suggests that participants' self-assessment of privacy awareness aligns with their objective privacy knowledge.

Moreover, most participants have a reasonable insight into their privacy awareness. In addition, the medium level of objective privacy awareness indicates that these participants have a basic understanding of privacy awareness. However, this also raises concerns about potential gaps in these participants' comprehension, suggesting a need to enhance users' privacy awareness for services that gather sensitive data. Moreover, the survey results are consistent with a recent survey conducted by Alghamdi et al. (2023) in Saudi Arabia to assess users' awareness of privacy and their ability to protect themselves from online threats while sharing sensitive information. They utilised an online questionnaire which included 26 questions (Likert scale and yes/no). They found that the average score for mobile operating system privacy awareness was 51%, with Apple IOS users (46%) scoring lower than Android users (53%). Their study involved only 66 computer science students; thus, their findings potentially do not reflect the entire population due to the limited diversity in their study sample. In contrast, our study (Study 1, section 4.2) had a larger sample size of 390 participants from diverse educational backgrounds. Nonetheless, the results of these studies were consistent with our findings.

4.4.2 Decision-making in IoMT Systems

In Study 2 (The Experiment), a within-subject experiment was conducted, and participants' decisions regarding disclosing their data in IoMT hypothetical scenarios were captured using two applications: application 'A' (the control condition) and application 'B' (the experimental condition). Figure 4.29 illustrates the decision-making process conducted by the participant using a hypothetical scenario while performing the tasks in conditions 'A' and 'B'. Based on the experiment results, in both the control condition 'A' and the experimental condition 'B', the request in Task 2 was found to have the highest acceptance rate among users with all levels of privacy awareness, followed by the request in Task 4. See Table 3.3 for more details about the tasks. These findings indicate that most participants made consistent decisions regarding the requests in these two tasks. In Task 2, the requester of the data was the same service provider (the hospital supervised by the Ministry of Health) who provided the user with the main service that they accepted in Task 1; they needed the data to provide the participant with a new main service. This agrees with Moon (2017) findings that one factor that affects users' willingness to share their data is trust in the service provider and its ability to apply data

security measures. Furthermore, study 2 (The Experiment) results suggest that participants are willing to share their data in some cases when they know the requester's name and purpose, even if they are not informed about all the details, such as in Task 4. During the semi-structured interview, one participant stated, "I am willing to share my information as long as it is supervised by the Ministry of Health". Regarding Task 4, the requester of the data was a third party (Kau Research Centre) that needed to use it for a secondary purpose (research with social benefits). Our results agree with those of Gupta et al. (2023), who found that the greatest willingness to provide digital health information was when data were used for research purposes by university hospitals, provided there were privacy safeguards and user consent was sought. However, further investigation is required to determine the role of the purpose and the requester's name and reputation in terms of users providing consent. Only two participants (one with medium privacy awareness and one with low) rejected the request in Task 2 in condition 'A' but accepted it in condition 'B'. Similarly, one participant with a medium level of privacy awareness rejected the request in Task 4 in condition 'A' and then accepted it in condition 'B', while another participant with low privacy awareness accepted Task 4 in 'A' and rejected Task 4 in 'B'.

However, the results show that in both Task 3, where the requester is the service provider and uses the data for a secondary (educational) purpose and Task 5, where a third-party pharmaceutical company uses the data and results for a secondary (commercial) purpose, there was a lower acceptance rate for the requests in both conditions 'A' and 'B'. Gupta et al. (2023) also found that marketing purposes negatively affect users' willingness to share their data, consequently causing them to reject the request to share and use their data. However, the acceptance rates of requests increased in condition 'B' for these two tasks (Tasks 3 and 5), indicating that application 'B' had a significant impact on the participants' decisions regarding the requests in Tasks 3 and 5.

Moreover, there was no significant relationship between users' privacy awareness level and their decision-making behaviour, as participants with medium and low levels of privacy awareness interacted almost the same with applications 'A' and 'B'. Also, users with different levels of privacy awareness responded positively to the features of consent mechanism 'B'. These findings support the concept of privacy usability, which suggests that designing user-friendly privacy features can help bridge the gap between users with varying levels of privacy awareness.

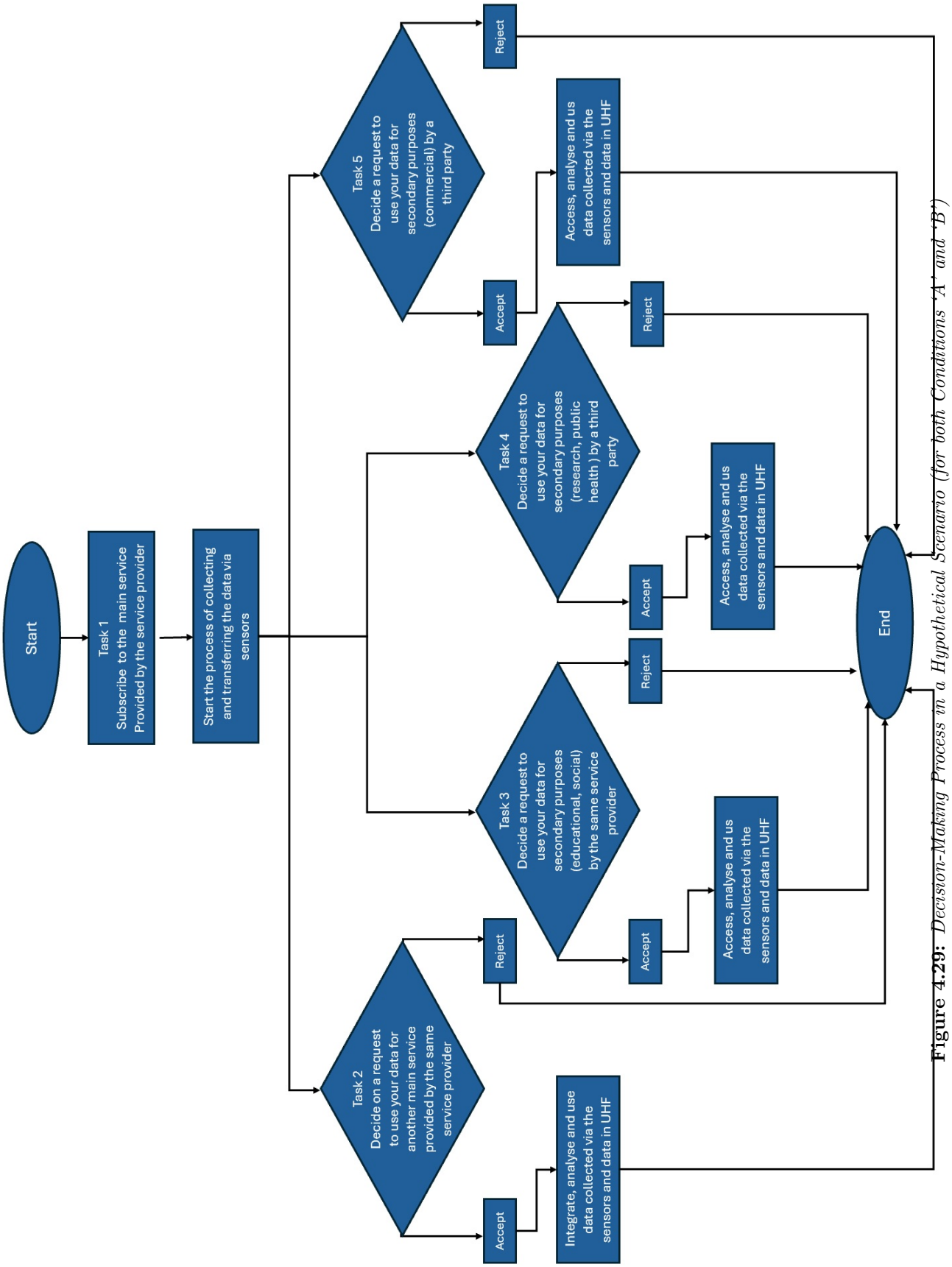

Figure 4.29: *Decision-Making Process in a Hypothetical Scenario (for both Conditions 'A' and 'B')*

4.4.3 Informed Consent in IoMT Systems

As described in Study 2 (The Experiment), a post-experiment questionnaire was utilised to evaluate the effectiveness of each feature of consent mechanism 'B' in helping participants make informed decisions, revealing that most features positively influenced user informedness. Users should be informed about security and privacy measures to protect their data, including threat notifications and solutions for handling threats (Zimmermann et al. 2019). The post-experiment questionnaire responses indicate that users greatly value clear indications of these measures, with 97.5% of participants finding them helpful for making informed decisions. When users know that there are robust security and privacy measures to protect their health data, their confidence in using IoMT increases Alraja et al. (2019). Therefore, ensuring robust security and privacy measures for health data in IoMT is crucial to fostering trust and addressing potential concerns. Additionally, clear indications of security and privacy measures empower users to make informed decisions regarding their participation in IoMT.

Moreover, balancing the benefits and risks is associated with users' willingness to share their data (Moon 2017). However, Kim et al. (2019) found that despite the benefits of IoT healthcare services, potential privacy risks make users less willing to disclose their data. Thus, explaining both benefits (personal or public) and risks is essential to enable users to make informed decisions regarding their data in IoMT services. According to Study 1 (The Survey) results, only a few participants had excellent or good knowledge about the benefits of agreeing to share their data with the service provider for purposes other than the service to which they originally agreed. Furthermore, it was observed that most participants have medium knowledge and understanding of the potential risks of disclosing their data (see Section 4.2). In Study 2 (The Experiment), the post-experiment questionnaire revealed that 95% of participants found that clarifying the benefits and potential risks of accepting requests helped them make informed decisions (see Section 4.3). In addition, explaining the benefits that users will gain from accepting requests was the second most preferred feature among the participants in the interviews, and explaining the risks associated with accepting requests was the third.

Based on the results of the semi-structured interview, the icons used to illustrate titles and sections and the videos that explain services or requests are the least important features that can help participants make informed decisions. Moreover, the within-subject experiment showed that 87.5% (35 participants) did not see or evaluate any videos in any task, while only 12.5% (just five) of the participants opened the videos explaining the services and requests, and not all of these watched them. Two participants opened the video when they performed Task 1 but did not watch it, as they spent zero seconds on it. Similarly, for Task 2, two participants opened the video, but only one watched it (based on time spent). For Task 3, two participants opened the video, and both watched it. No participant opened the video when they performed Task 4. For Task 5, only one participant opened and watched the video. However, all five participants rated the videos as a useful feature when they filled out the post-experiment questionnaire. In the semi-structured interview, one participant suggested that it would be better to design videos that include stories based on particular scenarios focusing on enhancing users' privacy awareness rather than explaining information. This suggestion is reminiscent of the recommendation by Wilbanks (2018) for the use of fictional characters called "personas", where users could choose a persona that best represents them and place them in stories that illustrate the available options and outcomes, allowing them to explore the consequences of their decisions from different perspectives. Although all the participants evaluated the icons in the post-experiment questionnaire, the results suggest that the evidence is insufficient to make a definitive conclusion. Thus, further research is needed to confirm the findings with greater confidence. However, during the discussion of the semi-structured interview, two participants specifically highlighted the significant benefits of using icons, particularly for individuals who are elderly or people who prefer visual aids.

4.4.4 Privacy Regulations Awareness

Privacy regulations are a set of rules that organisations and service providers must follow to protect users' personal information (Stallings 2019). These regulations are among the most critical factors in shaping users' awareness of information privacy (Correia & Compeau 2017). As explained in Study 1, a survey to understand the current situation of users' privacy awareness regarding health services, we investigated user awareness about the existence of privacy regulations in Saudi Arabia showing that approximately half of the participants (53.6%) were aware of the personal data protection regulations in Saudi Arabia. However, almost half (46.4%) were unaware of these regulations, indicating the need to increase awareness among the people about regulations that safeguard their personal data. Since most of our survey participants are well educated (holding a bachelor's degree (53.6%) or a higher education degree (32.3%)), there is an even greater need to educate Saudi citizens about these regulations regardless of their level of education.

In Study 2, which used an experimental approach, it was observed that most participants ignored the privacy regulation link. Of the participants, 27.3% (11 of 40) clicked on the link without reading its content. Additionally, the post-experiment questionnaire responses revealed that 55% (22 of 40) of the participants claimed that privacy regulation was not significant in supporting them in making informed decisions. The semi-structured interview helped us to understand these results, as some participants stated the reasons for their behaviour and responses. The most common view was that the regulation page text was long and complicated. One participant stated there was no reason for them to know the law, as the service provider must uphold it, whether they knew it or not. This indicates a lack of awareness about privacy regulations. Moreover, this lack of awareness may also indicate the participants' inability to comprehend the purpose and implications of consent mechanisms or privacy settings. It implies a need to enhance users' knowledge and understanding regarding their privacy rights and the regulations and laws governing their data.

4.4.5 Privacy Policy Awareness

With the classic design of service providers' privacy policy documents, most users do not read them even when provided with IoMT services that rely on their personal and sensitive health data. In Study 1 (The Survey), the participants were asked how frequently they read privacy policies when using new applications or services. Of all the participants, 30% responded that they did so rarely, and 32.5% responded that they never read the privacy policy. Together, this indicates that the majority usually do not read it. Moreover, in Study 2 (The Experiment), the results showed that none of the participants read the privacy policy in the control condition 'A', although it could be accessed through the login page, main menu, and the footer of the main requests page. Our results align with other studies that demonstrate that, although users demand transparency and have concerns about their privacy, they do not tend to read privacy policies when they provide e-consent (Rowan et al. 2017, Harle et al. 2019). For example, Rowan et al. (2017) explored users' behaviours when using online consent on a health social network, revealing that no participants in the registration step had read the privacy policy. This was due to many reasons, including that they "don't have the time" or "are not interested in it". However, the authors clarified that they used a mock-up profile, and participants may have behaved differently when asked to provide their health data in real life. In Study 2, when participants used the experimental condition 'B', where the privacy policy was displayed before participants made decisions regarding their data in the IoMT system, almost all who had medium and low levels of privacy awareness read the privacy policy in Task 1. Additionally, most of them read the critical sections in the policy for the other tasks, which was confirmed by calculating the average time spent by participants in each section (refer to Table 4.8). This confirms that a straightforward UX/UI design can improve users' understanding of privacy

regulations, resulting in higher engagement rates (Sebastian 2021).

Moreover, our results align with the results of an experiment conducted by Steinfeld (2016). using an eye-tracking method to investigate if users read privacy policies. The authors discovered that users were more willing to read privacy policies when they were presented to them by default, i.e. without the need to click to open the privacy policy page. These results suggest that having a mandatory display of the privacy policy at least once before user consent in services that request users' personal and sensitive data increases the proportion of people who read it, which can help users give informed consent. The post-experiment questionnaire indicated that 97.5% (39 out of 40) of the respondents found it helpful to have a mandatory display of the privacy policy section links before making any decision. This enhances the chance of reading them, which enables the participants to make informed decisions. However, in the interview, six participants indicated that they did not like being forced to open and read each section of the text. The idea that users had to click on each section link and read it, then click on 'OK' to move to the next section was stressful and impractical. Thus, it is enough to display the privacy policy section links before making a decision and let the users decide which sections to read rather than forcing them to read all sections. They found it sufficient to have questions assessing their understanding to ensure they had read and understood the privacy policy sections.

4.4.6 Privacy Paradox

Privacy paradox arises when people claim to care about their privacy and have concerns but prioritise convenience over protection. Many studies have discussed the issue of the privacy paradox in the IoT area. For example, Pathmabandu et al. (2023) focuses on developing a consent solution for a smart building that addresses the privacy paradox issue. Aleisa et al. (2020) conducted a study in Saudi Arabia that demonstrated a privacy paradox among users of IoT home devices (smart plugs). None of the participants in the experiment read the device's privacy policy. The same issue of privacy paradox emerges in our experiment. Although the participants had concerns about privacy risks, as the results of Study 1 showed (Section 4.2.4), the participants did not open the link to privacy policies in condition 'A'. However, in condition 'B', when the privacy policy was displayed as mandatory before taking decisions regarding requests, and it was in sections (not one piece of long text), it has been observed that the time spent in each section suggests that many participants had read the necessary information.. The results suggest that mandatorily displaying the privacy policy before any request enhances the chances of people reading, which would help minimise the privacy paradox.

4.5 Chapter Summary

This chapter comprehensively discuss the results of Study 1 (The Survey) and Study 2 (The Experiment) and then integrates the results of both studies for a deep understanding of the main findings. Study 1 explored users' privacy awareness in Saudi Arabia using a quantitative questionnaire that focused on factors such as regulation, privacy policies, potential risks, and user experience. The subjective assessment (self-assessment) results showed that 61.8% of respondents had medium privacy awareness, 27.7% had low awareness, and 10.5% had high awareness. Regarding the objective assessment, where questions have right and wrong answers and do not depend on participants' opinions, the majority (72.3%) of respondents have medium awareness, and 23.1% have low awareness, only 4.6% have high awareness. However, it is important to note that while both results indicate a medium level of privacy awareness among the majority, 35.6% subjectively assessed their privacy awareness differently from an objective assessment. This suggests that few respondents have either overestimated or underestimated their level of privacy awareness. This information can be useful in designing IoMT systems that cater to users' needs. Study 2 investigated the impact of enhanced consent mechanisms

on users in IoMT systems, collecting data via quantitative approaches with the integration of a qualitative method, showing that most participants showed a positive interest in the features. Many participants have read the first task's privacy policy in experiment condition 'B'. Also, in the 'B' condition, the features of the enhanced design of the consent mechanism positively influenced participants' decisions regarding the request in Tasks 3 and 5, which means they accepted these requests after rejecting them in the control condition 'A'. Moreover, participants found all of the features helpful in providing informed consent. Dividing the privacy policy into sections displayed before making decisions was the most preferred factor, but the link to the privacy regulation was not useful. Moreover, this study has shown that many participants are unaware of how privacy regulations protect their personal information. Thus, there is a need to enhance users' awareness of their privacy rights and the regulations that govern their data. Additionally, even if users are aware of the importance of privacy policies, they often do not read them; thus, displaying the privacy policy as a default option before users make decisions about their data can significantly increase their likelihood of reading it.

Chapter 5

Conclusion and Future Work

5.1 Introduction

This chapter starts with a summary of the thesis; it then highlights the main contributions of each study in detail. It also discusses the limitations that were encountered and presents opportunities for future research, thereby paving the way for further exploration and advancements in the field.

5.2 Summary of the Thesis

In this thesis, we investigated how to enhance the design of the consent mechanism to assist the users of IoMT systems in providing their informed consent. First, we conducted a survey to discover the privacy awareness of healthcare service users in Saudi Arabia. Then, an experiment was conducted to explore how these users make informed decisions when using two different consent applications for IoMT services.

Chapter 1 defined the research aims, motivations, research questions and study contributions. Chapter 2 outlined the most important concepts related to this thesis and provided a background of related work. The chapter consisted of two parts: the first discussed privacy and privacy awareness by focusing on the importance of understanding privacy requirements and regulations, and the second discussed information privacy and awareness in IoMT. The second part also discussed informed consent, its relationship with privacy requirements, and the available solutions for obtaining user consent in the IoT.

Chapter3 explained the various aspects of the survey methodology that was adopted for Study 1 and the experimental methodology for Study 2. In Study 1 (The Survey), a questionnaire was designed to discover users' awareness of their privacy regarding collecting, using, and sharing their personal and identifiable data. The validity and reliability of the questionnaire were evaluated through expert review and a pilot study. The survey was conducted online, and the data were collected and analysed to establish the results. Study 2 (The Experiment) investigated the effects of two consent mechanism designs on a subset of the users who had completed the questionnaire in Study 1. One design had basic features and the other had more enhanced features. First, we investigated the design of the e-consent mechanisms used in healthcare and IoT systems to identify essential features that should be considered in IoMT systems for obtaining users' informed consent. Next, a within-subject experiment was conducted using two mobile applications, namely 'A' (the control condition) and 'B' (the experimental condition). A pilot study was conducted to ensure the validity of the experiment design. The experiment was conducted remotely at the participants' convenience.

Chapter 4 presented and analysed the results of Study 1 to understand the users' perceptions of their privacy in healthcare systems. Moreover, categorising the users according to their privacy awareness helped in terms of investigating the differences in their decision-making regarding their health data in Study 2. Next, the results of the within-subject experiment, the post-experiment questionnaire and the semi-structured interview of Study 2 were explained in detail. Finally, the most significant findings from the two studies were discussed.

5.3 Research Contributions

The research comprised two main studies that focused on the users of digital health services in Saudi Arabia. The first was a survey that explored the users' current privacy awareness. This study addressed the first research question (RQ1). The second study was a within-subject experiment that investigated the improved design of the consent mechanism for IoMT. The goal was to assist users with varying levels of awareness in making informed decisions about their data. This study addressed the second and third research questions (RQ2 and RQ3) as well as the sub-question (SQ1) (see Section 1.5.)

5.3.1 Study 1 (The Survey): Privacy Awareness among the Users of Digital Healthcare Services in Saudi Arabia

The first research question was as follows:
RQ1 (User privacy awareness): How does the awareness of privacy issues relating to personal data vary among digital health system users? A survey was conducted to answer this question, and it offered several contributions:

- **Factors Affecting User Privacy Awareness**
  We designed and developed a comprehensive questionnaire that captured the participants' insights into five key factors that influence user privacy awareness: privacy regulation, privacy policy, perceived benefits, potential risks and user experience. This approach provides a nuanced understanding of privacy awareness among users of digital health systems.

- **Subjective and Objective Assessments**
  We employed both subjective and objective assessments to investigate user privacy awareness. For the subjective assessment, we designed questions that focused on self-assessment using a 5-point Likert scale. For the objective assessment, we designed questions with right and wrong answers unrelated to the users' opinions. To the best of our knowledge, this is the first study to integrate and compare these two assessment types in the context of healthcare service privacy awareness. The use of two types of assessment improves the methodology of investigating privacy awareness and gives a deeper understanding. Researchers can utilise the concept of subjective and objective assessments in other contexts to gain a deeper understanding when examining users' awareness of privacy. The results from both the subjective and objective assessments indicated a medium level of privacy awareness among most users, with no significant difference between them. However, using subjective and objective assessments to investigate the privacy of users of different services may yield different results in other contexts.

5.3.2 Study 2 (The Experiment): An Empirical Investigation of Informed Consent for IoMT Services

To answer the second and third research questions, we designed and developed a rigorous experimental framework focused on a within-subject experiment. We designed and developed two mobile applications: 'A' (the control condition) and 'B' (the experimental design with enhanced features). We addressed the second research question (RQ2) by analysing how the participants interacted while they performed specific realistic consent related tasks (the same tasks in each application). The applications recorded decisions and various elements of interaction data in real-time. The third research question (RQ3) was addressed through a post-experiment questionnaire. To provide valuable support for interpreting the findings of RQ2 and RQ3 we conducted semi-structured interviews to address subquestion 1 (SQ1): How do users with different privacy awareness levels perceive the specific features of the enhanced design of the consent mechanisms?

RQ2 (Decision-making): How does the enhanced design of consent mechanisms affect the decision-making of users with different privacy awareness levels on the collecting, processing, usage, and sharing of their data in IoMT systems?

- **The Experimental Framework**
  We addressed the interface design of the informed consent in the context of IoMT by conducting a within-subject experiment. We designed and developed two mobile applications: 'A' (the control condition) and 'B' (the experimental design with enhanced features). We ensured that the two applications were identical except for the features we wanted to investigate. We were very careful with designing the interface and screen elements, such as the buttons' positions and colours, to minimise their effects on the users' decisions. This enhanced the validity and reliability of our findings. To the best of our knowledge, our work is the first to consider the influence of user interface design on eliciting consent for data collection and use in the context of IoMT services.

- **Decision-making in IoMT**
  We identified critical aspects of the content and decisions communicated via e-consent systems and how users interacted with two different smartphone-based consent applications. This approach indicates how the design of consent systems can improve informed consent and how contextual aspects (such as who is requesting access to data) affect the decisions that are made. This combined methods approach allowed us to better understand both what users do and why. The findings indicated that the users' decisions were influenced by the data requester. That is, the requester's name and reputation could have an impact on the participants' choices. We found that there was no significant relationship between users' privacy awareness level and their decision-making behaviour.

RQ3 (Informedness): To what extent do the features of the enhanced design of consent mechanisms in IoMT affect the informedness of users with different privacy awareness levels when they make decisions about their data?

- **Providing Informed Consent**
  We identified some of the key features that can be included in the interface and help users provide their informed consent in IoMT. These features can assist users in obtaining their informed consent, which can help other developers incorporate some or all of these features into their designs. The results showed that the most important features that helped participants provide their informed consent were: dividing the privacy policy into sections, displaying the sections before asking the user to make a decision, focusing only on the service or request that they were dealing with, specifying the security and privacy measures used to protect their data, explaining the withdrawal procedure, explaining the benefits and potential risks of their decisions, and displaying questions to assess participant understanding.

5.4 Limitations and Future Work

Although this study successfully achieved its goals, it does have certain limitations. This section discusses these limitations and outlines potential directions for future work.

5.4.1 Study 1 (The Survey): Privacy Awareness among the Users of Digital Healthcare Services in Saudi Arabia

Limitations

- **Sampling bias**
  Sampling bias, or selection bias, poses an internal threat to a study's validity. Two types of sampling bias occurred in this study: geographic bias and educational level bias. We used the snowball technique, and the initial sample was selected based on accessibility and the main researcher's location. As the demographic profile shows, 66% of the participants were from Jeddah, while the others were from large cities, such as Riyadh and Almadinah. Thus, the study's results mainly reflect the privacy awareness of the participants in these cities. However, to obtain results that can represent society more generally, participants from small towns or villages should be included in future work. Although the number of participants in the study was 390 and there was variety in terms of their education level, education level bias still occurred: 32.3% of the participants held higher education degrees (master's degree or PhD). In contrast, 13.3% of the participants had only a high school diploma, and 0.5% had an education level of less than high school. The majority of the participants held bachelor's degrees (53.6%). The study found that the participants with higher education degrees were more aware of privacy policies, benefits and risks related to healthcare services. However, people with higher education degrees are generally considered well-educated and may have distinct perspectives, values or priorities compared to those with lower levels of education.

- **Number of Factors Investigated**
  Five features that influence users' privacy awareness were investigated in this study. Our selection was based on the most compelling features identified in the literature review. However, more features could and should be investigated in future work. For example, Sah & Jun (2023) found that trust in IoT service providers has a greater effect than concerns about privacy issues on people's decisions to provide personal information.

Future Work

- For future work, it is possible to adapt the survey to examine privacy awareness in different contexts and determine if the type of data being measured has an impact on the objective and subjective assessments. For instance, comparing objective and subjective assessments of financial systems or social media could reveal significant differences.

- The results showed that the older participants had a higher level of awareness of the benefits and potential risks of using healthcare applications than the younger participants. Further research is necessary to understand why older users appear to have higher awareness levels and to explore how younger users perceive the benefits and risks of health services. In addition, the study found that the female participants were more aware of the benefits and risks associated with healthcare services. More research is necessary to explore the disparities between males and females in their awareness of the perceived benefits and potential risks of sharing personal data.

5.4.2 Study 2 (The Experiment): An Empirical Investigation of Informed Consent for IoMT Services

Limitations

- **Sampling Bias and Size**
  Because the sample used in this study was essentially drawn from the same participants who were part of Study 1, the same issue of sampling bias (i.e. an internal threat) occurred because most of the participants were from Jeddah and most held higher education degrees. Additionally, the study included only 40 participants due to time limitations. Therefore, further research with a larger sample size needs to be conducted.

- **Hypothetical Scenario**
  We used hypothetical scenarios in the experiment. These scenarios may have been less complex than real-life situations, which involve many factors that influence decision-making and behaviour. In contrast, the remote conduct of the experiments is more realistic.

- **Historical Threat**
  Historical threats, which are a type of external threat to a study, refer to events that happen during a study and may affect the results. When we conducted Study 1, privacy regulation had not yet come into force in Saudi Arabia. However, it had been enforced by the time Study 2 was conducted. This event may have influenced the results because society may have been more aware of the privacy regulations while Study 2 was underway. Therefore, further investigation is necessary to understand how users of digital services perceive privacy regulations.

Future Work

- Our experiments concerned the users' responses to various scenarios. However, the users had no previous experience with the tools. Thus, we might legitimately ask whether increased familiarity with such tools, e.g. as might occur from regular usage in real systems, has a longer-term effect on user awareness and the decisions users make. That is, a longitudinal investigation might also raise important issues.

- Wilbanks (2018) found that icons and images can influence a participant's understanding and interpretation of a subject. However, the experiment results were unclear as to whether the use of icons to illustrate concepts affected informed consent. Further research is necessary to determine its effectiveness.

- The questions that assessed user understanding in the enhanced consent mechanism included one question for each request to achieve the research purpose and to reduce the user's experiment time. However, future research could develop an electronic questions system that presents users with multiple questions, selected randomly from a larger pool, focusing on privacy policies they have read. The users could pass according to specific scores.

- In the experiment tasks, we focused on accepting and rejecting each request. It would be possible in future work to add a third option, negotiation, where, for example, the user could negotiate the benefits that he/she may gain by disclosing personal data. By including this negotiation option, users would have more control over how their data are used and could potentially receive greater benefits from sharing these data.

- No significant change was observed in the participants' decisions regarding accepting the requests in task 2 and task 4 between the two conditions 'A' and 'B'. In task 2, most of

the participants agreed to disclose their data to the same service provider (the hospital) that provided them with the main service. In task 4, most of the participants agreed to disclose their data to a third party (the research centre at King Abdulaziz University (KAU)) to use the data for secondary purposes, which refers to research that can benefit public health. The findings indicate that the users' decisions may have been influenced by their trust in the requester. That is, the requester's name and reputation could have had an impact on the participants' choices. Further research is required to explore how trust and requester reputation affect users' decisions about IoMT services data use requests.

Bibliography

Abi Sen, A. A., Eassa, F. A., Jambi, K. & Yamin, M. (2018), 'Preserving privacy in internet of things: a survey', *International Journal of Information Technology* **10**, 189–200.

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. & Saadi, M. (2017), 'Big data security and privacy in healthcare: A review', *Procedia Computer Science* **113**, 73–80.

Acharya, A. S., Prakash, A., Saxena, P. & Nigam, A. (2013), 'Sampling: Why and how of it', *Indian Journal of Medical Specialties* **4**(2), 330–333.

Aftab, M. U., Hamza, A., Oluwasanmi, A., Nie, X., Sarfraz, M. S., Shehzad, D., Qin, Z. & Rafiq, A. (2022), 'Traditional and hybrid access control models: a detailed survey', *Security and Communication Networks* **2022**(1), 1560885.

Ahmed, A., Latif, R., Latif, S., Abbas, H. & Khan, F. A. (2018), 'Malicious insiders attack in iot based multi-cloud e-healthcare environment: a systematic literature review', *Multimedia Tools and Applications* **77**(17), 21947–21965.

Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M. R. & Qi, L. (2022), 'A blockchain-and artificial intelligence-enabled smart iot framework for sustainable city', *International Journal of Intelligent Systems* **37**(9), 6493–6507.

Al Bassam, N., Hussain, S. A., Al Qaraghuli, A., Khan, J., Sumesh, E. & Lavanya, V. (2021), 'Iot based wearable device to monitor the signs of quarantined remote patients of covid-19', *Informatics in medicine unlocked* **24**, 100588.

Al-Sharekh, S. I. & Al-Shqeerat, K. H. (2020), An overview of privacy issues in iot environments, *in* '2019 International Conference on Advances in the Emerging Computing Technologies (AECT)', IEEE, pp. 1–6.

Alani, M. M. (2017), 'Android users privacy awareness survey.', *International Journal of Interactive Mobile Technologies* **11**(3).

Aleisa, N., Renaud, K. & Bongiovanni, I. (2020), 'The privacy paradox applies to iot devices too: A saudi arabian study', *Computers & Security* p. 101897.

Alghamdi, F. A., AlAnazi, W. S. & Snoussi, S. (2023), Awareness of mobile operating system privacy among computer science students, *in* '2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)', IEEE, pp. 1–5.

Alhirabi, N., Rana, O. & Perera, C. (2021), 'Security and privacy requirements for the internet of things: A survey', *ACM Transactions on Internet of Things* **2**(1), 1–37.

Ali, A., Pasha, M. F., Guerrieri, A., Guzzo, A., Sun, X., Saeed, A., Hussain, A. & Fortino, G. (2023), 'A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial internet of medical things', *IEEE Transactions on Network Science and Engineering* **10**(5), 2402–2418.

Alkhatib, S., Waycott, J., Buchanan, G. & Bosua, R. (2018), Privacy and the internet of things (iot) monitoring solutions for older adults: A, *in* 'Connecting the System to Enhance the Practitioner and Consumer Experience in Healthcare: Selected Papers from the 26th Australian National Health Informatics Conference (HIC 2018)', Vol. 252, IOS Press, p. 8.

Allen, C. (2016), 'The path to self-sovereign identity'.
URL: *https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/*

Alraja, M. N., Farooque, M. M. J. & Khashab, B. (2019), 'The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the iot-based healthcare: the mediation role of risk perception', *Ieee Access* **7**, 111341–111354.

Alvi, M. (2016), 'A manual for selecting sampling techniques in research'.

Atlam, H. F. & Wills, G. B. (2020), 'Iot security, privacy, safety and ethics', *Digital twin technologies and smart cities* pp. 123–149.

Avgerou, A. D. & Stamatiou, Y. C. (2015), 'Privacy awareness diffusion in social networks', *IEEE Security & Privacy* **13**(6), 44–50.

Ayci, G., Sensoy, M., Özgür, A. & Yolum, P. (2023), 'Uncertainty-aware personal assistant for making personalized privacy decisions', *ACM Transactions on Internet Technology* **23**(1), 1–24.

Babun, L., Denney, K., Celik, Z. B., McDaniel, P. & Uluagac, A. S. (2021), 'A survey on iot platforms: Communication, security, and privacy perspectives', *Computer Networks* **192**, 108040.

Barkley, J. E. & Lepp, A. (2021), 'The effects of smartphone facilitated social media use, treadmill walking, and schoolwork on boredom in college students: Results of a within subjects, controlled experiment', *Computers in Human Behavior* **114**, 106555.

Bélanger, F. & Crossler, R. E. (2011), 'Privacy in the digital age: a review of information privacy research in information systems', *MIS quarterly* pp. 1017–1041.

Bellekens, X. J., Nieradzinska, K., Bellekens, A., Seeam, P., Hamilton, A. W. & Seeam, A. (2016), 'A study on situational awareness security and privacy of wearable health monitoring devices.', *Int. J. Cyber Situational Aware.* **1**(1), 74–96.

Bellini, P., Nesi, P. & Pantaleo, G. (2022), 'Iot-enabled smart cities: A review of concepts, frameworks and key technologies', *Applied Sciences* **12**(3), 1607.

Bergmann, M. (2008), Testing privacy awareness, *in* 'IFIP Summer School on the Future of Identity in the Information Society', Springer, pp. 237–253.

Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P. & Kumar, A. (2023), 'Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends', *Sustainability* **15**(7), 6177.

Blanco-Justicia, A., Sánchez, D., Domingo-Ferrer, J. & Muralidhar, K. (2022), 'A critical review on the use (and misuse) of differential privacy in machine learning', *ACM Computing Surveys* **55**(8), 1–16.

Brace, I. (2018), *Questionnaire design: How to plan, structure and write survey material for effective market research*, Kogan Page Publishers.

Braunstein, A., Granka, L. & Staddon, J. (2011), Indirect content privacy surveys: measuring privacy without asking about it, *in* 'Proceedings of the Seventh Symposium on Usable Privacy and Security', pp. 1–14.

Brysbaert, M. (2019), 'How many participants do we have to include in properly powered experiments? a tutorial of power analysis with reference tables', *Journal of cognition* **2**(1).

Brysbaert, M. & Stevens, M. (2018), 'Power analysis and effect size in mixed effects models: A tutorial', *Journal of cognition* **1**(1).

Budin-Ljøsne, I., Teare, H. J., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., Collett, C., D'Abramo, F., Felzmann, H., Finlay, T. et al. (2017), 'Dynamic consent: a potential solution to some of the challenges of modern biomedical research', *BMC medical ethics* **18**(1), 1–10.

Budiu, R. (2023), 'Between-subjects vs. within-subjects study design'.
URL: *https://www.nngroup.com/articles/between-within-subjects/*

Castelluccia, C., Cunche, M., Le Métayer, D. & Morel, V. (2018), Enhancing transparency and consent in the iot, *in* '2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)', IEEE, pp. 116–119.

Cavoukian, A. (2009), 'Privacy by design: The 7 foundational principles', *Information and privacy commissioner of Ontario, Canada* **5**, 12.

Cha, S.-C., Hsu, T.-Y., Xiang, Y. & Yeh, K.-H. (2018), 'Privacy enhancing technologies in the internet of things: perspectives and challenges', *IEEE Internet of Things Journal* **6**(2), 2159–2187.

Charness, G., Gneezy, U. & Kuhn, M. A. (2012), 'Experimental methods: Between-subject and within-subject design', *Journal of economic behavior & organization* **81**(1), 1–8.

Chaudhry, S. A., Irshad, A., Nebhen, J., Bashir, A. K., Moustafa, N., Al-Otaibi, Y. D. & Zikria, Y. B. (2021), 'An anonymous device to device access control based on secure certificate for internet of medical things systems', *Sustainable Cities and Society* **75**, 103322.

Cheng, X., Hou, T. & Mou, J. (2021), 'Investigating perceived risks and benefits of information privacy disclosure in it-enabled ride-sharing', *Information & Management* **58**(6), 103450.

Clarke, R. (1997), 'Introduction to dataveillance and information privacy and definitions of terms', *http://www.rogerclarke.com/DV/Intro.html* .

Coiera, E. & Clarke, R. (2004), 'e-consent: The design and implementation of consumer consent mechanisms in an electronic environment', *Journal of the American medical informatics association* **11**(2), 129–140.

Consent to treatment (2022).
URL: *https://www.nhs.uk/conditions/consent-to-treatment/*

Correia, J. & Compeau, D. (2017), Information privacy awareness (ipa): a review of the use, definition and measurement of ipa, *in* 'Proceedings of the 50th Hawaii International Conference on System Sciences'.

Creswell, J. W. & Clark, V. L. P. (2017), *Designing and conducting mixed methods research*, Sage publications.

Creswell, J. W. & Creswell, J. D. (2017), *Research design: Qualitative, quantitative, and mixed methods approaches*, Sage publications.

Čučko, Š., Bećirović, Š., Kamišalić, A., Mrdović, S. & Turkanović, M. (2022), 'Towards the classification of self-sovereign identity properties', *IEEE access* **10**, 88306–88329.

Cumyn, A., Barton, A., Dault, R., Cloutier, A.-M., Jalbert, R. & Ethier, J.-F. (2020), 'Informed consent within a learning health system: A scoping review', *Learning Health Systems* **4**(2), e10206.

Cunche, M., Métayer, D. L. & Morel, V. (2020), Colot: a consent and information assistant for the iot, *in* 'Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks', pp. 334–336.

De Michele, R. & Furini, M. (2019), Iot healthcare: Benefits, issues and challenges, *in* 'Proceedings of the 5th EAI international conference on smart objects and technologies for social good', pp. 160–164.

Deuker, A. (2010), Addressing the privacy paradox by expanded privacy awareness–the example of context-aware services, *in* 'Privacy and Identity Management for Life: 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September 7-11, 2009, Revised Selected Papers 5', Springer, pp. 275–283.

Dinev, T. & Hart, P. (2004), 'Internet privacy concerns and their antecedents-measurement validity and a regression model', *Behaviour & Information Technology* **23**(6), 413–422.

Dinev, T. & Hart, P. (2005), 'Internet privacy concerns and social awareness as determinants of intention to transact', *International Journal of Electronic Commerce* **10**(2), 7–29.

Duckert, M. & Barkhuus, L. (2022), 'Protecting personal health data through privacy awareness: A study of perceived data privacy among people with chronic or long-term illness', *Proceedings of the ACM on Human-Computer Interaction* **6**(GROUP), 1–22.

Durán-Vega, L. A., Santana-Mancilla, P. C., Buenrostro-Mariscal, R., Contreras-Castillo, J., Anido-Rifón, L. E., García-Ruiz, M. A., Montesinos-López, O. A. & Estrada-González, F. (2019), 'An iot system for remote health monitoring in elderly adults through a wearable device and mobile application', *Geriatrics* **4**(2), 34.

Dwork, C. (2006), Differential privacy, *in* 'Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33', Springer, pp. 1–12.

Dwork, C., Roth, A. et al. (2014), 'The algorithmic foundations of differential privacy', *Foundations and Trends® in Theoretical Computer Science* **9**(3–4), 211–407.

Endsley, M. R. (1988), Situation awareness global assessment technique (sagat), *in* 'Proceedings of the IEEE 1988 national aerospace and electronics conference', IEEE, pp. 789–795.

Ermakova, T., Fabian, B. & Zarnekow, R. (2014), 'Acceptance of health clouds-a privacy calculus perspective'.

Esmaeilzadeh, P. (2019), 'An empirical evaluation of factors influencing patients' reactions to the implementation of health information exchanges (hies)', *International Journal of Human–Computer Interaction* **35**(13), 1135–1146.

Fantin Irudaya Raj, E. & Appadurai, M. (2022), Internet of things-based smart transportation system for smart cities, *in* 'Intelligent Systems for Social Good: Theory and Practice', Springer, pp. 39–50.

Farooqi, S. A., Abd Rahman, A. & Saad, A. (2024), Differential privacy based federated learning techniques in iomt: A review, *in* '2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM)', IEEE, pp. 1–7.

Feng, Y., Yao, Y. & Sadeh, N. (2021), 'A design space for privacy choices: Towards meaningful privacy control in the internet of things', pp. 1–16.

Ferreira, C. M. & Serpa, S. (2018), 'Informed consent in social sciences research: Ethical challenges', *Int'l J. Soc. Sci. Stud.* **6**, 13.

Finn, R. L., Wright, D. & Friedewald, M. (2013), 'Seven types of privacy', *European data protection: coming of age* pp. 3–32.

Fox, G. & James, T. L. (2021), 'Toward an understanding of the antecedents to health information privacy concern: a mixed methods study', *Information Systems Frontiers* **23**, 1537–1562.

GDPR (2018), 'General data protection regulation (gdpr) – official legal text'.
URL: *https://gdpr-info.eu/*

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A. & Jain, R. (2020), 'Recent advances in the internet-of-medical-things (iomt) systems security', *IEEE Internet of Things Journal* **8**(11), 8707–8718.

Groß, T. (2021), 'Validity and reliability of the scale internet users' information privacy concerns (iuipc)', *Proceedings on Privacy Enhancing Technologies* .

Gupta, R., Iyengar, R., Sharma, M., Cannuscio, C. C., Merchant, R. M., Asch, D. A., Mitra, N. & Grande, D. (2023), 'Consumer views on privacy protections and sharing of personal digital health information', *JAMA Network Open* **6**(3), e231305–e231305.

Harle, C. A., Golembiewski, E. H., Rahmanian, K. P., Brumback, B., Krieger, J. L., Goodman, K. W., Mainous III, A. G. & Moseley, R. E. (2019), 'Does an interactive trust-enhanced electronic consent improve patient experiences when asked to share their health records for research? a randomized trial', *Journal of the American Medical Informatics Association* **26**(7), 620–629.

Harle, C. A., Golembiewski, E. H., Rahmanian, K. P., Krieger, J. L., Hagmajer, D., Mainous 3rd, A. G. & Moseley, R. E. (2018), 'Patient preferences toward an interactive e-consent application for research using electronic health records', *Journal of the American Medical Informatics Association* **25**(3), 360–368.

Heale, R. & Twycross, A. (2015), 'Validity and reliability in quantitative studies', *Evidence-based nursing* **18**(3), 66–67.

ISO/IEC 27556 (2022).
URL: *https://www.iso.org/obp/ui/#iso:std:iso-iec:27556:ed-1:v1:en*

ISO/IEC 29100 (2011).
URL: *https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en*

ISO/IEC 29151 (2017).
URL: *https://www.iso.org/obp/ui/#iso:std:iso-iec:29151:ed-1:v1:en*

Ivanova, D. & Katsaounis, P. (2021), 'Real-time dynamic tiered e-consent: A novel tool for patients' engagement and common ontology system for the management of medical data', *Innovations in Digital Health, Diagnostics, and Biomarkers* **1**(2), 45–49.

Jaton, E., Stang, J., Biros, M., Staugaitis, A., Scherber, J., Merkle, F., Mohr, N. M., Streib, C., Klein, L. & Puskarich, M. A. (2020), 'The use of electronic consent for covid-19 clinical trials: Lessons for emergency care research during a pandemic and beyond', *Academic Emergency Medicine* .

Javaid, M., Haleem, A., Singh, R. P., Rab, S. & Suman, R. (2021), 'Upgrading the manufacturing sector via applications of industrial internet of things (iiot)', *Sensors International* **2**, 100129.

Johanson, G. A. & Brooks, G. P. (2010), 'Initial scale development: sample size for pilot studies', *Educational and psychological measurement* **70**(3), 394–400.

Kankam, P. K. (2019), 'The use of paradigms in information research', *Library & Information Science Research* **41**(2), 85–92.

Keshta, I. & Odeh, A. (2021), 'Security and privacy of electronic health records: Concerns and challenges', *Egyptian Informatics Journal* **22**(2), 177–183.

Khando, K., Gao, S., Islam, S. M. & Salman, A. (2021), 'Enhancing employees information security awareness in private and public organisations: A systematic literature review', *Computers & security* **106**, 102267.

Kim, D., Park, K., Park, Y. & Ahn, J.-H. (2019), 'Willingness to provide personal information: Perspective of privacy calculus in iot services', *Computers in Human Behavior* **92**, 273–281.

Kjærgaard, M. B., Ardakanian, O., Carlucci, S., Dong, B., Firth, S. K., Gao, N., Huebner, G. M., Mahdavi, A., Rahaman, M. S., Salim, F. D. et al. (2020), 'Current practices and infrastructure for open data based research on occupant-centric design and operation of buildings', *Building and environment* **177**, 106848.

Knutzen, K., Weidner, F. & Broll, W. (2021), Exploring augmented reality privacy icons for smart home devices and their effect on users' privacy awareness, *in* '2021 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)', IEEE, pp. 409–414.

Kotsenas, A. L., Balthazar, P., Andrews, D., Geis, J. R. & Cook, T. S. (2021), 'Rethinking patient consent in the era of artificial intelligence and big data', *Journal of the American College of Radiology* **18**(1), 180–184.

Kouzinopoulos, C. S., Giannoutakis, K. M., Votis, K., Tzovaras, D., Collen, A., Nijdam, N. A., Konstantas, D., Spathoulas, G., Pandey, P. & Katsikas, S. (2018), Implementing a forms of consent smart contract on an iot-based blockchain to promote user trust, *in* '2018 Innovations in Intelligent Systems and Applications (INISTA)', IEEE, pp. 1–6.

Krasnova, H., Veltri, N. F. & Günther, O. (2012), 'Self-disclosure and privacy calculus on social networking sites: The role of culture: Intercultural dynamics of privacy calculus', *Wirtschaftsinformatik* **54**, 123–133.

Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N. & Volkamer, M. (2020), Security and privacy awareness in smart environments–a cross-country investigation, *in* 'Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24', Springer, pp. 84–101.

Kumatongo, B. & Muzata, K. K. (2021), 'Research paradigms and designs with their application in education', *Journal of Lexicography and Terminology (Online ISSN 2664-0899. Print ISSN 2517-9306).* **5**(1), 16–32.

Kurtz, C., Wittner, F., Vogel, P., Semmann, M. & Böhmann, T. (2020), 'Design goals for consent at scale in digital service ecosystems'.

Kusyanti, A., Santoso, N., Catherina, H. P. A. & Oktavia, E. (2022), 'Investigating mobile users' intention: Technology acceptance and privacy perspectives', *Procedia Computer Science* **197**, 576–582.

Kuznetsov, M., Novikova, E. & Kotenko, I. (2022), An approach to formal desription of the user notification scenarios in privacy policies, *in* '2022 30th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)', IEEE, pp. 275–282.

Laurent, M., Leneutre, J., Chabridon, S. & Laaouane, I. (2019), 'Authenticated and privacy-preserving consent management in the internet of things', *Procedia Computer Science* **151**, 256–263.

Lee, G. Y., Cha, K. J. & Kim, H. J. (2019), Designing the gdpr compliant consent procedure for personal information collection in the iot environment, *in* '2019 IEEE International Congress on Internet of Things (ICIOT)', IEEE, pp. 79–81.

Liu, Y., Ju, F., Zhang, Q., Zhang, M., Ma, Z., Li, M., Yang, A. & Liu, F. (2023), 'Overview of internet of medical things security based on blockchain access control', *Journal of Database Management (JDM)* **34**(3), 1–20.

Lopez, J., Rios, R., Bao, F. & Wang, G. (2017), 'Evolving privacy: From sensors to the internet of things', *Future Generation Computer Systems* **75**, 46–57.

Loukil, F., Ghedira-Guegan, C., Benharkat, A. N., Boukadi, K. & Maamar, Z. (2017), Privacy-aware in the iot applications: a systematic literature review, *in* 'OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"', Springer, pp. 552–569.

MacKenzie, I. S. (2012), 'Human-computer interaction: An empirical research perspective'.

Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004), 'Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model', *Information systems research* **15**(4), 336–355.

Menard, P. & Bott, G. J. (2020), 'Analyzing iot users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment', *Computers & Security* p. 101856.

Miller, A. R. et al. (2022), 'Privacy of digital health information', *Economics of Privacy* .

Montori, F., Bedogni, L., Iselli, G. & Bononi, L. (2020), Delivering iot smart services through collective awareness, mobile crowdsensing and open data, *in* '2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)', IEEE, pp. 1–6.

Moon, L. A. (2017), 'Factors influencing health data sharing preferences of consumers: A critical review', *Health policy and technology* **6**(2), 169–187.

Moore, A. D. (2003), 'Privacy: its meaning and value', *American Philosophical Quarterly* **40**(3), 215–227.

Morales-Trujillo, M., García-Mireles, G. A., Piattini, M. & Matla-Cruz, E. O. (2019), 'A systematic mapping study on privacy by design in software engineering'.

Morel, V., Cunche, M. & Le Métayer, D. (2019), A generic information and consent framework for the iot, *in* '2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)', IEEE, pp. 366–373.

Mugariri, P., Abdullah, H., García-Torres, M., Parameshchari, B. & Abdul Sattar, K. N. (2022), 'Promoting information privacy protection awareness for internet of things (iot).', *Mobile Information Systems* .

Mulder, T. & Tudorica, M. (2019), 'Privacy policies, cross-border health data and the gdpr', *Information & Communications Technology Law* **28**(3), 261–274.

Neisse, R., Baldini, G., Steri, G., Miyake, Y., Kiyomoto, S. & Biswas, A. R. (2015), An agent-based framework for informed consent in the internet of things, *in* '2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)', IEEE, pp. 789–794.

Neisse, R., Copigneaux, B., Biswas, A. R., Prasad, R. R. V. & Baldini, G. (2016), A policy-based approach for informed consent in internet of things, *in* 'Security and Privacy in Internet of Things (IoTs)', CRC Press, pp. 541–564.

Nijhawan, L. P., Janodia, M. D., Muddukrishna, B., Bhat, K. M., Bairy, K. L., Udupa, N. & Musmade, P. B. (2013), 'Informed consent: Issues and challenges', *Journal of advanced pharmaceutical technology & research* **4**(3), 134.

Nunes, D. S., Zhang, P. & Silva, J. S. (2015), 'A survey on human-in-the-loop applications towards an internet of all', *IEEE Communications Surveys & Tutorials* **17**(2), 944–965.

Nusbaum, L., Douglas, B., Damus, K., Paasche-Orlow, M. & Estrella-Luna, N. (2017), 'Communicating risks and benefits in informed consent for research: a qualitative study', *Global Qualitative Nursing Research* **4**, 2333393617732017.

Ogonji, M. M., Okeyo, G. & Wafula, J. M. (2020), 'A survey on privacy and security of internet of things', *Computer Science Review* **38**, 100312.

Okoyomon, E., Samarin, N., Wijesekera, P., Elazari Bar On, A., Vallina-Rodriguez, N., Reyes, I., Feal, Á., Egelman, S. et al. (2019), On the ridiculousness of notice and consent: Contradictions in app privacy policies, *in* 'Workshop on Technology and Consumer Protection (ConPro 2019), in conjunction with the 39th IEEE Symposium on Security and Privacy'.

O'Connor, Y., Rowan, W., Lynch, L. & Heavin, C. (2017), 'Privacy by design: informed consent and internet of things for smart health', *Procedia computer science* **113**, 653–658.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, T. (2017), 'The human aspects of information security questionnaire (hais-q): two further validation studies', *Computers & Security* **66**, 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. (2013), The development of the human aspects of information security questionnaire (hais-q), *in* 'ACIS 2013: Information systems: transforming the future: Proceedings of the 24th Australasian Conference on Information Systems', RMIT University, pp. 1–11.

Patel, K. K., Patel, S. M. & Scholar, P. (2016), 'Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges', *International journal of engineering science and computing* **6**(5).

Pathmabandu, C., Grundy, J., Chhetri, M. B. & Baig, Z. (2023), 'Privacy for iot: Informed consent management in smart buildings', *Future Generation Computer Systems* **145**, 367–383.

PDPL (2023), 'Personal data protection law, saudi arabia'.
URL: *https://sdaia.gov.sa*

Pelet, J.-É. & Taieb, B. (2017), Privacy protection on social networks: A scale for measuring users' attitudes in france and the usa, *in* 'Recent Advances in Information Systems and Technologies: Volume 2 5', Springer, pp. 763–773.

Pesch, P. J., Pandit, H. J., Jesus, V. & Santos, C. (2022), Consent 2022: 2nd international workshop on consent management in online services, networks and things, *in* 'Companion Proceedings of the Web Conference 2022', pp. 509–513.

Ploug, T. & Holm, S. (2016), 'Meta consent–a flexible solution to the problem of secondary use of health data', *Bioethics* **30**(9), 721–732.

Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehia, A. & Popoola, J. (2023), 'A critical literature review of security and privacy in smart home healthcare schemes adopting iot & blockchain: problems, challenges and solutions', *Blockchain: Research and Applications* p. 100178.

Pötzsch, S. (2009), Privacy awareness: A means to solve the privacy paradox?, *in* 'The Future of Identity in the Information Society: 4th IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School, Brno, Czech Republic, September 1-7, 2008, Revised Selected Papers 4', Springer, pp. 226–236.

Pradhan, B., Bhattacharyya, S. & Pal, K. (2021), 'Iot-based applications in healthcare devices', *Journal of healthcare engineering* **2021**.

Pramanik, P. K. D., Pareek, G. & Nayyar, A. (2019), Security and privacy in remote healthcare: Issues, solutions, and standards, *in* 'Telemedicine technologies', Elsevier, pp. 201–225.

Protecting data and opening data (2018).
URL: *https://data.europa.eu/en/publications/datastories/protecting-data-and-opening-data*

Pruski, C. (2010), e-crl: A rule-based language for expressing patient electronic consent, *in* '2010 Second International Conference on eHealth, Telemedicine, and Social Medicine', IEEE, pp. 141–146.

Psychoula, I., Chen, L., Amft, O. & Van Laerhoven, K. (2020), 'Privacy risk awareness in wearables and the internet of things', *IEEE Pervasive Computing* **19**(3), 60–66.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. & Fang, B. (2020), 'A survey on access control in the age of internet of things', *IEEE Internet of Things Journal* **7**(6), 4682–4696.

Rantos, K., Drosatos, G., Kritsas, A., Ilioudis, C., Papanikolaou, A. & Filippidis, A. P. (2019), 'A blockchain-based platform for consent management of personal data processing in the iot ecosystem', *Security and Communication Networks* **2019**.

Rhahla, M., Abdellatif, T., Attia, R. & Berrayana, W. (2019), A gdpr controller for iot systems: application to e-health, *in* '2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)', IEEE, pp. 170–173.

Rivadeneira, J. E., Jiménez, M. B., Marculescu, R., Rodrigues, A., Boavida, F. & Sá Silva, J. (2023), A blockchain-based privacy-preserving model for consent and transparency in human-centered internet of things, *in* 'Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation', pp. 301–314.

Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., Rodrigues, A., Fernandes, J. M. & Boavida, F. (2021), A privacy-aware framework integration into a human-in-the-loop iot system, *in* 'IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)', IEEE, pp. 1–6.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W. & Thapliyal, H. (2023), 'A systematic literature review of cybersecurity scales assessing information security awareness', *Heliyon* **9**(3).

Rowan, W., O'Connor, Y., Lynch, L. & Heavin, C. (2017), 'Exploring user behaviours when providing electronic consent on health social networks: A 'just tick agree'approach', *Procedia Computer Science* **121**, 968–975.

Runeson, P. & Höst, M. (2009), 'Guidelines for conducting and reporting case study research in software engineering', *Empirical software engineering* **14**, 131–164.

Sah, J. & Jun, S. (2023), 'The role of consumers' privacy awareness in the privacy calculus for iot services', *International Journal of Human–Computer Interaction* pp. 1–12.

Salim, M. M., Kim, I., Doniyor, U., Lee, C. & Park, J. H. (2021), 'Homomorphic encryption based privacy-preservation for iomt', *Applied Sciences* **11**(18), 8757.

Sarmah, H. & Hazarika, B. B. (2012), 'Determination of reliability and validity measures of a questionnaire', *Indian Journal of Education and information management* **1**(11), 508–517.

Saxena, A. K. (2020), 'Balancing privacy, personalization, and human rights in the digital age', *Eigenpub Review of Science and Technology* **4**(1), 24–37.

Scarpato, N., Pieroni, A., Di Nunzio, L. & Fallucchi, F. (2017), 'E-health-iot universe: A review.', *management* **21**(44), 46.

Schardong, F. & Custódio, R. (2022), 'Self-sovereign identity: a systematic review, mapping and taxonomy', *Sensors* **22**(15), 5641.

Schraefel, M., Gomer, R., Alan, A., Gerding, E. & Maple, C. (2017), 'The internet of things: interaction challenges to meaningful consent at scale', *interactions* **24**(6), 26–33.

SDAIA (2022), 'Data and ai dictionary', `https://sdaia.gov.sa/files/Dictionary.pdf`.

Sebastian, G. (2021), 'A cross-sectional study on improving privacy policy read rate and comprehension via better ux/ui design', *Communicat IBIMA* **2021**.

Sengul, C. (2017), Privacy, consent and authorization in iot, *in* '2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)', IEEE, pp. 319–321.

Sharma, S., Chen, K. & Sheth, A. (2018), 'Toward practical privacy-preserving analytics for iot and cloud-based healthcare systems', *IEEE Internet Computing* **22**(2), 42–51.

Shirey, R. (2007), 'Internet security glossary, version 2. august 2007', `https://www.rfc-editor.org/rfc/rfc4949`.

Sim, I., Liginlal, D. & Khansa, L. (2012), 'Information privacy situation awareness: Construct and validation', *Journal of Computer Information Systems* **53**(1), 57–64.

Siponen, M. T. (2000), 'A conceptual foundation for organizational information security awareness', *Information management & computer security* **8**(1), 31–41.

Skelton, E., Drey, N., Rutherford, M., Ayers, S. & Malamateniou, C. (2020), 'Electronic consenting for conducting research remotely: A review of current practice and key recommendations for using e-consenting', *International journal of medical informatics* **143**, 104271.

Smith, H. J., Dinev, T. & Xu, H. (2011), 'Information privacy research: an interdisciplinary review', *MIS quarterly* pp. 989–1015.

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996), 'Information privacy: Measuring individuals' concerns about organizational practices', *MIS quarterly* pp. 167–196.

Solove, D. J. (2006), 'A taxonomy of privacy', *University of Pennsylvania law review* pp. 477–564.

Solove, D. J. (2008), *Understanding privacy*, Harvard University Press, May.

Soumelidou, A. & Tsohou, A. (2021), 'Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness', *Telematics and Informatics* **61**, 101592.

Sowjanya, K., Dasgupta, M. & Ray, S. (2021), 'Elliptic curve cryptography based authentication scheme for internet of medical things', *Journal of Information Security and Applications* **58**, 102761.

Stallings, W. (2019), *Information Privacy Engineering and Privacy by Design*, Addison-Wesley Professional.

Steinfeld, N. (2016), '"i agree to the terms and conditions":(how) do users read privacy policies online? an eye-tracking experiment', *Computers in human behavior* **55**, 992–1000.

Straub, D., Boudreau, M.-C. & Gefen, D. (2004), 'Validation guidelines for is positivist research', *Communications of the Association for Information systems* **13**(1), 24.

Sun, Y., Lo, F. P.-W. & Lo, B. (2019), 'Security and privacy for the internet of medical things enabled healthcare systems: A survey', *IEEE Access* **7**, 183339–183355.

Taber, K. S. (2018), 'The use of cronbach's alpha when developing and reporting research instruments in science education', *Research in science education* **48**(6), 1273–1296.

Taherdoost, H. (2016), 'Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a research', *How to test the validation of a questionnaire/survey in a research (August 10, 2016)* .

Taherdoost, H. (2017), 'Determining sample size; how to calculate survey sample size', *International Journal of Economics and Management Systems* **2**.

Tanczer, L., Carr, M., Brass, I., Steenmans, I. & Blackstock, J. J. (2017), 'Iot and its implications for informed consent', *PETRAS IoT Hub, STEaPP: London* .

The EPSU guide on GDPR (2019), *Intersoft Consulting, Accessed in October* **24**(1).

Tzafestas, S. G. (2018), 'Ethics and law in the internet of things world', *Smart cities* **1**(1), 98–120.

Udoh, E. S. & Alkharashi, A. (2016), Privacy risk awareness and the behavior of smartwatch users: A case study of indiana university students, *in* '2016 Future Technologies Conference (FTC)', IEEE, pp. 926–931.

Urbano, D., Chouzal, F. & Restivo, M. T. (2017), Usefulness of remote experiments, *in* '2017 4th Experiment@ International Conference (exp. at'17)', IEEE, pp. 253–257.

Van Teijlingen, E. R. & Hundley, V. (2001), 'The importance of pilot studies'.

Varkonyi, G. G., Kertész, A. & Varadi, S. (2019), Privacy-awareness of users in our cloudy smart world, *in* '2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)', IEEE, pp. 189–196.

Verreydt, S., Yskout, K. & Joosen, W. (2021), 'Security and privacy requirements for electronic consent: a systematic literature review', *ACM Transactions on Computing for Healthcare* **2**(2), 1–24.

Vishnu, S., Ramson, S. J. & Jegan, R. (2020), Internet of medical things (iomt)-an overview, *in* '2020 5th international conference on devices, circuits and systems (ICDCS)', IEEE, pp. 101–104.

Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S. & Usman, M. (2020), 'Security and privacy in iot using machine learning and blockchain: Threats and countermeasures', *ACM Computing Surveys (CSUR)* **53**(6), 1–37.

Wakenshaw, S. Y., Maple, C., Schraefel, M., Gomer, R. & Ghirardello, K. (2018), 'Mechanisms for meaningful consent in internet of things'.

Warren, S. & Brandeis, L. (1989), The right to privacy, *in* 'Killing the Messenger', Columbia University Press, pp. 1–21.

Wazid, M. & Gope, P. (2023), 'Backm-eha: A novel blockchain-enabled security solution for iomt-based e-healthcare applications', *ACM Transactions on Internet Technology* **23**(3), 1–28.

Wilbanks, J. (2018), 'Design issues in e-consent', *The Journal of Law, Medicine & Ethics* **46**(1), 110–118.

Wu, G., Wang, S., Ning, Z. et al. (2021), 'Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things', *IEEE Internet of Things Journal* **9**(11), 8091–8104.

Xu, H., Dinev, T., Smith, H. J. & Hart, P. (2008), 'Examining the formation of individual's privacy concerns: Toward an integrative view'.

Xu, H., Gupta, S., Rosson, M. B. & Carroll, J. M. (2012), 'Measuring mobile users' concerns for information privacy'.

Yan, H., Yin, M., Yan, C. & Liang, W. (2024), A survey of privacy preserving methods based on differential privacy for medical data, *in* '2024 7th World Conference on Computing and Communication Technologies (WCCCT)', IEEE, pp. 104–108.

Yang, Y., Liu, X. & Deng, R. H. (2018), 'Lightweight break-glass access control system for healthcare internet-of-things', *IEEE Transactions on Industrial Informatics* **14**(8), 3610–3617.

Yin, R. K. (2018), 'Case study research and applications'.

Zhang, R., Liu, G., Kang, H., Wang, Q., Tian, Y. & Wang, C. (2021), 'Improved bell–lapadula model with break the glass mechanism', *IEEE Transactions on Reliability* **70**(3), 1232–1241.

Zhou, W., Jia, Y., Peng, A., Zhang, Y. & Liu, P. (2018), 'The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved', *IEEE Internet of Things Journal* **6**(2), 1606–1616.

Zimmermann, V., Gerber, P., Marky, K., Böck, L. & Kirchbuchner, F. (2019), 'Assessing users' privacy and security concerns of smart home technologies', *i-com* **18**(3), 197–216.

Zlatolas, L. N., Welzer, T., Heričko, M. & Hölbl, M. (2015), 'Privacy antecedents for sns self-disclosure: The case of facebook', *Computers in Human Behavior* **45**, 158–167.

Appendix A

The Questionnaire: User's Information Privacy Awareness in Healthcare

A.1 Questionnaire Consent Form

User's information privacy awareness in healthcare

Dear Participant,

You are invited to participate in a survey entitled "User's Information Privacy Awareness in Healthcare". This survey is part of PhD research at The University of Sheffield (United Kingdom) in cooperation with King Abdulaziz University. The main researcher is a staff member of King Abdulaziz University. The survey aims to determine users' awareness of privacy when using healthcare applications and services in order to enhance digital healthcare systems. In this survey, you will be asked about some factors related to data privacy. Some data related to how you regard personal data privacy when using health care applications, particularly the "Sehhaty" application, will be collected. Also, some data about using medical devices at home will be collected. Your participation in this research project is completely voluntary, and your responses will remain confidential and anonymous. The researchers will uphold any legal requirements concerning the release of data. The data will be collected and stored securely and will not be released without your explicit consent for any purposes other than the indicated research. You may withdraw from participating in the survey whilst taking it (i.e. you do not complete it) or you may withdraw at any time before 01/03/2022. You do not have to give any reasons why you no longer want to take part and there will be no adverse consequences if you choose to withdraw. You may inform the researchers that you wish to withdraw using the email: mabualkhair@kau.edu.sa. If you want to report an incidents or you have some concerns you can contact the via the Graduate Studies and Scientific Research Unit at the College of Computing and Information Technology, KAU : fcitg-gsu@kau.edu.sa If you agree to participate in this part of the research, please answer the survey questions as best you can. It should take approximately 30 minutes to complete. You should answer each question in turn. You will not be able to return to previous questions. There is a second phase to the research programme that is concerned with performing certain tasks on a prototype of a system that will be designed. If you are willing to consider participating in this second part of this research, please add your contact information when prompted as part of this survey. The researchers will subsequently contact you again to explain about the second phase of the research and to ask you to confirm your willingness to participate in it, i.e. you will be asked to give your explicit consent again. You are not obliged to do so; participation is entirely voluntary. If you require additional information, or have questions, please contact the primary researcher using the email listed below. Thank you for taking the time to assist this research. Sincerely primary researcher:

Hebah Albatati. Project contact details for further information:

- If you require additional information, or have questions, please contact the primary researcher. Mobile phone:0550554032, Email: halbatati1@sheffield.ac.uk, halbatati@kau.edu.sa.
- If you want to withdraw your responses before 01/03/2022 please contact the local supervisor: Email: mabualkhair@kau.edu.sa.
- If you want to report an incident, complaint or you have some concerns, you can contact the Graduate Studies and Scientific Research Unit at the College of Computing and Information Technology, KAU. Email: fcitg-gsu@kau.edu.sa.

I have read and understood the project information sheet I agree to take part in the project. I understand that taking part in the project will include completing a questionnaire.

I understand that by choosing to participate as a volunteer in this research, this does not create a legally binding agreement nor is it intended to create an employment relationship with the University of Sheffield or with King Abdelaziz University (Saudi Arabia).

I understand If I provide my personal data such as name, phone number and email address to participate in the second part of the project, this data will not be revealed to people outside the project.

I understand and agree that the project's authorised researchers will have access to this data only if they agree to preserve the confidentiality of the information as requested in this form.

I agree to assign the copyright I hold in any materials generated as part of this project to The University of Sheffield (United Kingdom) and King Abdelaziz University (Saudi Arabia).

I have read and understand the information above concerning the survey and I agree to participate in the survey.

- Yes
- No

A.2 The Questionnaire

User's information privacy awareness in healthcare

Part 1: Demographic

Your age:	
The city you live in:	
Your gender:	Male / female
Your education level:	Less than high school High school or diploma Bachelor degree Higher education (Master degree, or PhD) Other
If you agree to participate in the second stage of the research, which requires performing tasks using a prototype of the system, please fill out the following part:	
Your e-mail	
Your mobile number	

Part 2: Privacy Regulations

1	How would you describe your knowledge of the laws and regulations related to data privacy in Saudi Arabia?	1 , 2, 3, 4, 5 1 being "no knowledge of" and 5 being "an excellent knowledge of".
2	Which of the following sentences describes the current state of personal data protection in Saudi Arabia:	1-The personal data protection regulation has been approved by the government and will come into force by March 2022. 2-There is no specific personal data protection regulation in Saudi Arabia.
3	how would you describe your level of understanding of the regulations that you know regulate users' personal data in Saudi Arabia?	1, 2, 3, 4, 5 1 being "no understanding" and 5 being "an excellent understanding".

4	It is allowed for a service provider whose application or service you have used to collect your personal information and data associated with you if:	1- Its collection was identified (implicitly/explicitly) in the privacy policy, which you approved when using the application or system. 2- The application or system is related to government entities that need your data for security purposes. 3- The application or system is related to government entities that need your data to protect public health or safety. 4- Its collection was not identified in the privacy policy which you approved, and they need this data for any reason. 5- Its collection was not identified in the privacy policy, and the company obtained your approval before they started to collect it.
5	It is allowed for a service provider whose application or service you have used and shared your personal data with to further process and use this data if:	1- The reason was stated (implicitly/explicitly) in the privacy policy, which you approved when using the application. 2- The reason was not stated in the privacy policy, which you approved, and they need the data. 3- The reason was not stated in the privacy policy which you approved, and they gained your approval (by other means) for its use before processing the data.
6	It is allowed for a service provider whose application or service you have used and shared your personal data with to further share that data with a third party if:	1- The third party is explicitly identified in the privacy policy that you approved when using the application. 2- The third party belongs to category of organisation (e.g. healthcare manufacturers) (implicit/explicit) identified in the privacy policy that I approved when using the application. 3- The third party is a government entity that needs your data for security purposes. 4- The third party is a government entity that needs to protect public health or safety. 5- The third party is not identified in the privacy policy which you approved, and the service provider shares your data with the third party to get certain benefits, such as financial return. 6- The third party is not identified in the privacy policy, and the service provider obtained your approval for this sharing before they started to collect it.

Part 3: Privacy Policies

1	How often do you read the Privacy Policies when you use a new application or system?	Never, Rarely, Sometimes, Often, Always.
2	If you read the Privacy Policies and, what is your main reason for reading them?	Text (Open end question)
3	Which of the following topics would you expect to be defined in a Privacy Policy for any application?	1- Data collection issues such as what types of data are being collected and for what reasons. 2- The rules and guidelines that users must follow when using the application or the system. 3- The usage and processing of the collected data. 4- The responsibilities of the users. 5- The reasons for termination of a user's account, e.g. termination of a user account if the user performs suspicious activities such as hacking or phishing. 6- The disclosure and sharing of the data, such as information about the third parties that they will share the data with.
4	The Ministry of Health has policies that define the acceptable use of information resources by employees, including patients' information.	Yes, No, I don't know
5	If yes, How would you describe your knowledge of the Ministry of Health acceptable use policies?	1 , 2, 3, 4, 5 1 being "no knowledge of" and 5 being "an excellent knowledge of".
6	The Ministry of Health allows:	1- Accessing health records by authorised employees only. 2-taking photos of health records by employees using a camera (including a camera on a mobile phone) for any reason at any time. 3- Releasing information such as electronically protected health information with appropriate approval and after verifying the identity and authenticity of the requester. 4- Releasing information such as electronically protected health information If they personally well know the requester.
7	"Sehhaty" application has a privacy policy that users must agree to before registering or using the Services. Have you read this privacy policy?	Yes, No, I don't know that there is a privacy Policy.
8	If yes, Have you read the Privacy Policy before registering for the service?	Yes, No
9	If yes, Have you ever read the Privacy Policy using the link on the login page?	Yes, No
10	If yes, Have you ever read the Privacy anytime while using the application via the link that appears in the main menu?	Yes, No

If yes to any of 8 ,9 or 10 then How would you evaluate the following?		
11	Ease of access to the Privacy Policy.	1, 2, 3, 4, 5 1 being "poor" and 5 being "excellent".
12	The clarity of the language used in the Privacy Policy.	1, 2, 3, 4, 5 1 being "poor" and 5 being "excellent".
13	The length of the Privacy Policy text	1, 2, 3, 4, 5 1 being "poor" and 5 being "excellent".
14	how would you describe your level of understanding of the Sehhaty application Privacy Policy	1, 2, 3, 4, 5 1 being "no understanding" and 5 being "an excellent understanding".
15	When you use the Sehhaty application, the administration of the application collects information such as:	1-User identifiable data including, but not limited to, name, address, email address, and phone number. 2- Device information such as the display language that the user uses on the device, and the type of operating system. 3- Some of the vital signs that are automatically measured by the application, such as body temperature. 4- Users' financial data and preferred payment methods.
16	Sehhaty platform administration maintains the privacy and confidentiality of users' personal data. However, they will disclose a user's personal information and data associated with them to:	1- A non-government entity authorised by government entities to optimise the platform services or provide new services on it. 2- A government entity if the data has been required according to the regulations in Saudi Arabia. 3- A non-government entity, such as an advertising company, to provide users with their new product information. 4- A non-government entity authorised by government entities to provide services such as observing or storing, or processing that data. 5- Any non-government entity if they pay for the data. 6- Anyone who needs users' data for personal reasons, for example, someone who needs to know data about his/her relatives.

Part 4: Potential Risk and Perceived Benefits

1	How would you describe your level of knowledge of the potential risks that might occur when an application or service provider collects and uses your personal information and data associated with you?	1, 2, 3, 4, 5 1 being "no knowledge of" and 5 being "an excellent knowledge of".
2	If you approved for any service provider to collect your personal information and data associated with you to provide a specific service for you: (If you have concerns please choose all options that apply.)	You will have no concerns, Or 1- You will have concerns about collecting unnecessary personal data. 2- You will have concerns about using the collected data for other purposes without your approval. 3- You will have concerns about sharing the collected data with a third party without your approval. 4- You will have concerns about insecure data transmission, such as unencrypted data transmission. 5- You will have concerns about data corruption or loss. 6- Other (Please state.....)
3	If you approved for any service provider to use your personal information and data associated with you (which have been collected before after your approval to provide you with a service) to provide a new service for you: (If you have concerns please choose all options that apply.)	You will have no concerns, Or 1- You will have concerns about data leakage or breach (where the data could be used for phishing or identity theft). 2- You will have concerns about unauthorised access by employees (where the data could be sold or used without a permit) 3- You will have concerns about sharing data with a third party without your permission. 4- other.
4	How would you describe your level of knowledge of the risks that might occur if you approved for any service provider to share your personal information and data associated with you with a specific third party?	1, 2, 3, 4, 5 1 being "no knowledge of" and 5 being "an excellent knowledge of".
5	If you approved for any service provider to share your personal information and data associated with you to a specific third party: (If you have concerns please choose all options that apply.)	You will have no concerns. Or 1- You will have concerns about data leakage or breach (where the data could be used for phishing or identity theft). 2- You will have concerns about security and privacy measures that are used by the third-party to protect the data. 3- You will have concerns about third-party privacy policies. 4- other.

6	Any service provider that collects, processes, and uses personal information and data associated with users must: (Choose all options that apply.)	1- Assess the potential risks and impacts of system activities. 2- Prepare and document procedures necessary to manage and address privacy violations. 3- Provide sufficient privacy measures to protect personal and identifiable data.
7	how would you describe your level of knowledge of the benefits that you can get if you agree to collect and use your personal information and data associated with you by an application or service provider to provide you with a service?	1, 2, 3, 4, 5 1 being "no knowledge of" and 5 being "an excellent knowledge of".
8	If you agree to the collection and use of your personal information and data associated with you by a service provider, which of the following benefits may be gained? (Choose all options that apply.)	1- Personalized services. 2- Higher quality of services. 3- Discount or offers on some services
9	It is possible to use your personal information and data associated with you for purposes other than the main service that you agree about (after obtaining your approval); how would you describe your level of knowledge of the additional benefits that may be gained?	1, 2, 3, 4, 5 1 being "no knowledge of" and 5 being "an excellent knowledge of".
10	In return for giving your approval to an application or service provider to use your personal information and data associated with you for purposes other than the service, you would like to have: (Choose all options that apply.)	1- Personal benefits: priority in services, discount or offers. 2- Public benefits: improve the design, efficiency, and outcomes of services. 3- Nothing. 4- Other (Please state.....)
11	It is possible to share your personal data with a third party for a specific reason.	1, 2, 3, 4, 5 1 being "no knowledge of" and 5 being "an excellent knowledge of".
12	In return for giving your approval to an application or service provider to share your data with a third party for a specific reason, you would like to have: (Choose all options that apply.)	1- Personal benefits: priority in services, discount or offers. 2- Public benefits: improve the design, efficiency, and outcomes of services. 3- Nothing. 4- Other (Please state.....)
13	The new E-health systems in Saudi Arabia are designed to reduce potential privacy risks.	Yes, No, I don't know.
14	If yes, what are some of the potential privacy risks that you expect the new E-health systems will reduce:	1- Unauthorised access. 2- Management costs of Big data analytics. 3- Collecting unnecessary data. 4- Personal data leakage. 5- Infections.
15	The new E-health systems in Saudi Arabia are designed with the consideration of giving the users (patients) many benefits.	Yes, No, I don't know.

16	If yes, what are some of the benefits of the new E-health systems for the users (patients):	1- Increasing job opportunities in health institutions. 2- Ease of management of files and reports by administrative staff. 3- Reduction of employee paperwork because all records are computerized. 4- Ease of finding health services requested through internet services. 5- Reducing the need to re-visit service providers resulting from lack of correct information or difficulties resulting from setting appointments. 6- The ability to view the patient's health information at any time and the ability to know the people familiar with it and for what purpose.
17	The administration of "Sehhaty" application collects users' information who have agreed to their privacy policy, such as the user device's language and the type of operating system to improve the user's experience.	Yes, No, I don't know.
18	The administration of "Sehhaty" application will share user information, who have agreed to their privacy policies, with partners and all related entities, including the Ministry of Health, to:	1- Provide users with information regarding new services. 2- Send invitations to participate in the screening of applicants regarding new products or new/current services. 3- Optimize "Sehhaty" services. 4- Help advertising companies to use users' personal data. 5- Increase the procedures patients are required to follow. 6- Obtain financial benefits.
19	The administration of "Sehhaty" application requires users that have agreed to their privacy policies to:	1- Call the administration immediately if they suspect an unauthorised person is accessing their private information. 2- Not give private information over the phone or the internet to an unidentified person or entity. 3- Monitoring other users' activities to ensure that they are using the programme correctly. 4- Respond to any email requesting private information such as a username and password if the sender says he/she an employee in the Ministry of Health.

Part 5: Previous Experience

1	Do you use any medical devices at home?	Yes, No.
2	If yes, what device do you use the most: (Choose one)	1-Digital thermometer. 2- Blood Glucose Monitor. 3- Blood Pressure Monitor. 4- Weighing Scales. 5- Nebulizer. 6- Other
3	Do you use a mobile application related to this device?	Yes, No.
4	How would you describe your level of concern about privacy when using this device?	1, 2, 3, 4, 5 1 being "not at all a concerned" and 5 being "very concerned".
5	If you have privacy concerns when using these healthcare devices, what type of privacy concerns do you have: (Choose all options that apply.)	1- Collecting unnecessary data, such as your location, without your knowledge. 2- Using your data to steal your identity. 3- Using your data to discover your behaviour. 4- Using your data for phishing scams. 5- Using your data for reasons you did not approve such as research. 6- Sharing data with third party you did not approve such as an advertising company. 7- Use of your data by an unauthorised person or party.
6	For what do you use the "Sehhaty" application?	1- Book an appointment for COVID-19 test. 2- Book an appointment for COVID-19 vaccine. 3- Tele-consultation. 4- Search for medication and the nearest pharmacies that provide it. 5- View issued sick leave. 6- View prescribed medication. 7- Book an appointment in primary healthcare centres. 8- Registration of vital signs readings. 9- Steps tracker. 10- Other (Please state. . . . .).
7	How would you describe your level of concern regarding privacy when using the"Sehhaty" application?	1, 2, 3, 4, 5 1 being "not at all a concerned" and 5 being "very concerned".
8	If you have privacy concerns when using "Sehhaty" application what type of privacy concerns do you have: (Choose all options that apply.)	1- Collecting unnecessary data, such as your location, without your knowledge. 2- Using your data to steal your identity. 3- Using your data to discover your behaviour. 4- Using your data for phishing scams. 5- Using your data for reasons you did not approve such as research. 6- Sharing data with third party you did not approve such as an advertising company. 7- Use of your data by an unauthorised person or party. 8- Other (Please state. . . . .)

9	Do you use healthcare applications other than the "Sehhaty"?	Yes, No.
10	What are the main reasons to use this application?	1- Book appointments in clinics. 2- General medical advice. 3- Remote medical advice. 4- Monitor general health (fitness, vitality, sleep monitoring...etc). 5- Other (Please state. . . . .).
11	How would you describe your level of concern regarding privacy when using other applications?	1, 2, 3, 4, 5 1 being "not at all a concerned" and 5 being "very concerned".
12	If you have privacy concerns when using these healthcare applications, what type of privacy concerns do you have: (Choose all options that apply.)	1- Collecting unnecessary data, such as your location, without your knowledge. 2- Using your data to steal your identity. 3- Using your data to discover your behaviour. 4- Using your data for phishing scams. 5- Using your data for reasons you did not approve such as research. 6- Sharing data with third party you did not approve such as an advertising company. 7- Use of your data by an unauthorised person or party.
13	Has your data privacy ever been breached?	Yes, No.
14	If yes, please describe briefly how you discovered that your privacy had been breached.	Text (Open end question).
15	What was your response to this situation?	1- Do nothing. 2- Report to the authority. 3- Solve the problem by yourself, for example contact the person or entity who exposed your data and ask them to stop.
16	How would you describe your level of privacy awareness?	1, 2, 3, 4, 5 1 being "very low" and 5 being "very high".

Appendix B

The Experiment: Users' Consent in IoMT System

B.1 Experiment Information Sheet

Users' Consent in IoMT System

Dear Participant,

You are invited to participate in an experiment entitled "Users' Consent in IoMT System". You were chosen to participate in this experiment based on the initial approval that you provided when you filled out the questionnaire "User's data privacy awareness in healthcare." Please read the following information carefully before deciding whether to participate in this experiment or not. This experiment is part of PhD research at The University of Sheffield (United Kingdom) in cooperation with King Abdulaziz University (Saudi Arabia). King Abdulaziz University is funding the research where the main researcher is one of their staff members. Both the University of Sheffield (United Kingdom) and King Abdulaziz University (Saudi Arabia) will act as the data controller for this study, guaranteeing that your data will be used properly. This experiment has been ethically approved via the University of Sheffield Ethics Review Procedure, as administered by the Computer Science department. This experiment aims to discover whether features of the proposed informed consent mechanism help users with different privacy awareness to make appropriately informed decisions regarding the collection, processing, use and sharing of their health and personal data when using IoMT systems. Participation in the experiment has no immediate benefits; however, this project will help improve healthcare systems in the long term. The experiment is being carried out to improve public health services. The legal basis for processing your personal data is, therefore, the performance of carrying out a task in the public interest. Your participation in this research is completely voluntary, and your data will remain confidential only the main researcher and supervisors can access it. The results of this study may be published in 2023 but will not contain any information that can identify you. The researchers will uphold any legal requirements concerning the release of data. It is intended that the data will be anonymised and made public, that is, it will not be possible to identify you as a participant in the experiment. All identifying information (names, email addresses, contact phone numbers) will be destroyed withdrawal date has passed. The researchers themselves will then no longer be able to link available data to individual participants. The data will not be released or otherwise used without your explicit consent for any purposes other than the indicated research. Only anonymous data and results will be saved securely at the University of Sheffield and King Abdulaziz researcher storage units, which can be accessed only by the supervisors and the researcher. The university protocols will be applied to the data after the completion of the research, and anonymous data and results will be archived for ten years in the University of Sheffield research database for research integrity purposes.

If you decide to participate in this experiment, you will perform the following tasks:

1. Read the experiment information sheet.
2. Read and sign the experiment consent form.
3. Download two applications on your mobile phone.
4. Receive the following:
5. The experiment scenario and tasks sheet, which includes five real-life tasks.
6. The post-questionnaire, which includes multiple choice questions.
7. Read the experiment scenario and tasks sheet and use the first application to perform the tasks.
8. Use the second application to perform the same tasks.
9. Fill out the post-questionnaire form.
10. Participate in a short interview.

It is expected that the full experiment procedure will take from 30 to 60 minutes. All links to files and applications will be sent to you via e-mail or WhatsApp. The experimental task depends on a hypothetical scenario you might face in real life. The point is to provide a context in which service users might use a system and allow us to investigate the appropriateness of the interfaces provided. No actual health data will be collected. It is the way you interact with the system and your opinions on it that are of interest. Your interaction and choices while using the applications will be saved. Firebase and Google Analytics will be used to collect your actions, such as clicking a link or triggering an event. However, Google Analytics will display real-time location (city) and mobile type only for the last 30 minutes. We will not collect or save this information because it is unrelated to our experiment. The interview will be audio recorded if you provide your consent. The experiment will be held electronically remotely at a place and time convenient for you. However, If you are not comfortable with downloading the programmes on your own device, you can set an appointment with the researcher to meet at King Abdulaziz University or any suitable place and use the device for research (procedures related to the Coronavirus will be taken into account .) You may withdraw from participating in this experiment whilst taking it (i.e. you do not complete it) or you may withdraw at any time before 30/06/2023 by sending an email to the local supervisor: mabualkhair@kau.edu.sa. You do not have to give any reasons for why you no longer want to take part and there will be no adverse consequences if you choose to withdraw. You have already participated in Phase 1 of the research, where you completed a questionnaire concerning privacy in digital healthcare services and consented to its processing. Summary information based on the data collected in that questionnaire has been analysed and the results have been published. No identifiable personal data was published, only statistical information about the whole sample. Withdrawal from this Phase 2 (this experiment) is separate to the withdrawal from the Phase 1 survey.

If you want to report an incident, wish to raise a complaint, or if you have some concerns about the project, you can contact the Graduate Studies and Scientific Research Unit at the College of Computing and Information Technology, KAU: fcitg-gsu@kau.edu.sa

or the Computer Science Head of the department at the University of Sheffield : g.j.brown@sheffield.ac.uk

If you require additional information, or have questions, please contact the primary researcher using the email listed below. Thank you for taking the time to assist this research.

Sincerely

Name: Hebah Ali Albatati (Primary Researcher) Mobile number: 0550554032 Email: halbatati1@sheffield.ac.uk, halbatati@kau.edu.sa

The local supervisor Email: mabualkhair@kau.edu.sa Date: 04/03/2023

B.2 Experiment Consent Form

Users' Consent in IoMT System

Please tick the appropriate boxes:	Yes	No
Taking Part in the Project		
I have read and understood the project information sheet dated 31/03/2023 and the project has been fully explained to me. (If you will answer No to this question, please do not proceed with this consent form until you are fully aware of what your participation in the project will mean.)		
I have been given the opportunity to ask questions about the project.		
I agree to take part in the project. I understand that taking part in the project will include: 1. Read the experiment information sheet (PDF). 2. Read and sign the experiment consent form (Google Form). 3. Download two applications on my mobile phone. 4. Receive the following: 5. - The experiment scenario and tasks sheet, which includes five real-life tasks. 6. The post-questionnaire (Google Form), which includes multiple choice questions. 7. Perform the tasks using the first application. 8. perform the tasks using the second application. 9. Fill out the post-questionnaire form. 10. Participate in short interview.		
I understand that all links to files and the applications will be sent to you via e-mail or WhatsApp. Your interaction and choices while using the applications will be saved. Screen recording might be needed. Also, the interview will be audio recorded.		
I agree to audio record my interview. If I disagree, the researcher will write my answers.		
I understand that by choosing to participate as a volunteer in this research, this does not create a legally binding agreement nor is it intended to create an employment relationship with the University of Sheffield or King Abdulaziz University.		
I understand that my taking part is voluntary and that I can withdraw from participating in the experiment at any whilst taking it (i.e. you do not complete it) or any time before 30/06/2023 by sending an e-mail to the e-mails provided in the information sheet; I understand that withdrawal after 30/06/2023 is not possible because all contact and personal information will be deleted. I do not have to give any reasons for why I no longer want to take part and there will be no adverse consequences if I choose to withdraw.		
How my information will be used during and after the project.		
I understand my personal details such as name, phone number, address and email address etc. will not be revealed to people outside the project.		
I understand that all personal data and identifiable information (names, email addresses, contact phone numbers) will be destroyed after the withdrawal date has passed.		

I understand that only anonymous data and results will be saved securely at the University of Sheffield and King Abdulaziz researcher storage units and that these can be accessed only by the supervisors and the researcher.		
I understand that the University of Sheffield protocols will be applied to the data after the completion of the research, and anonymous data and results will be archived for ten years in the University of Sheffield research database for research integrity purposes.		
I understand and agree that my words may be quoted in publications, reports, web pages, and other research outputs. I understand that I will not be named in these outputs unless I specifically request this.		
I understand and agree that other authorised researchers will have access to this data only if they agree to preserve the confidentiality of the information as requested in this form.		
So that the information you provide can be used legally by the researchers.		
I agree to assign the copyright I hold in any materials generated as part of this project to The University of Sheffield.		

Name of participant:
Signature:
Date:

Name of Researcher: Hebah Ali ALbatati
Signature:
Date:

Project contact details for further information:

- If you require additional information, or have questions, please contact the primary researcher : Hebah Ali Albatati Mobile phone: 0550554032 Email: halbatati1@sheffield.ac.uk, halbatati@kau.edu.sa
- If you want to withdraw, contact local supervisor via email: mabualkhair@kau.edu.sa
- If you want to report an incident, wish to raise a complaint, or if you have some concerns about the project, you can contact: The Graduate Studies and Scientific Research Unit at the College of Computing and Information Technology fcitg-gsu@kau.edu.sa or Computer Science Head of the department at the University of Sheffield: g.j.brown@sheffield.ac.uk

B.3 Experiment Scenario and Tasks

Experiment scenario: Obesity, diabetes, and high blood pressure are common chronic diseases in Saudi Arabia (According to the Ministry of Health reports in 2017 and 2013). Suppose you have spoken with your doctor or therapist, and you both agreed that you need to subscribe to the Basic Vital Signs Monitoring service provided by the Remote Patient Services department in the hospital to monitor your vital signs by specialists from anywhere. According to the doctor's request, the hospital sent you a "medical wristband device". You can manage the devices, data, and consent via your mobile phone using a specific mobile application. Suppose that you received the wristband device and downloaded the application. Now, you have to do the following tasks using the first app. Then, you have to do the following tasks using the second app. All tasks must be completed in one session in the same order below.

The Required Tasks:

1. Use the username and password sent to you to log in to the application.
2. Subscribe to the *Basic Vital Signs Monitoring service* provided by the *Remote Patient Services department* in the hospital from which you received the wristband.
3. Log out of the application and then sign in again.
4. Assume that you have subscribed to the Basic Vital Signs Monitoring service. Decide on an offer from the *Remote Patient Services* department in the hospital, which already provides you with the main service to provide you with an *Advanced Early Disease Detection service*.
5. Decide on a request from the *Remote Patient Services department team*, which already provides you with Basic Vital Signs Monitoring, to use your collected data, personal information, and results in the new employees' training course.
6. Decide on a request from the *Research Centre at King Abdulaziz University (KAU)* to access and use your collected data, personal information, and results in specific research.
7. Decide on a request from the *Research Centre in Alpha pharmaceutical company* to access and use your collected data, personal information, and results in specific research.
8. Log out of the application

B.4 Post-experiment Questionnaire

	The Question	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
1	The Mandatory display of privacy policy sections before making any decision makes me read it, which consequently helps me make an informed decision					
2	Displaying privacy policy in sections focusing only on the service or request that I deal with instead of one piece of long text makes it easier to read, which consequently helps me make an informed decision.					
3	Explaining the benefits which I will gain from accepting a service or request helps me make an informed decision.					
4	Explaining the potential risk that could occur from accepting a service or request helps me make an informed decision.					
5	Explicit indication of security and privacy measures that are used to protect my data helps me make an informed decision.					
6	Clarifying the withdrawal procedure in an explicit section helps me make an informed decision.					
7	Icons that illustrate titles and sections help me visually understand the general idea, which consequently helps me make an informed decision.					
8	Questions that assess my understanding before accepting a service or request help me make an informed decision.					
9	Did you see the videos that explain services and requests?	Yes	No			
	If yes, how strongly do you agree or disagree with the sentence: Videos that explain services and requests help me make an informed decision.					
10	Did you see the link to data protection laws and regulations that govern personal data in Saudi Arabia.	Yes	No			
	If yes, how strongly do you agree or disagree with the sentence: The existence of a link to data protection laws and regulations that govern personal data in Saudi Arabia helps me make an informed decision.					

B.5 Semi-structured Interview

- Which consent mechanism do you prefer 'A' or 'B' ? and why?
- In your opinion, what are the three most important factors that helped you make an informed decision? why?
- Are there any factors that did not help you make the decision? why?
- In your opinion, do the consent mechanism features help to increase privacy awareness?
- If yes, name the top three and how?
- Are there any other factors you believe, from your point of view, that help increase privacy awareness .
- Would you like to add anything else?

Appendix C

The Main Screens of the Applications that Represent Conditions ‘A’ and ‘B’

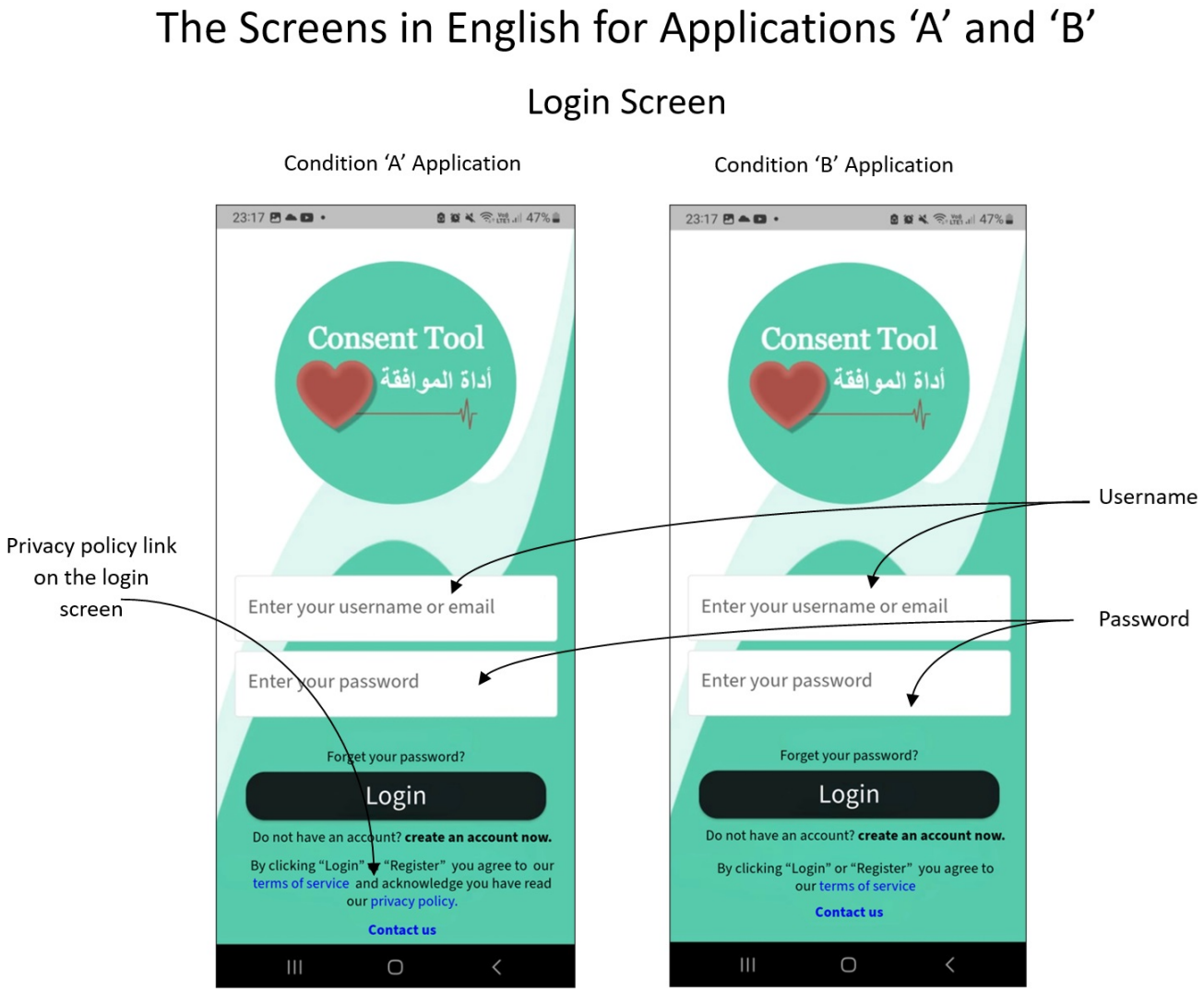

Figure C.1: *Login screen in 'A' and 'B' applications*

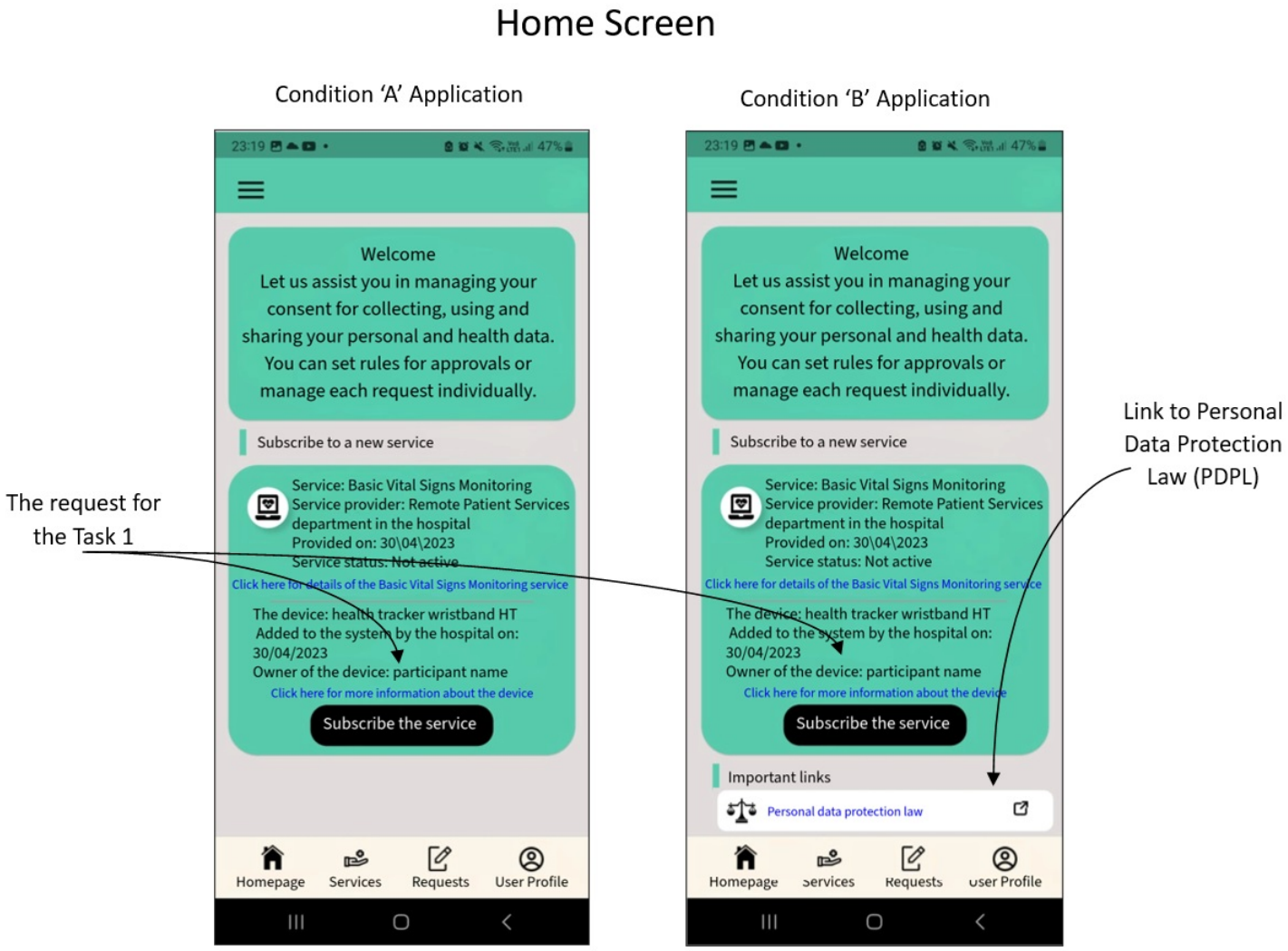

Figure C.2: *Home screen in 'A' and 'B' applications*

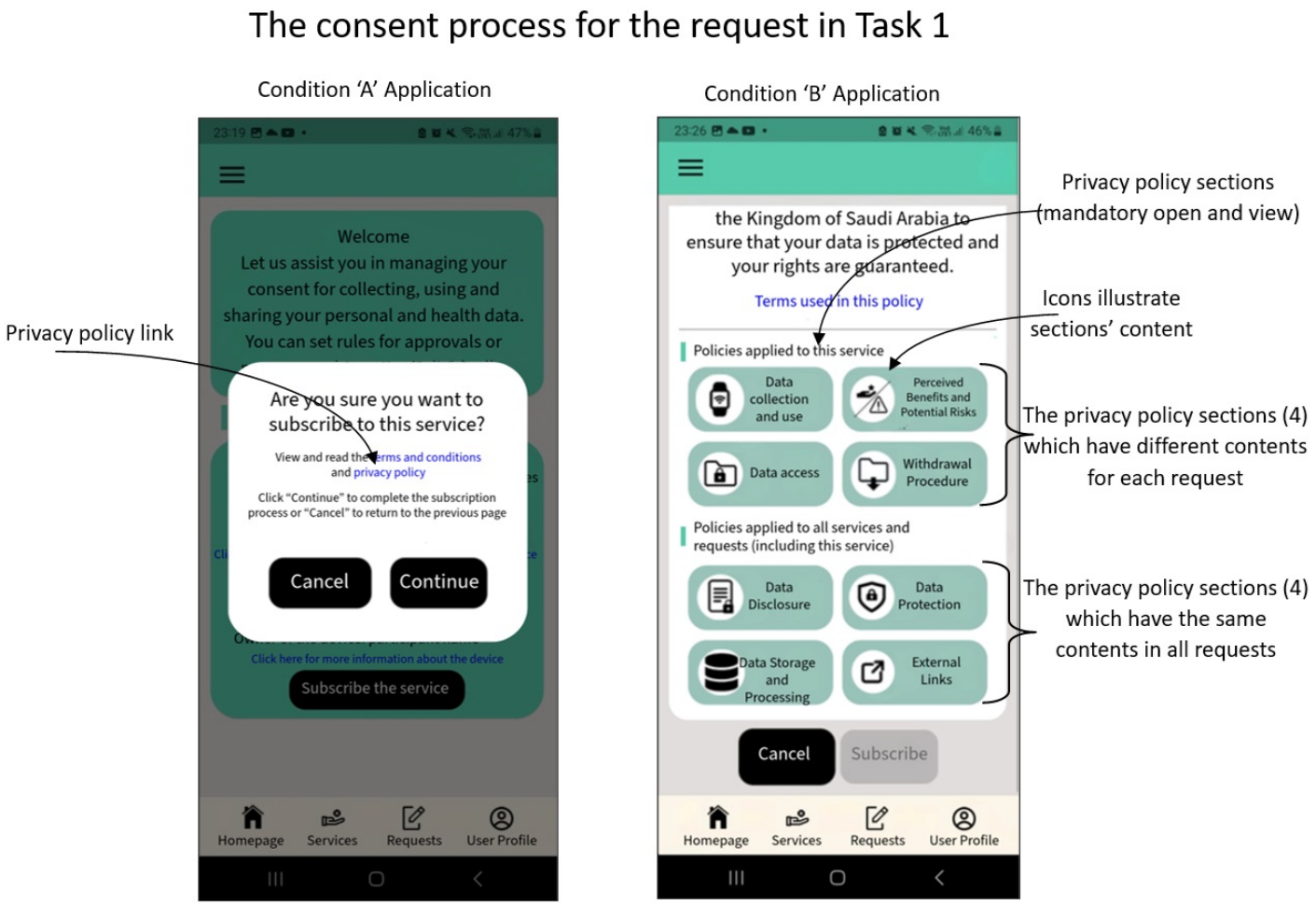

Figure C.3: *The consent process for the request in Task 1 in 'A' and 'B' applications*

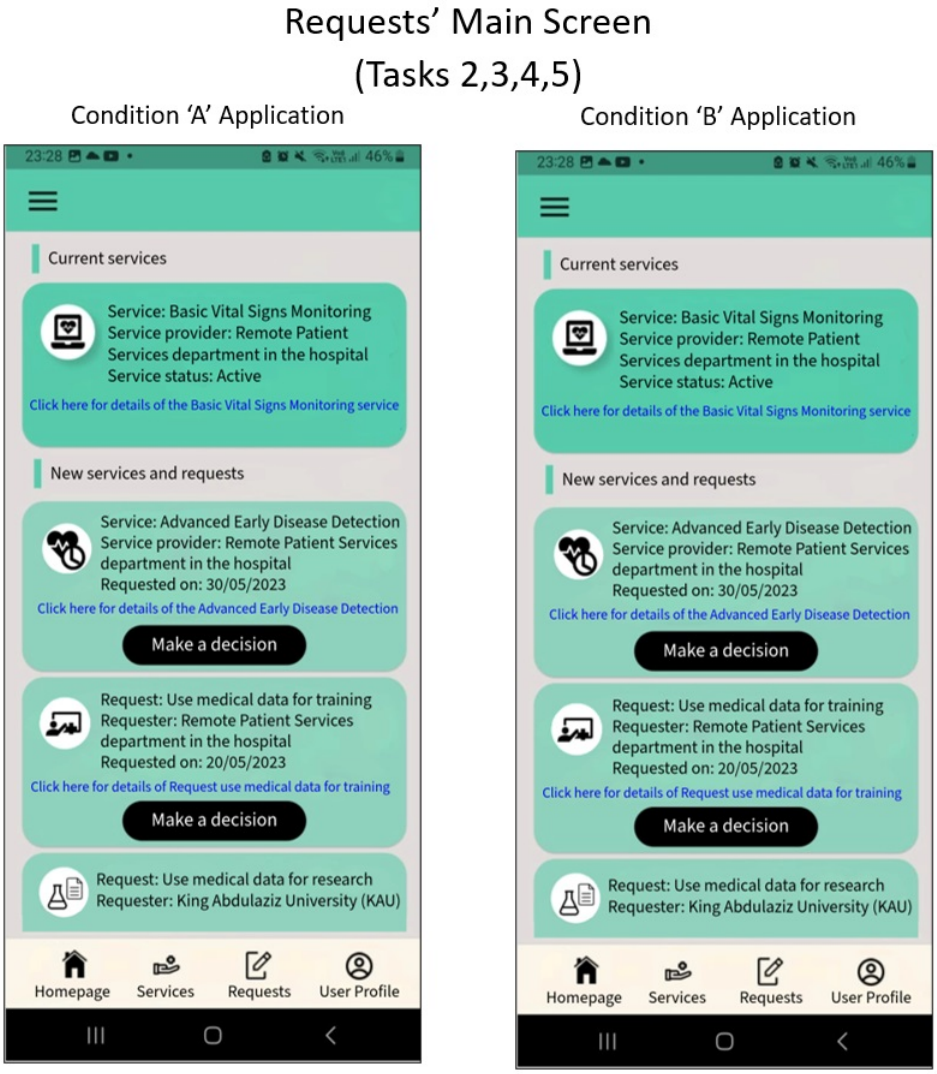

Figure C.4: *The requests' main screen in 'A' and 'B' applications (requests' in Tasks 2,3,4,5)*

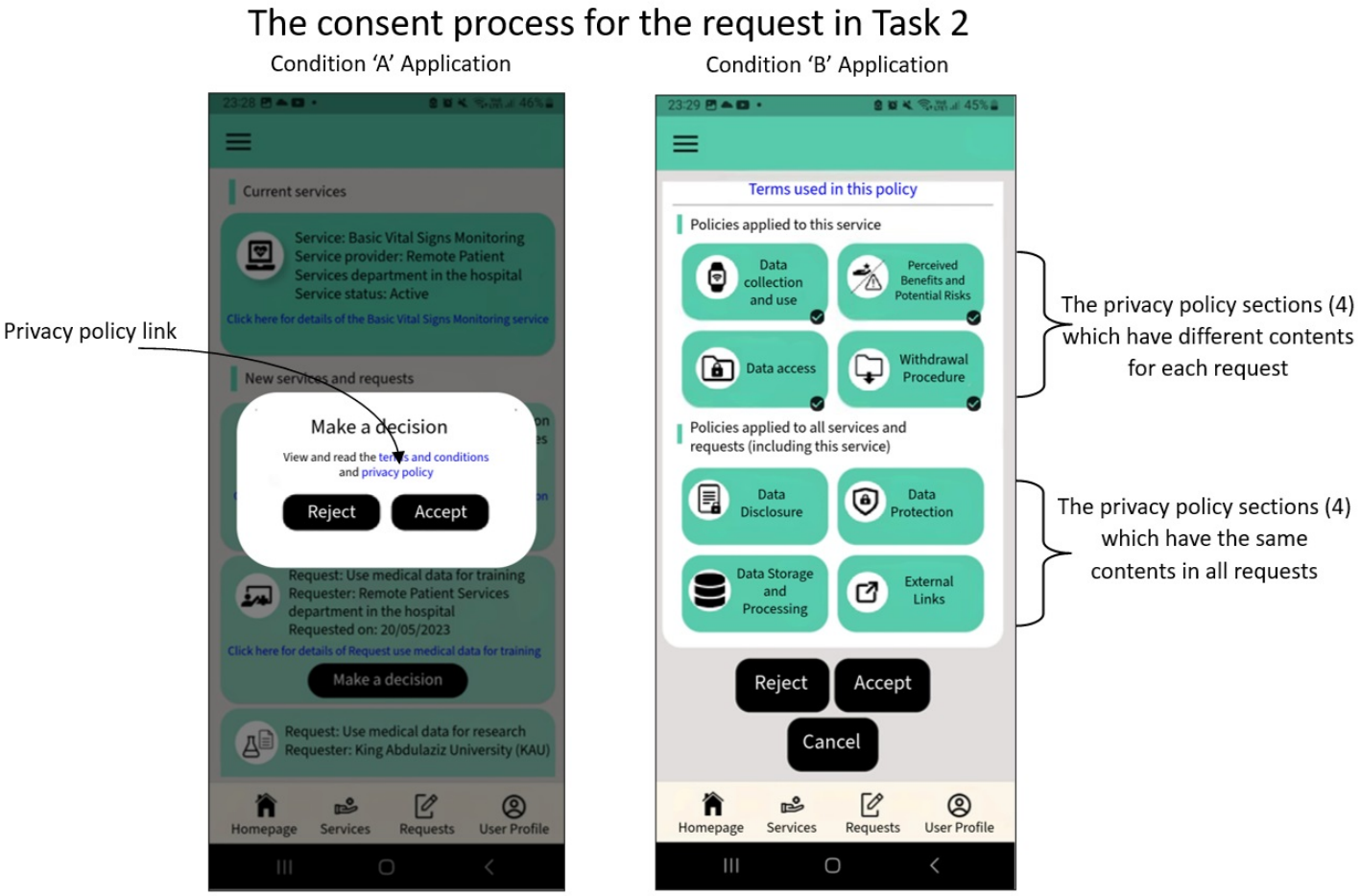

Figure C.5: *The consent process for the request in Task 2 in 'A' and 'B' applications*

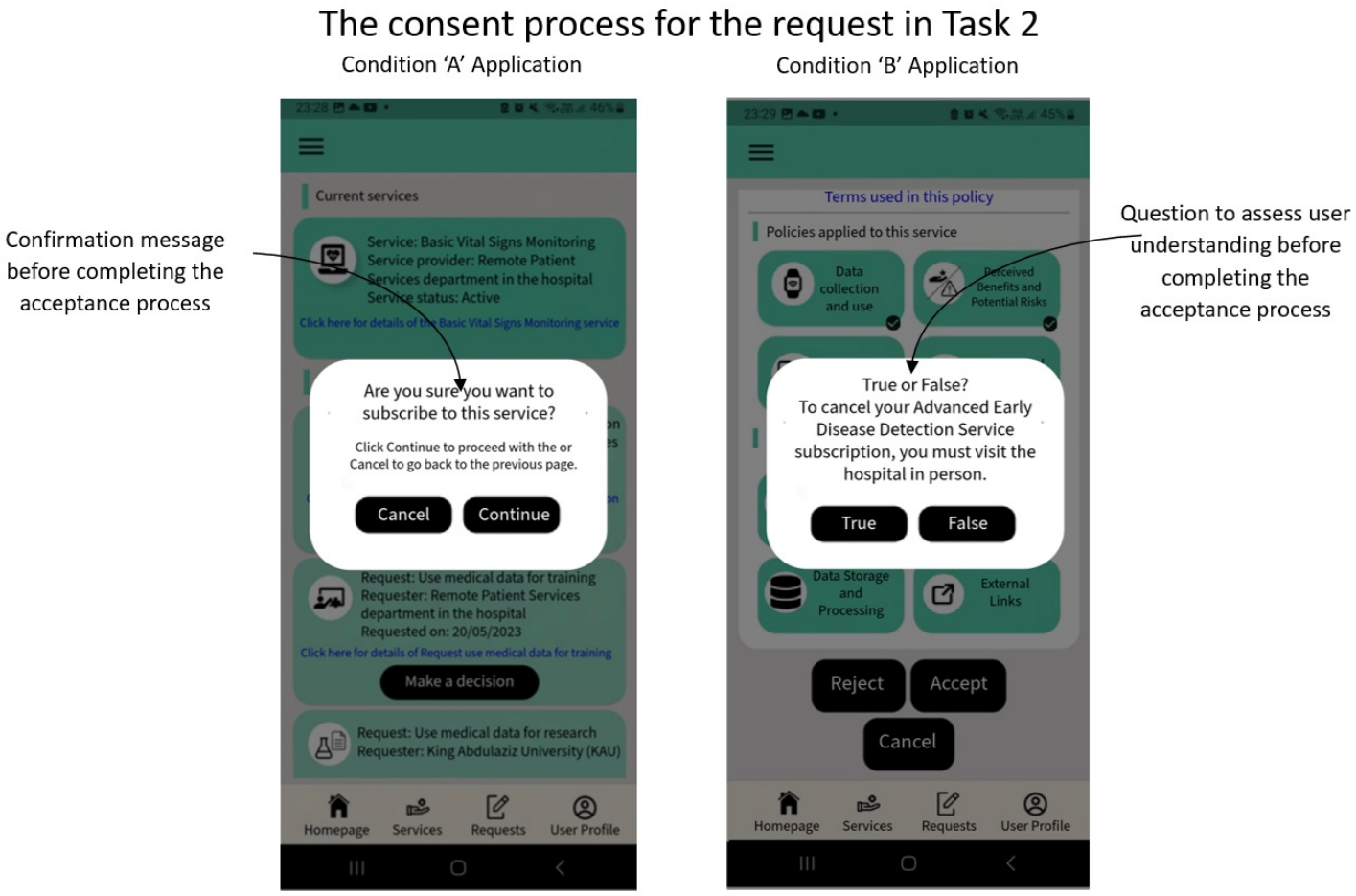

Figure C.6: *The consent process for the request in Task 2 in 'A' and 'B' applications (question to assess user understanding in 'B')*

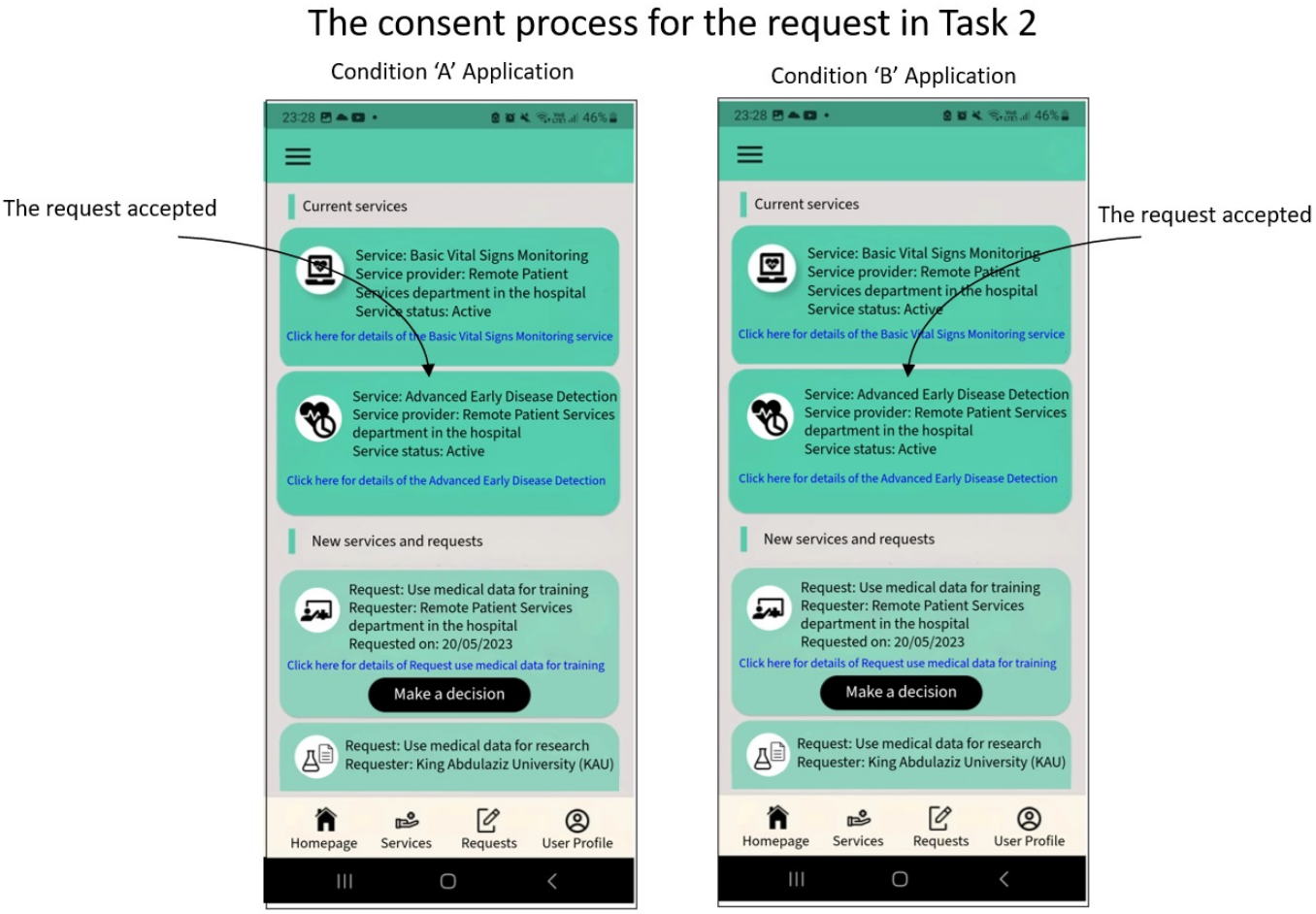

Figure C.7: *The consent process for the request in Task 2 in 'A' and 'B' applications (the request accepted)*

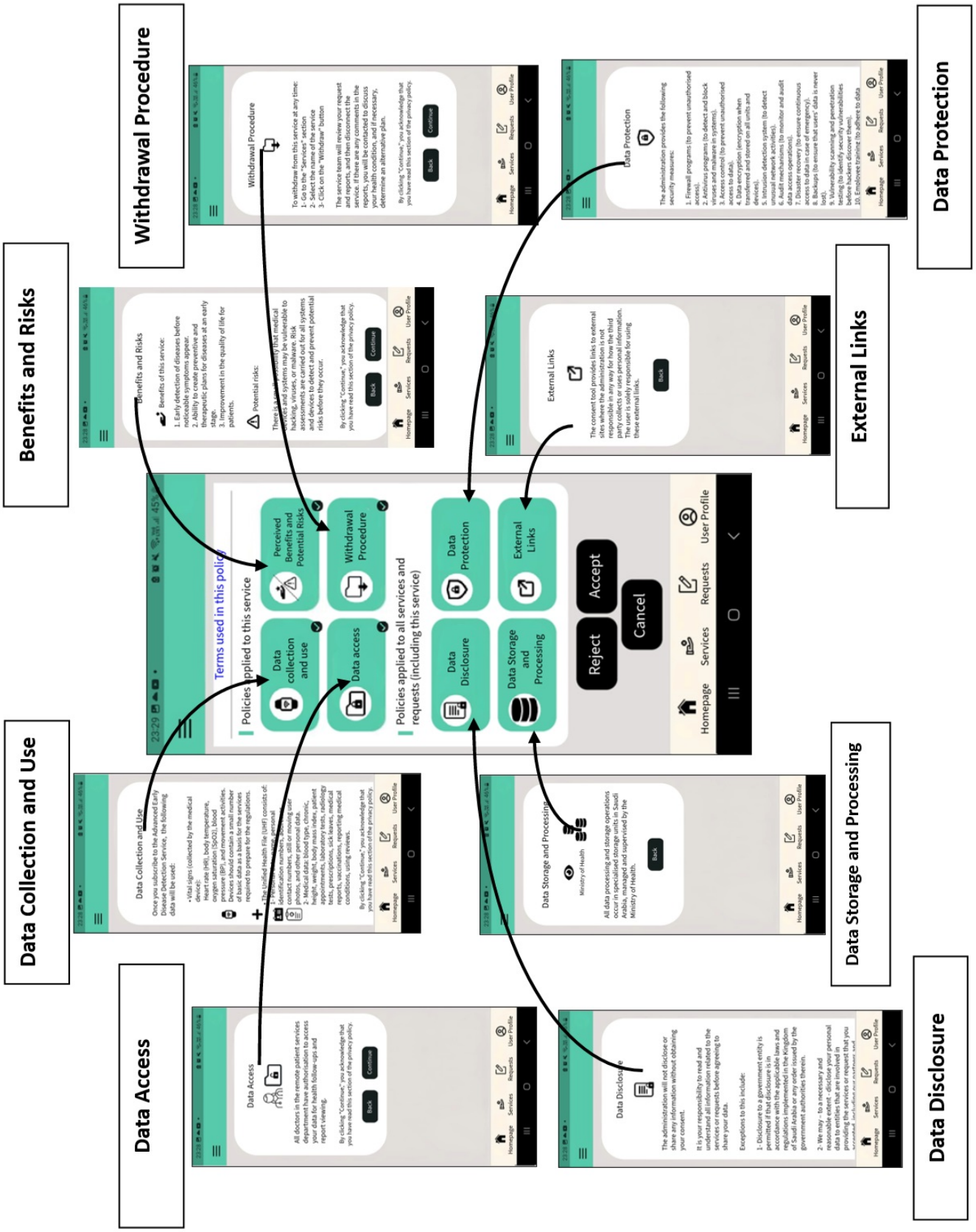

Figure C.8: *The Privacy Policy Sections in 'B' (the experimental condition) for Task 2*