Applying data protection part of ISO 27001 to patient and user data produced by medical devices – Case: disease specific quality registers

Master's Thesis
University of Turku
Department of Future Technologies
Software Engineering
May 2020
Aapo Torkkeli

UNIVERSITY OF TURKU
Department of Future Technologies

AAPO TORKKELI: Applying data protection part of ISO 27001 to patient and user data produced by medical devices – Case: disease specific quality registers

Master's Thesis, 82 p., 9 app. p.
Software Engineering
May 2020

Data protection may be considered a subset of information security, consisting of the rules that define who may have access to what data and under what conditions. Rules concerning the handling of personally identifiable information have also become a major topic of discussion with regulation such as the GDPR by the European Union. To improve data protection of personally identifiable information, initiatives such as MyData and IHAN have been developed. In the field of information security, standards such as ISO 27001 exist to improve and unify information security in organizations.

This thesis studies the requirements that the data protection initiatives MyData and IHAN impose on organizations processing personally identifiable information, as well as the requirements imposed by the ISO 27001 standard. The requirements of MyData and IHAN are compared to the ISO 27001 standard, along with a case study that looks at the requirements of both in the context of patient data stored and processed in disease specific quality registers. A gap analysis of the ISO 27001 - security controls is performed to evaluate the current situation against the standards requirements. Suggestions for measures to meet the different potential requirements of MyData and IHAN are also given, along with discussion of their relevance to disease specific quality registers. Considerations of legal aspects of the protection of patient data related to these are however omitted.

Keywords: data protection, information security, ISO 27001, MyData, IHAN, medical information systems

I would like to thank my supervisor at the University, as well as BCB Medical for providing guidance while working on this thesis.

Contents

Chapter 1

Introduction

The term data protection has no explicit, universally agreed upon academic definition. Data protection takes on different meanings in different contexts.

An article by De Hert P. and Gutwirth S. states the following: ”It is impossible to summarise data protection in two or three lines. Data protection is a catch-all term for a series of ideas with regard to the processing of personal data. By applying these ideas, governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc”[1].

Different ISO standards offer differing definitions for the term:

- ”technical and social regimen for negotiating, managing, and ensuring informational privacy, confidentiality, and security”[2, definition 3.15].
- ”implementation of appropriate administrative, technical or physical mean to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data”[3, definition 3.6.5.1].
- ”use of means such as legal safeguards to prevent the misuse of information stored on computers, particularly information about individual people”[4, definition 2.1.3].

In the context of this thesis, data protection refers to the requirements for data-processing systems that stem from an individual’s rights to their personal data. These rights may be

related to privacy, free flow of data or implementing safeguards. Data protection may be considered the process and rules which determine who have access to what data, and under what conditions.

As the amount of data collected of people is constantly increasing, so is the concern for control and ownership of that data. Legal and regulatory approaches have been taken to increase the control and protect the rights of individuals in handling their data. One such approach has been the General Data Protection Regulation (GDPR)[5] by the EU which ”introduced several new rights designed to empower users and regulate imbalances of power between those who collect and control data and those to whom the data refer”[6]. Some more technology-focused actions have also been taken, such as different data protection initiatives. Examples of such initiatives can be found in the MyData - initiative[7], and the IHAN - project[8]. These initiatives attempt to provide tools and frameworks to improve individuals control of their own data. One significant way these initiatives attempt to do this, is by improving their right to data portability (the right to receive data about them from controllers and transfer that data between controllers) which currently leaves room for improvement[6].

Organizations that collect, store or process data need to practice information security to protect the confidentiality, integrity and availability of that data. From an organization's view, data protection may be considered a part of information security.

ISO 27001[9] is an information security standard that provides requirements and a framework for an information security management system (ISMS). The standard provides a collection of different information security controls to be implemented.

This thesis looks at data protection, the ISO 27001 standard and data protection initiatives from the perspective of BCB Medical (also just BCB), a company which stores, processes and analyzes medical data. Disease specific quality registers are looked at as a case study. In terms of GDPR[5] BCB Medical acts as a data processor, not as a controller.

This thesis aims to answer the following questions:

RQ1: Do the data protection initiatives MyData and IHAN overlap with the ISO 27001 standard? May organizations benefit from the standard when partaking in data protection initiatives? Are there potential conflicts between the requirements of the standard and the requirements of MyData and IHAN?

RQ2: How can BCBMedical implement the Annex A data protection controls of the ISO 27001 standard in the scope of patient data in their disease specific quality registers?

RQ3: How can BCBMedical implement the requirements of MyData and IHAN in their disease specific quality registers? How can they do that while utilizing the beneficial overlap and addressing the detrimental overlap identified in Chapter 4?

Chapters 2 and 3 of the thesis provide background information on ISO 27001, MyData and IHAN. Chapter 3 will also identify requirements that MyData and IHAN impose on data processing systems.

Chapter 4 compares the security controls of ISO 27001 to the requirements of MyData and IHAN, identifying potential overlap and conflicts. Chapter 5 provides a description of disease specific quality registers, the case study system. Chapter 6 performs a gap analysis on disease specific quality registers and on the ISO 27001 information security controls, comparing current controls to the requirements of the standard. Chapter 7 attempts to identify the necessary actions that need to be taken to apply the requirements of MyData and IHAN to disease specific quality registers.

Chapter 2

ISO 27001

2.1 The ISMS and the ISO 27001 standard

2.1.1 Information security management systems

An information security management system (ISMS) is defined as follows: ”An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.”[10].

An ISMS is a systematic way of applying and documenting security controls in an organization to protect their information assets[10]. An ISMS does not necessarily refer to only technical measures taken by the organization, but all processes and procedures taken to protect information assets.

An asset is ”anything that has value to the organization”[11] and they ”include but are not limited to human, physical, information, intangible, and environmental resources”[11]. Information security consists of all actions taken and controls implemented for the ”preservation of confidentiality, integrity and availability of information”[10]. In the case of information security and the ISMS, of special interest are information assets (information valuable to the organization) and the assets used to process that information (software,

databases, computer networks etc.).

2.1.2 The ISO 27001 standard

ISO 27001 is an information security standard that ”specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems within the context of the organization’s overall business risks”[10]. The standard gives requirements for implementing information security controls in organizations and provides requirements for developing and operating an ISMS.[10]

2.1.3 Structure of the ISO 27001 standard

The ISO 27001 standard consists of ten parts and one annex listing the different controls referred to by the standard. The first three parts of the standard include background information of the standard and terminology definitions, but do not specify direct requirements. Parts 4 through 10 define requirements for organizations wishing to implement the standard.

The seven parts are (adapted from [12] and [9]):

4. Defining and documenting ISMS scope and organizational context.
5. Leadership and management of information security.
6. Planning and risk management.
7. Resources required for ISMS.
8. Operating the ISMS.
9. Evaluating ISMS performance.
10. Continuous improvement of ISMS.

Each of the parts defines certain activities that must be completed and documented.

2.2 Process and core concepts of ISO 27001

2.2.1 PDCA and the ISO 27001 process

The plan-do-check-act - cycle (PDCA) is a tool and process for continuous quality improvement and project management. It splits the process of managing quality and continuous improvement into four phases of a cycle. The first phase, ”plan” refers to activities taken planning the project/process and defining quality objectives. The do-phase refers to the actual implementation of said plan, while collecting data about the success of the plan. In the check-phase, the quality objectives are compared to the data collected in the do-phase. Finally, in the act-phase corrective actions are entered into the plan to solve problems in reaching the quality objectives. [13][14]

While the ISO 27001 standard is not officially split into the phases of the PDCA-cycle, the standard follows similar activities - such as defining information security objectives - in its different requirements. The different parts of the standard can be placed in the different phases of the PDCA-cycle as follows (adapted from [14] and [12]):

- Plan - phase: 6. Planning and risk management - part (Parts 4., 5. and 7. could also be considered a part of the planning-phase).
- Do - phase: 8. Operating the ISMS - part.
- Check - phase: 9. Evaluating ISMS performance - part.
- Act - phase: 10. Continuous improvement of ISMS - part.

2.2.2 Scope and Context

Dependencies refer to business processes that are outside the ISMS scope, but that processes inside the scope rely on, for example outsourced IT-services. Interfaces are the points where the processes inside the ISMS scope exchange resources or information with processes outside the scope.[15] These dependencies and interfaces may be technical or non-technical in nature - they may be anything from the connection point to the public internet to legal services received by the organization. [15]

The internal context refers to the organization, policies, resources and culture of the organization that is implementing the ISMS, while the external context is the regulatory, financial, competitive and cultural environment in which the organization wants to achieve its goals.[16] Contextual factors to consider may be for example: responsible parties inside the organization, potential competitors and regulatory requirements for their activities. [16]

Organizations implementing ISO 27001 must define the internal and external context, interfaces and dependencies of their systems. From that the scope of their ISMS must be defined. The scope of the ISMS defines its boundaries and applicability.[9][15] In practice this means defining which processes, services and information systems are included in this ISMS. [9][15]

2.2.3 Risk management

In the context of information security, risks refer to the ”potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization”[10]. Risks are deviations from the expected behaviour. Risk management is the activity of directing and controlling an organization with regard to risks.[10]

Risk management is an important part of the ISO 27001 standard, as it is used to identify necessary safeguards - controls - in the ISMS. To define the necessary controls,

it is necessary to conduct a risk assessment on the systems and processes that are in the scope of the organization.

Risk assessment can be divided into three parts: *identification*, where risks are found and described; *analysis*, where the nature, consequences and likelihood of a risk are analyzed and *evaluation*, where it is determined if a risk is acceptable[10]. When risks have been assessed, the organization should know which risks require treatment, which may involve modifying, transferring or avoiding the assessed risk.[17] An important tool of risk treatment in the ISO 27001 standard are the controls, discussed in the next section.

2.2.4 Controls

Controls are measures that are intended modify risks. These measures can include any process, policy, device, practice or other action which modifies risks. Controls are not guaranteed to completely remove a risk, but are often used to mitigate risks found in risk management, i.e. controls are a method for risk treatment.[10]

Annex A of the standard[9] defines a set of 114 information security controls, divided into 14 categories. The categories of controls are described in Table 2.1 (adapted from [9]and[18]). The controls are described in more detail in Appendix A.

Table 2.1 – Control categories

Category	Is concerned with
Information security policies	Writing and reviewing IS policies.
Organization of information security	Assigning IS responsibilities, mobile device - policy, teleworking - policy.
Human resources security	IS considerations in employment.
Continued on next page	

Table 2.1 – continued from previous page

Asset management	Asset inventory, information classification and labeling, physical media handling.
Access control	Access management and control, user responsibilities.
Cryptography	Encryption, key management.
Physical and environmental security	Secure areas, protection and entry control.
Operational security	Operational procedures, malware avoidance, backup, logging etc.
Communications security	Networking security.
System acquisition, development and maintenance	Software development and maintenance, outsourcing.
Supplier relationships	Supplier management and agreements.
Information security incident management	Reporting security events, responsibilities and procedures.
Information security aspects of business continuity management	Information security considerations in business continuity.
Compliance	Laws and regulations, personally identifiable data protection.

2.3 Applying ISO 27001 in organizations

2.3.1 Planning

The plan-phase of the ISO 27001 standard includes activities related to the context of the organization as well as the leadership, planning and support of information security.

In the plan-phase, the context, interfaces and dependencies of the organization are determined. From these the scope of the ISMS is determined. The leadership of information security, as well as organizational roles and policies are also determined. Risk assessment is performed and risk treatment processes implemented in the plan-phase along with determining information security objectives. The necessary resources, competence, awareness, communication and documented information needed for information security are also determined in this phase.

Statement of applicability and Gap Analysis

The statement of applicability (SoA) is a mandatory document in the ISO 27001 standard. The SoA is based on the risk management process, and contains a list of the controls that are described in Annex A of the standard and whether or not the control is deemed necessary in the implementing organization. If a control is not deemed necessary in the implementing organization, a justification for the exclusion must be given (e.g. no risk requiring the control exists).

When the SoA has been produced, the organization now knows desired level of controls in the organization. Now a gap analysis may be performed to find the controls that are missing or lacking. From the gap analysis, necessary actions can be derived.

The gap analysis is a tool for comparing actual performance to the requirements of a standard[19]. In this case each data protection control is compared against actual performance of the system and organization[19]. The result is ”Not compliant”, ”Partially compliant” or ”Compliant”. These are defined as:

- Not compliant: No controls in place to meet standards requirement.
- Partially compliant: Some controls in place to meet standards requirements, but additional work required.
- Compliant: Controls are in place, no further work needed.

If the result is ”Not compliant” or ”Partially compliant”, suggestions may be given to meet the requirements. This method is adapted from the article ”ISO 27001 Gap Analysis-Case Study”[19] by Ibrahim Al-Mayahi and Sa’ad P. Mansoor. The gap analysis tool is used for the ISO 27001 case study in this thesis (Chapter 6).

2.3.2 Implementation, monitoring and continuous improvement

Do-, check- and act-phases of the ISO 27001 standard include activities related to the operation, performance evaluation and improvement of the organizations ISMS. The do-phase deals with operational processes and plans for information security along with risk assessments and risk treatment. The check-phase covers the monitoring, measurement, analysis and evaluation of the ISMS along with internal auditing and management reviews. Finally, the act-phase consists of identifying information security nonconformities and their corrective actions, and the overall continual improvement of the ISMS.

2.4 Data protection and the ISO 27001 standard

The ISO 27001 standard does not explicitly distinguish, which parts of the standard are related to privacy, regulation, free flow of information or other data protection related topics. For the purpose of this thesis, the ”data protection part” of the standard has been identified. This has been done by identifying the controls that are used for data protection purposes. Controls for non-data protection purposes are omitted from this thesis. The identified data protection controls are listed in Annex B.

Chapter 3

MyData and IHAN

The contents of this chapter are based on the MyData white papers[7][20], The MyData Architectural document[21] and the IHAN Blueprint[8].

3.1 Human-centric data-economy

Data protection regulation like the General Data Protection Regulation, GDPR, by the European Union attempts to unify and improve the way people's personal data is used. Although legislation and regulation have given people more rights and more control over their personal data, individuals' control over usage of their personal data is still very organization centric. In organization centric control, data usage control is based mainly on separate contracts between individuals and organizations. The organization/contract centric data protection model is often based on organizations providing the minimum legally required control to the individual. [7][20][8]

Projects, like MyData by the Finnish Ministry of Transport and Communication and IHAN by Sitra - the Finnish Innovation Fund - aim to shift data protection systems from organization centric to human-centric. In a human-centric data-economy the individual would be central in how their personal data may be used. A human-centric system would give people a more effective system to consent to usage of their personal data. This would

require a more centralized system of consent-management. MyData and IHAN both propose models/frameworks for managing this consent in a way that puts the individual into the center of data protection. [7][20][8]

3.2 MyData and IHAN requirements

Sections 3.3 and 3.4 identify the requirements that MyData and IHAN impose on data processing systems and the organizations that govern them. The types of requirements are split into ”Architectural and technical”, ”Integration” and ”ISMS” requirements. Architectural and technical requirements (ARCH) relate to technical solutions that must be implemented and software architectural modifications that must be made into the data-processing systems. Integration requirements (INT) relate to connections and interfaces that must be defined and established into systems outside the data-processing organization. ISMS requirements relate to requirements that require changes to the ISMS and/or processes of the organization managing the data-processing systems or other activities that must be taken.

Each requirement’s identifier is organized as follows: ”MyData(MD) or IHAN”_”Type of requirement”_”Ordinal of requirement.”. For example: IHAN_ARCH_01

3.3 MyData

3.3.1 Introduction

MyData refers to two concepts: first, it refers to an approach to personal data management and processing, second it refers to personal data as a resource which is under the control of the persons themselves. The MyData-approach aims to shift the management and processing of personal data from an organization- and API-centric to a human-centric system in which the individual has the practical means to control, obtain and use their

personal data beyond the minimum legal requirement. MyData is personal data that is under the control of the individuals themselves. As such MyData may be considered a subset of personal data: all MyData is personal data, but not all personal data is necessarily MyData. [7][20]

This thesis refers to MyData as the model defined by the report of the Finnish Ministry of Transport and Communication[7][20]. The report outlines the MyData model, which is an architectural framework that provides data-interoperability and portability, which allows consent-based data management across different data-repositories and services.[20] The MyData model aims to give individuals control over their personal data, organizations tools and processes for accessing personal data and governing bodies a system for protecting individuals data. [20][7]

3.3.2 Model and terminology

The MyData-model is not a strict technical specification, but an architectural framework for consent-based data management. This is done with an infrastructure-level framework that allows individuals to grant consent to use their personal data and organizations to use personal data based on individuals' consent. [21]

The model is based around the *MyData account* and four operational roles: The *account owner*, the *MyData Operator*, *data source* and *data sink*. The MyData account is a record which contains the individuals digital identity, linked services and authorizations. The account owner (or data subject) refers to the individual who created and uses the account to manage consent. The MyData Operator hosts the MyData account and provides an interface for managing the account. A data source is an entity that holds data of an individual (an account owner) and may be authorized by the account owner to provision data to a data sink. Sinks are entities that may, when authorized by the account owner, fetch data from a source and use it to provide a service. The source and the sink may be the same entity, in which case the account owner authorizes the entity to store and process

data of the account owner. [7] [21]

Important activities in the MyData-model are *service linking* and *authorization*. Service linking is an action, where an account owner links a service (source or sink) to their account. After service linking the account owner can manage authorizations for that service. The account owner may authorize a linked service to transfer their data to a sink for processing, and define how the data may be processed. Service linking and authorization happen through the MyData operator, and together these two actions allow an individual to manage consent of using their data. The flow of authorization and data is described in described in Figure 3.1. [7] [21]

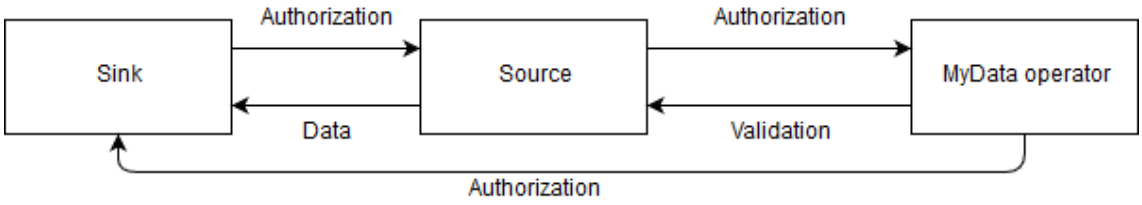

Figure 3.1: Simplified flow of authorization and personal data in an MyData-model, based on [21]

All the requirements in the next three subsections are based on the MyData architectural document[21].

3.3.3 ISMS requirements

In the MyData-model, services that wish to use an individual's data must provide a definition of what the reason of using their data is. This means that an organization storing, collecting or processing personal data must give a MyData-compliant explanation of the usage of that data. If the usage of the data changes or they use the data for a different purpose, the explanation needs to be updated and consent must be re-issued by the account owner. Data processing systems must categorize their usage in order to receive consent.

MD_ISMS 1 (Data usage of different services is categorized)**.** *The organization managing services must recognize all the sources of data that each of their service requires and document them.*

The explanation of how the service stores, receives or processes data is done with the different descriptions MyData defines: the human readable description and service data description.

To receive consent for a service to use an account owner's data, the service must be represented in an end-user friendly format, the human readable description. The goal of the human readable description is to provide the account owner with an overview of the service when making the decision of whether to link it to their account.

MD_ISMS 2 (Human readable description is produced)**.** *A human readable description is a human-readable textual representation of a service containing a unique service ID, textual representation, and possible promotional material.*

In addition to the human readable description, a service data description is required, which provides metadata of the service such as its official name and publisher. In addition to that metadata, the service data description gives a description of the data the service provides. If the service is a source, the service data description describes what data the source produces. For a sink the service data description describes what data it needs.

MD_ISMS 3 (Service data description is produced)**.** *A service data description contains at least what data and in which format the service produces if it is a source and what data elements it needs, if it is a sink.*

3.3.4 Architectural and technical requirements

Services that act as sources (eg. they store and provide personal data of account holders) must register a technical service description with the MyData-operator. Therefore a

system that is to be registered as a source, must produce a technical service description.

MD_ARCH 1 (Technical service description is produced)**.** *A technical service description is a description of the API used for accessing the resources offered by the service. For example if a service provides data through a REST-API, the technical service description could be a WADL[22] document.*

For service linking (on both sources and sinks) a service must implement a software component that handles the functionality of service linking in that service.

MD_ARCH 2 (Service management - component is implemented)**.** *The service management - component must handle the actions of linking a MyData - account to the service, removing a link when so requested and updating the Service link record(SLR), a data element which records the details of that specific service link. When service linking, the process is initiated by the MyData-operator, after which the operator asks the service to produce a unique surrogate ID (a unique id that identifies the service and the user) for that account and service. The MyData-operator then produces an SLR, which is an indication of a successful link. The service management - component should also handle service registration, which is the process of registering the service in a MyData-operators service registry. The registration process requires transferring the service description (a human-readable and a service data description) and a service instance (a data structure describing a single active instance of a service). If there are multiple instances of a service, the registration process needs to be completed for each one.*

In order for a service (source) to store or process an Account owner's data, they need to be able to define and manage the data from a consent perspective. This functionality is implemented as the Resource set registration - component.

MD_ARCH 3 (Resource set registration - component is implemented)**.** *The resource set registration - component is responsible for dividing the account owner's data it stores or processes into different resource sets. A resource set is a data element or set of data elements that may be issued consent by the account owner. The resource set registration - component must be capable of connecting account owner consent to resource sets. The component needs to be able to create, remove and update resource sets.*

In addition to managing resource sets connected to the data, a service needs a component which manages authorizations from the account owner (i.e. consent). This is done by the authorization enforcement - component.

MD_ARCH 4 (Authorization enforcement - component is implemented)**.** *The authorization enforcement - component handles issuing, removing and modifying consent to resource sets. The component handles authenticating requests for data transfers and as such enforcing authorization. The component needs to be able to create consent records (data structures describing an account owners consent), link consent records to resource sets and update consent record status.*

All MyData-compliant services must have compatible audit logging to record all actions to account owner data.

MD_ARCH 5 (Audit logging is implemented)**.** *All transactions regarding account owner data and consent records must be logged by the service. This requires an audit logging component. This component should handle logging all data transfers of personal data and all actions of issuing, removing or modifying consent.*

3.3.5 Integration requirements

In addition to implementing the different components in the previous section, the service must also implement different API's to connect to MyData operators and other services.

In order for the Service management - component to function, it must communicate with MyData operators. This requires implementation of the Service management API.

MD_INT 1 (Service management API is implemented)**.** *The service management API must be implemented and configured according to the MyData Service Linking Specification[23]. Network connections to MyData operators must be established.*

In order for the Authorization enforcement - component to function, it must communicate with MyData operators and other services. This requires implementation of the authorization enforcement API.

MD_INT 2 (Authorization enforcement API is implemented)**.** *The authorization enforcement API must be implemented and configured according to the MyData Authorization Specification[24]. Network connections to MyData operators and other relevant services must be established.*

In order to allow the actual transaction of data between services, a data API must be established.

MD_INT 3 (Data API is implemented)**.** *The data API must be implemented and configured according to the MyData Data Connection Specification[25]. Network connections to MyData operators and other relevant services must be established.*

3.4 IHAN

3.4.1 Introduction

IHAN is a project that ”intends to build a governance framework, architectural definitions and requirements for essential components to build a data-driven world”[8].

Automated data interchange is possible with a consistent, unambiguously and explicitly defined format for personal data. Standards and protocols for methods of transferring personal data between systems are needed for automated and real-time data transfer. Processes and tools for managing data subject consent across all data processors are also required. The IHAN - project aims to answer these problems by clarifying the format, governance and method of personal data sharing. [8]

IHAN aims to benefit all involved parties: end users benefit from the ability to control the use of their personal data, service providers benefit from being able to combine data from multiple sources and data providers benefit from standardized consent management. [8]

From a technological and architectural perspective, the IHAN - project is a set of architectural definitions and requirements. IHAN has outlined several software components that provide IHAN-functionality and compatibility such as consent management, authorization and logging for the end user, service provider and data provider. [8]

3.4.2 Terminology

End user refers to an individual to whom services are created for. A *service provider* is an organization that provides Services to End Users and other service providers. *Data providers* collect, store and process end-user data and provide that data to end users and service providers. The data processing systems covered in this thesis are both service providers and data providers. [8]

The three base components of IHAN are *consent*, the *IHAN identifier* and *logging*.

Consent is given by the end user to a service provider, and allows the service provider to access data from a data provider. The IHAN identifier is a unique identifier that identifies a connection between a person and a data entity. The flow of consent and data is described in Figure 3.2. [8]

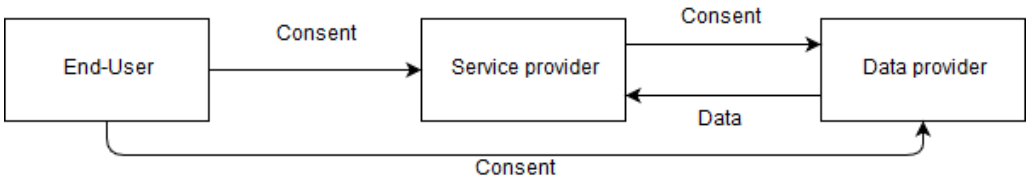

Figure 3.2: Simplified flow of consent and personal data in an IHAN-compliant system. Based on [8]

All the requirements in the next three subsections are based on the IHAN blueprint[8].

3.4.3 ISMS requirements

Services must be published in the *public service directory*, a system available for the end-users which lists services and allows end-users to give consent to service providers. As such for a service to receive consent, and consequently personal data from data providers, the service must be registered on the public service directory.

IHAN_ISMS 1 (Services are catalogued and described)**.** *Service providers must identify all the services they provide and produce both technical and human-readable descriptions.*

In the public service directory, service providers must disclose to the end-users all the data providers required to provide that service. In order to disclose this all data providers that this service uses must be identified and described.

IHAN_ISMS 2 (Data providers used by the service are identified)**.** *The service provider must identify all the different data providers that are required to provide their ser-*

vices.

In the public service directory, service providers may request consent for mandatory and optional data providers. Mandatory data providers are required for the service, and the optional are not necessary for using the service but provide some additional value. The service provider must categorize the data providers into mandatory and optional ones.

IHAN_ISMS 3 (Data providers are categorized into mandatory and optional)**.** *Data providers required by services must be categorized into mandatory and optional. The end users must consent to mandatory data providers if they want to use the service.*

Finally when the organization's service is described, data providers identified and categorized, the service must be registered in the public service directory. The service must be registered in the public service directory.

IHAN_ISMS 4 (Services are registered on the Public service directory)**.** *Services, their data providers and descriptions are registered on the Public service directory.*

3.4.4 Architectural and technical requirements

Service software architecture needs to be modified to utilize IHAN components. This requires implementation of new software components.

For all services that wish to receive data from IHAN data providers, certain software components must be implemented.

IHAN_ARCH 1 (Service implements IHAN software components)**.** *The service provider service directory (SPSD) stores metadata of all services offered by that organization and provides that metadata to relevant public service directories. The consent directory (SPCD) stores and manages the consents received from end-users, these consents connect an IHAN identifier to a data source and as such enable receiving data from that data source. Consent is a record consisting of information on the relevant data*

source and and an encrypted data access record. The data access record is received by the service from the end-user and is used by the service to "prove" to the data source that the consent is legitimate. The inbound data adapter (IDA) is required for the service to interface with data sources, and is used to receive data from data sources. The IDA must decrypt and decompose the data as well as deliver it to the correct services. The service provider log (SPL) stores log entries of service changes (changes to the service itself), service usage and data usage.

For services that act as data providers, additional components must be implemented to allow transferring data to other services and end-users.

IHAN_ARCH 2 (Service implements data provider IHAN software components)**.** *The data source -component (DS) provides the public service directory with technical and human-readable descriptions of a data source. The DS provides a description of its outbound interface for services that request data from it. The data access control (DAC) is a component that receives data requests from services, verifies that the requesting service has consent to use that data and interfaces with the ODA to deliver the data to the service. The outbound data adapter (ODA) is required for the data provider to interface with services. The ODA interfaces with service IDA's, by facilitating the transferring of the data. The ODA also interfaces with relevant data source DAC's to ensure consent. The data provider log (DPL) must log data source changes (changes to the data provider itself) and data accesses (what data was accessed, by whom, when etc.).*

Services that use other services as data providers, must implement functionality that allows the service to recognize between mandatory and optional data providers. The service might for example hide certain functionality from the end-user if they have not consented to use their data from an optional data provider.

IHAN_ARCH 3 (Mandatory and optional data providers are recognized)**.** *Service distinguishes between mandatory and optional data providers. Service is capable of functioning if the end user has not consented to one or more optional data providers.*

3.4.5 Integration requirements

Interfaces that move data in or out of the system, must use proper data formats and communication protocols to ensure compatibility with inbound and outbound data adapters.

IHAN_INT 1 (Inbound and outbound data interfaces implemented)**.** *The inbound data interface is tasked with providing interfaces to the data providers, decrypting incoming data and forwarding it to the relevant components in the service. The outbound data interface communicates with external services requesting personal data from a data source. Both interfaces should provide a RESTful API using JSON or XML, secured by HTTPS[8]. Network connections to relevant services must also be established.*

In order for the service to receive data from data providers, functionality to receive consent from end users personal consent directory is required.

IHAN_INT 2 (Consent interfaces implemented)**.** *An interface to receive consent forms from the end-users personal consent directory needs to be implemented. Network connections to relevant public service directories must also be established.*

Chapter 4

MyData, IHAN and ISO 27001

This chapter compares the requirements identified in Chapter 3 to the controls listed in Annex A of the ISO 27001 standard.

As the ISO 27001 standard and the data protection initiatives (MyData and IHAN) may be considered as a set of requirements, there may be overlap in the two sets. This overlap may be either beneficial or detrimental. Beneficial overlap means that implementing a requirement/requirements in one set, will make meeting the requirement in the other set easier. Detrimental overlaps refer to situations where meeting certain requirements for both sets causes extra work.

Beneficial requirements are often situations where the standard and the data protection initiatives have similar goals. Detrimental requirements are conflicting situations, where the meeting requirements from both the standard and the data protection initiatives requires extra work outside the two requirements.

This chapter attempts to answer RQ1 of this thesis. This chapter is based on the ISO 27001 standard[9] and the ISO 27002 standard[26] which provides further specification to the Annex A controls. The ISO 27000 standard[9] was used as terminology-reference. The book ”ISO 27001 Annex A Controls in Plain English”[27] by Dejan Kosutic was also used for reference.

4.1 Information security policy

While ISO 27001 does not give an exact definition of how the implementing organization should write their information security policies, A.5.1.1 does list certain lower-level topics which should be covered. Some of these lower level topics, such as “access control”, “information classification”, “information transfer” and “privacy and protection of personally identifiable information” need to take into account MyData / IHAN if they are to be implemented as well.

4.1.1 Detrimental overlap

If the organization has an existing information security policy (A.5.1.1), it and some of its sub-policies will likely need to be modified and reviewed to mention MyData and/or IHAN in relevant parts.

4.2 Organizational structure and responsibilities

A.6.1.1 requires that organizational entities responsible for the protection of assets and information security procedures should be defined. Responsibility for the personal data under MyData- and IHAN-control needs to be defined. Also responsibility for implementing the different software components, integration connections and their information security should be defined.

A.6.1.4 requires that contact with special interest groups should be maintained. While MyData and/or IHAN may not necessarily count as a special interest group, contact with those project groups should be maintained to ensure that the organization’s information on the projects is up to date and to potentially receive support when necessary.

4.3 Assets

A.8.1 requires that organizational assets are identified and appropriate protection responsibilities are defined. This identification is likely to be documented as an asset inventory which lists all organizational assets (including intangible assets like data) along with the responsible organizational entities.

Since information and data may be considered assets, they should be inventoried as such (A.8.1.1). Data under control of MyData and/or IHAN should be inventoried as personal data and separated from other types of data assets.

Since data under MyData and/or IHAN should be categorized as its own asset, ownership of this data needs to be defined (A.8.1.2).

A.8.1.3 requires that acceptable use of assets is defined. Usage of data under MyData and/or IHAN control must happen in accordance with consent, service description and technical requirements of MyData and IHAN. The acceptable usage definition should reflect that, and all life cycle stages (i.e. creation, processing, transmission and deletion) of this type of data need to take into account these requirements.

A.8.2 requires that information is classified and labeled according to its security requirements. A.8.2.1 of the ISO 27001 standard requires information to be classified in terms of legal requirements, value, criticality and sensitivity. Data under MyData or IHAN control should be classified into a category which clearly identifies it as personal data.

Also, all data under MyData or IHAN controls should be labeled as data which needs to meet the requirements of MyData or IHAN (A.8.2.2).

Procedures for handling of data classified and/or labeled as MyData or IHAN personal data should be defined (A.8.2.3). These procedures should include at least processes for receiving personal data from other sources, receiving consent and transferring data to other systems.

4.3.1 Beneficial overlap

While A.8.2.1 is not directly related to classifying data in terms of the subject of data, the controls and systems used to meet A.8.2.1 may be beneficial in meeting requirements such as MD_ISMS_1 and IHAN_ISMS_3.

Both MD_ISMS_1 and IHAN_ISMS_2 require identifying the different data / data providers the service uses. Considering A.8.2.1 and these requirements, classification and labeling of data is necessary in both sets of requirements. While the A.8.2 - controls likely work on somewhat different abstraction levels, the same systems and documentation may likely be used to categorize data to meet both requirements.

4.4 Access control

A.9.1.1 requires that organizations define an access control policy, which defines how access control to organizational assets (once again, information is also an asset) is performed. The access control policy needs to take into account the requirements of MyData and IHAN. For example, if consent from a MyData user has been received to use their personal data in the organizations systems, it must be determined who in that organization may access that data and how access to that data may be granted while the organization is storing it.

According to A.9.2, the organization must ensure authorized users have access to assets and take measures to prevent unauthorized access to assets. To enforce this, a formal user provisioning process needs to be defined (A.9.2.2). This should define how new access rights are granted. This process should take into account MyData and IHAN to ensure that access rights to systems with personal data are only granted for purposes that comply with the consent given by the data subject. For example if a user has consented to their data being used for the purpose of medical research, users working with marketing should not gain access rights to that data.

Access to information in systems and applications should be restricted by technical measures (A.9.4.1). Technical measures should be implemented to ensure that personal data controlled by MyData and IHAN is only accessible to users who have proper access rights.

4.4.1 Beneficial overlap

For organizations dealing with personal data, some type of formal process for gaining access to that data will likely be necessary. If implemented simultaneously, the access control policy (A.9.1.1) and the consent based personal data management of MyData and IHAN can work as mutually supporting systems. For example the process of receiving consent through either MyData or IHAN works as a basis for granting access to that data for certain purposes.

MyData and IHAN can act as an effective part of an access provisioning process when dealing with personal data since they offer a technical solution to receive consent for different types of data use from the data subject.

4.4.2 Detrimental overlap

Existing access control policies (A.9.1.1) and user provisioning processes (A.9.2.2) will likely need to be modified to accommodate the requirements of MyData and IHAN.

4.5 Cryptography

A.10.1.1 requires that the organization defines a policy of cryptographic controls. This policy should include a reference to meeting the requirements that MyData and IHAN impose in terms of cryptography. For example, the MyData Architecture[24] requires that cryptographic keys used by actors are expressed as JSON Web Key (JWK)-structures[28].

4.5.1 Beneficial overlap

MyData and IHAN may be beneficial to the organization if the organization has not yet implemented cryptographic controls (A.10.1) in their systems as the requirements set by MyData and IHAN may serve as a starting point.

4.5.2 Detrimental overlap

MyData and IHAN may be detrimental if a policy and controls are already in place and they need to be modified to accommodate them.

4.6 Operations

A.12.1.1 requires that the organization documents its operational procedures associated with information processing and communication. These documented operating procedures should include a procedure or procedures for dealing with personal data from MyData and IHAN. These procedures might include a procedure for requesting consent for personal data from an external system, or changing the public service description of a service provided by the organization.

A.12.1.4 requires that development, testing and operational environments should be separated. In the case of MyData and IHAN, this means that a testing environment for MyData and IHAN connectivity is required. In practice this may mean developing simulated environment for sinks and sources of personal data, or a simulated server for the MyData operator.

Event logs recording user activities should be produced (A.12.4.1). These should record transactions (accesses, modifications etc.) of personal data.

4.6.1 Beneficial overlap

A.12.4.1 requires logging records of user activities. MD_ARCH_5 requires logging all transactions regarding account owner data. These requirements may likely be combined to utilize the same software logging component.

4.6.2 Detrimental overlap

Changes to existing operating procedures required by MyData and/or IHAN may cause additional work. Creating a separate development/testing environment to implement MyData and/or IHAN - components could require additional work if separate environments require modification.

4.7 Communication and networking

A.13.1.1 requires that networks and connections are managed and controlled in systems and applications to protect information. As complying with MyData and IHAN requires implementing new network connections with external systems, such as the MyData-operator and external sinks and sources, these connections must be established in a controlled manner. This means assigning responsibility for the connections, establishing safeguards for confidentiality and integrity as well as logging and monitoring.

A.13.1.2 requires that security mechanisms, service levels and management requirements are included in network service agreements. In the case of MyData or IHAN, this control would require that established network connections used to transfer personal data may need a network service agreement ensuring proper security in transferring personal data. Whether these connections should be considered network services (in the context of ISO 27001) needs to be determined specifically for each connection: a simple connection from one system to another likely would not be a network service, but a more complex agreement where on party provides data to another likely would.

A.13.1.3 requires that different groups of information services and systems as well as users should be segregated on networks. While the specific implementation of network segregation will depend on the organization, usage of personal data under the control of MyData and IHAN should be considered when segregating networks. This consideration should include the access control policy of the organization, i.e. only users with access to personal data should have access to network segments that use personal data. Personal data may be for example managed through a designated network segment that includes the authorization mechanisms required for MyData and IHAN.

Formal information transfer policies, procedures and controls are required by A.13.2.1. These should include a mention that data owner consent is required when transferring personal data, e.g. if an external organization requests data from databases containing personal data, consent from all persons in that database must be received before transferring data.

If personal data is transferred to external parties, transfer agreements required by A.13.2.2 should include mentions of MyData and IHAN to ensure that the data is properly labeled and only used for purposes which the data owner has consented to.

4.7.1 Beneficial overlap

Central to data protection initiatives is giving persons control of transferring their data. This generally requires a certain level of standardization in transferring data between parties. This leads to requirements such as MD_INT_3, which requires implementing a standardized data API in the service. This combined with A.13.2.1, which requires formal transfer policies, procedures and controls to protect information in transfer, can be mutually supporting since when transferring personal data to external systems consent must be ensured. These formal transfer policies and procedures can be used to enforce that.

4.7.2 Detrimental overlap

These requirements may be problematic for organizations that have already implemented the ISO 27001 standard, since these formal policies may need to be updated and modified to match requirements such as MD_INT_3. This may require additional effort from the organization, especially since these data transfer policies may be based on contracts to outside parties.

4.8 Software development and maintenance

Appropriate analysis to identify information security requirements of MyData- and IHAN-interfacing components within software must be done to meet A.14.1.1. In practice this means that different types of security analysis methods such as threat modeling and incident reviews should be used to identify security threats to all software components, including components used to fulfill MyData and IHAN requirements.

Application services processing personal data under control of MyData and IHAN on public networks should be protected with appropriate measures to prevent unauthorized disclosure and modification of said personal data to meet A.14.1.2. This is likely implemented with systematic use of different cryptographic controls. Similarly, A.14.1.3 requires that application service transactions are protected by encryption, authentication and other methods if necessary. This includes transactions with MyData- and IHAN-systems. As such, the implementation must meet the requirements identified in A.14.1.1 and the requirements from MyData and IHAN.

A.14.2 gives several requirements for the software development process. These requirements such as secure development rules (A.14.2.1), system change controls (A.14.2.2) and system security testing (A.14.2.8) must be taken into account when developing software components necessary for MyData and IHAN. If personally identifiable information, such as information from MyData or IHAN, is used in system testing the security controls

regarding test data in A.14.3.1 should be implemented.

4.8.1 Beneficial overlap

MyData and IHAN may complement ISO 27001 as they offer standardised solutions for fulfilling information security requirements, for example by giving reference designs for authentication methods for information transfer to external systems[24].

4.8.2 Detrimental overlap

Information security requirements and analysis must be applied to MyData- and IHAN-functionality (A.14.1.1), which may require additional work.

Meeting the requirements of A.14.2 may increase the amount of work required to implement MyData- and IHAN-functionality into existing systems, as secure development rules and change controls need to be followed and security testing completed.

4.9 Compliance with legislation, regulation and contracts

MyData and/or IHAN should be identified as contractual requirements to the organization, since A.18.1.1 requires identifying and documenting all legislative, regulatory and contractual requirements for the organization. A.18.1.4 requires that organizations develop and implement a policy on the privacy and protection of personally identifiable information. This policy should mention that the organization complies with MyData and/or IHAN.

4.9.1 Beneficial overlap

MyData and IHAN may be useful for implementing A.18.1.4 since they provide ready made frameworks for controlling the usage personal data, and provide a set of technical

requirements for ensuring data owner consent. As such, implementing MyData and/or IHAN may be beneficial in developing this policy.

4.10 Summary

These tables summarize both the beneficial and detrimental overlap identified in this chapter. The overlap is summarized in the second column, with the first column indicating the control in ISO 27001 in question. In parentheses the section of this chapter where this is mentioned is referenced.

Table 4.1 – Beneficial overlap

Control	Requirements of MyData and IHAN
A.8.2.1	The same system of classifying data may be used both in ISO 27001 compliance as well as MyData and IHAN compliance. (Section 4.3.1)
A.9.1.1	MyData and IHAN may be used to support access control systems. (Section 4.4.1)
A.10.1.1	MyData and IHAN may serve as a standardised starting point for cryptography. (Section 4.5.1)
A.12.4.1	Logging systems for transactions on data may likely be combined. (Section 4.6.1)
A.13.2.1	Transfer policies may be used to support consent-based data flow. (Section 4.7.1)
A.14.*	MyData and IHAN may offer standardized solutions for information security. (Section 4.8.1)
A.18.1.4	MyData and IHAN may be useful in creating policy on personally identifiable information. (Section 4.9.1)

Table 4.2 – Detrimental overlap

Control	Requirements of MyData and IHAN
A.5.1.1	Some sections of the information security policy must be modified to take into account MyData and IHAN. (Section 4.1.1)
A.9.1.1	Existing access control policies may need to be modified. (Section 4.4.2)
A.9.2.2	Existing user provisioning process may need to be modified. (Section 4.4.2)
A.10.1.1	If cryptographic controls are already in place, MyData and IHAN may cause additional work. (Section 4.5.2)
A.12.1.1	Existing operating procedures may need to be modified. (Section 4.6.2)
A.12.1.4	Ensuring a separate environment for MyData and/or IHAN - component may require additional work. (Section 4.6.2)
A.13.2.2	Existing transfer policies may need to be changed for MyData and IHAN. (Section 4.7.2)
A.14.1.1	Information security requirements and analysis of MyData- and IHAN-functionality may cause additional work. (Section 4.8.2)
A.14.2.*	Secure development rules and system change controls need to be followed and security testing completed when implementing MyData- and IHAN-components into existing systems. (Section 4.8.2)
A.14.2.8	MyData- and IHAN-components must be tested according to system security testing requirements. (Section 4.8.2)

This chapter has answered RQ1 of the thesis. Overlap between MyData, IHAN and the ISO 27001 standard has been identified: potential benefits from this overlap have been summarized in Table 4.1 and potential conflicts from the overlap have in turn been

summarized in Table 4.2.

Chapter 5

Disease specific quality registers

The intended use of Disease specific quality registers is defined as follows: ”BCB’s Disease specific register is an independent software product for healthcare. The intended use of the product is to collect and formulate information of disease monitoring and treatment planning of the patient in question. The information is intended for healthcare professionals. Healthcare professionals may utilize the information to support their diagnostic and therapeutic decisions. Disease specific register combines and formulates the information to needed numerical, textual or graphical views depending on the disease and the treatment of the patient”[29].

This chapter will give a high-level description of disease specific quality registers from an organizational, technical and a data flow point of view.

5.1 Business environment

Quality registers act as data processing systems for organizations providing treatment for that group of diseases. Quality registers are not used as resource planning systems, but rather they are used for assessing treatment effectiveness and quality, improvement of treatment and clinical data analysis. Quality registers do not replace patient information systems but are rather used as complementary systems. Customers using quality registers

include Finnish health care districts and several private clinics and hospitals.

In addition to the quality registers which provide a direct user interface to hospital or clinic staff, quality registers are connected to a specifically developed integration platform and the MyHealth-system. The integration platform is used to bring data to the quality register from the hospital or clinic patient information systems. The integration platform provides a central interface through which patient, treatment, appointment, operation and laboratory data are transferred to the register.

MyHealth is a patient facing software product produced by BCB that provides an interface for patients to provide information related to the treatment of a disease. MyHealth allows the patient to answer questions relating to background information and disease specific questionnaires. This information is stored in the quality register. General business environment is described in Figure 5.1.

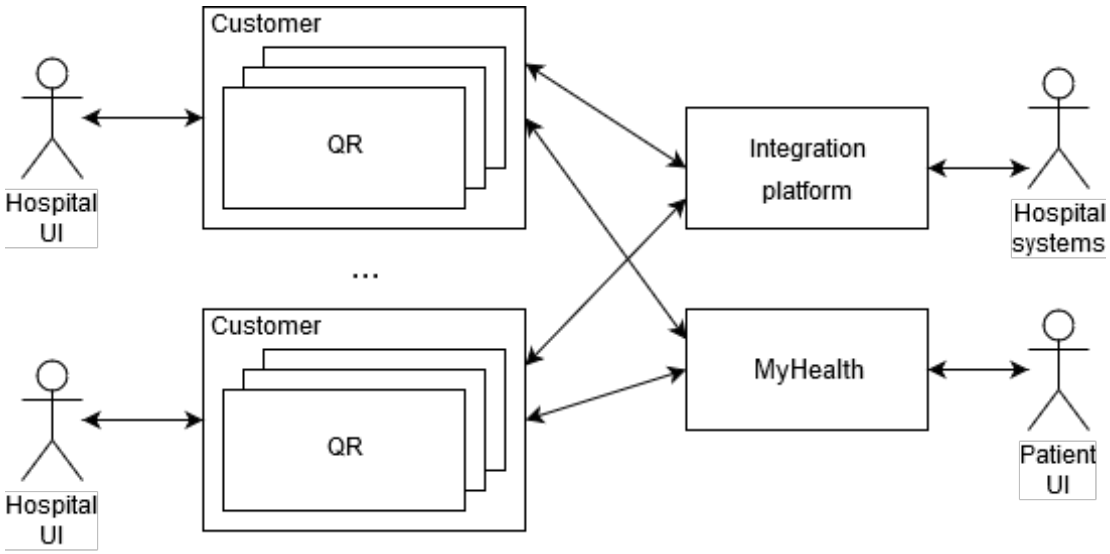

Figure 5.1: General environment of quality registers.

5.2 Architecture and technology

The quality registers are implemented as Web - based software systems hosted on application servers. The quality registers provide a direct web user interface for the hospital

or clinic staff. In addition to the web user interface, the quality register interfaces with the integration platform and the MyHealth system. High-level architecture is described in Figure 5.2.

Figure 5.2: High-level architecture of a quality register.

Quality registers are implemented as Java-based applications hosted in Java Servlet Containers. Each quality register is hosted as its own application. In addition to the application code, different outside interfaces need to be implemented into the register, along with relevant network connections. These include interfacing with the integration platform and the MyHealth - system. Interfacing with other register-specific systems may also be needed. The quality registers also utilize a common single-sign-on system for user-access control.

5.3 Data in disease specific quality registers

Figure 5.3 describes the flow of patient data in and out of disease specific quality registers. The numbered transitions in the figure are described after the figure:

1. Data about surgical and other operations performed on patients is transferred to the integration platform.

2. Basic data about the patient, background information and data about relevant health-care visits (doctors appointments etc.) are transferred to the integration platform.

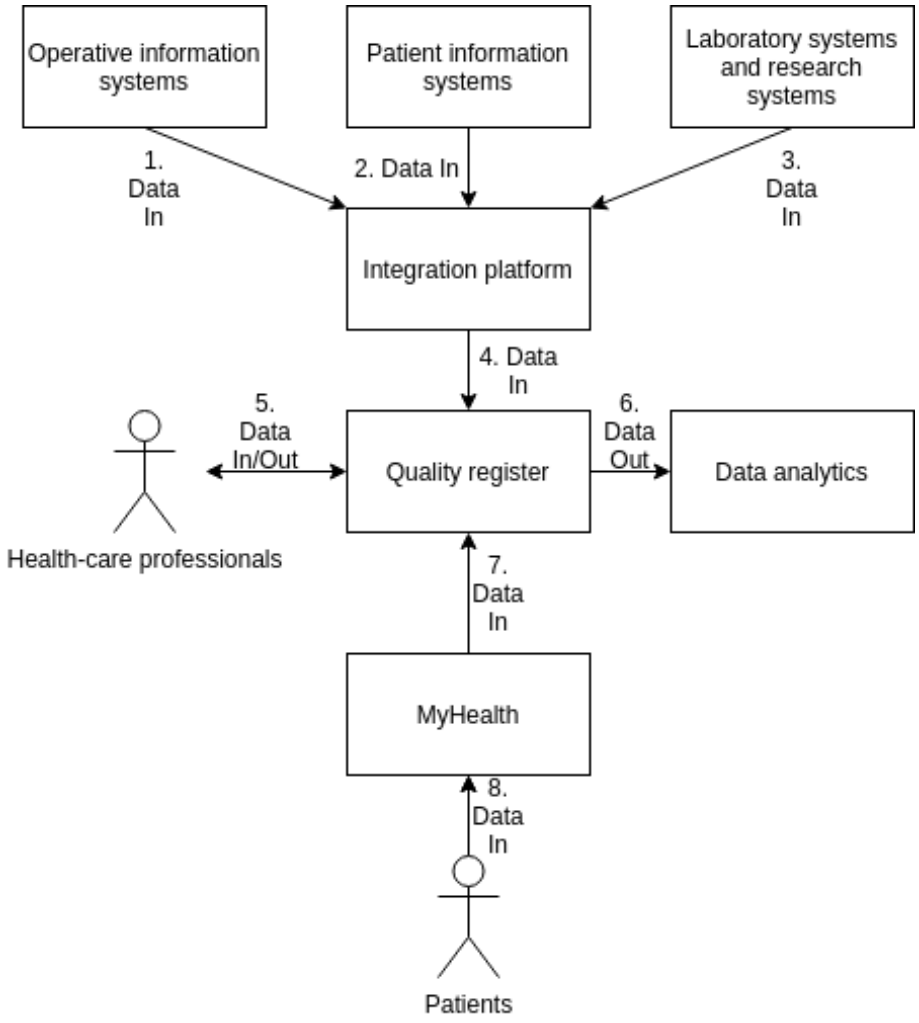

Figure 5.3: Data flow in disease specific quality registers.

3. Laboratory test results and other research information are transferred to the integration platform.

4. Data is filtered by the integration platform to different quality registers. For example surgical operations relevant to a disease are filtered to that disease specific quality register.

5. Health-care professionals (doctors, nurses, etc.) input disease specific data about the patient into the quality register, and utilize data in the quality register in their treatment. This is done through the web user interface.

6. Data is transferred to data analytics systems, that process disease specific data so it may be utilized for research purposes etc.

7. The MyHealth - system inputs patient questionnaire data into the quality register. This data may then be viewed by health-care professionals and utilized in data analytics.

8. Patients input data about their treatment into the MyHealth-system. This includes questionnaires about treatment satisfaction etc.

Chapter 6

Case study: ISO 27001

This chapter attempts to answer RQ2 of the thesis by performing a gap analysis of the data protection controls in the case of disease specific quality registers. The gap analysis compares the data protection controls of Annex A[9][26] and the current situation of the storage and processing of patient data in disease specific quality registers, as well as the organization that governs them. The gap analysis method that is used here has been described in Section 2.3.1.

The results have been omitted from the published thesis due to them being confidential information of BCB Medical. This chapter describes the gap analysis through the considerations taken for each control to produce the results of the analysis.

The ISO 27001 standard is referred to as ”the standard” and BCB Medical is referred to as ”the target organization”. Controls covered in the case study have been summarized in Appendix A.

6.1 Controls

Certain parts of the standard’s requirements have been omitted for this gap analysis. These have been listed in Appendix B. The controls that have not been omitted and are addressed in the gap analysis have been summarized in Appendix A.

6.1.1 Information security policies

A.5 gives controls that relate to information security policies.

A.5.1.1 requires that an information security policy exists. Here, the organization's information security policies will need to be reviewed and potentially supplemented with other more specific policies (such as a supplier information security policy). Finally, coverage needs to be reviewed to reach compliance with the standard.

A.5.1.2 requires that information security policies are regularly reviewed. It will need to surveyed and determined, how and when policies are reviewed in the target organization. If some policies are not reviewed, their reviewing should be determined to reach compliance with the standard.

For the gap analysis, both two controls in Table A.1 have been evaluated for compliance. For both controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.2 Organization of information security

A.6 gives controls that relate to the organization of information security.

To be compliant with A.6.1.1, information security responsibilities should be defined in the target organization. To determine compliance with this, different information security roles and responsibilities in the target organization will need to be surveyed and determined. These need to be compared to the requirements of the standard.

A.6.1.2 requires that conflicting duties and responsibilities are segregated if necessary. For this, the responsibilities identified earlier need to be reviewed to ensure that conflicting areas of responsibility do not exist.

A.6.1.3 requires keeping contact with relevant authorities is appropriately maintained. To evaluate this, relevant authorities for the target organization need to be surveyed. It will then need to be assessed if contact with the identified authorities is appropriately maintained.

Similarly to A.6.1.3, A.6.1.4 requires appropriate contact with special interest organizations. Similarly these organizations need to be surveyed and contact with them evaluated to ensure appropriate contact.

In order to be compliant with A.6.1.5, all types of projects in the target organization must take into account information security. This is evaluated by surveying all rules and procedures that exist in the target organization relating project management, and evaluating whether these meet the requirements of the standard. It should also be evaluated whether these rules are enforced for all types of projects.

A.6.2.1 and -2 require that mobile and teleworking policies exist in the target organization. For these it should first be surveyed whether these policies exist. If the policies exist, they should be reviewed against the standard.

For the gap analysis, all seven controls in Table A.2 have been evaluated for compliance. For the seven controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.3 Asset management

A.8 gives controls that relate to managing assets in the organization.

Central to A.8 is a comprehensive and up-to-date inventory of all organizational assets (A.8.1.1). In addition to this, to be compliant with A.8.1.2, each asset must be assigned an owner who is responsible for that asset. To evaluate compliance with these, existing asset inventories in the target organization should be surveyed. The comprehensiveness of these should then be evaluated to ensure that all assets are covered. The inventory/inventories should then be reviewed against the standard to ensure compliance with its requirements. After evaluating the compliance of the inventories, it needs to be verified that each asset is owned.

Along with the asset inventory, acceptable use of each asset should be defined (A.8.1.3). In addition to this, A.8.1.4 requires that the return of of organizational assets is controlled.

Assessing compliance with these should be done by surveying all rules, processes and procedures in the target organization that control the use and return of assets. When these have been found, their compliance with the standard should be reviewed by ensuring that each asset has a definition of acceptable use and their return is controlled in accordance with the standard.

A.8.2.1 and -2 require that the target organization classifies(1) and labels(2) information. A.8.2.3 requires the organization to create procedures for handling information based on their classification, e.g. more confidentially classified information would have more strict handling procedures. These should be evaluated in the target organization by surveying how information is classified and labeled, along with all the different procedures for handling different types of information. If information is classified, the classification scheme should be reviewed against the standard along with ensuring that information is appropriately labeled according to the classification scheme. After this, the procedures for handling information should be reviewed against the standard, by ensuring that each information class has an appropriate handling procedure.

A.8.3.1, -2 and -3 require procedures for handling removable media (1), disposal of media (2) and transferring physical media (3). These should be evaluated by surveying all procedures and rules in the target organization that are relevant to the handling, disposal and transfer of physical media. It should then be evaluated whether these procedures and rules comply with the standard, i.e. are there procedures for handling removable media that are in accordance with the information classification scheme, is physical media safely disposed of and is physical media appropriately protected during transportation?

For the gap analysis, all ten controls in Table A.3 have been evaluated for compliance. For the ten controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.4 Access control

A.9 gives controls that relate to managing access to information systems in an organization.

A.9.1.1 is the fundamental control in this category as it requires that the organization creates an access control policy which describes when, how and to whom access to information systems is granted. In the target organization, it should be surveyed if an access control policy exists. If it exists, it should be reviewed against the standard. Along with the access control policy, A.9.1.2 requires that users are only given access to networks and services if they have been specifically given permission to access them. In the target organization it should be surveyed how access to networks and services is given and if authorization is required. The way access is granted should be reviewed against the standard.

A.9.2.1 and -2 require processes for user registration and de-registration (creating and removing accounts), and access provisioning (granting and removing access rights for accounts). This should be evaluated by surveying all rules and procedures relevant to user registration and granting access rights. These should then be reviewed to evaluate if they meet the standards requirements for user registration- and access provisioning.

A.9.2.3 requires restricting and controlling privileged access rights (e.g. admin rights to systems). Similarly to A.9.1.2, allocation and control of privileged access rights in the target organization should be surveyed and reviewed against the standard.

To be compliant with A.9.2.4, secret authentication information (e.g. passwords) should be controlled through a formal process. To assess compliance with this, such processes should be surveyed. These should be reviewed to ensure that the requirements of the standard are met, e.g. is the identity of a person requesting a new password verified?

Regular reviews of access rights should be conducted by asset owners responsible for information systems (A.9.2.5). It should be surveyed, whether the target organization requires all asset owners to review user access rights at specified intervals. Access rights

must also be removed when employees leave the organization (A.9.2.6). This may be assessed by evaluating the off-boarding process for leaving employees and contractors. The off-boarding process should include removing access rights.

In order to be compliant with A.9.3.1, usage of secret authentication information should be controlled by organizational rules. This should be evaluated by surveying and reviewing all organizational rules that relate creating and using passwords and other secret authentication information. It should be evaluated whether these rules meet the requirements of the standard, e.g. are users instructed to not use the same password for several systems?

A.9.4.1 and -2 require that access to information systems is restricted based on the access control policy (1) and that secure log-on is used (2). The functionality and security of log-on processes of information systems in the target organization should be evaluated against the standards requirements. These processes should provide functionality that allow restricting user access based on the access control policy, e.g. allow hiding certain data from certain groups of users. Also these processes should implement security mechanisms, e.g. by protecting against brute force attacks.

The password management systems (i.e. password changing interfaces, sso-interfaces etc.) used by the organization should enforce strong passwords, preventing usage of weak and/or repeated passwords (A.9.4.3). To evaluate compliance with this requirement, the password management systems of the target organization should be reviewed. It should be evaluated whether these systems fulfill the standards requirements, e.g. by enforcing strong passwords.

A.9.4.4 requires restricting and controlling the use of privileged utility programs (programs that may be potentially used to bypass normal security measures). The measures that the target organization takes to restrict and control use of these utility programs should be evaluated against the standards requirements, e.g. does the target organization log all cases where privileged utility programs are used?

In order to be compliant with A.9.4.5, access to program source code should be restricted. The way in which program source code is stored, accessed and handled in the target organization should be evaluated. Whether or not the requirements of the standard (e.g. not storing program code on operational systems) are met, should then be evaluated.

For the gap analysis, all 14 controls in Table A.4 have been evaluated for compliance. For the 14 controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.5 Cryptography

A.10 defines controls for the use of cryptography in the organization.

A.10.1.1 and -2 require policies for cryptographic controls (1) and management of cryptographic keys (2). These policies should instruct the use cryptographic controls (e.g. the type, strength and quality of encryption algorithms), and the use of cryptographic keys (e.g. by defining how public key certificates are obtained). The existing rules, procedures and policies of the target organization should be evaluated against the standards requirements.

For the gap analysis, both two controls in Table A.5 have been evaluated for compliance. For both controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.6 Operational security

A.12 defines controls that guide operational security in the organization.

A.12.1.1 to -3 require documenting operating procedures (1), controlling changes relevant to information security (2) and monitoring resource usage (3), i.e. certain procedures relating to information processing must be documented, changes to information processing systems must be appropriately controlled and the capacity and resource usage of information processing facilities must be monitored and planned. These should be eval-

uated in the target organization by surveying operational procedures and reviewing them against the standards requirements. Change controls should be evaluated by surveying and reviewing how changes to information systems are controlled, e.g. are all information system changes assessed for their potential security impact. Resource monitoring should be evaluated by surveying and reviewing how the capacity of information systems is monitored and controlled, e.g. is obsolete data systematically removed to save storage space.

A.12.1.4 requires separating the development, testing and operational environments in the organization. In order to evaluate compliance with this, the current way that information systems are deployed and updated needs to be reviewed against the standards requirements. It should be ensured that for example, all changes to operational systems are tested before their deployment.

For compliance with A.12.2.1, controls to protect against malware should be implemented. The controls required by the standard take the form of anti-malware software, user awareness and operating procedures, e.g. application whitelisting in information processing facilities. This should be evaluated by surveying all the controls that the target organization has in place to protect against malware, and reviewing them against the requirements of the standard.

A.12.3.1 requires a backup-policy and -testing, i.e. a backup plan must be created with appropriate testing of the plan and physical backup media along with other controls. To evaluate compliance, the target organization's procedures for backups need to be reviewed against the standards requirements. If a specific policy exists, it should be reviewed.

A.12.4.1 to -3 give requirements for event logging on information systems (1), protection of information system logs (2) and the logging of system administrator actions (3). The target organization's logging procedures should be evaluated against the standards requirements, e.g. do information systems log both successful and unsuccessful access attempts?

A.12.4.4 requires information systems to be synchronized to a single time source. Compliance with this should be evaluated simply by surveying how information systems set their clock and whether it is ensured that all information systems utilize the same reference time source.

Compliance with A.12.5.1 requires that installation of software on operational systems is controlled, e.g. by ensuring that only trained and approved personnel are allowed to install software on operational systems. This should be evaluated by surveying how the target organization manages the installation of software on operational systems, and reviewing the procedures against the standards requirements.

A.12.6.1 requires that technical vulnerabilities are managed by collecting information on technical vulnerabilities of information systems and taking measures to address those vulnerabilities. Compliance with this should be evaluated by surveying and reviewing the processes that the target organization uses to control technical vulnerabilities in information systems. A.12.6.2 requires that the organization restricts the type of software that users are allowed to install. To evaluate compliance with this control, all software installation controls need to be surveyed and reviewed.

Whenever auditing is performed on operational systems, it should be planned to minimize disruptions (A.12.7.1). To evaluate this, the way the target organization conducts system auditing should be surveyed and reviewed.

For the gap analysis, all 14 controls in Table A.6 have been evaluated for compliance. For the 14 controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.7 Communications security

A.13 defines controls that guide the use of communication and computer networking in the organization.

Controls 13.1.1 to -3 give requirements for network security, with requirements for

protecting computer networks in the organization (1), managing network services (2) and segregating networks (3). Evaluating A.13.1.1 should be done by evaluating the way computer networks are controlled and managed in the target organization, e.g. is operational responsibility for networks separated from computer operations? To assess compliance with A.13.1.2, the network services used by the target organization should be reviewed against the requirements of the standard to ensure an appropriate security level. Evaluating A.13.1.3 should be done by surveying the network structure of the target organization and evaluating whether the network is appropriately segregated into sub-domains.

Controls A.13.2.1 to -4 give requirements for transferring information between different parties within, as well as to and from the organization. These requirements relate to transfer policies (1) and agreements (2), electronic messaging (3) and non-disclosure agreements (4). To evaluate the compliance with A.13.2.1 and -1, the target organization's transfer policies and agreements should be reviewed against the standards requirements. To assess compliance with A.13.2.3, all electronic messaging applications (including e-mail, chat-applications and social networking) used by the target organization should be surveyed and reviewed against the security requirements set by the organization and the standard. A.13.2.4 should be evaluated by reviewing all contracts with employees and external parties against the requirements of the standard.

For the gap analysis, all seven controls in Table A.7 have been evaluated for compliance. For the seven controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.8 System acquisition, development and maintenance

A.14 defines controls that guide developing and maintaining information systems.

A.14.1.1 states that requirements of information systems that are developed or acquired should include relevant information security requirements. Compliance with this should be assessed by reviewing the requirements that the target organization has defined

for software it has developed or acquired and evaluating whether the requirements of the standard have been addressed.

Requirements for networked software are addressed in A.14.1.2 and -3. These relate to protecting software applications on public networks (1) and protecting service transactions (such as API's offered by the organization's systems) (2). For A.14.1.3, all networked software should be reviewed against the standards requirements (e.g. is the used communication path encrypted?). For networked services on public networks, they should also be reviewed against the requirements of A.14.1.2 (e.g. is the identity of external parties appropriately authenticated?).

Controls A.14.2.1 to -5 give requirements for how an organization develops and maintains its software. These relate to development rules (such as coding guidelines and vulnerability avoiding) (1), change control procedures (such as testing and documenting changes) (2), operating platform changes (3), modifications to software packages (4) and secure engineering principles (5). For these controls, the software engineering processes and rules of the target organization should be surveyed and reviewed against the standards requirements.

A.14.2.6 requires that software development environments are secured, e.g by controlling access to the development environment. A.14.2.7 requires that outsourced development is monitored and supervised, e.g. by escrow agreements if applicable. Here, once again, the target organization's approach to securing their development environment and outsourced development needs to be reviewed against the standard.

Software testing is addressed in controls A.14.2.8, -9 and A.14.3.1. These relate to security testing to ensure that the system meets security requirements (A.14.2.8), acceptance testing to ensure that the system meets overall requirements (A.14.2.9) and protecting test data (A.14.3.1). To evaluate compliance with these controls, the testing processes, rules and systems of the target organization should be surveyed and reviewed against the standards requirements.

For the gap analysis, all 13 controls in Table A.8 have been evaluated for compliance. For the 13 controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.1.9 Compliance

A.18 defines controls that guide achieving and maintaining compliance with legislative, regulative and contractual requirements.

A.18.1.1 requires an organization to identify the relevant legislative and contractual requirements for their systems. The standard requires that these requirements are documented. As such the target organization should have a document listing relevant legislative and contractual requirements. If such a document exists, it should be reviewed, otherwise the organization is not compliant.

To ensure that the organization fulfills all legislative, regulative and contractual requirements for intellectual property (2), protecting of records (3), protection of personally identifiable information (4) and usage of cryptographic controls (5) the standard requires controls A.18.1.2 to -5. These controls give a guideline for identifying the legislative, regulative and contractual requirements that the target organization must follow in terms of the aforementioned categories. To evaluate compliance, the target organization's policies, procedures and rules regarding intellectual property, storage of records, personal information and cryptography should be reviewed against the standard.

Controls A.18.2.1 to -3 give controls related to reviewing and auditing the organization's information security. According to these controls, the organization's information security should regularly reviewed by an independent party (1), be compliant with all appropriate policies and standards (2) as well as regularly reviewing their information systems for compliance with all policies (3). To assess compliance with A.18.2.1 controls, the records of independent security reviews should be reviewed (these are required for compliance). For A.18.2.2, the management approach for ensuring compliance with

policies and standards should be reviewed against the standard. Finally, for A.18.2.3 the procedures for information system security reviewing should also be reviewed against the standard.

For the gap analysis, all eight controls in Table A.9 have been evaluated for compliance. For the eight controls, the target organization's compliance has been evaluated, but the results have been omitted.

6.2 Summary

This chapter has answered RQ2 of the thesis. A gap analysis has been performed on the controls deemed relevant for this thesis (Appendix B has identified the data protection controls). It has been analyzed whether the target organization is compliant with the controls requirements. In the case of partial- or non-compliance suggestions for how compliance might be achieved have also been given. The results of the analysis have been omitted from the published thesis, but this chapter has described the way each control has been assessed to evaluate compliance. The omitted results are used by the target organization to evaluate their compliance with the standard.

Chapter 7

Case study: MyData and IHAN

This chapter attempts to answer RQ3 of the thesis by providing suggestions for solutions to meet the requirements identified in Chapter 3.

The impact of MyData and IHAN on quality registers depends greatly on how the customer's systems (e.g. patient information systems at a hospitals) implement the MyData or IHAN functionality. This chapter works from the assumption, that the consent to use patient data in quality registers would happen through the customer's systems rather than as separate services. Due to this assumption, the relevance of the changes in this chapter is difficult to evaluate. If for example a customer would use some type of a centralized system to handle all consent management, these changes might not be relevant. Overall this chapter has attempted to give some type of suggestion for each requirement, but not explore the relevance of that requirement to quality registers further.

7.1 Implementing MyData requirements

In the context of MyData, disease specific quality registers may be considered a data source and a data sink. They are data sources in the sense that they collect personal data and offer it for purposes such as research. Quality registers may be considered data sinks since they receive personal data from different data sources such as other hospital systems.

In Chapter 3 eleven different requirements were identified for organizations wishing to function in the MyData - ecosystem. This section attempts to describe how disease specific quality registers may reach all of these requirements. The following changes must be implemented in the disease specific quality registers.

7.1.1 ISMS changes

Categorization of data

To meet the requirements of MD_ISMS_1, for each quality register all data sources should be identified. In other words, the external systems that each quality register receives patient data from should be identified. In practice this would likely mean a documented listing needs to be created for each quality register, that lists each data source and what data is received from that source. Most of the quality registers receive data from shared sources such as patient information systems, operative information systems and laboratory information systems of the Finnish health care system. Registers may also use data sources specific to that quality register. The specific data sources used by each register need to be identified.

Human readable description

The human readable description (MD_ISMS_2) of a register is, as the name suggests, a description of a service meant to describe it to MyData account owners considering that service consent to use their personal data. The human readable description would likely be quite similar to marketing material, describing the quality register as a service that stores and processes medical data that may be used to assess the quality and effectiveness of treatment of that disease group. Each register needs to provide this kind of a description.

Service data description

The service data description (MD_ISMS_3) is a definition of what data is stored in that service. This description is of a specified format defined by the MyData architectural specification[30]. Each quality register must have service data description defined for them. The service data description defines different data sets, which are logical sets of data stored in that service. In the case of quality registers, different data sets could include e.g. ”patient basic information”, ”patient medication information” and ”patient laboratory results”. Figure 7.1 gives an example of one data point (patient weight) defined in a service data description. Some information has been omitted for simplicity. Each register needs to define a similar definition for each data point they store as these vary greatly between registers.

```
{
    "serviceDataDescription": [
        {
            "dataset": [
                {
                    "description": "Patients background infromation in a disease specific quality
                    "title": "Patient background information",
                    "serviceDataType": "input",
                    "language": "fi",
                    "structure": [
                        {
                            "dataStructureDefinitionID": "patient_basic_information",
                            "component": [
                                {
                                    "componentSpecificationID": "patient_basic_measurements",
                                    "componentProperty": [
                                        {
                                            "label": "Weight (kg)",
                                            "range": "0-999"
                                        }
                                    ]
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```

Figure 7.1: Example of a data set with one data point.

7.1.2 Architectural and technical changes

In terms of software components, MyData would require implementing three software components (classes) in the quality registers. The relation of these three to each other is visualized in Figure 7.2. These are based on [31], and the accompanying specifications ([30], [23], [24] and [25]).

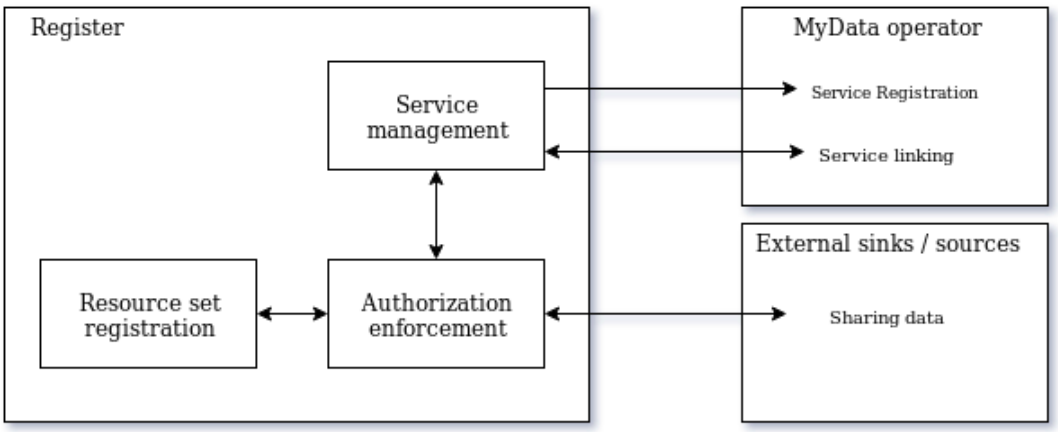

Figure 7.2: Necessary software components for MyData-functionality.

The flow of consent between different systems is described Figure 7.3.

Technical service description

Disease specific quality registers do not act as data sources on public networks but rather data sinks, and as such a technical service description is not required and MD_ARCH_1 is not relevant for these systems. Technical service descriptions are mainly relevant for systems acting as sources on public networks, as the technical service description provides a technical description of the interfaces through which the service provides access to data.

Service management - component

For the service management- component (MD_ARCH_2), a service must implement a component that manages service registering and service linking. Service registration re-

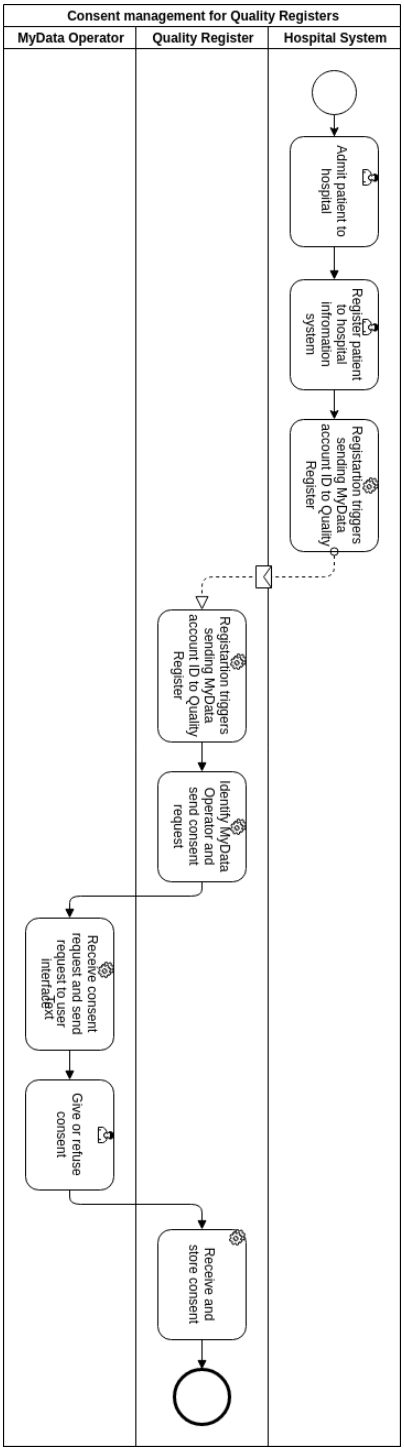

Figure 7.3: Flow of consent management.

quires identifying relevant MyData operators. The service management component likely would need general functionality for MyData service registration, which is then configured for each customer based on which MyData Operator they have registered their services in. As can be seen from Figure 7.3, the service linking process is triggered from a hospital information system when a patient is registered. Due to this, the implementation in the quality register will be heavily dependant on how the hospital systems implement service linking, and how the information of the patient is received by the register.

For this a ServiceManagementService-class will need to be implemented in the quality registers. This class would offer functionality related to registering the quality register as a service in a MyData-operators service registry as well as linking the quality register to an account owner's MyData account.

When a quality register is taken into use, the service registration process should be triggered. This should be done once for each environment (client) that the register is deployed into. The service linking process should preferably be triggered whenever an account owner is registered as a client to a certain health care - department. If this is not possible, some other process for linking the quality register - service needs to be defined.

The ServiceManagementService-class is meant to provide functionality to fulfill the requirements of MD_ARCH_2. It achieves that by offering the following functions:

```
/**
 * Create a service description - object from the human readable
   description, technical service description and the service data
   description. This should be a JSON object constructed from quality
    register specific configurations.
 */
produceServiceDescription()

/**
 * Send the service description and and the service instance object to
    the service registry. The service instance described a single
```

```
     active instance of a service to the service registry. If there are
      multiple instances of a service all must provide their own
     instance. The format of both the service description and instance
     are defined in the Service Registry Specification.
 */
registerService()

/**
 * Produce a unique identifier for the specific MyData account in this
      service. The surrogate ID is used to identify the account owner
     in this service. Each patient in a quality register needs a unique
      identifier in a register.
 */
generateSurrogateID()

/**
 * Create a service link record, which indicates a link between a
     service (the quality register), a MyData operator and an account
     owner (surrogate id). Service link record is stored along with
     necessary public keys to ensure authenticity when communicating
     with the MyData operator and ensuring validity of consent records.
 */
createSlr()

/**
 * Create a service link status record which is a database record
     indicating whether a consent record is active or revoked.
 */
createSsr()

/**
 * Update the status of a service link.
 */
```

```
updateSlr()
```

Resource set registration - component

Resource sets (RS) are the logical sets of personal data that a consent may be issued. Practically this would mean that all personal data in a data source must be split into resource sets that are given a unique id, and as such consent for usage from the account owner may be linked to that set of personal data. A format for the resource sets is defined in the MyData Authorization Specification[24].

In the quality registers, the resource sets would likely encompass the entirety of a patient's data in that register. In other words consent is either issued or revoked for the entirety of that patient - the patient either consents to using their data for the purposes of that register (and linked data sinks). As a technical process, this would mean that each time a new patient is added into a quality register, a new resource set would be created that encompasses all data stored in the register about that patient.

The high-level process for receiving consent for storing and using the patients data is described in Figure 7.3. In quality registers the patient's resource set is created when a hospital system triggers the consent requesting process. The consent given by the patient (MyData Account owner) may then be linked to this resource set.

The ResourceSetService-class offers functionality that satisfies the requirements of MD_ARCH_3. To achieve this, it should offer the following functions:

```
/**
 * Generate a resource set id to identify a set of personal data. The
   resource set must follow a unique format defined in the MyData
   Authorisation Specification.
 */
generateRsId()

/**
```

```
 * Create a database record which links a resource set id to a certain
     set of personal data. The resource set must follow a unique
     format defined in the MyData Authorisation Specification.
 */
createResourceSet()

/**
 * Send a request to a MyData Operator to request consent to use a
     patient's data. Link the received consent to that patient's
     resource set.
 */
requestConsent()

/**
 * Get all data in a resource set in the quality register, format must
     be defined specifically for each register. This should provide a
     uniform way of fetching all patient data from a register.
 */
getResourceSetData()
```

Authorization enforcement - component

Software functionality is needed to handle and enforce account owner consent. As the resource set registration component is used to handle creating new resource sets, the authorization enforcement component would be used to issue these resource sets consent from the account owner. For installing consent to a resource set, a consent record (CR) and consent status record (CSR) must be created. The consent record states, what kind of usage has received consent from the account owner for that set of personal data (the resource set in question). The consent status record states whether the consent is valid or if the consent has been revoked.

In the case of quality registers, consent records would be initially installed when a

user links the service to their MyData account, and are asked whether or not they consent to using their data for the purposes of that register/registers. If consent is given then the CR and CSR are created. Consent may also be related to transferring data outside the register and as such the required consent for each register must be separately defined (such as outside reports). Overall the granularity of consent in quality registers is coarse, as consent is generally either given for usage of account owner data fully in that registers context or not given at all (in which case data of that patient will not be saved or processed in the register).

According to MD_ARCH_4, a component to handle and enforce authorization must be implemented. In quality registers, this is achieved by the AuthorizationEnforcementService-class, which offers functionality for handling and enforcing consent issued to resource sets. To fulfill MD_ARCH_4, it should offer the following functions:

```
/**
 * Create consent record and link it to a resource set and consent
   status record. These together will define consent for a set of
   personal data.
 */
installConsent()

/**
 * Create a consent record which links a account owner, resource set
   and rules of usage for that data.
 */
createCr()

/**
 * Create a consent status record which is a database record
   indicating whether a consent record is active, inactive or revoked
   .
 */
```

```
storeCsr()

/**
 * Update the consent status of a consent.
 */
updateConsent()

/**
 * Check rules of usage of a set of personal data (a resource set).
 */
checkConsent()
```

Audit logging

Since the registers implement audit logging in their current state MD_ARCH_5 likely would not require major changes to be fulfilled. As quality registers already implement logging, including a type of audit logging, and this could likely be re-used to also cover the requirements of MD_ARCH_5.

MyData consent in Quality Registers

Implementing the consent management described in the MyData Authorization Specification [24] is described in Section 7.1.2. Technically each quality register needs to store consent records and authorization tokens (defined by [25]) for each patient in the register. One consent record needs to be stored for using the patients data in the register itself and a consent record and authorization token combination for each outside system from where that patients data is to requested.

The process for receiving consent is described in Figure 7.3. From the patients point of view, giving consent to quality registers would take the form request to their MyData Operator to give consent in using their data in a disease specific quality register. Exactly how the consent would be described to the patient would depend on the human-

readable description of the quality register (Section 7.1.1). The process of receiving consent would however be highly dependant on how the treating hospital would implement their MyData-solutions.

7.1.3 Integration changes

To establish communication with outside systems for MyData purposes, such as the MyData-operator as well as data sources and sinks, network connections and software endpoints need to be established. While the MyData project does not give strict definitions for communication protocols, it is implied that they should be RESTful[31]. As such the implementation suggestions in this section should be implemented as REST-API endpoints.

Service management API

For service management purposes, a service management API will need to be implemented (MD_INT_1). This would expose necessary functionality in the service management component[23].

In quality registers the following REST-API endpoints would need to be implemented to fulfill the requirements of MD_INT_1 (adapted from [32]):

- `/surrogate_id`: Provide the surrogate ID to the MyData operator once it begins the linking process.
- `/linking`: Initiate service linking from an account owner.
- `/slr`: Provide the service link record to the MyData operator.
- `/status`: Provide information about service and its status to sinks and the MyData operator.

Authorization enforcement API

For authorization and consent management purposes, an authorization enforcement API will need to be implemented (MD_INT_2). This would expose necessary functionality in the authorization enforcement component.

In quality registers the following REST-API endpoints would need to be implemented to fulfill the requirements of MD_INT_2 (adapted from [32]):

- `/cr_management`: Allow storing and fetching of the consent record and the consent status record of patients.

Data API

For the actual data transfer between data sources and sinks, a data API needs to be implemented (MD_INT_3).

In quality registers the following REST-API endpoints would need to be implemented to fulfill the requirements of MD_INT_3 (adapted from [32]):

- `/datarequest`: Process data requests from data sinks. This would include validating the request and transferring the requested data.

7.2 Implementing IHAN requirements

A disease specific quality register both ”provides Services to End Users and other Service Providers”[8] (e.g. providing disease specific data analysis and the MyHealth system) and ”provides data for Service Providers and/or End Users”[8] (e.g. integrating with other medical information systems). As such - in terms of IHAN - they are a service provider and a data provider. This section is based on the IHAN blueprint[8].

In Chapter 3, ten different requirements were identified for organizations wishing to function in the IHAN - ecosystem. This section attempts to describe how disease specific

quality registers may reach all of these requirements. The following changes must be implemented in the disease specific quality registers.

7.2.1 ISMS changes

Cataloguing services

In order to fulfill IHAN_ISMS_1, the services must be catalogued. In the case of disease specific quality registers this would take the form of a full list of all different registers. Some of the registers might be combined to a single service to make linking services more convenient for customers.

Identifying needed data providers

IHAN_ISMS_2 requires that data providers used by a service are identified. In practice this means identifying or external systems / databases that provide personal data to the service. For disease specific quality registers, this would mean listing integrated data sources for each register separately, since they differ from register to register and client to client.

General data sources used by quality registers would include at least patient information systems, operative information systems and laboratory systems.

Categorizing data providers into mandatory and optional

In order to fulfill IHAN_ISMS_3, data sources need to be categorized as mandatory and optional. For disease specific quality registers, the data sources are likely to be hard to fully understand for the end-user and as such it is likely better that all sources are mandatory. As such a end-user would either consent to their data being used in a register or not.

Registering on the public service directory

To meet the requirements of IHAN_ISMS_4, all public service directories used by the relevant clients need to be identified and the quality registers registered as services there. Quality registers should be registered as services on all public service directories where clients are registered.

7.2.2 Architectural and technical changes

Implementing IHAN service provider components

In order to fulfill the requirements of IHAN_ARCH_1, implementing certain IHAN specific software components is necessary. These components include the service provider service directory, consent directory, inbound data adapter and the service provider log.

The service provider service directory (SPSD) is a component which stores records of all IHAN services. The SPSD stores records with metadata of services offered by that organization, and transfers those to public service directory. For disease specific quality registers, the SPSD could be implemented as a centralized service (i.e. an internal application server) which keeps an automated list of all the registers and their descriptions. The SPSD would need to be configured with connections to all relevant public service directories and should update service records of the quality registers when changes are made to a register and when a register is added or removed.

The service provider consent directory (SPCD) is component which stores and handles records of end-user (patients in this case) consent. For quality registers, these consent records allow receiving patient data from other IHAN compliant medical information systems. A consent record is required for each patient and each medical information system from which data is needed. Each quality register would need to implement a component that stores consent records and use them when requesting data from the integration platform.

The inbound data adapter (IDA) is an interface which is used to receive data from data providers. In the case of quality registers, the IDA would likely be implemented in the integration platform utilized by all quality registers. This way the outside IHAN inbound data interface would meet the IHAN requirements but no changes to the quality registers would be needed.

The service provider log (SPL) is a component which stores log entries of service changes (changes to the service itself), service usage and data usage. Also the SPL must also provide an API to access log entries, e.g. an end-user can access logs that relate to their personal data. The IHAN blueprint however provides very limited specification on this API. In quality registers, the SPL would likely be implemented as a part of the existing logging component (which handles audit and event logging), which would be extended to meet the requirements of IHAN. The existing logging system would also need to implement the SPL API.

Implementing IHAN data provider components

For serving data to other IHAN-compliant services - i.e. acting as a data source - some data provider specific components (IHAN_ARCH_2) are required. For quality registers these include the data source, the data access control - component, the outbound data adapter and the data provider log.

The data source (DS) is a description of an IHAN data source. The DS is similar to the SPSD. For quality registers, the DS could be implemented together with the SPSD, as a service which stores the service descriptions as well as the data source descriptions and transfers them to the public service directories.

The data access control - component(DAC) implements authorization of data accesses by verifying the consents received from services. In practice this mainly means verifying data requests against consent forms to ensure consent. For quality registers, this component would need to be implemented. In quality registers the DAC would interface with

the ODA in the integration platform. When the register receives a data request, it verifies consent and forwards it to the integration platform ODA along with the data.

The outbound data adapter (ODA) is an interface which is used to respond to requests from services and transfer data to services. As with the IDA, the ODA would likely be implemented in the integration platform, allowing the quality registers to remain unchanged. The services requesting data from quality registers could likely be other medical information systems, for instance when constructing medical records.

Similarly to the SPL, data providers must implement the data provider log (DPL). For quality registers, the DPL could likely be implemented together with the SPL as an extension of the existing logging component. Along with the SPL API, the DPL API would be implemented since they are quite similar.

Functionality for working without optional data providers

Since it was determined in Section 7.2.1 that no data providers are optional, it will not be necessary to implement functionality that would allow functioning without optional data providers. As such IHAN_ARCH_3 will not require extra work.

IHAN consent in Quality Registers

Each quality register would need to store a consent form for each patient - data source combination, i.e. for each patient in the register whose data is to be requested from other systems (patient and operational information systems etc.) a consent form for each of those is needed. This consent form is a database record which defines the data source and an encrypted message to the data source which is used to verify the legitimacy of that consent. With that consent form, the quality register can request that patient data from the data source. The IHAN blueprint[8] does not yet give a detailed description of the content of the consent.

From the point of view of the patient, consent would likely be received along with

their consent for other medical information systems. In practice, when they are requested for consent for using their data in medical information systems relevant for their treatment in the hospital they are treated in, then the consent request would include a clause which states that they accept their data is used disease specific quality registers. The IHAN blueprint[8] however gives little definition to the exact form and content of the consent so defining the practical form and process of consent here is difficult.

7.2.3 Integration changes

Inbound and outbound adapter interfaces

For incoming and outgoing data, implementing interfaces defined by the IHAN blueprint are required (IHAN_INT_1).

In the case of requesting data from external data sources, the inbound data adapter is required. In the case of quality registers, this would take the form of a REST-API endpoint which forwards data to relevant components in the registers. Similarly, the outbound data adapter is needed to interface with external services requesting patient data from the quality register.

In addition to these, network connections to data providers and relevant external services need to be established.

Consent interfaces

In addition to interfaces for data transfer, interfaces for communicating end-user consent for that data transfer must be implemented (IHAN_INT_2). In the quality registers, the consent directory must - in addition to the features mentioned in Section 7.2.2 - also implement an interface to receive consent forms from the end-users personal consent directory. The implementation of that may vary but the interface should match the one defined by the IHAN-project.

Also, network connections to the public service directory and the end-users personal consent directory need to be established.

7.3 Combining MyData, IHAN and ISO27001

Chapter 4 identified potential challenges and benefits of implementing the requirements of both ISO 27001, MyData and/or IHAN. This section addresses these benefits and challenges in the case of disease specific quality registers.

7.3.1 Utilizing ISO27001 - Potential benefits

As mentioned in Section 4.3.1 ISO 27001, MyData and IHAN may potentially complement each in terms of categorizing and labeling data. In disease specific quality registers, the existing system used to categorize data for A.8.2.1 may prove useful when identifying the personal data used and received by the registers.

Section 4.4.1 mentions that in the case of access control (A.9.1.1), ISO 27001, MyData and IHAN may support each other. In disease specific quality registers however, this chapter has defined the consent as ”all or nothing” so there is likely no need to combine it with access control controls of ISO 27001.

Disease specific quality registers have already implemented a set of cryptographic controls, and as such the beneficial overlap mentioned in Section 4.5.1 can likely not be utilized here.

The existing audit logging system used by the disease specific quality registers may be used for MyData and/or IHAN. This way the beneficial overlap mentioned in Section 4.6.1 can be utilized.

Formal data transfer policies (A.13.2.1) may be useful enforcing consent management when transferring personal data from disease specific quality registers to outside systems - the beneficial overlap identified in Section 4.7.1 can likely be utilized.

Disease specific quality registers already implement a large set of information security solutions, so the standardised solutions potentially offered by MyData and/or IHAN can likely not be utilized here (Section 4.8.1). Likely, the changes to information security required by MyData and/or IHAN would need to implemented considering both the requirements of A.14 and existing information security.

MyData and/or IHAN can likely be useful in creating a policy on personally identifiable information (A.18.1.4) for disease specific quality registers. This way the potential beneficial overlap mentioned in Section 4.9.1 can be utilized here.

7.3.2 Challenges of combining MyData, IHAN and ISO27001

The existing information security policies (A.5.1.1) for disease specific quality registers will likely need to be reviewed and potentially modified to accommodate MyData and/or IHAN. The detrimental overlap mentioned in Section 4.1.1 is thus realized.

Similarly, access control policies of disease specific quality registers (A.9.1.1) and user provisioning processes (A.9.2.2) will need to accommodate MyData and/or IHAN, realizing the detrimental overlap identified in Section 4.4.2. Existing data transfer policies (A.13.2.2) will also need to be reviewed and updated as mentioned in Section 4.7.2.

In order to implement MyData and/or IHAN in disease specific quality registers, where a set of cryptographic controls and a policy is already in place, additional work will be needed to combine existing controls with the requirements of MyData and/or IHAN (e.g. JWK[28] and JWT[33] [31]), as mentioned in Section 4.5.2.

The systems change controls (A.14.2.2) that restrict the changes made to disease specific quality registers will cause additional work when implementing MyData- and IHAN-components, realizing the detrimental overlap identified in Section 4.8.2. These change controls include things like documenting and reviewing changes. Similarly, system testing required by A.14.2.8 will need to be performed on these components, causing further additional work.

7.4 Summary

This chapter has answered RQ3 of the thesis. Section 7.1 gives suggestions for implementing the requirements of MyData (identified in Section 3.3) while Section 7.2 gives suggestions for the requirements of IHAN (identified in Section 3.4). Section 7.3 attempts to both utilize the beneficial overlap and address the detrimental overlap identified in Chapter 4 in the context of quality registers.

Chapter 8

Conclusions

This thesis has studied data protection as a subset of information security. MyData and IHAN - Data protection initiatives aimed improving data protection of personally identifiable data - have been studied alongside the ISO 27001 information security standard. A medical information system that processes and stores patient data has been analyzed as a case study.

ISO 27001 is an information security standard. The thesis summarized the main terminology of the standard and the framework that the standard gives for defining and operating information security management systems (ISMS) in organizations. Main focus has been the information security controls of the standard, which gives a set of requirements for the ISMS.

MyData and IHAN are data protection initiatives providing solutions to improve data protection and persons control over their personal data. Requirements of MyData and IHAN impose on systems and organization processing and storing personal data were identified. Requirements were identified related to the management of the organization, technical and architectural solutions and integrating with other systems.

The requirements of MyData and IHAN, that were identified, were compared with the information security controls of ISO 27001. Comparison was done by comparing the controls with the identified requirements and identifying any overlap between the two.

Both beneficial and detrimental overlap was found, as implementing both ISO 27001 along MyData and/or IHAN, can be useful but also cause additional work. The overlap that was found answers RQ1.

The ISO 27001 controls and the requirements of MyData and IHAN were addressed in the context of disease specific quality registers as a case study. The architecture and environment of quality registers were defined.

A gap analysis of the ISO 27001 information security controls was carried out on disease specific quality registers and the governing organization. The gap analysis compares the current situation to the requirements of the standard. Some categories of controls were deemed to be out of scope of the thesis, but otherwise all controls in the standard were addressed by concluding whether the organization operating the quality registers was compliant, partially compliant or not compliant with the control. Suggestions for potential actions to reach compliance were also given where relevant. The gap analysis and the accompanying suggestions answer RQ2.

Suggestions on how to meet the identified requirements of MyData and IHAN in quality registers were given. The suggestions took the form of software architectural changes, technical solutions, integrating with other systems and other activities. The identified overlap between the ISO 27001 controls and MyData and IHAN requirements was also addressed in the context of quality registers. The suggestions as well as addressing the overlap attempts to answer RQ3. The relevance of MyData and IHAN on quality registers was also discussed.

Future study on the subjects of data protection, information security and handling of personally identifiable information could potentially cover implementing MyData and IHAN in other contexts or further develop a reference implementation of them. The relationship between Finnish law and MyData and IHAN would also need to be studied. The data protection coverage of the ISO 27001 standard could also be further evaluated.

References

[1] De Hert P. and Gutwirth S. Data protection in the case law of strasbourg and luxemburg: Constitutionalisation in action. *Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?*, 2009.

[2] ISO/IEC. 25237:2008 Health informatics — Pseudonymization. Standard, International Organization for Standardization, 2008.

[3] ISO/IEC. 20944-1:2013 Information technology — Metadata Registries Interoperability and Bindings (MDR-IB) — Part 1: Framework, common vocabulary, and common provisions for conformance. Standard, International Organization for Standardization, 2013.

[4] ISO/TR. 12859:2009 Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems. Standard, International Organization for Standardization, 2009.

[5] European Parliament and Council. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, 2016.

[6] Janis Wong and Tristan Henderson. How portable is portable? exercising the gdpr's right to data portability. In *Proceedings of the 2018 ACM International Joint Con-*

ference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, UbiComp '18, page 911–920, New York, NY, USA, 2018. Association for Computing Machinery.

[7] Antti Poikola, Kai Kuikkaniemi, Ossi Kuittinen, Harri Honko, and Aleksi Knuutila. MyData – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen. -, 2018.

[8] Antti Larsio, Juhani Luoma-Kyyny, Jyrki Suokas, and Teemu Karvonen. IHAN Blueprint 2.0v261018. -, 2018.

[9] ISO/IEC. 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Standard, International Organization for Standardization, 2013.

[10] ISO/IEC. 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Standard, International Organization for Standardization, 2018.

[11] ISO/IEC. 28002:2011 Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use. Standard, International Organization for Standardization, 2011.

[12] Odunayo Owopetu. *Achieving ISO 27001 Certification by implementing an Information Security Management System*. University of Turku, 2018.

[13] M Sokovic, D Pavletic, and K Kern Pipan. Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS. *Journal of achievements in materials and manufacturing engineering*, 43(1):476–483, 2010.

[14] Zaydi Mounia and Nassereddine Bouchaib. A new comprehensive solution to handle information security governance in organizations. In *Proceedings of the 2nd International Conference on Networking, Information Systems and Security*, NISS19, New York, NY, USA, 2019. Association for Computing Machinery.

[15] Dejan kosutic. how to define the isms scope. https://advisera.com/27001academy/knowledgebase/how-to-define-the-isms-scope/. Accessed: 2019-04-17 and 2019-04-24.

[16] APB Consultant Pretesh Biswas. ISMS: Context of the organization. http://isoconsultantpune.com/isms-context-of-the-organization/. Accessed: 2019-04-24.

[17] Dejan Kosutic. Iso 27001 risk assessment & treatment – 6 basic steps. https://advisera.com/27001academy/knowledgebase/iso-27001-risk-assessment-treatment-6-basic-steps/. Accessed: 2019-04-24.

[18] Dejan Kosutic. Overview of iso 27001:2013 annex a. https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/. Accessed: 2019-04-17.

[19] Ibrahim Al-Mayahi. ISO 27001 Gap Analysis-Case Study. In -, 2012.

[20] Antti Poikola, Kai Kuikkaniemi, and Harri Kuikkaniemi. MyData – A Nordic Model for human-centered personal data management and processing. -, 2014.

[21] Alén-Savikko et.al. MyData Architecture - Consent Based Approach for Personal Data Management, Release 1.2.1. http://bit.ly/mydata_stack. Accessed: 2019-03-20.

[22] The World Wide Web Consortium (W3C). Web application description language. https://www.w3.org/Submission/wadl/#x3-10001. Accessed: 2019-03-24.

[23] MyData Architecture - Service Linking. https://raw.githubusercontent.com/HIIT/mydata-stack/gh-pages/mydata-service-linking.pdf. Accessed: 2019-10-19.

[24] MyData Authorisation Specification. https://raw.githubusercontent.com/HIIT/mydata-stack/gh-pages/mydata-data-authz.pdf. Accessed: 2019-10-19.

[25] MyData Architecture - Data Connection. https://raw.githubusercontent.com/HIIT/mydata-stack/gh-pages/mydata-data-connection.pdf. Accessed: 2019-10-19.

[26] ISO/IEC. 27002:2013 Information technology — Security techniques — Code of practice for information security controls. Standard, International Organization for Standardization, 2013.

[27] Dejan Kosutic. *ISO 27001 Annex A Controls in Plain English: Step-by-step handbook for information security practitioners in small businesses*. Advisera Expert Solutions Ltd, 2016.

[28] Michael B. Jones. Rfc 7517: Json web key (jwk). https://tools.ietf.org/html/rfc7517. Accessed: 2019-10-21.

[29] BCB Medical. Internal document.

[30] MyData Architecture - Service Registry. https://raw.githubusercontent.com/HIIT/mydata-stack/gh-pages/mydata-service-registry.pdf. Accessed: 2019-10-19.

[31] MyData Architecture - Consent Based Approach for Personal DataManagement, Release 1.2.1. https://raw.githubusercontent.com/HIIT/mydata-stack/gh-pages/stack.pdf. Accessed: 2019-10-19.

[32] Harri Honko. Reference implementation of mydata architecture framework 2.0. https://github.com/mydata-sdk/mydata-sdk. Accessed: 2020-03-08.

[33] M. Jones. RFC 7519: JSON Web Token (JWT). https://tools.ietf.org/html/rfc7519. Accessed: 2020-03-08.

Appendix A

ISO 27001 Controls

This Appendix summarizes all the controls handled in Chapter 6. This appendix has been summarized from the ISO 27001[9] and 27002[26] standards.

Table A.1 – Controls: Information security policies

Code	Control
A.5.1.1	Company has a formal information security policy.
A.5.1.2	Information security policy is reviewed in specific intervals.

Table A.2 – Controls: Organization of information security

Code	Control
A.6.1.1	Information security responsibilities are defined.
A.6.1.2	Duties for different assets are segregated.
A.6.1.3	Contact with relevant authorities maintained.
A.6.1.4	Contact with relevant special interest groups maintained.
A.6.1.5	Information security is taken into account in all types of projects

Continued on next page

Table A.2 – continued from previous page

Code	Control
A.6.2.1	Policy for mobile devices exists.
A.6.2.2	Policy for teleworking exists.

Table A.3 – Controls: Asset management

Code	Control
A.8.1.1	Asset inventory exists.
A.8.1.2	Owner is defined for each asset.
A.8.1.3	Acceptable use of assets and information is defined.
A.8.1.4	Assets are returned when an employee leaves the organization.
A.8.2.1	All information is classified.
A.8.2.2	Information is labeled based on its classification.
A.8.2.3	Procedures for handling assets based on classification exists.
A.8.3.1	Procedures for handling removable media exists.
A.8.3.2	Procedures for disposal of media exists.
A.8.3.3	Procedures for transferring physical media exists.

Table A.4 – Controls: Access control

Code	Control
A.9.1.1	Access control policy exists.
A.9.1.2	Access to networks and services requires authorization.
A.9.2.1	User registration and de-registration process exists.

Continued on next page

Table A.4 – continued from previous page

Code	Control
A.9.2.2	User access provisioning (granting and removing access to systems) process exists.
A.9.2.3	Privileged access rights (admin rights) are restricted and controlled.
A.9.2.4	Authentication information is controlled through a formal process.
A.9.2.5	Asset owners regularly review access rights to their systems.
A.9.2.6	Access rights are removed when employment, contract or agreement ends.
A.9.3.1	Users follow organizational practices in use of authentication information.
A.9.4.1	Access to information systems is restricted based on the access control policy.
A.9.4.2	Information systems require secure log-on based on the access control policy.
A.9.4.3	Password management systems are used to ensure strong passwords.
A.9.4.4	Use of privileged utility programs is controlled and restricted.
A.9.4.5	Access to program code is restricted.

Table A.5 – Controls: Cryptography

Code	Control
A.10.1.1	Cryptographic control policy exists. This policy describes the use of cryptographic controls for protection of information.
A.10.1.2	Cryptographic key control policy exists. This policy describes the use, protection and lifetime of cryptographic keys.

Table A.6 – Controls: Operational security

Code	Control
A.12.1.1	Documented operating procedures exist and are available to users.
A.12.1.2	Changes that affect information security are controlled.
A.12.1.3	Resource use is controlled and monitored to ensure capacity and performance.
A.12.1.4	Development, testing and operational environments are separated.
A.12.2.1	Protections against malware are implemented, along with user awareness.
A.12.3.1	Backup policy exists. Backups are taken and tested regularly according to policy.
A.12.4.1	Logs of user activities, exceptions, faults and security events are kept and reviewed.
A.12.4.2	Logging is protected against tampering and unauthorized access.
A.12.4.3	System administrator and operator logs are kept, protected and reviewed.
A.12.4.4	Relevant information systems are synchronized to a single reference time source.
A.12.5.1	Installation of software on operational systems is controlled.
A.12.6.1	Technical vulnerabilities of information systems should be evaluated and appropriately addressed.
A.12.6.2	Installation of software by users is governed by rules.
A.12.7.1	Auditing of operational systems is planned to minimize disruptions.

Table A.7 – Controls: Communications security

Code	Control
A.13.1.1	Networks are controlled to protect information systems.
A.13.1.2	Network service agreements include security mechanisms, service levels and management requirements.
A.13.1.3	Networks are segregated into groups of services and information systems.
A.13.2.1	Policies, procedures and controls for security of transferring information exist.
A.13.2.2	Agreements for transferring information with external parties address information security requirements.
A.13.2.3	Information transferred in electronic messaging (e-mail, instant messaging etc.) is sufficiently protected.
A.13.2.4	Confidentiality and non-disclosure are included in contracts if relevant.

Table A.8 – Controls: System acquisition, development and maintenance

Code	Control
A.14.1.1	Information security is included in requirements of information systems.
A.14.1.2	Applications connected to public networks are protected from unauthorized disclosure and modification as well as other threats on public networks.
A.14.1.3	Application service transactions (transferring data to and from service users) are protected against information security threats.

Continued on next page

Table A.8 – continued from previous page

Code	Control
A.14.2.1	Rules and policy for secure development of information systems exists. This should include rules for avoiding vulnerabilities, secure coding guidelines and other requirements for secure development.
A.14.2.2	Procedures for controlling changes to systems exist. These should include controls for authorizing, testing and documenting changes to systems.
A.14.2.3	Operating platform (operating systems, databases and middleware) changes are reviewed and tested.
A.14.2.4	Changes to software packages should be controlled. Modifications to software packages are to be avoided, and a software update policy exists.
A.14.2.5	Principles for engineering secure systems exist.
A.14.2.6	Environments for information system development and integration are secured.
A.14.2.7	Outsourced development is supervised.
A.14.2.8	System security testing is carried out.
A.14.2.9	System acceptance testing is carried out.
A.14.3.1	Test data is protected.

Table A.9 – Controls: Compliance

Code	Control
A.18.1.1	Relevant legislative and contractual requirements for information systems are identified and documented.
A.18.1.2	Controls for managing intellectual property rights are defined. These include managing for example software licences.
A.18.1.3	Organizations records are protected according to legislative, regulatory and contractual requirements.
A.18.1.4	Personally identifiable information is protected according to legislative and regulative requirements.
A.18.1.5	Cryptographic controls are used according to legislative, regulative and contractual requirements.
A.18.2.1	Organizations information security is regularly and independently reviewed.
A.18.2.2	Organization is compliant with the appropriate security policies and standards.
A.18.2.3	Organizations information systems are regularly reviewed to ensure compliance with information security policies.

Appendix B

Data protection controls

The following categories of controls of ISO27001 have been excluded as irrelevant for this thesis. The categories marked red have been identified as not relevant to this thesis. The controls from the other categories can be considered the requirements set by the ISO27001-standard.

Table B.1 – Data protection controls

Number	Category	Reasoning
A.5	Information security policies	-
A.6	Organization of information security	-
A.7	Human resources security	More related to legal matters, than software engineering.
A.8	Asset management	-
A.9	Access control	-
A.10	Cryptography	-
A.11	Physical and environmental security	More related to physical protection of data, than software engineering.

Continued on next page

Table B.1 – continued from previous page

Number	Category	Reasoning
A.12	Operational security	-
A.13	Communications security	-
A.14	System acquisition, development and maintenance	-
A.15	Supplier relationships	More related to business management, than software engineering.
A.16	Information security incident management	More related to business management, than software engineering.
A.17	Information security aspects of business continuity management	More related to business management, than software engineering.
A.18	Compliance	-