NTNU
Norwegian University of
Science and Technology

Privacy by Design

John Nwachukwu Okoye

Master of Science in Telematics - Communication Networks and Networked
Submission date: July 2017
Supervisor: Lillian Røstad, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title: Privacy by Design

Student: John Nwachuwku Okoye

Problem description:

The protection of personal data using different privacy policies and privacy preserving mechanisms have either not been adequate to prevent privacy intrusions or have been implemented in ways that do not give control of personal data to the data subject, leading to data controllers and data processors flouting data protection regulations. Also, there may be trade-offs between adding system functionality and enabling stronger privacy and security features. This stems from the fact that privacy and security mechanisms are usually considered seriously at the latter stages of system development. Furthermore, the cost of mitigating privacy intrusions may outweigh the privacy risks, allowing for a waste of resources. Therefore, there is a need to embed privacy into the development lifecycle of systems.

The European Union parliament recently approved the new data protection rules that will come into effect for all member states, and also Norway as a member of EEA (European Economic Area). The objective is to hand over control of personal data to data subjects or data owners, and create a high, uniform level of data protection across the EU targeted at implementing a digital single market strategy. Among the requirements made more important by this new regulation is the use of privacy by design (PbD) in the design and development of technological systems and that every new use of personal data must undergo Privacy Impact Assessments. This project takes a look at how privacy by design will affect the development of these systems, with a focus on specific remote healthcare systems and applications. Privacy is an important component in healthcare systems due to the sensitive nature of health data, more so in such systems which are remotely operated outside of healthcare centres. Remote healthcare systems deal with the transfer of patients' sensitive and personal health information wirelessly, therefore privacy concerns do arise. Data collected from system documentations, observation, interviews, questionnaires, and Privacy Impact Assessments, will be analysed to be able to understand how implementing Privacy by design will change the way we develop such systems.

Responsible professor: Lillian Røstad, IIK

Supervisor: Lillian Røstad, IIK

Abstract

Currently, a popular topic in the ever growing world of information technology is the protection of users' personal data from unauthorised and illicit storage, disclosure or usage in any type of system. This is a big issue in this current technologically advanced world where huge data collection and processing is the norm. The European Union (EU) parliament recently approved the new data protection rules that will come into effect in 2018 for all member states, and also Norway as a member of European Economic Area (EEA). The objective is to hand over control of personal data to those it belongs to, and create a high, uniform level of data protection across the EU targeted at implementing a digital single market strategy. Among the requirements made more important by this new regulation is the use of Privacy by Design (PbD) in the design and development of systems. This project takes a look at this new way of engineering data privacy from the start in a system development life cycle, instead of adding privacy features at the tail end of development, and how it will affect development of technological systems henceforth. As a case study, we focus on some Remote healthcare Systems and Mobile Health Applications, where we investigate current privacy enhancing mechanisms being used in them, and how PbD will affect how we work in developing such systems. This master thesis contributes to the advancement of PbD from a conceptual framework to an engineering technique.

Preface

This thesis report is submitted in fulfillment of a requirement for the completion of the Master of Science degree in Telematics - Communication Networks and Networked Services at the Norwegian University of Science and Technology (NTNU). The author specialised in Information Security at Department of Information Security and Communication Technology (IIK), formerly the Department of Telematics (ITEM), which is overseen by the Faculty of Information Technology, Mathematics and Electrical Engineering (IME).

Special thanks goes to my Supervisor and Responsible Professor, Lillian Røstad, at the Department of Information Security and Communication Technology (IIK), for all the brilliant advice she gave, in guiding me towards a successful completion of this master thesis. I would also like to thank Arild Faxvaag, Professor at the Department of Neuromedicine and Movement Science (INB), NTNU, for his assistance, especially in recruiting project participants. I am also grateful to the interview participants and their organisations.

John Nwachukwu Okoye

Trondheim, Norway, July 2017

Contents

List of Figures

List of Tables

List of Acronyms

EEA European Economic Area.

EU European Union.

FIPPs Fair Information Practice Principles.

GDPR General Data Protection Regulation.

HTTPS Hypertext Transfer Protocol Secure.

IT Information Technology.

NSD Norwegian Data protection official for Research.

NTNU Norwegian University of Science and Technology.

OECD Organisation for Economic Co-operation and Development.

PbD Privacy by Design.

PDA Personal Data Act.

PET Privacy Enhancing Technology.

PETs Privacy Enhancing Technologies.

PHI Personal Health Information.

PIA Privacy Impact Assessment.

PII Personally identifiable information.

PIN Personal Identification Number.

PRIPARE Preparing Industry to Privacy-by-design by supporting its Application in Research.

RBAC Role Based Access Control.

REK Regional Committee for Medical and Health Research Ethics.

VPN Virtual Private Network.

Chapter 1
Introduction

Privacy and confidentiality are among the basic security goals in any Information Technology (IT) System. These security goals are usually misconstrued and taken to mean the other, but they are distinct goals which should not be mixed up. Confidentiality focuses on the non-disclosure of other people's data to unauthorised entities, while privacy ensures that there is control over how one's personal data is collected, stored and disclosed. Confidentiality focuses on data, while privacy focuses on the individual. Personal data is data belonging to an individual, that can be linked to the individual or identify such an individual directly or indirectly. These personal data include but is not restricted to: user location, national identification number, credit card details, biometrics, genetic information, telephone number, facial or body scans, email address, and background information that can be combined to identify a person. The European commission goes on to state that under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, individuals or organisations which collect and manage personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law [EC]. To ensure that developed systems do not contravene privacy laws and maintain regulatory compliance, imbibing privacy from the start in every stage of the system development and throughout the data lifecycle is the only way to go. Privacy by design is a framework that ensures that privacy is embedded proactively into the design and operation of IT systems, networked infrastructure, and business practices [DEL].

Current advancements in technology have led to the proliferation of Healthcare systems that enable better healthcare service delivery, within and out of healthcare centres. Several types of Remote healthcare systems exist including medication assistance systems, assisted living systems, mobile health applications, and remote patient monitoring systems which provide access to quality of life at home. However, with more healthcare services being provided with these systems, privacy concerns arise. This can have consequences ranging from minimal to highly dangerous for the patients, who are the data subjects. Remote healthcare systems deal with transfer of

patients' sensitive and personal health information wirelessly, therefore they should be extremely privacy conscious. Personal Health Information (PHI) is also transferred remotely from data subjects to data holders in Mobile Health Applications.

This project involves a study of how PbD principles can be effectively implemented, particularly in remote healthcare systems and retail systems, what ways its implementation will change the way we develop these systems. The privacy preserving mechanisms employed in these systems and how they are implemented are investigated. The scope of this study will be limited to investigating some Remote Healthcare systems, using interviews with system stakeholders, observation and system documentation to collect data that will be analysed. The analysis of the data collected helps us see the pros and cons of the current data protection practices and end up deciding what needs to change in order to operationalise PbD in such systems.

1.1 Project Motivation and Objectives

Essentially, the new EU General Data Protection Regulation (GDPR) 2016/679 which replaces the previous Directive 95/46/EC is to change a lot of things with respect to how privacy is effected. Among the requirements laid down in the reformed rules is the adoption of Privacy by Design or Data protection by design (as written in the regulation) in business practices and technological systems, also ensuring that every new use of personal data must undergo Privacy Impact Assessment (PIA). The reformed regulation will be applicable from May 25, 2018. This motivated the undertaken of this project, as Privacy by Design is still in its developing stages with a lot of grey areas in its application in technological systems. The problem stems from the fact that there is no standardised way of implementing PbD, also more work needs to be done in educating people about privacy by design.

This study seeks to reduce the occurrence of improper use of personal data, and the flouting of privacy regulations by individuals and organisations. This new EU directive on privacy by design will change how IT systems are developed and how personal data is managed, making it important that we investigate it. Over the past few years, computer systems and technology as a whole have evolved in tremendous proportions, with more and more large proportions of data being processed, this leaves us with the need to develop better strategies for ensuring privacy in systems. This has also motivated the undertaking of this study. Privacy is prime. This study was also driven by the need to make it possible for the standardisation of privacy implementation methods which can also play a huge role in the realisation of a single digital economy by the EU.

Notably, there have been limitations in implementing the principles of PbD,

because they remain abstract in engineering terms, and there is almost no specified standard of applying its principles in the design of technological systems. There is more concrete information about PbD as a policy or regulatory concept rather than clearly being a technological mechanism that needs to be engineered into systems.

1.1.1 Research Questions

Subsequently, this study poses some pertinent questions to be answered:

1. *Why is PbD needed?*

2. *What kind of methods have been proposed in the research of privacy by design implementation?*

3. *How can PIAs be better implemented in the systems development to effectively minimise privacy risks?*

4. *To what extent are the PbD principles evident in the systems under study?*

1.2 Scope and Limitations

This thesis focuses on some select Remote Healthcare Systems. A few participants from organisations that develop home healthcare, patient monitoring systems, and mobile health applications were interviewed. The reason the study has been limited to such health systems is because they are privacy sensitive systems in a privacy conscious field, therefore the current state of privacy in them will provide us with more ideas of how to employ technical measures to implement PbD.

Initially, the plan was to limit the study scope to some select online retail systems along with the remote healthcare systems, thereby providing a balance in the investigations between a group of 'less privacy conscious systems' and those of higher privacy consciousness. Unfortunately, no positive response was received from all the retail organisations contacted. They all declined the invitation to be part of the study for various reasons. There was therefore difficulty in recruiting such commercial retail projects for the study. This difficulty also arose to some extent in the recruitment of remote healthcare projects, but there was success in selecting a few systems and recruiting an interview participant for each system and organisation.

In selecting the projects or systems for the study, the idea from the onset was to recruit projects with adequate integrity and a large enough scope, not just a personal project like a mobile health application developed by a student or just any developer. The projects possess adequate funding, collect personal data or personal health information.. A decision was made to select a mix of full patient home care systems and mobile health applications.

To understand how the new EU regulation regarding the use of PbD will affect how we develop these systems, PIAs were carried out, which would help to answer many questions regarding the privacy risks and the privacy preserving mechanisms prevalent in such systems. Due to time restriction and in some cases the difficulty in getting the recruited organisations to agree to provide the needed time, and recruit other stakeholders, including end-users, Interviews were used to gather as much information as possible.

1.3 Ethics

Although the project will not involve the direct collection and use of personal data, a notification was sent to Norwegian Data protection official for Research (NSD), because background data such as names of workplaces, and job titles will be collected. A positive feedback and go ahead was received from NSD.

Names of organisations, job titles, System or project names will be replace with pseudo names throughout the course of the study and in this report. Participants are to receive written and oral information about the project, and give their consent to participate, while I ensure the safety of data in following NTNU guidelines regarding data security. Importantly, all collected data is to be made anonymous at the end of the project.

This project may be based on the study of health systems, but its purpose is not to acquire new knowledge about health or a disease. Subsequently, there was no need to send a notification to the Regional Committee for Medical and Health Research Ethics (REK).

1.4 Contribution

This thesis contributes to increasing people's knowledge of PbD, increasing awareness of the new EU data protection regulation, and most importantly, bridging the gap between regulatory PbD principles and the engineering domain. The main contribution of this study is to provide more insight into the engineering of PbD principles into the design of technological systems, which hopefully goes on to produce a standardised methodology for operationalising PbD in the development lifecycle of systems.

1.5 Outline

This thesis report consists of eight (8) chapters, ordered accordingly:

- Chapter 1, Introduction: Briefly establishes the subject of study, and also contains the motivation and objectives for the thesis. Ethical considerations, contribution, scope and limitations of the study are also stated.
- Chapter 2, Methodology: This chapter describes the research methods used in carrying out this study. A brief description of the systems investigated is also given.
- Chapter 3, Background: Gives a progressive description of concepts that either form the foundation of, or are related to the subject of study.
- Chapter 4, Towards Operationalising Privacy By Design: Describes some methods of implementing PbD that have been put forward by different authors.
- Chapter 5, Appraisal Using PIAs: The PIAs done for the studied systems are presented and separated into sections.

- Chapter 6, Comparison of Privacy Principles in Studied Systems: This chapter identifies privacy preserving techniques used in the studied systems and also maps them to PbD principles.
- Chapter 7, Discussion: Highlighting of answers to research questions, and stating of challenges that limited the study.
- Chapter 8, Conclusion: Concluding remarks and a description of the areas that will need more research work.

Chapter 2
Methodology

This chapter describes and justifies the process undergone to effectively answer the research questions set out in section 1.1.1. Research methods are the tools and techniques used by a researcher, while solving a research problem. A research methodology describes the steps taken to systematically solve the research problem systematically [Kot].

Two major types of scientific research are qualitative research and quantitative research. Qualitative research seeks to provide understanding of the problem, and opinions of a sample population which is usually very small in size. Quantitative Research has to do with quantity, amount, collation of numeric data, and statistical calculations. Here behaviours and opinions are processed numerically, rather than explanatory (in words). In quantitative research opinions are sampled from a larger population. Using Qualitative Research methods allows for more flexibility, where mostly open-ended questions are asked, allowing participants to respond in their own words, rather than replying with a YES or a NO [FHI].

In this thesis, the goal is understand properly the concept of PbD, its engineering, and how it will affect the way systems are developed. This is to be done by investigating the privacy compliance of some remote healthcare systems, sampling opinions of stakeholders on the subject and analysing findings. Consequently, a qualitative approach to the study was employed, and suitable research methods were used in understanding the problem and answering the research questions. This study will provide a platform for further research.

2.1 Methods

The research methods utilised in this thesis are explained as follows:

- **Literature Review.** A comprehensive study of relevant books, journals and articles which focus on or are related to privacy, PbD and privacy concerns in the type of systems under investigation. Literature review was used to collect secondary data, which is research data from previous projects. Effort was made to understand the problem area and previous work done in this area, leading up to this point. The review began by exploring the concept of privacy and privacy preserving mechanisms in use. Literature review was used to elicit as much information as possible from any previous work about privacy by design and its implementation. Study of the state of art in data protection and PbD. It is important to study the new EU data protection regulations and do a preview of previous privacy regulations and principles, such as Fair Information Practice Principles (FIPPs) and Organisation for Economic Co-operation and Development (OECD) guidelines .

- **Documentation analysis.** Data was collected from system specifications and other system documentations, both online and in paper form. The information gotten goes a long way in firstly, giving one an understanding of the system's architecture and technological component. Secondly, it provides foundational information about how the system under investigation functions. Secondly, it provided insight into areas in the systems where personal data or privacy considerations might be involved, and finally, it allows reading up on privacy or security policies of the organisation and any other security details that are specified. Some of the participants made available previous risk assessments performed for the systems being looked at. These risk assessments do not have privacy as a focus, unlike PIAs. However, they provide some useful information about some previous data protection risks encountered. The projects where I got risk assessment documents were MIGEX, REXAT and DELV.

- **Interviews.** Interviews played the biggest role in this study. One-on-One interviews were used to elicit technical information about the systems with respect to personal data handling, the use of PIA, and various PbD touchpoints. The interviews were held either face-to-face with participants that had the requisite technical knowledge of the systems under focus, or via Skype video call. An interview guide, structured with relevant questions was sent to these participants beforehand. This guide was also submitted to NSD as part of the notification sent before the start of data collection. The Interview guide

can be seen in Appendix A. The interview questions were structured to allow for: privacy risk analysis, privacy policy review, analysis of privacy preserving mechanisms employed, review of utilisation of PIA process, identification of privacy solutions, capturing of evidence of PbD principles in the system's development and how they were engineered. Some results of the interviews were presented and constructed into PIAs documented in Chapter 5. A good number of the interview questions were culled from [HNLL04], while others were formulated by the author, all in a bid to collect information relevant for answering the research questions.

– **Privacy Analysis.** Detailed examination of answers to questions from interview participants during interviews was carried out. Research data collected from interviews, and system documentation for each system, were assessed with respect to these talk points: compliance to EU regulation, system stakeholders, personal data in privacy domains, presence of principles, privacy controls, and PbD principles operationalising. PIAs were constructed for each project, providing a clear way to display some results and analyse some privacy risks. Analysing collected data was the major tool used to arrive at results for this study. Analysis of secondary data collected during literature review provided ideas for how PbD principles can be engineered into system development in general.

2.2 Systems and Projects studied

Five (5) systems were looked into, with a participant from each interviewed. The scope of this thesis being remote healthcare systems, meant that projects studied should be health related and capable of providing a form of health service outside a health institution, and also be one that makes use of patients' health information. All the projects made use Mobile Health Applications in some capacity.

MIGEX is a mobile health app, with plans on the way to include a communication interface with the hospital, allowing a link between the patient app and the doctor. REXAT is a standalone app that provides users with reminders to take their medicines and statistics on medicine consumption over a period. This project was started as a study in a university. The PYRO system comprises of medical measurement devices, a patient app, a user interface for healthcare personnel, a database, and back end servers. DELV is a standalone mobile health app that aids the treatment and monitoring of patient with a particular disease. Unlike others, a particular system could not be considered with Platac, instead the informant was able to only provide general information relating to the organisation's remote healthcare products. Further description of these systems or projects can be seen in sections 5.1.3, 5.2.3,

5.3.2, 5.4.2, and 5.5.1.

Chapter 3
Background

This chapter presents relevant background theory of the thesis. Effort is made to describe progressively, the terms, concepts and activities that formed the foundations upon which PbD came into existence. Data protection regulations in Norway and Europe are introduced, some relevant aspects of the new EU GDPR and privacy as it affects remote healthcare systems are discussed. An introduction to PbD is presented.

3.1 Privacy

The concept of privacy has been in existence for a long time, before the entrance of technological advancements. Humans have always wanted to protect their space, body, house, family life and conversations from unauthorised access. There has always been the need to clearly define boundaries between what is private and what is allowed to the public. Since the 14^{th} to 18^{th} century, court cases have occurred due to eavesdropping or gaining of unauthorised access to personal letters, but emphasis soon shifted to controlling one's personal information [Hol08]. In the early 19^{th} century Samuel Warren and Louis Brandeis published the paper *The Right to Privacy*, in the *Harvard Law Review* of 1890 [WB90], motivated largely by the advent of modern photography and the printing press. This article became very popular as many authors from then on began their papers by referring to it. Warren and Brandeis explained privacy as being a right to be left alone and a right to control over one's situation. Simply put: self determination. As time progressed, focus shifted to the control of who has access to an individual's personal information.

The prominence of privacy was evident in the 1960s when governments noticed automated data processing as an effective means to keep a registry its citizens [Lan01]. Nazis took advantage of detailed public records during world war II to easily locate Jews during raids, playing a part in making European countries to pass various data protection laws to prevent such exploitation and misuse of stored data [Lan01].

Privacy as it relates to the protection of personal data, is the ability to have control over one's personal information or any other background information that can be linked to the individual. This control encompasses collection, storage, processing and disposal of said personal data.

Personal data is defined in article 4 of the reformed EU regulation [EUR] 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".

Processing is defined in the regulation [EUR] as: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Personal data in form of background information such as place of work, school, age, job position, can be used to indirectly identify the data subject if combined with other personal information. Personal data or Personally identifiable information (PII) as some authors refer to it, in the context of health systems may include sensitive information such as personal health information. In the context of IT systems, a data subject provides some personal data as part of input to the system. This data is collected, stored, processed and disposed of by a data controller or essentially a service provider. For the service to be delivered, information may have to be shared with third-parties, who may also process the data subjects personal data. This means that a processor of such information may not be the data controller. These terms *data subject, data controller, and processor* are used in the Regulation (EU) 2016/679 [EUR], but other words may be used instead, for example data provider or data sharer instead of data subject.

3.1.1 Privacy Invasion

Invasion of a person's privacy do occur as a result of an adversary exploiting the occurrence of some activities or as a result of loopholes in the design of a system, or even due to carelessness on the part of the individual. Solove [Sol06] grouped harmful activities that may allow the occurrence of privacy invasion into four basic groups. Fig 3.1 showcases what Solove referred to as a Taxonomy of invasions.

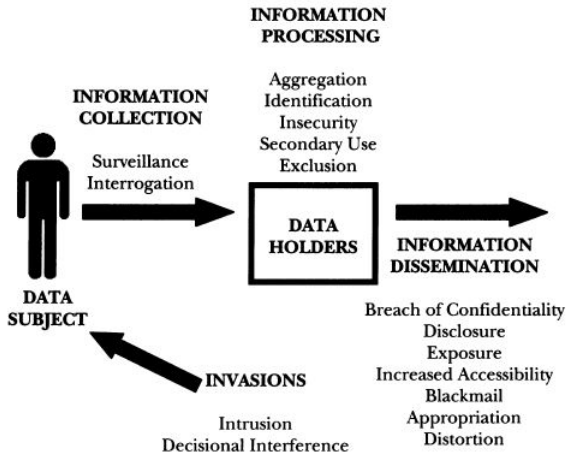

Figure 3.1: Taxonomy of invasions. Taken from [Sol06]

As more tasks are being done more effectively with the use of technological systems, privacy has encountered stiffer opposition due to the following factors [RAH+06]:

- **Big Data**: Due to the use of powerful and fast technological systems, large amount of data in varying forms can be easily collected and processed. Also, the cost of storing data is low, allowing more data to be kept longer and easy monitoring of user activity and data.
- **Easier Re-identification**: Attackers and researchers are capable of achieving more success in their aim to re-identify a user. Re-identification of a data-subject is more feasible across more types of data
- **Greater rewards**: with more data available, and more ways of analysing and linking them, attackers have more opportunity to capitalise on the data to their benefit.
- **More information made publicly available**: Legislation such as the US Freedom of Information Act and pressure on organisations to make their data publicly available creates privacy issues.

3.1.2 Privacy Controls

Simply encrypting data traffic may only be enough to provide confidentiality, but not privacy in some cases. It is therefore important to know the right mechanisms to use

in providing adequate privacy protection. Several techniques have been employed in a bid to enhance privacy protection in IT systems. Privacy Enhancing Technologies (PETs) are commonly known, with a lot of research work carried out on them, but are not the only privacy protection techniques that can be utilised. Other techniques can be grouped into: Privacy Policies, Privacy Design Patterns, Privacy design Strategies and PIAs.

Privacy Enhancing Technologies

Several software and hardware measures have been used to provide a means of privacy protection. These privacy preserving mechanisms implemented in information systems are usually referred to as PETs. Blarkom and Borking et al. [VBBO03] described PETs as: "a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system". It is safe to say that PETs are concrete implementations of privacy controls. Existing technologies can be utilised in a way that preserves privacy of individuals, therefore acting as a Privacy Enhancing Technology (PET). Some examples are: firewall, Virtual Private Network (VPN), re-mailers. Examples of other PETs include: 'Idemix' [CL01], 'u-prove' [Bra00], 'cut-and-loose techniques' [CFN90], 'The onion routing' [Din]. Hajny and Malina et al. [HMD15] clearly described technologies used in these PETs, such as: Public key Infrastructure, Group signatures, encryption, pseudonymisation, attribute-based authentication, and anonymous routing protocols.

Currently, PETs in use are made up of complex cryptographic primitives, which are very reliable. But this complexity means their cryptographic operations are increasingly difficult, therefore requiring more system resources to be performed in a short time span. Among the remote health care systems investigated in this thesis were mobile health applications used on smart phones. Hajny and Malina et al. posited that "the current smart-phones are powerful enough to compute all these primitives in tens of milliseconds" but "...the implementation of PETs on low resource devices, such as programmable smart-cards, mobile SIM cards and micro-controllers, is still difficult" [HMD15].

The security of personal data when processed in systems and services is one of the prominent dictates of the new EU data protection regulations. Article 32 in the regulations mentions the ability of the controller and processor to implement adequate technical and organisational measures to ensure: "*(a)the pseudonymisation and encryption of personal data; (b)the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*" [EUR]. PETs are a huge part of these technical measures that need to be implemented in order to secure personal data.

Privacy Policies

A privacy policy is a document or declaration specifying how an entity collects, stores, processes, shares and manages user's data. The policy should state the personal data collected, and if it will be shared with third parties. Privacy policies may cover the business operations of an organisation as a whole, or just the workings of a system developed by the organisation. These policies serve as a code of conduct for an entity, in order to protect client's data and comply to data protection laws. Client's have access to policy documents, which may be displayed in an application, on websites or given in paper form. An organisation's privacy policy may be an adaptation of national regulations, or a unique policy statement.

Privacy Design Patterns and Design Strategies

Privacy design patterns are solutions to privacy problems, and are based on the design of the system to varying extents. These design patterns usually do not give describe implementation details. PETs are used to implement them. Examples of some privacy design patterns include: anonymisation, use of pseudonyms, attribute based credentials, k-anonimity, data breach notification, location granularity, encryption, and onion routing. Privacy design strategies on the other hand, are far more abstract and even less implementation specific. Eight privacy design strategies and the privacy design patterns mapped to them are stated in [Hoe14]. The privacy design strategies are MINIMISE, HIDE, SEPARATE, AGGREGATE, INFORM, CONTROL, ENFORCE, and DEMONSTRATE.

3.1.3 Guidelines and Legislation

Over the past decades, effort has been made by organisations and governments to provide privacy principles as guidelines and enforce the implementation of these data protection principles in information systems and business processes across countries and continents.

OECD Guidelines

The US Privacy Act of 1994 brought about the definition of FIPPs which was pivotal in the enactment of privacy policies and regulations worldwide. These Fair Information Practices were contained in the Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data [OEC] released by OECD in 1980, with its aim being to minimise data collection and adequately protect collected data. The guidelines are summarised in [Hoe14] as follows:

- The collection of personal data is lawful, limited, and happens with the knowledge or consent of the data subject (*Collection Limitation*).

- Personal data should be relevant to the purposes for which they are to be used, and be accurate, complete and kept up-to-date (*Data Quality*).
- The purposes of the collection must be specified upfront (*Purpose Specification*), and the use of the data after collection is limited to that purpose (*Use Limitation*).
- Personal data must be adequately protected (*Security Safeguards*).
- The nature and extent of the data processing and the controller responsible must be readily available (*Openness*).
- Individuals have the right to view, erase, rectify, complete or amend personal data stored that relates to him (*Individual Participation*).
- A data controller must be accountable for complying with these principles (*Accountability*).

The FIPPs were enshrined in the OECD guidelines to prevent multiplication of different privacy laws.

Legislation in Norway

In Norway the regulatory body is the Norwegian Data Protection Authority, *Datatilsynet* in Norwegian. It is an independent administrative subordinate of the Ministry of Government Administration and Reform founded in 1980. It is tasked with managing laws and regulations of processing of personal data, ensuring the adherence to these laws, identifying risks to privacy and providing advice on privacy matters.

The **Personal Data Act (PDA)** of 14 April 2000, replaced the Data Register Act of 1978. As stated in the Act [Datb]:

Purpose: *The purpose of this Act is to protect natural persons from violation of their right to privacy through the processing of personal data.*

Substantive scope of the Act: *a) processing of personal data wholly or partly by electronic means, b) other processing of personal data which form part of or are intended to form part of a personal data register, and c) all forms of video surveillance, as defined in section 36, first paragraph.*

Norway, an EEA member state, is one of the countries that implemented the EU Directive 95/46/EC in its on regulations, the PDA. The PDA provides the general rules on the processing of personal data, the rights of the data subject, transfer of personal data to other countries, video surveillance, and sanctions for non-compliance. The Personal Data Regulations [Datc] was later issued on 15 December 2000, in

pursuant to the PDA. Other regulations with respect to the processing of data in healthcare will be touched upon in section 3.4.2.

Personal Data Protection in Europe

The **Data Protection Directive** (Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data) [Com], was adopted in 1995 within the EU. The OECD principles were included in this directive. The OECD principles were incorporated into the directive, providing a means to enforce them. The data protection directive has to do with personal data protection, while the European Convention on Human Rights (ECHR) focuses on a person's right to privacy (personal or family life). The directive is therefore a component of the ECHR.

The Directive has to be be included or merged with laws in all EU member states. This lead to different interpretations of the directive in its integration into law in different countries. This leads to legal challenges, in the transfer and protection of personal data across such member states. Therefore, a regulation, instead of a directive was needed. The regulation will be immediately enforced into law in all EU and EEA member states without the need to be integrated into each nation's laws. The European Commission set out to develop such a regulation by putting out a Data Protection Reform in January 2012, in a bid to give Europeans same data protection rights and an advancement of the digital single market strategy. The reform of the data protection rules lead to the publishing of Regulation (EU) 2016/679 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* and a Directive (EU) 2016/680 *on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data*. The directive is a replacement for a 2008 framework decision (2008/977/JHA) on cross-border data processing in police and judicial cooperation within the EU.

Regulation (EU) 2016/679 also known as the **GDPR** will replace the Data Protection Directive. The regulation will apply from 25 May 2018 and becomes immediately binding in all EU member states. The GDPR includes the following rights and obligations:

- Implementation of data protection by design and by default by a controller.
- Execution of data protection impact assessments (also known as PIAs) by the controller.
- Obligation of a controller to demonstrate compliance with the regulation.

- A data controller is obliged to issue a notification in case of a breach of data protection.
- Entities handling large amounts of sensitive data are required to appoint a data protection officer.
- Focus on obtaining consent for the collection of personal data, and the clarity of the request for consent.
- Fines of up to 4% of an organisation's global revenue for not complying to the dictates of the regulations.
- The right of a data subject to have his personal data erased and forgotten.
- A data subject's right to data portability.
- A data subject's right to restrict processing.
- A data subject's right to object to processing concerning him or her.
- A data subject's right to rectification of inaccurate or incomplete personal data.

The terms data controller and processor are defined in article 3(8),(9) of the regulation as follows [EUR]:

"*controller means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data;...*"
"*processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"

Data protection by design and by default (or PbD) and data protection impact assessments (or PIAs) feature heavily in the new regulation. The underlying privacy principles evident in the regulation are a subset of the foundational principles of PbD [FOU]. The regulation directs on safeguarding personal data using data protection principles and measures such as proportionality and data minimisation, access control, and compliance with the data subject's right to access his data and right to deletion.

In article 10 the GDPR describes data concerning health as a 'special category of personal data'. Sensitive information relating to the health of a person is therefore grouped as personal data. The use of PbD in healthcare is important in ensuring full protection of personal health data throughout the lifecycle of the data.

3.2 Design

To design is to create a plan for the construction of something. In systems development it is essential to come up with a suitable design structure before implementation. This also means drawing out suitable plan for how the system will be created from the onset. Design is a core stage of the Life cycle of systems. Specified System requirements and analysis of design goals are inputs that are used in the design of systems.

In the same way as system features or functionality are designed, PbD requires that privacy features are strategically planned for early on, not bolted on at the later stages of development. It simply tries to implement privacy preserving features in systems by engineering privacy into the design of the systems. Even as a system possesses defined boundaries or scope, in the same way PbD is limited to the boundaries of the system, implying that a system which utilised PbD principles in its design can still violate privacy regulations when used improperly [vRBE+12].

3.3 Privacy by Design

Privacy by Design (PbD) is a concept developed by Dr. Ann Cavoukian, the then Information and Privacy Commissioner of Ontario, Canada in the midnineties, when she documented the 7 Foundational Principles [FOU]. PbD began to be acknowledged by data protection professionals and Regulatory bodies in North America and beyond. In October 2010, PbD was unanimously adopted as an international privacy standard at the International Conference of Data Protection and Privacy Commissioners in Jerusalem. PbD is included in the U.S Commercial Privacy Bill of Rights Act. It has now been included in the GDPR of the EU and accepted by data protection commissioners worldwide as a concept that will ensure adequate privacy protection in a world of constantly evolving IT systems with capacity to collect and process massive amount of data.

PbD aims to embed privacy into the design of systems or products right from the start of their development and throughout its lifecycle, including the use of the system. The aim is to protect personal data in every phase of its lifecycle, in collection, processing, disclosure, storage and disposal. The PbD framework can be applied not only in IT, but also in business practices and Networked Infrastructure. Integrating data protection safeguards into processing is part of the description given to the concept of data protection by design in the GDPR. Actualising PbD involves the use of both technical and organisational measures.

Jeroen Van Rest et al. defined PbD extensively in [vRBE+12]:

"*The principle of 'Privacy by Design' envisions that privacy and data protective*

measures are operative throughout the entire life cycle of technologies: from the early design stage to their deployment, use and ultimate disposal. This is done by applying a design process that covers all life cycle stages and by applying privacy and data protection design patterns which are well understood and are the known best-practice for the particular purpose they are used for, and domain they are used in. The resulting design documents and systems should limit all the privacy invading activities to the minimum according to the foundational principles of privacy by design."

3.3.1 Data Protection by Design and by Default

The GDPR mentions data protection by design and data protection by default.

The principle of privacy/data protection by design revolves around engineering privacy features from the beginning into the design of systems, instead of doing this at a later stage.

The principle of privacy/data protection by default means that the default state of system, business practice or networked infrastructure, protects a data subject from a privacy breach. The user or data subject should not need to carry out any actions to turn on privacy.
Article 20 of the GDPR describes data protection by design and by default. However, the concept of PbD covers both principles.

3.3.2 Foundational Principles of PbD

Many a times when privacy is implemented into systems at the end of their development cycle, there is usually a tradeoff between adding some functionality of the system and adding some privacy feature. PbD seeks to eliminate tradeoffs yielding a win-win situation. This is one of the 7 foundational principles of PbD created by Ann Cavoukian. These principles were only meant to serve as a reference framework, they were not detailed enough to allow direct application or engineering into systems. This meant there was still a long way to go in making these principles operational in the development lifecycles of systems. The 7 foundational principles are described by Ann Cavoukian as follows [FOU]:

1. **Proactive** not Reactive; **Preventative** not Remedial

   The Privacy by Design approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred it

aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the **Default**

   We can all be certain of one thing the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy it is built into the system, by default.

3. Privacy **Embedded** into Design

   Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – **Positive-Sum**, not Zero-Sum

   Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "winwin" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

5. **End-to-End Security** – Lifecycle Protection

   Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and **Transparency**

   Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its compo-

nent parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!

7. Respect for **User Privacy**

   Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

Cavoukian also mapped each foundational principle to the related Fair Information Practices.

3.3.3 PbD in the EU GDPR

Article 20(1)of the GDPR dictates the embedding of appropriate technical and organisational measures such as pseudonymisation and data minimisation and other data protection principles into processing. It also encourages processing personal data based on the principle of purpose limitation.

Article 20(2) reads: "*Member States shall provide for the controller to implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*".

Data protection/**Privacy impact assessment** is also made mandatory for controllers in situations "where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons" [EUR]. PIAs will be needed to detect analyse privacy risks, propose privacy solutions and demonstrate compliance with the privacy regulations.

Consent as stated in the GDPR must be explicit, and a request for consent to a data subjet must be clearly stated to allow for lawful processing. The data subject should also be able to withdraw consent to the processing of the data subject's personal data at any given time. The GDPR clarifies that if a particular processing has different purposes, consent should be given by the data subject for each individual purpose. In the same vein, Notification and awareness is should be clear and in plain language. A notification can not be hidden among other information. Notification of data breach should also be in clear and plain language. Recital 39

of the regulation states that “In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language” [EUR].

3.4 Remote Healthcare Systems

A Remote Healthcare system is a technology or group of technologies that makes it possible for health services to be rendered to patients outside the medical centre, especially in patients' homes. Such types of systems are on the increase nowadays, increasing the flexibility, availability and reach of healthcare delivery. Advances in sensor technology, processing power and the internet are making it easier to deliver health care services into homes. Technologies involved in such systems include mobile devices, sensors, wireless technologies, digital medical devices, implantable devices, medical measurement devices, and portable computers etc. Remote healthcare services are delivered through different types of systems such as Telehealth, patient monitoring systems, mobile health applications, medication assistance, and healthcare social networks. These systems and technologies help provide critical health services to patients. A system may help track and assist patients' adherence to their medication, provide in-home assistance to the elderly, improved maternity care, or allowing healthcare workers remotely keep track of patients and visit the patient's home to provide emergency services when critical situations arise.

3.4.1 Privacy in Remote Healthcare

Privacy is important in Remote Health Systems because of the sensitivity and personal nature of health data. These systems make use of wireless and mobile technologies, allowing for the possibility of unauthorised access to patients' health information, with a malicious intent. Patients need to have control over who collects, uses, stores and discloses their PHI. Therefore, privacy needs to be integrated into the system at the design stage as imposing privacy restrictions on an already developed system has the potential to reduce the functionality, or restrict the purpose of the system [HL04]. There shouldn't have to be a choice between an added system functionality and a privacy feature. This significant problem of a trade-off between some critical system functionality and extra security or privacy features should be solved by implementing Privacy by Design principles in the development of remote health care systems.

Remote Healthcare Systems are generally at risk of privacy invasive activities from patients, health workers, health organisations, third parties and other non-health related entities or individuals. Avancha et al. in [ABK12] categorised privacy threats in mobile health systems into three groups, Identity threats, Access threats and Disclosure threats. They also discussed the importance of privacy preserving mechanisms such as Authentication, Anonymity and Location Privacy are important in mobile health systems. It is necessary to authenticate not only the patient but also the healthcare service provider and the devices. Authentication is mostly done using a username and password, which may be viable to successful attacks if not implemented with strict policies. Two-factor authentication mechanisms are also

growing in prominence. Patients' health records are usually identifiable with health systems because of the need to instantaneously appropriate a health information to the right patient for treatment and diagnosis. However, if such health records are to b shared with third parties for academic, commercial, or other reasons, it is compulsory for these information to be de-identified before sharing. The patients also must have been informed about this and its purpose, with their consent being gotten. These guidelines are made mandatory by health data protection laws in different European countries and the United States.

3.4.2 Privacy Law in Healthcare and it's Lack in Mobile Health

There is no European regulation specific to data protection in healthcare, but many European countries have their national privacy laws for health information. For example, in Norway there are some regulations that include: the Personal Health Data Filing System Act of May 2001 [Data], and the Code of Conduct for Information Security in The Healthcare and Care Services Sector [fHA]. The code of conduct contains all information security regulations relevant for organisations that process health data, developed from the Personal Data Act. The Personal Data Act is the broad data protection regulation in Norway covering the general protection of personal data. It is important to note that these kinds of laws in European countries usually do not cover the use of health data in mobile devices 1.e mobile health privacy issues. Most of the laws are applicable to health systems in healthcare centres or systems with a connection to a health centre's internal system, network or database. The practices of standalone mobile health applications are therefore not regulated. This is not ideal.

The EU's GDPR covers a wide range of personal data, which includes personal information. Because the GDPR applies to personal data collected and processed in any environment, mobile health data should fall under its umbrella.

The lack of proper regulations in mobile health allows for privacy invasive practices to be carried out easily. For example health data can be stored by device vendors and mobile network operators without the patient having control of over the flow of their PHI [ABK12]. Patients may think that only the operators of the mobile application have access to their health information.

Chapter 4
Towards Operationalising Privacy by Design

This chapter presents highlights of some relevant works that have been done to push forward the transition of PbD from a regulatory standpoint to an engineering framework. This is necessitated by the evident problem of PbD principles still being vague in IT software and systems engineering circles. Privacy in general is a fuzzy concept, which is usually misconstrued for security.

Kroener and Wright in [KW14] emphasised the importance of a PIA in the identification of privacy risks, thereby locating areas where PbD principles can provide solutions. They went on to inform that operationalising PbD will involve PbD principles, a PIA process, and several PETs [KW14].

Hoepman explained the importance of utilising design patterns as a design methodology [Hoe14]. He explained and differentiated between design strategies, design patterns and PETs. To tie privacy with the development process of a system, Hoepman informed of the application of privacy design strategies in concept development and analysis phases, design patterns applied in the design phase, and PETs during the implementation phase [Hoe14].

In NOKIA's efforts towards PbD application in engineering practices, it proposed the Privacy Engineering & Assurance Discipline [NOK]. Privacy activities were mapped onto production creation phases such as Education, Planning & Concepting, Design, Implementation, Testing, Release and Operations. The rivacy Engineering & Assurance Process is made up of the Privacy Engineering component, which involves a threat identification and mitigation cycle, and the Privacy Assurance component which involves verifying that privacy requirements have been properly implemented [NOK].

The EU funded Preparing Industry to Privacy-by-design by supporting its Application in Research (PRIPARE) programme came up with a methodology [CNDA$^+$] for the application of PbD that can be easily merged with most system development

phases. The proposed PbD process is divided into Analysis, Design, Implementation, Verification, Release, Maintenance, Decommission phases. There is also an additional phase called Environment and Infrastructure which is a central item that deals with the organisational structure. A PIA process is integrated in the lifecycle to run in parallel, beginning at the analysis phase. The Analysis phase consists of these processes: Functional Description and High-Level Privacy Analysis, Legal Assessment, Privacy and Security plan preparation, Detailed Privacy Analysis, Operationalisation of privacy principles, and Risk Management. The Operationalisation of Privacy Principles process aims to replace abstract privacy principles with technical observable measures [CNDA$^+$]. In this process privacy guidelines and principles are chosen, and then refined into a set of detailed privacy conformance criteria that define technical and organisational requirements that should be met. These privacy conformance criteria are a list checkpoints, that can also be later checked against for compliance. The complete list of all the processes in PRIPARE's eight methodology phases is presented in fig 4.1 . PRIPARE has produced a list of such criteria applicable to different situations. PRIPARE's published works have been the most detailed and productive.

These efforts have been a positive move towards operationalising PbD, but more work has to be done to create standardised frameworks for implementing PbD in different kinds of technological systems. Thus, the importance of this thesis in contributing to the PbD discuss.

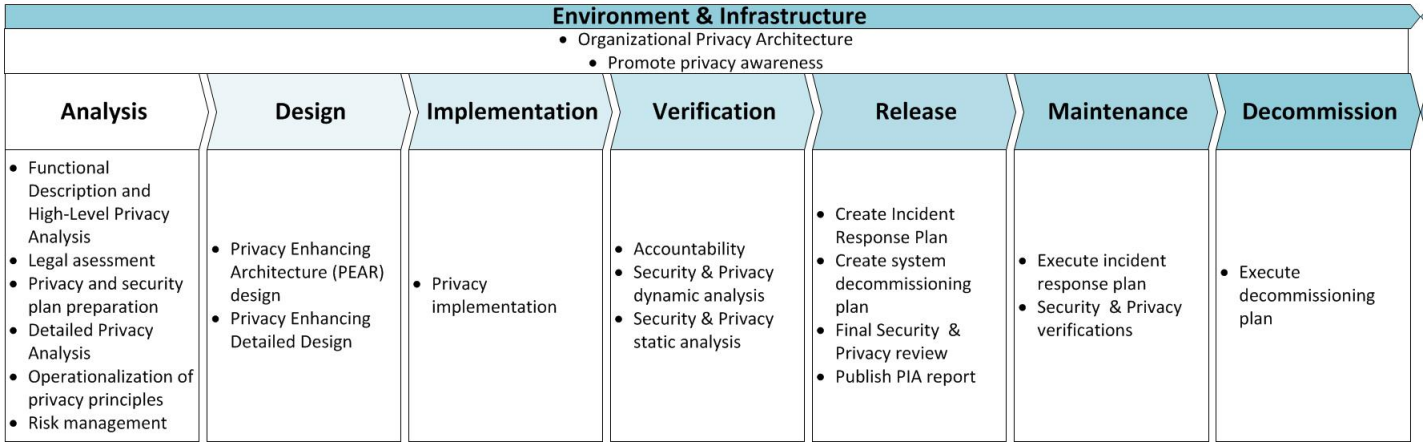

Figure 4.1: Phases and processes in PRIPARE methodology. Taken from [CNDA$^+$]

Chapter 5
Appraisal using PIAs

Privacy Impact Assessment (PIA) is an effective method used in this thesis to display some results from data collection during this study and more importantly, to analyse them. It has also been used here to some extent, to demonstrate the use of this technique and its relevance to engineering PbD. A PIA is a process used to detect privacy risks, analyse those risks and recommend solutions in form of privacy controls with respect to a system or project. A PIA is made of of different steps, risk analysis being the key step with respect to PbD [DDFH+15].

Responses from interview participants and documents such as risk assessments were used in formulating these PIAs. The PIA guide on privacy impact assessment in health and social care employed was that of the Health Information and Quality Authority in Ireland [IA]. It was used because of its specific focus on health projects and its suitability to the studied projects. The PIA threshold assessment questions from [IA] can be seen in Appendix C. Refer to other sections of [IA] for detailed explanations of topics considered in these PIAs.

Four PIAs are shown in this chapter, and one general privacy assessment of an organisation's development activities. The interview participant from Platac was only able to provide some information which was not specific to a particular system, among the number of remote healthcare systems the organisation produces.

5.1 MIGEX

Below the PIA created for the MIGEX project is displayed. Pseudonyms have been used for the names of organisations, disease being treated and the project or system itself.

5.1.1 Threshold Assessment

Questions from the initial assessment of the project that have a 'yes' answer are stated below. These questions led to the conclusion of the need for a PIA to be executed.

Does the project involve:

- The collection, use or disclosure of personal health information? Yes.
- Sharing of personal health information within or between organisations? Yes.
- The creation of a new, or the adoption of an existing identifier for service users; for example, using a number or biometric? Yes.

5.1.2 Privacy Management

There is a data protection policy for the Hospital's operations in general. It is not specific to the MIGEX project. The policy is the code of secrecy, which is in line with the national health and personal data regulations.

The service provider (the hospital) is the legal data controller for all personal data within the scope of the project.

There is an appointed Data protection officer at the hospital.

ExtraTrans, which is the organisation in charge of setting up the remote interface between the app on the user's smartphone and the hospital's electronic system or journal, is well versed in security, and therefore it is assumed that it will utilise a privacy policy.

5.1.3 Description of the Project

The project is a mobile health application that aids treatment of a disease - Piblio. The application has been developed and currently functions as a standalone app. A new feature which allows data to be transferred from the phone to the hospital's health records, allow doctors have access to a patient's Piblio data without having to see the patient and the application physically is to be implemented. This feature will be optional for an end-user.

The service provider or and data controller is a hospital. The secondary service provider is the ExtraTrans organisation that will provide the service that allows for the transfer of data from phone to Hospital health records. External software developers developed the application. The hospital also performs quality assurance for the project, with doctors specialised in Piblio treatment drawing out the guide for the design of the application. The hospital seeks to use this app to make it easier for its Piblio patients to keep track of symptoms and record occurrences using smart phones which are always with them, rather that recording them on paper. It is a standalone app, with all data stored on the patient's smart phone. The patient can take the phone to the doctor for the doctor to see the Piblio records before treatment. The patient registers the occurrence of symptoms and drug consumption over time.

The doctor must have told the patient to fill in records of the ailment occurrence for a period before the next appointment. The app in turn makes it possible for the physicians to prescribe medications correctly based on this record. Also, when a medication has been prescribed, the physician would like to track the effect of the medication on the illness over a period.

The Patient can send the Piblio and medication records from the phone to an email address.

The overall aim of the of the project is to drastically improve treatment of the disease.

Reasons behind the project:

- The inconvenience of patients having to register their Piblio symptom patterns on paper.
- The wrong use or overuse or abuse of prescribed drugs.
- Inaccurate record of the disease given to the doctors by patients.

The project is currently active in the home country, but with plans to release it to other parts of the world.

5.1.4 Project Type and Stage of Development

The mobile app which is already deployed, is to be altered to provide patients or end-users with an optional feature, which will allow for physicians at the hospital to access the patient's health data, by transferring the data from the phone to a server hosted by ExtraTrans, an IT service providing organisation, and from the server to the hospital's electronic journal. The current state of the project therefore focuses on creating a communication interface between the app in the user's phone and the hospital's information system via the ExtraTrans server. This will allow

patient data from the app to be uploaded to the server, and the doctor can log in to the ExtraTrans server and retrieve the information.

The new feature has only been conceptualised, no work has been done towards developing it apart from a risk assessment effected.

5.1.5 Project Scope

What information is to be collected?

The Information collected in this mobile application is Piblio records containing the frequency and intensity of symptoms, and medication consumption patterns, which are all personal health Information. The data about the disease is collected over a period. Also, a list of codes (for de-identification) linked to each patient will be stored at the hospital's end. The new option of data transfer brings about the need for proper awareness, notification and informed consent. The service providers stated that they have that in consideration, and that there will be an information page made available to users, for which they will agree to before making use of the option to transfer data from the mobile application to the hospital's e-journals or patient information system. Other ways of passing information along to users will also be considered.

The current state of the application does not have much by the way of informed consent. Information about data collection use and disclosure is done informally through the doctor handling the patient's case and the patient agrees to allow the doctor to access the data on the phone by taking it to the doctor.

Uses of Personal Health Information:

- Treatment of patients with frequent Disease symptoms.
- Graphical and numerical analysis of patient's Piblio records.
- Accurate prescription of drugs and monitoring of its effects.

The potential for data sharing in the standalone app is almost non-existent. The Hospital doesn't intend sharing data with any third party or selling data to pharmaceutical companies. With the new transfer option, the potential of patient's data being shared with ExtraTrans arises. The hospital is yet to consider how the patient will be informed.

After the ExtraTrans option is implemented, Information will be linked with hospitals' information system containing patient journals.

In the second phase of the project, that is the implementation of the ExtraTrans

option, a code will serve as an identifier for each app user, and the code list will only be stored at the hospital's end. To use the ExtraTrans option, a user will be assigned a code as an identifier. The user's data is sent electronically, accompanied by the identifier.

5.1.6 Information Flows

This section describes the flow of information in MIGEX system, making it possible to notice where privacy issues may arise. The information flow diagram 5.1 and table is able to show how PHI is collected, used stored, secured, disclosed and disposed of. The word 'secured' as it is used here, refers to every mechanism used to protect the information and maintain privacy.

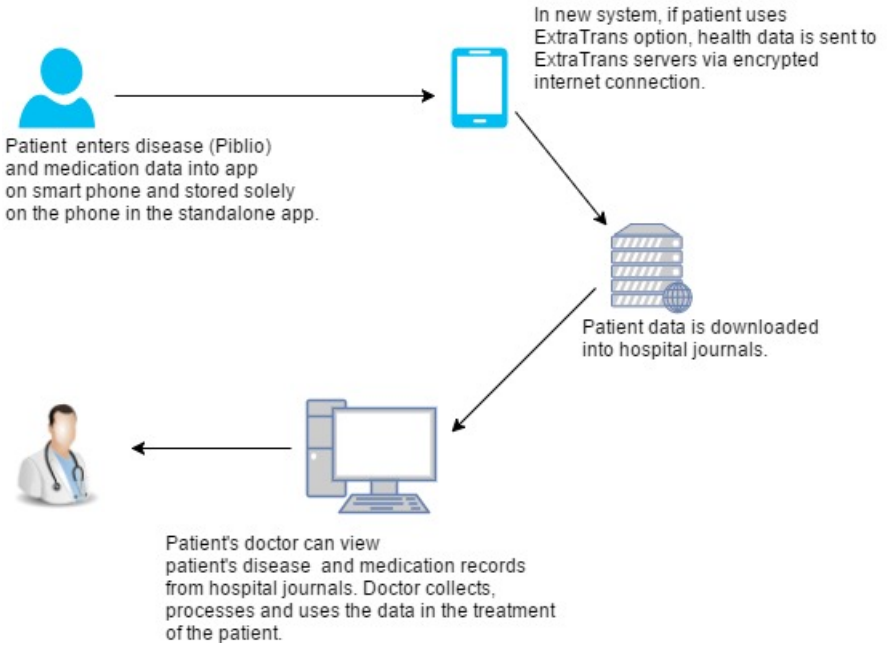

Figure 5.1: An illustration of the information flow in MIGEX. A communication interface which will allow doctors remotely access patients' health information from the app on their smartphones is to be implemented.

Table 5.1: Information flow table for MIGEX System. The PHI in the system is the Piblio record, Medication record and the code list. The privacy preserving mechanisms employed are stated in the column SECURED, with the Piblio and medication record being protected in five ways.

PHI	COLLECTED	USED	RETAINED	SECURED	DISCLOSED	DISPOSED OF
Piblio record, Medication record.	by: Doctor.	by: Doctor presiding over patient's treatment.	by: Patient, Hospital.	how: 1. Data only stored on the phone in the standalone app. 2. Only encrypted data is to be sent electronically using the ExtraTrans option. 3. Patient data is also sent de-identified.	by: patient or end user	
	how: patient takes phone containing app to the doctor. With the new ExtraTrans option, Doctor can access the data through hospital system remotely. In this case, the data is downloaded to the hospital journals via the ExtraTrans server.	uses: Treatment of patients with frequent disease symptoms. Graphical and numerical analysis of patient's Piblio records. Accurate prescription of drugs and monitoring of its effects.	where: patient's phone (standalone app), hospital journal/records (for the ExtraTrans option, or if doctor manually registers the data).	how: 4. One-way communication allowed, where end-user can push his personal health data via the ExtraTrans service, but can't pull or edit any data.	to: Doctor. how: physically presenting the phone, sending to an email, or using the ExtraTrans transfer option.	how: 1. Uninstalling the standalone app deletes all the data from the phone. 2. Patient data stored in hospital journals is not disposed of, but stored indefinitely.

	from: patient's phone.		how long: patient data is retained in the phone as long as the app is installed, and in the hospital's records Indefinitely.	how: 5. The hospital believes ExtraTrans to be an organisation that emphasises security. It expects them to use secure technologies that will protect privacy on their end of the system.		
Code list (Identifiers)	by:Hospital	by: Hospital	by:Hospital	by: Hospital		
	From: Patient or end user.		why: to match patient Piblio data coming from phone with the right patient record in hospital records.			
	How: patient enters a code to use the ExtraTrans transfer option.	How: code to be matched with real patient identity in code list.		How: secure storage in hospital system's database. Only doctor treating the patient will have access to it, ExtraTrans will not have access to it.		
	where: on user's phone.	where: in Hospital's information system	where: stored in database of hospital's info. system or hospital journal.			

Data subjects i.e. Patients or users, have access to their information on their smartphones using the app. They can also apply to see who has accessed their information in the hospital's journal. It is not clear if they can correct data stored in the hospital's journal.

5.1.7 Identification and Analysis of Privacy Risks

Privacy risks are concerns about privacy of individuals that have the probability of allowing a privacy intrusion, to the detriment of the individual and the service providing organisation. Some privacy risks in this project have been identified and ranked using the risk matrix structure [RC] shown in fig 5.2.

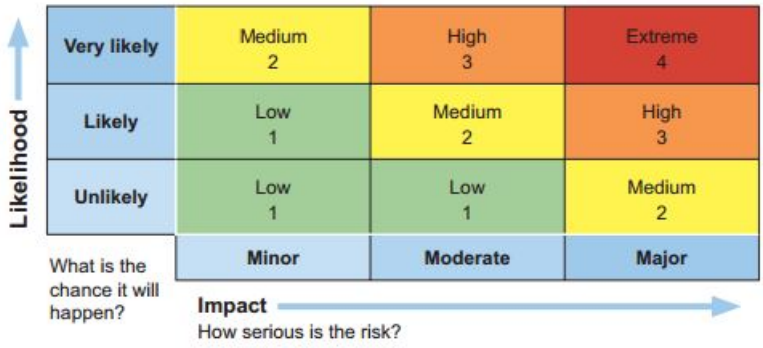

Figure 5.2: The Risk matrix combines impact and likelihood to give a risk rank or priority. Figure Taken from [RC].

Table 5.2: The table displays analysis of privacy risks to the MIGEX system. Privacy risk scores or ranking are based on the likelihood and impact, combined as shown in the risk matrix.

Privacy requirements	**Privacy concern**	**Likelihood**	**Privacy Impact**	**Risk**	**Comments**
Authorised collection of personal health Information.	A doctor in the hospital that is not treating the patient may access the patient's data from ExtraTrans server.	Unlikely	Moderate	Low	Hospital policy rules do not allow doctors to access a patient's information from hospital records if not in charge of treating that patient, with an exemption in case of emergency.
Notification of the user of collection and use of patient information.	Physician may access user data from ExtraTrans server without the knowledge of the patient.	Likely	Moderate	Medium	Patient or user must choose the ExtraTrans option before a physician can access data remotely. It is not clear if the physician can continue to collect the patient's data after that instance, without the knowledge of the patient.
Data and collection minimisation.	1. Collection and use of personal health information that is not needed for Piblio treatment.	unlikely	Moderate	Low	1. The fields in the app only ask for details meant for the needed purpose.
	2. Patient may no longer want to use the ExtraTrans Option, without uninstalling the app.				2. A feature that allows a user to opt-out of the ExtraTrans option should be provided to minimise the collection of unwanted data.

Prevent unauthorised disclosure.	Loss of phone may lead to disclosure of patient's information.	Likely	Major	High	Patients need to keep phones safe and protected, and not enter sensitive data not needed into app fields.
Accountability	Inability to carry out a proper audit, and see who has viewed patient information.	Likely	Moderate	Medium	In the hospital system, identities of doctors that access patient data are logged. It is currently not clear if any access to ExtraTrans server will be logged.
Confidentiality and authorised disclosure.	1. Attacker may access network traffic between app and ExtraTrans' server. 2. False user may try to collect data of server.	Likely	Moderate	Medium	1. Traffic is to be encrypted. 2. End users will only be able to push data, and not pull data.
	3. ExtraTrans employee access to user information. 4. Patient enters a mistaken email address when sending the health information from the phone.				3. Not clear if ExtraTrans will have any kind of access to patient information.
Unlinkability	Identifiers may be obtained by attacker, allowing patients to be linked with their data.	Unlikely	Moderate	Low	The code list will only be stored in hospital secured systems.

Compliance to GDPR	Non-compliance leading to fines, loss of trust from users. Also, fines from the EU.	Likely	Major	High	Currently standalone mobile health apps are not covered in national health data protection regulations as a health device, allowing for illicit collection, processing, disclosure and sale of user information. However, they will be under the jurisdiction of the GDPR.

5.1.8 Addressing the Risks

In this section solutions are put forward to avoid or mitigate the risks. Focus will be on risks with medium rating and above.

Table 5.3: Potential solutions in form of privacy controls to avoid privacy risks in MIGEX.

Privacy concern	**Risk**	**Privacy solution**
Physician may access user data from ExtraTrans server without the knowledge of the patient.	Medium	A clear statement should be sent to the app user data is to be collected or processed from his phone via the ExtraTrans server. The notification can be sent in-app or via email.
Loss of phone may lead to disclosure of patient's information.	High	App users should be informed about the risk, and keeping their phone secure and password protected. This is reflected in the risk assessment carried out by the hospital. Also, a privacy policy for the application needs to be put together, and communicated in simple and clear terms to end-users.
Inability to carry out a proper audit, and see who has viewed patient information.	Medium	Logging of activities or point of access by physicians to the ExtraTrans Server end must be done.
1. Attacker may access network traffic between app and ExtraTrans' server. 2. False user may try to collect data of server.	Medium	1. Encryption of data traffic is to be effected. 2. End users will only be able to push data, and not pull data from ExtraTrans server. Strong security mechanisms should be used to secure server.

3. ExtraTrans employee access to user information. 4. Patient enters a mistaken email address when sending the health information from the phone.	Medium	3. ExtraTrans should only be able to access data in rare cases for maintenance purpose. An employee should be enough and role based access can be used to ensure only such employee gets access to patient data. Also, data should not be retained at the ExtraTrans end after it has served the purpose of being sent to the hospital. Produce a data retention policy, and use secure destruction of the data. 4. Patients should be made aware of the risk of not entering correct email addresses when sending information.
Non-compliance leading to fines, loss of trust from users.	High	Steps should be taken to ensure that all parts of the application conform to the EU regulation. A privacy professional can guide the developers and hospital in making necessary changes. Privacy by design should be employed in the implementation of the updated version with the ExtraTrans communication interface feature. Also, a privacy policy for the application needs to be put together, and communicated in simple and clear terms to end-users. This policy can visible to the user via the app store, and displayed on the service provider's webpage.

5.2 PYRO

Below is the PIA created for the PYRO remote healthcare system developed and supplied by Pintex for home healthcare centres.

5.2.1 Threshold Assessment

Questions from the initial assessment of the project that have a 'yes' answer are stated below. These questions led to the conclusion of the need for a PIA to be executed.

Does the project involve:

- The collection, use or disclosure of personal health information? Yes.
- The linking, matching or cross-referencing of personal health information that is already held? Yes.
- Sharing of personal health information within or between organisations? Yes.

5.2.2 Privacy Management

Pintex has a privacy policy for the system which is based on the information and templates gotten from the national data protection authority. The whole policy document was not sent to the customers (home healthcare centres), due to its complexity, therefore it was summarised. This also means it was simplified. A data protection sheet was agreed upon by Pintex and their customers.

There is also a detailed document drafted from the health data protection law, it is used by Pintex to check and see that all requirements of the law have been fulfilled. Compliance check is done once each year.

A manager at Pintex also doubles as the security or privacy officer. He has an employee dedicated to attending conferences organised by the national data protection authority, in one of his efforts to keep abreast of the latest happenings regarding data protection techniques and regulations.

5.2.3 Description of the Project

PYRO is a software platform for health devices. It consists of two main parts; app running on a tablet of the patient or end user, and a database and user interface for healthcare personnel. The platform is made up of an Operating system for medical devices, and was developed using post SQL databases, python, and a little bit of JavaScript. It was developed from the bottom up by Pintex with Agile Software development methodology. PYRO provides a platform for integrating new health

apps and devices. The system allows medical measurement devices to be connected to a tablet via Bluetooth Low Energy connection. The PYRO project was developed by Pintex an organisation that helps healthcare providers implement new services. Pintex is both the developer and a service provider for the home care centres and regions. The home care centres are also service providers for the end user or patients. PYRO is a remote health care system that allows medical measurement devices and medication dispensers connect to a tablet (which has a specialised app on it) via Bluetooth. The patient's tablet and app is in turn connected to the Application and Database Servers, and all data are stored in a data center operated by web services organisation renowned for secure data storage. which are cloud based via the internet. The database server takes care of integrity and responds to requests for data, while the application server manages authorisations.

The tablet is set up with the app by Pintex and is not allowed for the patient to use it for any other purpose. Measurements such as the patient's body temperature, body weight, blood glucose, and blood pressure can be taking using medical measuring devices. All measuring devices possess Bluetooth Technology. The system can be tailor made to suit customer needs to some extent, also adjustments can be made to allow medication dispensers or a measuring device from two different suppliers to run with the system.

The system is currently being used by home healthcare centres which are being run by regional or community governments around the home country. The home care centres come equipped with workstations for nurses or clinicians to attend to incoming notifications from patients' devices. These workstations run the core PYRO Operating system. Also, the patient answers some survey questions daily which are also sent to the home care centre. The nurses at the home care centres can also view the medication history of the patients they have access to, showing which meds have been taken or not from the dispenser.

In summary, the PYRO platform Is made up of the patient app, the Operating system, backend system, and the user interface for nurses and clinicians at the home care centres. Medical measurements and relevant vital signs are sent to the patient's tablet (provided by Pintex at the behest of the home care centres), and then these measurements are from the app in the tablet to the backend servers via the internet, allowing the nurses to view the data and send patient records and journal notes the other way. The system also has the possibility of giving access to the patient's family doctor, but this is up to the home healthcare center to decide and create a user for the doctor.

Aim of the project. The aim of the system is to provide a combination of easy remote clinician consultation and patient monitoring, while giving the patient

more involvement and control. The goal is to keep track of the patient's health condition and use such information to send a clinician to attend to him at home in dire situations, or for the family doctor to diagnose, treat and track the patient's recovery.

The project is currently operating in some cities in the home country.

There is a plan to link the system with already functional systems in these home care centres such as old information systems and journals which were not developed by the service provider.

5.2.4 Project Type and Stage of Development

The system has been in existence for some time, and it was developed using an Agile software development methodology, which allows for development in iterative and incremental patterns. New features are planned to be added to the system. It is a remote healthcare system, merging some features of a patient monitoring system and a telehealth system.

5.2.5 Project Scope

What information is to be collected? The Personal Health Information to be collected in the PYRO remote care system includes: Patient's medical measurements, Medication collection records off medication dispensers, nurse's comments about patient's health. Other personal data to be collected includes: First and last names, national Identity number, gender, home address, zip code, city, zone, door/key box code, phone number, spoken languages, login information, messages nurses write to the patients and any other information about the patient that the nurse or clinician at the home care centre deems important to be written in the patient journal notes.

Service users are aware of the proposed collection, use and disclosure of their personal information. Pintex being the developer of this system is not the organisation to ask for consent from the patients, this is to be done by the Home healthcare centres who are the customers of Pintex. In this sense Pintex is a data processor and the Home healthcare centres are data controllers or owners because they are in full control of the system after they are deployed by Pintex. However, Pintex provides the regional or community government and home healthcare centres with a template eliciting consent from end users properly. Interview was only held with Pintex; therefore, no information is gotten regarding the consent process, but it is safe to assume consent was gotten from patients for the use of their data.

Uses of the personal information. The medical measurements from the patient's body are used by the home healthcare centres and optionally the family

doctor to keep track of the patient's health condition. Nurses or clinicians are sent from the home healthcare centres to attend to the patient in their homes when the need arises. A patient's family doctor information in the patient's journal to give diagnoses, medications, and track recovery. Patients can also see all their medical records on the tablet.

Personal data such as names, address, phone number etc. are important in a patient oriented healthcare system in knowing the person you are dealing with. Such personal data cannot be anonymised.

It is also important for nurses at the home healthcare centres to write comments into a patient's journal and send the patient messages on the tablet where the need arises.

Currently there are no changes to the initial purpose of using the information collected.

Potential sharing of information. A patient's family doctor may be given authorisation to access the patient's journal in the system. The patient and the home healthcare centre agree on taking this step or not. It is important to note that many a times the patient may elderly or unable to take this decision alone, therefore the home healthcare centre is left with the sole responsibility of deciding if this step is needed.

Also, after Pintex has completed the installation of the system, and training of the staff, it hands over the reins, but a single Pintex employee is assigned access to raw data in the database of the system. The home healthcare centres are aware of this. The Pintex employee works on the database. Apart from this employee, Pintex will have no other access to patient records unless the customer (home healthcare centre) makes an agreement with them to grant them access. This may be for technical support or other reasons. It is not clear how the end users or patients are informed of this.

There is the possibility that the system will be linked to other health systems that under the auspices of regional authorities. These other systems are not developed by Pintex.

5.2.6 Information Flows

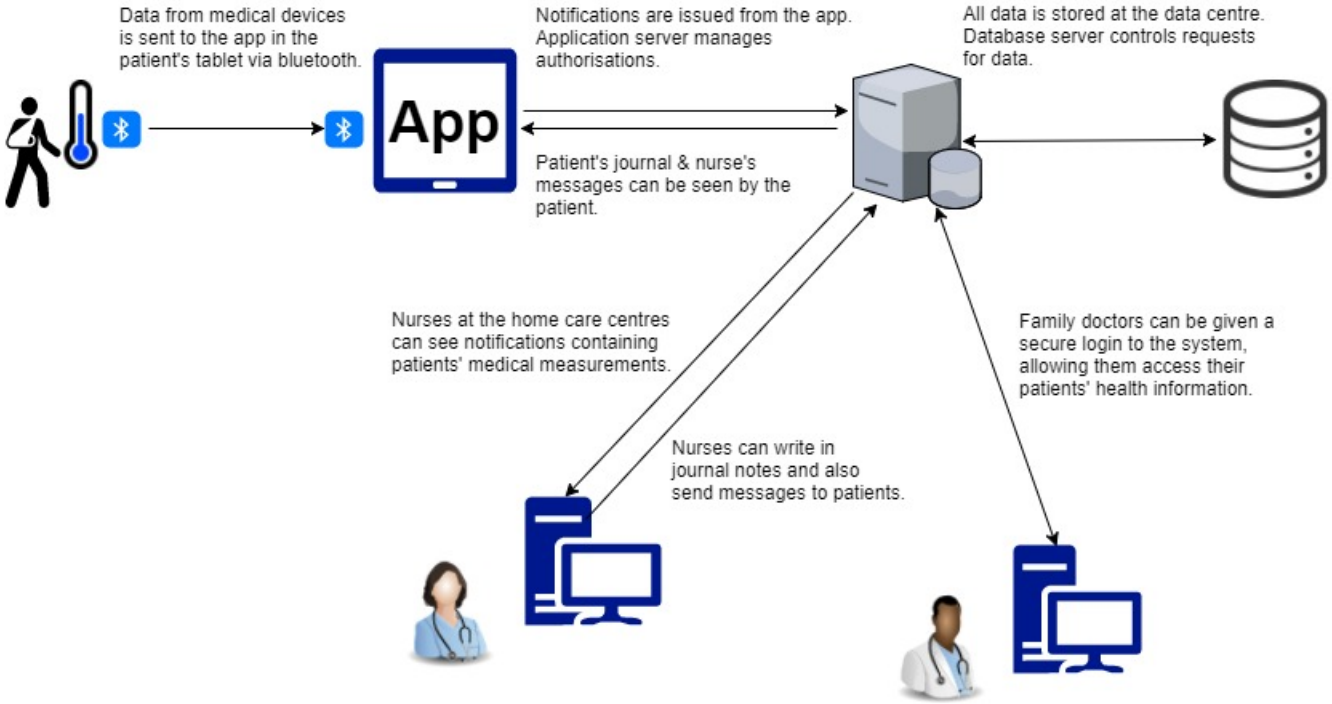

Figure 5.3: An illustration of the setup and information flow in the PYRO system. The client of patient end of the system consists of the medical measurement devices, medication dispenser and a tablet with the PYRO app running on it.

Table 5.4: Information flow table for PYRO System. The PHI in the system are grouped into three (3): medical measurements and medication dispensing records, Nurse's journal notes and messages to patients, and lastly patient's personal data.

PHI	COLLECTED	USED	RETAINED	SECURED	DISCLOSED	DISPOSED OF
Medical measurements and medication dispensing records.	By: Nurse or clinician at home healthcare centre. From: Medical measurement devices and medication dispensers in patient's home. Medical devices take measurements from patient's body, and the patient collects drugs from the medication dispenser.	By: nurses or clinicians at the home healthcare centres, and optionally family doctors. Uses: to monitor patients' health condition, symptoms, medication adherence and recovery. The information also allows the home healthcare centre and/or family doctors to know about emergencies or critical situations in the patient's health before they occur.	By: home healthcare centre, who have full access to the database of the system. Where: All information and patient journals are stored in a data centre operated by an internationally renowned web services organisation. Backups are taken and stored at the data centre every five minutes.	By: Pintex and home healthcare centres. How: 1. All internet communications in the system are encrypted using HTTPS, including security certificates to prevent phishing. It is not allowed to send any data via email. 2. Servers deployed by Pintex are protected by strong encryption at several levels.	By: Home Healthcare centre. To: 1. There is an option to give a patient's family doctor access to the patient's health information. 2. Patients are also able to see all their health information via the app on their tablet.	The law allows all patient data to be stored for at least 7 years due to its medical purpose. Sensitive information such as rape can be deleted if the patient requests that. A patient can ask for his data to be deleted but it's up to the regional authority which governs the home healthcare centre to decide if the wish will be granted.

	How: The data is sent form the medical devices to the patient's specialised tablet via a Bluetooth connection, and from the PYRO client app on the tablet to Pintex deployed servers, where the clinicians at the home healthcare centre can access the data from. This is made possible over an internet connection.	Uses: Notifications are sent to the home healthcare centre from the PYRO app in the tablet. The nurses can see notifications on a dashboard in the core system. Individual threshold measurements are set specific to a patient, and when it is exceeded a notification is sent to the nurse presiding over that patient.	How long: The national health laws allows patient information to be stored for at least seven years. Currently all data is aggregated and retained. It will be the responsibility of the regional authorities and the home healthcare centres they preside over to decide if they need to delete any data.	How: 3. Authentication is achieved using username and password (Home healthcare centre sets rules for password), 2-factor authentication with SMS, and network address for the nurse's log in PC is checked. 4. All access the system is logged. 5. Role based access control is used to decide what information anyone can see.	When: patient demands for the doctor to be given access.	
	Where: nurses collect information from their workstations at the offices of the home healthcare centres. When: Measurements are sent from the patient app to the core system real-time.			How: 6. nurses or clinicians are assigned to logical Zones after user accounts have been created for them by the home healthcare centre. Employees only have access to patients' information belonging to that zone i.e. a number of patients they are to monitor.		

				How: 7. By default a nurse has no zone once the user account is created and can therefore see no data. 8. Encrypted login is provided for family doctors. They are given access to only their patient's health information.		
				9. The Data centre is trusted to be highly secure and run by a renowned organisation. It is audited by an external organisation. 10. Automatic logout of nurse from the PYRO system after a certain duration of inactivity. 11. see section 5.2.2.		
Nurse's journal notes, and messages to patients.	By: PYRO system. From: Nurses or clinicians at the home healthcare centres.	By: Nurses' notes used by nurses, patients and optionally family doctors.	Same as above.	Same as above	Same as above	Same as above

Patient's personal data e.g. Name, address, phone number etc.	From: Patients.	By: Nurses or clinicians at the home healthcare centres, and optionally the family doctors.	Same as stated for medical measurements above.	Same as stated for medical measurements above.	Same as stated for medical measurements above.	Same as stated for medical measurements above.

It is important to note that Data subjects 1.e the patients, have access to their information using the PYRO app in their special Pintex delivered tablet.

5.2.7 Identification, Analysis and Addressing of Privacy Risks

Table 5.5: Privacy risks in PYRO are discussed and techniques to mitigate them proposed. Some risks that would have been considered at the early stages of development have been resolved.

Privacy requirements	**Privacy concern**	**Likelihood**	**Privacy Impact**	**Risk**	**Privacy solution**
Secure communications	An attacker may try to obtain data being transferred over communication channels.	Likely	Major	High	All communications over the internet are encrypted. It is not known how the transfer of data using Bluetooth is secured.
Confidentiality of Information.	Attacking network and storage facilities to obtain patient's information.	Unlikely	Major	Medium	Servers are well protected with several levels of encryption keys. Data centre is secure and run by a reputable organisation.
Authorised access to PHI.	Clinicians or family doctor may gain access to information they should not have.	Unlikely	Major	Medium	Role based access control is employed, logical zones are used to restrict access.
Proper user notice and consent.	Patients not being aware of the use of their health information, privacy policy, and any data breach.	Likely	Minor	Low	1. It is not known how the privacy policy, and any data breach are communicated to the end users.
					2. Patients, nurses, and family doctors and their caretakers should be made aware of practices that will amount to privacy risks when using the system.

Data and collection minimisation.	Sensitive information about patients that is not essential being entered into the system by nurses.	Unlikely	Moderate	Low	The fields used in the system at the home health care centres only allow information that is needed. However, journal notes from nurses may take any information. The Privacy policy should restrict nurses from entering any inessential and sensitive data.
Prevent disclosure of patient's health information due to patient's error.	Patient may mistakenly disclose information while using the tablet.	Likely	Moderate	Medium	The tablets have been designed to allow a singular use, which is to run the PYRO app.
Accountability And compliance	No records of access and transactions made in the system.	Unlikely	Major	Medium	1. All access to data and system resources are logged. 2. System audits and compliance checks should be carried out at home healthcare centres.

5.3 DELV

DELV is a mobile health application that aids the treatment of patients with the disease 'Enterese'. Enterese is used as a pseudonym. The PIA process actualised for the project is detailed below in the various subsections.

5.3.1 Threshold Assessment

Questions from the initial assessment of the project that have a 'yes' answer are stated below. These questions led to the conclusion of the need for a PIA to be executed.

Does the project involve:

- The collection, use or disclosure of personal health information? Yes.
- The collection, use or disclosure of additional personal health information held by an existing system or source of health information? Yes.
- The use of personal data for research or statistics, whether de-identified or not? Yes.

5.3.2 Privacy Management

The service provider which is the hospital is the legal data controller for all personal data within the scope of this project.

The service providing hospital in this case has a data protection officer and a data protection policy that covers personal data that comes into the hospital's health records.

5.3.3 Description of the Project

The DELV project included developing an app for managing the treatment of patients with enterese, which is a disease that demands serious monitoring from doctors and strict adherence to prescriptions by the patients. The project aims to develop ways to provide effective and safe home treatment of enterese patients with medication.

The project is currently limited to the set of patients used to test the DELV app at the hospital.

5.3.4 Project Type and Stage of Development

DELV is a mobile health application to be used on Android and iOS smartphones and devices of patients. The first stage, which is completing the stand-alone app is

now in its testing phase.

What information is to be collected?

The information to be collected includes: the names of drugs, how long the drugs are to be taken, dosage, consumption pattern (e.g. twice daily), and what other kinds of medicines can and can be taken alongside etc. It is the patient's doctor that will enter these details which can be called a treatment cure. A dosage calculator is also provided as a feature in the app. Reminders are generated by the app to guide the patient in following the proper treatment order.

DELV app is a standalone app, meaning that patients must take their mobile device containing the app physically to the doctor to enter this health information. There is a plan to make it possible for the doctor to make it possible for the doctor to do so remotely.

The patients are aware of the proposed collection, and use of their personal health information. The doctor informs them of verbally. Also on the about page of the app it is stated that data will be stored only on the phone, and won't be used for any other purpose.

The service users (patients) are seen to have consented to the use of their personal health information in accepting agreements and installing the app. Also, because they decide to use the app with the doctor in the hospital.

Uses of Personal Health Information

All patient's information is used in the treatment of the disease, monitoring of treatment progress, monitoring of patient responsiveness to medication and adherence to medication pattern. The application will remind patients of when to take their medicines and quantity to be taken.

5.3.5 Information Flows

Table 5.6: Information flow table for DELV app. The PHI in the system are grouped into two (2): treatment cure and medication record.

PHI	COLLECTED	USED	RETAINED	SECURED	DISCLOSED	DISPOSED OF
Treatment cure (comprising of names of medicine, dosage, dosage patterns etc.).	By: Doctor. The information is entered into the app by the doctor.	By: Patient.	By: Patient.	By: Hospital and patient.		By: Patient.
	How: Patient gives the phone to the doctor to enter information. When: It depends on the treatment cure. Patient may take phone to the doctor every 2 or 3 weeks.	How: Patient gets reminders and can also follow the schedule manually. This information is used by the patient to guide intake of medicines. Patients answer questions, to indicate medication taken or not.	Where: On patient's smartphone. How long: Indefinitely, until app is uninstalled.	How: 1. Patient keeps phone secure and may lock phone with a password. 2. Doctor is to enter a PIN code before being able to enter a new treatment cure into patient's phone.		How: Uninstalling the DELV app automatically deletes all the data.

				How: 3. Questions are limited so as not to collect information not needed. 4. When reminders appear on the screen of a patient's phone, they display no sensitive information that will disclose any health information to a person nearby.		
Medication record.	By: Doctor.	By: Doctor.	By: Patient and Doctor.	By: Same as for treatment cure.	By: Patient.	By: Same as for treatment cure.
	How: The doctor is able to check the app and see how the patient has been keeping to the treatment cure over a certain period.	How: The patient's record will aid the doctor in determining the next cause of action in treatment.		How: Same as for treatment cure.	How: Taking the phone to the doctor, and the doctor checking with the app.	How: Same as for treatment cure.

	From: The patient's phone using the app. When: The patient takes the smartphone containing the app to meet with the doctor.	Where: At the hospital.	Where: On the patient's phone, and may also be entered into the patient's journal at the hospital. How long: Pending the uninstallation of the app.		To: It is intended to be disclosed to a Doctor. Where: At the hospital.	

5.3.6 Identification, Analysis and Addressing of Privacy Risks

Table 5.7: Privacy risks in DELV are discussed and solutions proposed. Comments explain the privacy concern.

Privacy requirements	**Privacy concern**	**Comments**	**Likelihood**	**Privacy Impact**	**Risk**	**Privacy control or solution**
Confidentiality of PHI.	Patient losses phone.	Loss of phone containing the app may lead to a stranger gaining knowledge of a patient's health status and other health information.	Likely	Moderate	Medium	1. Patients are to be informed of the risk associated with losing their phone containing the app. 2. Patients should be told to keep phone safe and locked with password.
Authorised disclosure	Indiscriminate disclosure	Patient information can be disclosed to anyone with no restrictions on who gets to have it. This indiscriminate disclosure can be made by the patient or healthcare personnel.	Likely	Major	High	1. There should be an effective privacy policy for the app. It should be communicated clearly to the user. 2. The user should also be made aware of the risk in disclosing data to people without an important or useful cause.

						3. A disclaimer should be made to the app user that only authorised health professionals must enter the treatment cure into the app. This is pointed out in the risk assessment previously done for the app.
Data and collection minimisation	Collection of data not needed to achieve the project's aim.		Likely	Moderate	Medium	Questions patients are required to answer have been reduced or streamlined.

5.4 REXAT

PIA for REXAT, a mobile health application, is presented in the following subsections.

5.4.1 Threshold Assessment

Questions from the initial assessment of the project that have a 'yes' answer are stated below. These questions led to the conclusion of the need for a PIAs to be executed.

Does the project involve:

- The collection, use or disclosure of personal health information? Yes.
- A new use for personal health information that is already held? Yes.
- The use of personal data for research or statistics, whether de-identified or not? Yes. In the case of REXAT, users' personal data were de-identified during the study.

5.4.2 Description of the Project

Rexat is a mobile health application that gives the patients reminders of when to take their medications, and statistics on drug consumption over time. A medication list is entered manually by a pharmacist or physician, the patient or user receives reminders on the phone that he can respond to by selecting if the drug has been taken, not taken, or postponed, with reasons for the last two options given.

The development of this app was initiated as part of a study in a University, and further developed by a software developer with funding from the University. It is a standalone app with no connection to an external network and all patient health data stored on the phone. It is a native app that runs on Android and iOS smartphones. The medication history can be exported in a CSV (Excel format) file via email or using a USB cable. There is no data to be sent to the service provider.

The project aimed to improve adherence to taking medications and make it possible for a patient to track his/her medication intake by giving the patient more control and useful feedback.

The project was initiated as part of studying the effect of using technology in adherence to prescribed drugs for an ailment. It was restricted to a country.

5.4.3 Project Type and Stage of Development

This is a new project that has been completed and fully functional but in a test mode or beta version. The app may be modified in future updates. The university

study surrounding the start of the project has also been completed.

5.4.4 Project Scope

What information is to be collected?

Rexat allows for the collection of medication or drug prescription and consumption records, information about the medications, and reminders to take medications.

The medication list is collected to be able to provide reminders and serve as a basis for analysis over a period. Individual reminders entered by the user or the physician, which are separate from those created by the app due to the medication list entered by a health professional, can also be entered to allow for flexibility.

Users are aware of the collection of their personal health information, because is the one to give his phone to a physician or pharmacist to enter a medication list, the user also enters some reminders, and the user takes the decision on who to export the medication history and statistics to. The user may not be totally aware of how the exported information is used or disclosed, that is up to the recipient to inform the user.

Consent is given by accepting terms and conditions when installing the app on one's smartphone.

Uses of Personal Health Information

- The patient's data from the app is used by his doctor in tracking patient's adherence to prescribed drugs, treatment, and detecting the degree of advancement of the illness.
- The health information will also be used by the patient to self-manage their treatment and get useful feedback.
- The doctor or the patient will use information from the app to generate statistics and analyse them.
- During the initial University study, a select number of test patient information was used for study purpose, but anonymised and collected securely via USB cable into an encrypted hard drive, in a system with no connection to a network.

These uses of the information from the app are in line with the project's aim to improve adherence to medication by providing a tool to guide the patients drug consumption and motivate him to keep to the pre-arranged medication pattern.

There is to be no sharing of information with any third party and no linking of information to any existing or proposed system. This is a strictly standalone app.

5.4.5 Information Flows

Table 5.8: Table describing the Information flow in REXAT. The PHI in the system are grouped into two (2): medication list and drug information, and medication history.Secured column describes privacy techniques employed.

PHI	COLLECTED	USED	RETAINED	SECURED	DISCLOSED	DISPOSED OF
Medication list and information about the drugs	By: Rexat app.	By: Doctor and patient/app user.	By: Patient or user.	By: The app or the service provider and the patient.	By: Patient.	By: Patient.
	How: Patient's physician or pharmacist enters medications with dates, times and frequency of drug intakes into the app on the patient's smartphone. Information about the drugs may also be entered.	How: generate statistics of medication consumption from tables in the app's SQLite database exported in csv or excel file. Simple analysis of generated information or in-app data.	How: Stored by the app on user's phone.Where: In the app's SQLite database. How long: As long as the app remains installed.	How: 1. The Operating system guarantees that no other mobile app can access data stored in the SQLite database. 2. Rexat app does not store any data in the cloud, allowing no data to be accessible by the service provider.	How: exporting app data in a csv file and sending it to a system via USB cable or using the send-via-email option.To: Physician or anyone else.	How: uninstalling the app deletes all stored data.

	From: Doctor or Pharmacist.	How: Also, patient receives reminders with sound and a short text and responds to these.		How: 3. No sensitive information is displayed on the phone's screen when a reminder alert is activated.		
	Authority: It is advised that a trained physician or pharmacist enters the medication list. The patient authorises the doctor to use the app.	When: patient exports the health data from the app or sends it to the doctor via email field provided in the app. One may also send the information to oneself. Authority: Patient or user authorises the processing or use of the health information.		How: 4. Rexat app has no connection to external networks. 5. During the initial study, there was a code or pin to be entered by the user to gain access to the app. This was removed later to enhance usability for a commercialised app.		
Medication history.	By: patient or user.	By: Doctor, patient, and anyone else the user discloses it to.	By: Recipient of exported file.		By: patient or user.	By: patient and whoever holds the information.

	How: some tables in the SQLite database containing medication history of a certain period are converted to excel format. The excel or csv file is exported via USB cable.	Uses: Overall the app is useful in tracking patient's adherence to prescribed drugs, treatment, and detecting the degree of advancement of the illness. Other uses are mentioned above.	Where: in a smartphone, Computer system, hard disk or another storage device. How long: indefinite.	How: 1. the exported csv file can be stored in a system without connection to the internet or a network or in an encrypted hard disk as was done during the University study for the project.	To: physician or whoever the user decides to disclose it to.	
				2. The computer system can also be secured with password. 3. Also during the university study, data obtained from participants were de-identified.		

5.4.6 Identification, Analysis and Addressing of Privacy Risks

Table 5.9: Some Privacy risks in REXAT and probable solutions to mitigate them given.

Privacy requirements	**Privacy concern**	**Comments**	**Likelihood**	**Privacy Impact**	**Risk**	**Privacy control or solution**
Authorised disclosure	Indiscriminate disclosure.	Patient information can be disclosed to anyone with no restrictions on who gets to have it. A physician or pharmacist may also disclose it to others as they are not bound by any regulation or policy.	Likely	Major	High	There should be an effective privacy policy for the app. It should be communicated clearly to the user. The user should also be made aware of the risk in disclosing data to people without an important or useful cause, especially to non-physicians.
Confidential Transfer of data	Exporting medication history insecurely.	The app user may export the csv file to an unsecure system which can be exploited via the Internet. The csv file is not encrypted.	Likely	Major	High	The csv file can be locked with a passcode which only the user will know.
	Loss of phone.	User's phone gets lost or stolen.	Likely	Moderate	Medium	Make the user aware of the risk, and that the phone should be protected with a passcode.

5.5 Overview of Privacy in Platac Products

In the last interview held with a participant from the organisation Platac, responses to the questions were about the organisations products in general, not specific to a particular system, and the participant giving as much technical information as he could. A general assessment is described in the following subsections, instead of a PIA.

5.5.1 Service Provider & Product Description

Platac is an organisation that develops innovative IT products and solutions for healthcare organisations, hospitals, home care centres, regions and municipalities etc. who are their clients or customers. They develop several types of remote healthcare systems, mobile health apps, and patient management systems. Platac also carries out the installation and configuration of these products or systems.

The actual users of the systems produced by Platac are healthcare workers (including nurses, secretaries, medical transport staff, doctors etc.), elderly and patients in general.

All products are based on a Platac platform which is comprised of an OS, database servers (relational database and in some cases a reporting database), an integration server, application server and a messaging server. Platac systems are produced using Agile development, mostly based on the Scrum Methodology.

5.5.2 Data Control & Third Party Sharing

Platac systems share no data with third parties once they have been deployed. The customer is the sole data controller. Platac will have no access to data, unless the customer allows for the option of support and maintenance from Platac in their contracts. This will mean that designated employees at Platac will be able to log on to such systems, and have access to some users' personal information.

Platac customers will have technical employees e.g. Database administrators, who will have a high level of access to end user's personal information. Platac provides the means for client organisations to create users for the systems.

5.5.3 Access Control

Role based access control is employed in Platac systems. A newly created user has no access to any data until a role is assigned, then the user gets access to a section of data that is available to that role.

5.5.4 Use of Risk Assessment

Although Privacy impact assessments were not used in development processes, Risk assessments were utilised. The risk assessments which were full scale, were carried out at the beginning of developments and improved upon in a continuous process throughout development.

5.5.5 EU GDPR & PbD

The interviewed participant is aware of the EU GDPR but not in detail. The participant also stated that the organisation is not big enough to have a privacy officer, but some employees have good knowledge of the regulations consider it to make sure they adhere to it.

5.5.6 Privacy Controls

Platac as an organisation has a privacy policy.

Authentication and authorisation mechanisms use in products and systems. Authentication is mostly using username and password, but Platac is considering employing 2-factor authentication in some cases. When a user is authenticated, a token is generated for the user. The authorisation level for that user determines what he/she as access to.

Data transfer between client and server devices are encrypted using Hypertext Transfer Protocol Secure (HTTPS). Some, not all data stored in databases are encrypted.

A form of anonymisation and pseudonymisation is utilised in some cases.

Every logon, registration and parts of systems accessed are registered in access logs.

Platac has implemented a 3-layer architecture for their software to ensure that SQL injections and other attacks are very difficult to accomplish. Several layers of business logic sewn into the software.

Customers have locked networks, with only specific IP ranges having access systems.

Informing the end users (patients and health workers) of what their data will be used for is the responsibility of Platac's customer organisations. That's also the case for notifications and awareness.

5.5.7 Challenge

In trying to mitigate a risk, it sometimes leads to making the system or product less user friendly. For example, making use of password to gain access to sensitive data or to an application can be found not to be appreciated by users.

5.5.8 Considerations

Platac should have a designated privacy officer, because they develop systems for big organisations, and the projects are large. Privacy Impact Assessments should be carried out, not performing general Risk assessments.

Authentication should evolve beyond username and password.

Chapter 6
Comparison of Privacy Principles in Studied Systems

6.1 Comparison in the use of Privacy Design Patterns

In this section, the presence of privacy design patterns used in each project are compared as can be seen in table 6.1 , while analysing touchpoints.

Eliciting privacy requirements at the beginning of a development process lays the foundation of building privacy into a system. Privacy requirements go a long way in helping to convert abstract principles into operational requirements [NCM+15]. Inputs to the process of generating these requirements include: Functional description of the system, stakeholders, roles and responsibilities, information flows and privacy principles. Most of these can be arrived at when a detailed PIA is conducted or at least a risk assessment with an appreciable level of focus on privacy. It is therefore good to see that all the systems investigated had risk assessments done for them in some scale. The negative though, is that risk assessments are different from PIAs, in that their focus was not on privacy. It included non-technical topics such as business risks.

Patients' identities and personal health information are usually not anonymised because of the extreme importance of a doctor being able to immediately identify the patient a health record belongs to, in order to render the right medical assistance. For the REXAT case where the identities of test patients where anonymised, these patient identities were not needed in that scenario. Anonymisation is therefore not expected to be utilised in remote healthcare systems. However, pseudonyms can be employed, which can allow for patient's identities to be linked to their health information when needed. MIGEX is the only project that made use of pseudonymisation. It was expected that large and more complex systems such as PYRO and Platac systems will make use of pseudonyms in a way, although this is not mandatory in health systems.

The main method of authenticating users in the studied systems was the use

of a username and password, with 2-factor authentication method only utilised in one system. The standalone apps function without authenticating the user because it tends to diminish usability, leading to a tradeoff between usability and privacy preserving authentication. It is therefore important that this issue is discussed at the beginning of development, when privacy requirements are considered.

Encryption as a privacy preserving pattern was missing in DELV and REXAT, which are standalone apps. This is expected because data is only stored on a user's smartphone, with no external connections. HTTPS is commonly used to encrypt transfer of data in MIGEX, PYRO, and Platac systems.

Role Based Access Control (RBAC) is a technique commonly employed in remote healthcare systems. This ensures that information meant for a specified role is only available to users assigned such a role, preventing unauthorised access to personal health information.

Privacy policies are essential for any system that makes use of personal data. They inform and educate users of the system on how their information is used, disclosed, and collected with respect to that technological system. It is therefore a very important privacy control measure. An organisation's privacy policy differs from a system specific policy, in that the former relates to handling of personal information in organisation processes. Only PYRO had a system specific privacy policy. Mobile apps do also put out privacy policies or privacy statements, either on the app or on the developer's website. This was missing in DELV and REXAT. A privacy policy or statement can go a long way in providing requisite notification, awareness, and ultimately drive informed consent to the end users of these apps or systems.

Providing notice and making users are of data breaches, how to opt-out of a service, how to delete personal data among other things, is clan be linked to the PbD principle of Visibility and transparency. The mobile health apps DELV and REXAT are deficient in this area. In well-structured systems like PYRO, and those developed by Platac, notification and awareness is usually carried out by the data controller, in this thesis it was the system developer that was interviewed. This studied systems showed a lack in providing patients and users of the health solutions with adequate information on how their personal data and PHI is collected, used, disclosed and stored. More significantly there is no clear information to users of MIGEX, DELV and REXAT about how to delete their data.

Logging and auditing ensure accountability and compliance respectively, which therefore help implement the visibility and transparency principle of PbD [FOU]. These are not needed in standalone apps such as DELV and REXAT. The development of the complete MIGEX system equipped with the communication interface to and server is yet to take off. It is recommended that all access to server(s) must be logged

and audits carried out at certain intervals. It is preferable that the audits are carried out by trusted external auditors.

Different levels and forms of minimising the use of inessential PHI in the studied remote healthcare systems were used.

Table 6.1: The table showcases the presence of privacy design patterns in the studied systems. DELV and REXAT are standalone apps. Empty cells indicate the absence of the privacy design pattern at the beginning of a row.

Privacy Objectives & Privacy Design Patterns	**MIGEX System**	**PYRO System**	**DELV App**	**REXAT App**	**Platac Systems**
Privacy Requirements	Risk Assessment done at the start of development included some requirement for protecting PHI.	Risk Assessments	Risk Assessments	Risk Assessments	Risk Assessments
Anonymisation & Pseudonymisation	Use of codes as identifiers (pseudonym).			Anonymised patient information for selected test patients.	
Authentication		Username and password, 2-factor authentication with SMS.	PIN code for a use case.		Username and password. 2-factor authentication under consideration.
Encryption	Encrypted communications.	Levels of encryption keys to protect servers. HTTPS encrypted communications.			Encrypted communications between client devices and server, using HTTPS.
Access control	Only patient's doctor to access patient's PHI via server.	Role based access control & Logical zoning.			Role based access control.

Privacy Policy	Hospital's data protection policy for health workers.	Privacy policy for the system.			Organisation's privacy policy.
Notification & Awareness	Information page for user agreement to be implemented in new system.				
Logging		All access to data and system resources are logged.			All system access are registered in access logs.
Auditing		Auditing and compliance check of data controller and organisation providing data centre services once a year.			
Data minimisation	Present.	Present.	Present.		

6.2 Other Talking Points

The interviews held with participants from the organisations building the studied systems brought up some talking points that are not mentioned in previous sections.

Knowledge of the GDPR and PbD. All interview participants were aware of the existence of the new EU regulation, but have very limited knowledge of what it entails, and how it will affect their organisation's technical and business processes. However, the presence of a privacy or **data protection officer** in an organisation will play a major role in ensuring the compliance of the such organisation to the new regulation, and also educate the owners and employees about PbD. For example, Platac develops several kinds of home healthcare solutions, but does not have an employee dedicated to overseeing the privacy concerns of the organisation. These organisations largely stay up to date with privacy techniques and data protection regulations by looking up information on the country's Data Protection Authority website. This will be done in a rather less organised manner, because such employees are not specialists in the privacy topic and also do not perform the job of a privacy officer regularly.

PIA & Risk Assessment. Participants from the five projects discussed the use of risk assessments or evaluations in the development process of their systems. The risk assessments carried out were scaled according to the size of the project. In MIGEX and DELV the assessments were carried out by the privacy officers in the service provider, which is the hospital. In the other projects the risk assessments were carried out by an employee who has his designated position and also doubles a privacy officer. The disadvantage with these risk assessments is that they inadequately consider privacy risks and privacy as whole. If a risk assessment is to be used it is advisable to include more privacy considerations, and a compliance check. The participants were all in agreement that **automating a PIA process** is only needed for huge projects were it can be a tedious process. In PYRO, challenges faced in carrying out several risk assessments include: consultations with several people, evaluation of probability of an occurrence, and general challenges in multiple discussions with stakeholders.

Privacy by Default. This principle involves ensuring that the personal data are protected automatically from the first use of the system by a user, without the user having to turn on privacy settings. This is a major principle of PbD that goes along way in guaranteeing privacy safeguards. In the PYRO system, a case of privacy by default is evident where a user account is created, by default it is assigned no zone and therefore the user has no access to data until a zone is assigned. In DELV and REXAT, reminders displayed on the screen of a patient's phone are automatically designed not to contain any sensitive health information. This is another way privacy has guaranteed by default. These scenarios show that the importance of the privacy

by default principle can not be overemphasized.

Structured implementation of PbD principles. A standardised framework for building in privacy into different types of IT systems allows for easier and more effective use of PbD. Although privacy design patterns which are used to operationalise PbD principles, were present in the systems studied, there was neither a deliberate nor coordinated effort to develop these systems while systematically implementing PbD principles in each stage of development. Frameworks will differ for different kinds of IT systems. A PbD framework used for a patient monitoring system, may not be suitable for a telehealth system, or even a Human Resource Management system.

Informed Consent. Notification and awareness is a function of consent. Providing data subjects with relevant information about their personal information and privacy policies allows the individual take an informed decision whether to accept or deny consent. There were gray areas in the aspect of consent in the studied systems. More work has to be done to ensure that a patient or user's specific consent is clearly gotten for the collection and use of their personal information in these remote health systems.

Privacy Enhancing Technologies. Interview participants only gave high level information about the privacy preserving mechanisms used in their projects or systems. Hence, mostly privacy design patterns were discussed, and a few PETs such as HTTPS, AES encryption, and RBAC mentioned.

6.3 Mapping Privacy Controls to PbD Principles

In section 6.1 the privacy design patterns evident in the studied systems are technical measures that can be used in engineering PbD principles into a system's development process. Using [FOU] as a guide, some of these privacy preserving measures can be matched with their corresponding principles.

Table 6.2: Privacy preserving measures utilised in the studied systems have been mapped to their corresponding PbD principles. A privacy preserving measure may satisfy multiple principles.

	Proactive not Reactive	Privacy by Default	Privacy Embedded into Design	Full Functionality	Lifecycle Protection	Visibility and Transparency	Respect for User Privacy
Privacy Requirements	X	X	X	X	X	X	X
Anonymisation & Pseudonymisation		X			X		
Authentication					X		
Encryption					X		
Access control	X	X					X
Privacy Policy						X	X
Notification & Awareness							X
Logging						X	
Auditing						X	X
Data minimisation		X					
PIA & Risk Assessment			X				

Privacy requirements should be elicited continuously throughout a development process. These privacy requirements can be mapped to any of the seven foundational principles of PbD because when the requirements have been made operational they may replace any of those abstract principles. PIAs and Risk Assessments are necessary methods that can be used to determine the privacy requirements of a system. Privacy requirements can be engineered using privacy controls such as privacy design patters, privacy policies, and PETs. As explained in section 6.2 the risk assessments carried out by the service providers in the studied systems produced only a few privacy requirements.

Anonymisation, pseudonimisation and encryption all ensure confidentiality and integrity of personal data, providing end-to-end protection in the entire lifecycle of the personal data.

Logging, auditing and privacy policies ensure accountability and compliance,

while notification and awareness creates openness. Therefore they all satisfy the visibility and transparency principle. Notification is a subset of Informed consent, therefore it is mapped to Respect for user privacy because it has the uttermost interest of a data subject in mind.

Chapter 7
Discussion

So far, this thesis has included a look into authors' works on how to operationalise PbD, investigated privacy preserving measures in some remote healthcare systems, presented results and performed privacy analysis using PIAs, and lastly, analysis of the privacy design patterns and the evident PbD principles in the studied projects. The content of this chapter entails directly connecting the results of this study from previous chapters to the research questions, in a bid to clearly express answers to these research questions in relation to the kind of health systems studied. Although previous chapters have been able to adequately answer the research questions drawn out at the beginning of this study, it is necessary to highlight some of these answers.

7.1 Why is Privacy by Design needed?

PETs are closely related to PbD in their goal of ensuring data privacy. They have therefore been understood by many to be what PbD is all about, and that implementing a few random PETs ensures that privacy has been embedded into the design of the system. This a wrong notion. While PETs are specific technological tools used to implement a type of privacy preserving feature, PbD on the other hand is is a process that guides the engineering of privacy into the design of systems, and business or organisational processes. Therefore a holistic approach to preserving privacy is needed. The importance of PbD even in remote healthcare technologies cannot be overstated.

Below a few of the reasons why PbD is needed as generated from this study are discussed.

1. *Evident amount of privacy risks and the increase in security breaches.* Although health technologies are usually privacy and security conscious, there are still some privacy risks that exist, especially in mobile health applications. This can be seen in the PIAs produced in this thesis report. These risks can be

detected and resolved with a PbD employed in the design of these systems. Section 6.3 clearly displayed that PbD principles can be seen in the studied systems, this was however not due to the use of a structured PbD framework. With PbD being a de-facto design process and guideline, risks such as those seen in MIGEX, DELV, and REXAT can be detected using a continuous PIA process and effectively solved using privacy design strategies, patterns and PETs according to a structured PbD framework.
Also, the increase in security and privacy breaches especially in mobile applications in recent years, demands a better and more effective means of plugging loop holes that can be exploited both in mobile health apps and other remote healthcare technologies. PbD provides a proactive way of defending against privacy invasions.

2. *Putting an end to a choice between system requirements and privacy.* A scenario was seen in the REXAT app, where user authentication with the use of a Personal Identification Number (PIN) was later sacrificed to enhance usability, which is a system requirement. The PIN or passcode would have ensured that security is designed into the fabric of the app, and in doing so provide extra privacy protection. In some cases privacy features may be sacrificed for an added system functionality. Embedding privacy in the design of systems using PbD ensures that these tradeoffs and dilemmas do not occur, allowing both the privacy mechanism and the system requirement or functionality to be implemented.

3. *Complying with the GDPR.* The GDPR directs that data controllers should adopt measures that operationalise the principles of data protection by design and data protection by default. PbD principles when implemented, transcends a wide range of privacy requirement and laws in the GDPR. It is therefore necessary to imbibe PbD into design and development activities, and business processes. This will prevent the flouting of the regulation to a great extent, and enhance customer confidence in one's products, activities, and handling of customers' personal data.

4. *Ensuring that all necessary privacy requirements are envisaged and designed.* In this study, it has been clear to see the importance of stating privacy requirements early on in a system development. This also applies to a network design or business practices. PIAs are instrumental in determining the necessary privacy requirements for a system. PIAs are prominent in a PbD process. When conducting a PIA, the consultations to be had with stakeholders provide the platform that helps determine privacy requirements. Privacy requirements in the PIAs produced in chapter 5, serve as a guide in designing the right privacy features.

7.2 What kind of methods have been proposed in research of privacy by design implementation?

This research question has been answered in Chapter 4. It was important to find out about the research works that have been done in relation to PbD implementation, as they provide a veritable foundation for further improvements. Translating PbD from a regulatory realm into an engineering domain has been the major challenge to making PbD a common denominator for IT professionals, data controllers and data processors. There is therefore the need to discover suitable methods of implementing the vague principles of PbD. A continuous PIA process that runs across several phases of system development, is a common denominator in the methods put forward. Privacy analysis, privacy architecture & design, privacy design patterns, privacy design strategies, and PETs also feature prominently. The most detailed work on implementing PbD was carried out by the EU funded PRIPARE programme.

7.3 How can PIAs be better implemented in the systems' development to effectively minimise privacy risks?

PIAs used in Chapter 5 showed its importance in the PbD process, although they were not full scale PIAs. A more effective PIA should not only identify privacy risks and propose solutions, but also involve checking compliance to previous PIA recommendations and evaluating results of privacy controls. A check to see that all aspects of the system comply to privacy regulations should also be included. When conducting a PIA, third parties that will have data shared with them, or have other form of interaction with the system, all have to be reviewed thoroughly. The focus should not be only on the system owner or developer, but on all stakeholders. Automating activities in the PIA process using software will be suitable for large projects, help to reduce the stress that comes with having so many one-on-one consultations, and ensure a more organised collection of information. It is however not beneficial for small projects, as interview participants acknowledged.

The PIAs created in chapter 5 showed the importance of stating privacy requirements and associated privacy concerns, to serve as a guide in choosing the right privacy solutions. Information flows were also clearly described and diagrammatically illustrated in some cases. This allows you to easily notice parts of the system where privacy concerns should be taken into consideration.

7.4 To what extent are the PbD principles evident in the systems under study?

Technological systems used in the health sector tend to be more security and privacy conscious because of the highly sensitive information they deal with. Therefore, it was not unusual to see that privacy controls feature to an appreciable extent in the studied systems. Section 6.1 discussed the privacy design patterns present in each system or application, while section 6.3 linked these patterns to PbD principles. These section, deductions from the interviews, and PIAs in chapter 5 provides the conclusion that the studies systems had a good level of PbD principles evident, even though a PbD process was not consciously employed. However, some areas that were lagging behind were Informed Consent and PIA as described in 6.2. Privacy Design Patterns, PETs and Risk Assessments were utilised in the studied systems. To implement PbD principles completely, PIAs should be utilised instead of the risk assessments that touched on only a few privacy concerns. PIA should not just be used once but in different phases of the system's lifecycle, especially in analysis and design. Also privacy design strategies, privacy design patterns and PETs should be implemented using a structured PbD framework.

Chapter 8
Conclusion

Ensuring privacy in IT systems has become increasingly important over the past few years with more big data processing, increased surveillance, and more personal data of users being collected, shared and processed. Towards this end, several privacy preserving measures have been taken, ranging from enforcing privacy regulations to implementing Privacy Enhancing Technologies in systems. PbD as a design process, can be used to build in privacy into the design of IT systems, thereby ensuring that privacy is factored throughout the data lifecyle in a system. Understanding how PbD principles can be transformed into engineering requirements suitable for system developers and IT professionals to use has been slow process.

This thesis has investigated how some Remote Healthcare Systems protect users' Personal Health Information, to better understand how these protective measures can be utilised in a PbD framework, and identify places that need to be improved upon. A look was taken into some methods of operationalising PbD that have been proposed by some authors through their research work. Interviews were held with participants for each system and each organisation. Questions touched upon the privacy mechanisms employed in the system and the use of PIAs. Based on the answers from the interviews and risk assessment documents, PIAs were conducted. A PIA is a tool that must be part of a PbD implementation. It is also made mandatory in the GDPR. Privacy techniques employed in the studied systems were analysed, privacy risks identified, solutions proffered, and implemented PbD principles identified.

The study identified weak points with respect to Informed Consent, notification and awareness, the use of PIAs and privacy policies. PIAs were not employed in the systems, instead small scale risk assessments which did not touch much on the subject of privacy, were utilised. Some mobile health applications did not have privacy policies or did not communicate them to end users. The EU's GDPR is clear on the issue of notification ad informed consent. Data subjects have to be notified about data breaches, privacy risks, policy documents, in simple, clear and understandable

terms. This is also the same for getting he consent of the data subject. This was clearly not the case in some of the studied systems, especially the standalone mobile health apps. It could also be seen that PbD principles are evident to a good degree in such health systems, but a definitive PbD implementation framework needs to be developed for such type of systems. Based on the study, this framework will consist of the use of privacy design patterns and PIAs. This thesis provides a basis for further research work.

8.1 Further Work

Building upon the work done in this thesis, these areas require further research work.

- A study that will end up developing an actionable framework for operationalising PbD into remote healthcare systems, especially ones that consist of mobile health applications. This framework will provide a structured guide system developers to ensure they implement PbD in totality.

- It is also important that research should be carried out into the extent personal data and PHI that network operators have access to, and the measures that need to be taken to ensure that data subjects have total control of the personal data the network infrastructure collects.

References

[ABK12] Sasikanth Avancha, Amit Baxi, and David Kotz. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR)*, 45(1):3, 2012.

[Bra00] Stefan A Brands. *Rethinking public key infrastructures and digital certificates: building in privacy.* Mit Press, 2000.

[CFN90] David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In *Proceedings on Advances in cryptology*, pages 319–327. Springer-Verlag New York, Inc., 1990.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 93–118. Springer, 2001.

[CNDA+] Alberto Crespo, Yod-Samuel Notario, Nicolás Martín, Jose M Del Alamo, Daniel Le Métayer, Inga Kroener, David Wright, and Carmela Troncoso. Privacy- and security-by-design methodology handbook. http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf. Last Accessed: 2017-04-07.

[Com] European Commission. Directive 95/46/ec of the european parliament and of the council of 24 october 1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Accessed: 2017-04-07.

[Data] Datatilsynet. Act of 18 may 2001 no. 24 on personal health data filing systems and the processing of personal health data (personal health data filing system act). https://www.datatilsynet.no/globalassets/global/english/personal_health_data_filing_system_act_20100907.pdf. Last Accessed: 2017-04-07.

[Datb] Datatilsynet. Personal data act. https://www.datatilsynet.no/English/Regulations/Personal-Data-Act-/. Last Accessed: 2017-04-07.

[Datc] Datatilsynet. Personal data regulations. https://www.datatilsynet.no/English/Regulations/Personal-Data-Regulations/. Last Accessed: 2017-04-07.

[DDFH+15] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea, and Stefan Schiffner. Privacy and data protection by design-from policy to engineering. *arXiv preprint arXiv:1501.03726*, 2015.

[DEL] Privacy by design, setting a new standard for privacy certification. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF. Last Accessed: 2016-10-28.

[Din] R. Dingledine. "tor: anonymity online," world wide web electronic publication,. https://www.torproject.org/. Last Accessed: 2017-04-02.

[EC] European commission, protection of personal data. http://ec.europa.eu/justice/data-protection/index_en.htm. Last Accessed: 2017-04-08.

[EUR] Eu data protection rules, (eu) 2016/679. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. Last Accessed: 2017-03-30.

[fHA] Directorate for Health and Social Affairs. Code of conduct for information security. the healthcare and care services sector. https://ehelse.no/Documents/Normen/Engelsk/Code%20of%20Conduct%20v%205.2%20final.pdf. Last Accessed: 2017-04-05.

[FHI] Family Health International FHI. Qualitative research methods: A data collector's field guide. http://www.ccs.neu.edu/course/is4800sp12/resources/qualmethods.pdf. Last Accessed: 2017-03-17.

[FOU] Ann cavoukian. privacy by design the 7 foundational principles. implementation and mapping of fair information practices. https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. Last Accessed: 2017-04-11.

[HL04] Jason I Hong and James A Landay. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 177–189. ACM, 2004.

[HMD15] Jan Hajny, Lukas Malina, and Petr Dzurenda. Practical privacy-enhancing technologies. In *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*, pages 60–64. IEEE, 2015.

[HNLL04] Jason I Hong, Jennifer D Ng, Scott Lederer, and James A Landay. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, pages 91–100. ACM, 2004.

[Hoe14] Jaap-Henk Hoepman. Privacy design strategies. In *IFIP International Information Security Conference*, pages 446–459. Springer, 2014.

[Hol08] Jan Holvast. History of privacy. In *IFIP Summer School on the Future of Identity in the Information Society*, pages 13–42. Springer, 2008.

[IA] Health Information and Quality Authority. Guidance on privacy impact assessment in health and social care. https://www.hiqa.ie/sites/default/files/2017-03/HI_Privacy_Impact_Assessment.pdf. Last Accessed: 2017-06-12.

[Kot] C.R. Kothari. Research methodology, methods and techniques. http://www2.hcmuaf.edu.vn/data/quoctuan/Research%20Methodology%20-%20Methods%20and%20Techniques%202004.pdf. Last Accessed: 2017-03-17.

[KW14] Inga Kroener and David Wright. A strategy for operationalizing privacy by design. *The Information Society*, 30(5):355–365, 2014.

[Lan01] Marc Langheinrich. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[NCM+15] Nicolás Notario, Alberto Crespo, Yod-Samuel Martín, Jose M Del Alamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener, and David Wright. Pripare: integrating privacy best practices into a privacy engineering methodology. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 151–158. IEEE, 2015.

[NOK] NOKIA. Privacy engineering & assurance, the emerging engineering discipline for implementing privacy by design. https://iapp.org/media/pdf/resource_center/Privacy_Engineering+assurance-Nokia_9-14.pdf. Last Accessed: 2017-04-07.

[OEC] OECD. Oecd guidelines on the protection of privacy and trans-border flows of personal data. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Last Accessed: 2017-04-02.

[RAH+06] Sasha Romanosky, Alessandro Acquisti, Jason Hong, Lorrie Faith Cranor, and Batya Friedman. Privacy patterns for online interactions. In *Proceedings of the 2006 conference on Pattern languages of programs*, page 12. ACM, 2006.

[RC] Australian Transaction Reports and Analysis Centre. Risk management, a tool for small-to-medium sized businesses. http://www.austrac.gov.au/sites/default/files/documents/risk_management_tool.pdf. Last Accessed: 2017-06-20.

[Sol06] Daniel J Solove. A taxonomy of privacy. *University of Pennsylvania law review*, pages 477–564, 2006.

[VBBO03] GW Van Blarkom, JJ Borking, and JGE Olk. Handbook of privacy and privacy-enhancing technologies. *Privacy Incorporated Software Agent (PISA) Consortium, The Hague*, 2003.

[vRBE+12] Jeroen van Rest, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen. Designing privacy-by-design. In *Annual Privacy Forum*, pages 55–72. Springer, 2012.

[WB90] Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard law review*, pages 193–220, 1890.

Appendix A
Interview Guide

This interview guide had some questions drafted from [HNLL04].

A.1 Preliminary Questions

1. Who are the users of the system?
2. Who are the users of the system? Who are the data sharers, the people sharing personal information? Who are the data observers, the people that see that personal information?
3. What kinds of personal information are shared? Under what circumstances?
4. What is the value proposition for sharing personal information? What are the relationships between data sharers and data observers? What is the relevant level, nature, and symmetry of trust? What incentives do data observers have to protect data sharers' personal information (or not, as the case may be)?
5. Is there the potential for malicious data observers (e.g. spammers and stalkers)? What kinds of personal information are they interested in?
6. Are there other stakeholders or third parties that might be directly or indirectly impacted by the system?

A.2 PIA Related

1. Was a PIA conducted at the start or early phase of system development?
2. Who was responsible for conducting a PIA in the project? E.g. A privacy officer, project leader, software developer etc.
3. In what stages of development were they carried out?

4. In relation to the project characteristics, was a small-scale or a full-scale PIA utilized?
5. What were the challenges faced in the PIA process?
6. What was the breakdown of the time needed to conduct the PIA process?
7. What is your general take on the use of PIAs?
8. What are your views on automating the PIA process? Is it unnecessary or dependent on project size? What challenges do you envisage in the use of such automated PIAs.

A.3 Privacy by Design Touchpoints

1. Are you aware of the new EU Data protection regulations?
2. What are the steps taken to ensure that requirements of data protection regulations (local and continental) are adhered to?
3. How is privacy of personal data and personal health information actualized in this system?
4. What are the privacy preserving mechanisms employed?
5. What is your knowledge of Privacy By design?
6. Do you consider privacy from the start of system development? If so how?
7. How do you ensure that only information that is needed for a specific purpose is collected?
8. Is the collection, use, retention and disposal of data and other activities in the system logged?
9. Is there a defined privacy policy for the organization or project?
10. Is compliance to privacy policies verified, evaluated, and monitored? How?
11. Discuss the privacy preserving mechanisms employed in the development of the system. Mention the stages of development these features are implemented.
12. Are users aware of proposed collection, use and disclosure of their personal information? Identify and describe what information is given and how it is given.
13. Explain how the personal information is collected, stored, processed (or used) and disposed. Also, who has access to such information and for what purposes? Who has control over the computers and other devices used to collect

information?

14. How do you ensure information collected, processed, or stored are needed at that particular time for the purpose of the system functioning? (data minimisation)
15. Describe how these privacy design patterns are employed in your system
    - privacy requirements patterns;
    - anonymisation and pseudonymising;
    - hiding of personal data;
    - data minimization;
    - transparence, auditing, and accounting patterns;
    - informed consent.
16. How is the sharing of personal information to third-parties secured?
17. How is personal information shared? Is it opt-in or is it opt-out (or do data sharers even have a choice at all)? Do data sharers push personal information to data observers? Or do data observers pull personal information from data sharers?
18. How much information is shared? Is it discrete and one-time? Is it continuous?
19. What is the quality of the information shared? With respect to space, is the data at the room, building, street, or neighborhood level? With respect to time, is it real-time, or is it several hours or even days old? With respect to identity, is it a specific person, a pseudonym, or anonymous?
20. How long is personal data retained? Where is it stored? Who has access to it?
21. How much choice, control, and awareness do data sharers have over their personal information? What kinds of control and feedback mechanisms do data sharers have to give them choice, control, and awareness? Are these mechanisms simple and understandable? What is the privacy policy, and how is it communicated to data sharers?
22. What are the default settings? Are these defaults useful in preserving one's privacy?
23. In what cases is it easier, more important, or more cost-effective to prevent unwanted disclosures and abuses? Detect disclosures and abuses?
24. Are there ways for data sharers to maintain plausible deniability?
25. What mechanisms for recourse or recovery are there if there is an unwanted disclosure or an abuse of personal information?

Appendix B
Information Letter

As part of NSD's requirements, this document was sent to potential participants in the thesis, requesting for participation in the research project; Privacy by Design.

B.1 Background and Purpose

The European Union parliament recently approved the new data protection rules that will come into effect for all member states, and also Norway as a member of EEA (European Economic Area). Among the requirements made more important by this new regulation is the use of privacy by design (PbD) in the design and development of systems and that every new use of personal data must undergo Privacy Impact Assessments (PIAs).

This is a master's thesis which investigates some remote healthcare systems and applications. The objective of this study is to see how the privacy by design framework, which emphasizes the consideration of privacy from the start of system development and the extensive use of privacy impact assessments; will affect how we develop such systems.

You have been selected to participate in this study because you are a stakeholder who is affected by or influences the system being studied, therefore your views will be important.

B.2 What does participation in the project imply?

The methods of data collection employed in this project will include structured Interviews of personnel with requisite knowledge of the system, system documentations and specifications, data that may be gotten from previous privacy impact assessments (PIAs) conducted and if possible conduct a small-scale PIA. By participating in this project, you get to be part of an important subject topic, get to learn more about privacy by design and the soon to be implemented EU data protection regulations,

and you get to have feedback from the analysis of the collected data that will be of great use to you.

B.3 What will happen to the information about you?

All personal data will be treated confidentially. Only student and supervisor will have access to the data. To ensure confidentiality data will be stored on a server in NTNU's network and computer will be password protected and kept securely always. Personal data will be pseudonymised during the project and for the final report, therefore all background information such as name of organization, job titles will be pseudonymised.

The project is scheduled for completion by July 31, 2017. Personal data will be made anonymous at the completion of the project.

B.4 Voluntary participation

It is voluntary to participate in the project, and you can at any time choose to withdraw your consent without stating any reason. If you decide to withdraw, all your personal data will be made anonymous.

If you would like to participate or if you have any questions concerning the project, please contact: Lillian Røstad, +47 9xxxxxxx

The study has been notified to the Data Protection Official for Research, NSD - Norwegian Centre for Research Data.

Consent for participation in the study

I have received information about the project and am willing to participate

---

(Signed by participant, date)

Appendix C
PIA Threshold Assessment

Checklist - Does the project involve any of the following:

1. The collection, use or disclosure of personal health information?
2. The collection, use or disclosure of additional personal health information held by an existing system or source of health information?
3. A new use for personal health information that is already held?
4. Sharing of personal health information within or between organisations?
5. The linking, matching or cross-referencing of personal health information that is already held?
6. The creation of a new, or the adoption of an existing identifier for service users; for example, using a number or biometric?
7. Establishing or amending a register or database containing personal health information?
8. Exchanging or transferring personal health information outside the Republic of Ireland (Insert home country)?
9. The use of personal data for research or statistics, where de-identified or not?
10. A new or changed system of data handling; for example, policies or practices around access, security, disclosure or retention of personal health information?
11. Any other measures that may affect privacy or that could raise privacy concerns with the public?