NTNU – Trondheim
Norwegian University of
Science and Technology

Securing software systems in the health care domain

Monika Katrin Kosmo

Master of Science in Communication Technology
Submission date: June 2014
Supervisor: Poul Einar Heegaard, ITEM
Co-supervisor: Karin Bernsmed, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem Description

Medical sensor networks are seeing increased use for monitoring health and well-being, such as remote monitoring and analysis of patients in their own homes. The large amount of data generated by such sensors requires high capacity storage and processing. A cloud-based solution will be considered to get a cost-efficient and flexible solution. Since health care data represent sensitive personal information, there are many security and privacy challenges that must be addressed.

To help cloud customers manage the risks associated with the cloud, a few years ago SINTEF created a checklist for cloud security, which contains a number of security requirements. These requirements were derived from a number of different publicly available sources, whereof many have been updated during the last few years. In this task the student will review existing best-practices, guidelines and standards of cloud security and update the security requirements checklist to reflect the recent changes. The student will then apply the checklist on a cloud-based health care solution as described above, and evaluate to what degree it manages to address its main security and privacy challenges.

Student:	Monika Katrin Kosmo
Assignment given:	January 27th, 2014
Supervisor:	Karin Bernsmed
Responsible professor:	Poul Einar Heegaard

Abstract

Cloud computing is a continuously emerging technology of which new areas of utilization is adopted. Among these, medical sensor networks are increasingly used for purposes like remote monitoring of the health condition of patients in their own homes. As healthcare data are characterized as sensitive personal data, there are many security and privacy issues that are essential to address. Currently, cloud consumers find it difficult to assess these issues.

In order to assist cloud consumers in managing the security risks associated with the cloud, this thesis created a security checklist that can be utilized for assessing the security and privacy risks of a cloud service. The resulting checklist consists of 35 security requirements formulated as questions that a consumer can ask a potential provider, to discover the security offered for a cloud service.

The security checklist was applied to a cloud-based healthcare service, to evaluate the extent of which it manages to encompass the main security and privacy issues of this service. The results of the evaluation revealed that the most important security and privacy issues are covered by the checklist. However, it is not detailed enough to guarantee that protection of data in the cloud service is sufficiently implemented. Hence, the security checklist is reliable as guidance for a cloud consumer to utilize for discovering the overall security protection offered for a cloud service.

Sammendrag

Dagens teknologi ser en økning i bruk av nettskytjenester, og stadig nye bruksområder utvikles. Blant disse er bruken av medisinske sensornettverk i økende grad brukt til formål som fjernovervåkning av helsetilstanden til pasienter i sine egne hjem. Helsedata er karakterisert som sensitive personopplysninger, noe som medfører mange sikkerhets- og personvernsspørsmål det er viktig å identifisere. Forbrukere av nettskytjenester synes det er vanskelig å identifisere disse problemene selv.

For å bistå forbrukerne av nettskytjenester med å håndtere sikkerhetsrisikoer forbundet med nettskyen, ønsker denne masteroppgaven å lage en sjekkliste som kan brukes for å vurdere sikkerhets- og personvernsrisikoer ved en skytjeneste. Sjekklisten resulterte i 35 sikkerhetskrav formulert som spørsmål, som forbrukeren kan stille til en potensiell leverandør, for å avdekke sikkerheten som tilbys for en skytjeneste.

Sjekklisten ble anvendt på en skybasert helsetjeneste, for å vurdere i hvilken grad den omfatter de viktigste sikkerhets- og personvernsrisikoene for denne aktuelle tjenesten. Resultatene av evalueringen viste at sjekklisten inneholder de viktigste sikkerhets- og personvernsrisikoene for helsetjenesten, men at den ikke er detaljert nok til å kunne garantere at tilstrekkelig sikkerhet er implementert. En forbruker kan bruke sjekklisten som en god veiledning for å avdekke den overordnede sikkerheten en leverandør tilbyr for sin skytjeneste.

Preface

This master's thesis is submitted to the Norwegian University of Science and Technology (NTNU), as a completion of the five year Master of Science in Communication Technology program at the Department of Telematics.

I would like to thank my supervisor Karin Bernsmed and my professor Poul Einar Heegaard for valuable advise and insightful feedback throughout the project. Their contributions have been invaluable to the completion of this thesis.

Monika Katrin Kosmo
Trondheim, Norway
June 23rd, 2014

Acronyms

CESG National Technical Authority for Information Assurance

CSCC Cloud Standards Customer Council

EEA European Economic Area

EHRs Electronic Health Records

ENISA European Network and Information Security Agency

ETSI European Telecommunications Standards Institute

EU European Union

FedRAMP Federal Risk and Authorization Management Program

IaaS Infrastructure as a Service

IDS Intrusion Detection Systems

ISO International Organization for Standardization

IT Information Technology

NIST National Institute of Standards and Technology

NTNU Norwegian University of Science Technology

PaaS Platform as a Service

PII Personal Identifiable Information

RAM Random Access Memory

SaaS Software as a Service

SAML Security Assertion Markup Language

SLA Service Level Agreement

SSO Single Sign-On

TOS Terms of Service

Contents

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Motivation

The cloud computing technology is still in its early days, though rapidly emerging and expected to have a prominent impact on business in coming years. The cloud induces benefits like 20 percent reduction in costs, unlimited computing capacity for processing the excessive amounts of data produced, and hundreds of thousands of new services to be developed [1]. Together with these new services, also new areas of utilization arise. Among them, medical sensor networks are increasingly used, e.g. for remote monitoring of the health condition of patients in their own homes. Such sensors generate large amounts of data, which enables the cloud to be a suitable solution. Data processed within the healthcare domain are characterized as sensitive personal data, of which there are many security and privacy challenges to address.

A major concern about the cloud computing technology is the security and privacy protection provided for the cloud services. Currently, there are no standards for describing security and privacy requirements in the Service Level Agreement (SLA) defined by the cloud service providers. Consequently, it is problematic for the cloud consumer to discover the security and privacy procedures offered for a service. A security requirements checklist would help the consumers manage the risks associated with the cloud, and raise consciousness about security elements to beware of regarding cloud services. Similar checklists already exist, though many of them are either out of date, overly detailed or vague, and generally hard to use.

1.2 Objectives

The aim of this thesis is to create a new security requirements checklist that a cloud consumer can utilize when evaluating the security and privacy risks associated with public cloud solutions.

The research questions of this thesis are:

RQ 1: What should a security checklist contain in order to address the security and privacy guarantees offered for a public cloud service?

RQ 2: To what extent will such a security checklist encompass the main security and privacy challenges in the cloud-based healthcare solution?

1.3 Methodology

This section describes the research method used to carry out this thesis. The chosen method is based on 'The Research Process' by Bhattacherjee [2]. The model is modified to be suitable for the research process of this particular study. First, the original process will be presented, followed by a description of the model adapted for this thesis.

1.3.1 Original Research Process

The original research process consists of three phases, as illustrated in Figure 1.1. Each phase will be described separately.

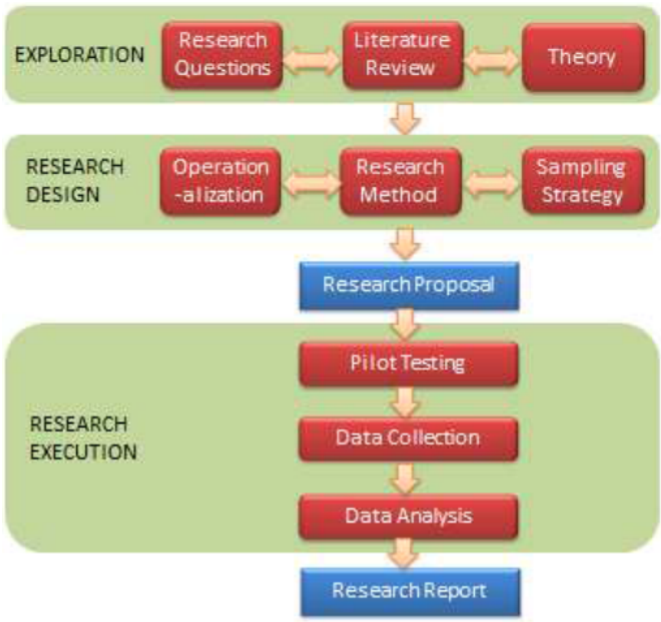

Figure 1.1: The original research process is a research method defined by Bhattacherjee, and consists of three phases [2].

The **exploration** phase is the first of the three phases defined for 'The Research Process'. The first step is to identify and define specific *research questions* that the study will seek answers to. Step number two is to perform a *literature review* of the relevant subject area for education and knowledge about the matter of interest. An essential factor of the review is to recognize key findings and existing solutions in the present domain, to be able to identify undiscovered fragments in the current knowledge of the research area. The third and last step of this phase is the *theory* step, which consists of identifying theories or hypotheses that could assist the solving of the defined research questions.

The **research design** is the second phase of the process where the first step is called the *operationalization* step. The purpose of the operationalization process is to identify the relevant factors for solving the problem of interest. Another important aspect with this step is to identify previous measurements related to the current problem, and determine whether these previous results can be utilized or modified to solve this particular problem. Step two is to choose the appropriate *research method* for the project. This involves finding the suitable method for collecting data to address the problem, in particular the research questions defined. The third and last step of this phase is to decide a *sampling strategy* for selecting the desired population of which the collection of data for the research will be conducted. In the transition between the second and the third phase, a step called *research proposal* is recommended, which consists of writing a proposal with the details from the planning of the research process so far. The purpose is to achieve a proper feedback before continuing to the execution of these designs.

The third and last phase is the **research execution** phase. Initially it consists of three steps; *pilot testing*, *data collection* and *data analysis*. Pilot testing is the concept of e.g. making a prototype before implementing a solution or testing a theory on a small subset of the total quantity for the research. The next step is the data collection, which consists of acquiring information for the study, followed by the data analysis, which is the last step of this phase. The data analysis method applied should be chosen depending on the type of data acquired. The final stage of 'The Research Process' is the documentation of the process with the research findings in the form of a *research report*.

1.3.2 Modified Research Process

As recommended by Bhattacherjee [2], modifications were applied to the original research process, to adjust it to the specific research method conducted in this thesis. For this process, the original third phase is divided into two separate phases, but otherwise defined equally. The steps for each phase are somewhat changed; some are swapped between two phases, some are added to the process, while others are

removed. All changes made to this modified process are illustrated in Figure 1.2, and will be further described in this section.

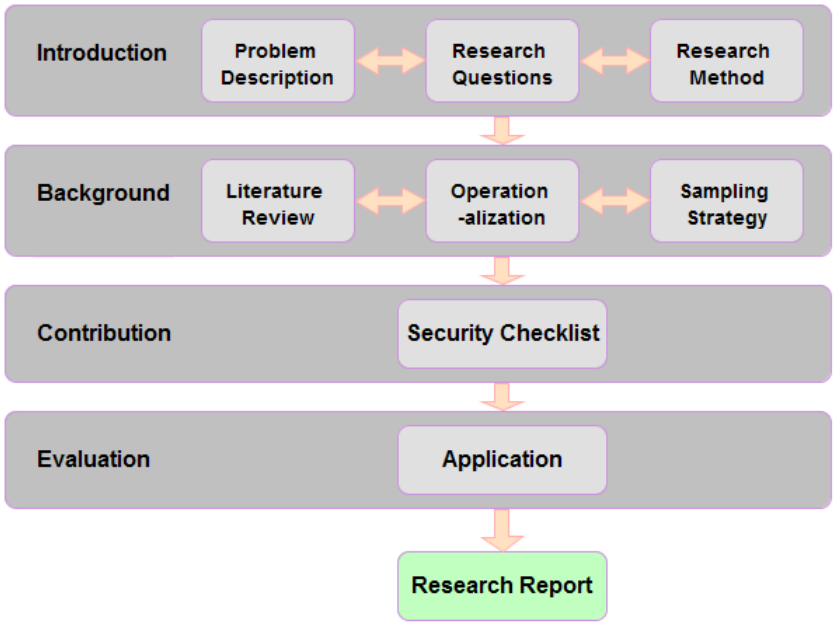

Figure 1.2: The modified research process describes the research process of this thesis, modified by [2].

Introduction Phase

The first phase of this research process is the introduction phase, which consists of an introduction to what the research will accomplish, and how. This phase is equal to the exploration phase of the original process. The following steps were identified for the introduction phase; *problem description*, *research questions* and *research method*. The problem description step is added to this modified process. This step initiated the research by formulating a problem description to restrict the area of research and to define the superior aim for the study. The scope of this research concerns security and privacy risks with cloud solutions, in particular for cloud services in the healthcare domain. The superior aim is to create a security requirements checklist that a cloud consumer can utilize when evaluating security and privacy risks of a cloud service. Next, the research questions were defined to specify what the research will attempt to answer, and to confine the scope of the study. Two research questions were identified for this case, as defined in Chapter 1.2. The first question specifies that the checklist will be applied to public cloud services, and that this thesis will

attempt to determine what a security checklist must contain to discover the security and privacy guarantees given for a service. The second question will determine whether such a security checklist manages to address the main security and privacy issues of a particular cloud service in the healthcare domain.

The third step of this phase is to choose a research method for conducting this study. In the original process, this step was included in the second phase, but for this particular research the method was chosen at an earlier stage. To conduct this thesis and attempt to address the research questions defined, a background study is fundamental to acquire knowledge about the problem defined in the problem description. For this thesis, general knowledge about the cloud computing environment is essential, together with information about public cloud services and the related security and privacy issues. Further, a data collection of related work must be conducted to review existing solutions and findings. To create a new security checklist it is important to investigate existing checklists and other closely related results, to ensure that the solution does not exist already and to arrange for the best result possible. When both background information and data necessary for creating the security checklist are collected, the next step is the construction of the actual checklist. The security checklist is the main result of this thesis. An analysis of the result will be performed, as the third part of this research method. This is to evaluate the applicability of the security checklist created.

To summarize, the research method for this thesis is threefold:

1. A background study is conducted concerning cloud computing, public cloud services and related security and privacy issues (Background phase)
2. Data collection of similar work and construction of the security checklist (Contribution phase)
3. A validation of the created checklist is performed by applying the checklist to a cloud service (Evaluation phase)

Background Phase

Background is the second phase of this research process. This phase is equal to the research design phase of the original process. This phase should be regarded as part one of the research method explained in the previous paragraph, and will describe the background study conducted in this thesis. The steps identified for this phase are; *literature review*, *operationalization* and *sampling stategy*. The literature review is performed to obtain an understanding of the cloud environment in general, and to acquire knowledge of the current state of security and privacy issues in the public cloud. The search for relevant literature contained keywords like 'public cloud', 'security standards', 'security checklist' and 'privacy'. Before creating a new

security checklist, it is essential to investigate similar findings of related studies, like reviewing existing checklists, best-practices, guidelines and security standards. This is important to ensure that a security checklist like the one attempted to create in this thesis does not already exist. An investigation like this is also important to assess the feasibility of creating such a checklist. The investigation detected a great variety in the findings of previous studies, of which will be further addressed in Chapter 2.4.

Both of the next steps are important specifications regarding the related work of this thesis. The operationalization step consists of specifying the relevant factors for solving the research questions. The essential factor of this research is the level of detail of the new security checklist. The existing checklists are either too detailed, or too vague for a cloud consumer to utilize on any cloud service. The aim for this thesis is to create a security checklist that a cloud consumer can apply to a public cloud service, and be confident that all the security issues relevant to the service are addressed and covered by the checklist. Hence, the level of detail of the checklist is crucial. Reasoning about this decision will be further described in Chapter 2.4. The sampling strategy for this process concerns the selection of relevant best-practices, security standards and existing checklists that the construction of the new security checklist will be based on. The selection must be representative, which in this case denotes differences in the level of detail in the descriptions of security and privacy issues, publication dates as the cloud is a dynamic environment with rapid changes, and several different authors and publishers, e.g. reviewing security standards defined by various organizations. The sample of literature chosen for this study are highly dependent on the operationalization factor presented above, the level of detail of previous studies. The sample will be presented in more detail in Chapter 2.4.

The intermediate stage of the original process in Figure 1.1 included a research proposal. This stage is not included in this particular research as feedback was provided continuously throughout the process.

Contribution Phase

The original research process had one more phase, the research execution phase. For this process, the third phase is divided into two separate phases. In addition, this process does not include the pilot testing step which originally is a part of the third phase. The third phase of this process is the contribution phase. This phase consists of part two of the research method defined in phase one, which is the data acquisition to construct the security checklist, and the actual creation of the checklist. The acquisition process starts by examining every paper selected in the sampling strategy of phase two, to extract the important aspects of the security and privacy issues described. These aspects are collected in a spreadsheet, to reflect the occurrence of

each element, to get an impression of which issues that are most important and most frequently mentioned. When this procedure is completed, the next step will be to convert these descriptions into defined security requirements. The requirements will be formulated as questions, intended for a consumer to ask the provider of a cloud service, or to apply to the service contract. The final stage to achieve the aim of this thesis, is to carefully select the requirements that fulfil the level of detail defined for the checklist. The results of this process is presented in Chapter 3.

Evaluation Phase

The final phase of this research process is the evaluation phase. The evaluation process will be conducted by applying the security checklist to a cloud-based healthcare solution, to evaluate the applicability of the checklist. To perform the analysis, some additional material must be examined, and supplementary definitions regarding the healthcare domain must be specified, as data in this domain represent sensitive personal data.

An essential precondition for this analysis and for the healthcare solution is that compliance to Norwegian regulations are presumed. The Norwegian law for privacy protection[1] [3] is based on guidelines from the European Data Protection Directive[2] ('the Directive') [5], which is valid for the members of the European Economic Area (EEA), and defines directions to protect processing of individuals' sensitive personal data. In addition to these, a standard that describes necessary security measures for processing data in the healthcare sector will be examined, "Norm for Informasjonssikkerhet" ('the Norm') [6]. It is a Norwegian standard that defines security requirements for information systems in the healthcare sector, and ensures legally sufficient implementation of security measures by following these recommendations. Also, a paper that addresses the risks with processing Electronic Health Records (EHRs) in the cloud, "Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems" [7] is studied. The paper directly suggest protection measures related to the confidentiality of the health records, together with some general issues related to security in the cloud. Based on these guidelines, laws and articles, the special requirements for processing sensitive personal data will be reviewed and linked to the M Platform. The findings from the analysis is presented in Chapter 4.

Lastly, this document will be the resulting report for this research process.

[1] Personopplysningsloven.

[2] Directive 95/46/EC, a European Union directive that governs management of personal data within the European Union (EU). As of March 2014, a new law, the 'General Data Protection Regulation' has been established which eventually will replace the Directive. It will take years to introduce this law, but when it becomes effective there will be important changes. An example is greater demands towards the processors (providers) of personal data [4].

1.4 Limitations

This thesis has focused on the security issues of cloud services. Challenges with other functional requirements like availability, performance and cost has not been considered in this research. Another limitation concerns the validation process. As the checklist was applied to one cloud service only, generalization was not attainable.

1.5 Outline

Chapter 2 presents a background study on cloud computing in general, an introduction to the public cloud and the related security and privacy concerns. Also, an overview of similar studies relevant for this thesis is provided.

Chapter 3 describes the creation of the new security checklist and presents the resulting requirements defined.

Chapter 4 introduces the cloud-based healthcare service. An analysis of the security and privacy requirements for the service is conducted, together with an evaluation of the new security checklist.

Chapter 5 discusses the results presented in Chapter 3 and 4.

Chapter 6 concludes the findings of this thesis, together with proposals for future work.

Appendix A contains the complete security checklist created in this thesis, as presented in Chapter 3.

Appendix B holds a predefined contract that the Norwegian Data Protection Authority require. This appendix is in Norwegian.

Appendix C consists of the resulting list of requirements derived from the application of the security checklist conducted in Chapter 4.

Chapter 2
Background

This chapter presents relevant background information with regard to cloud computing, the public cloud and the related security and privacy issues. An overview of related studies like best-practices, existing checklists and security guidelines are also presented.

2.1 Cloud Computing

Data production increases with 40 percent every year, which demonstrates the maturity of the era of Big Data[1] [8]. Cloud computing is a continuously emerging technology that offers huge benefits for the incredible amounts of data produced, both for private consumers and large organizations [1]. Many definitions of cloud computing exist, of which one of them is formulated by US analysts Gartner:

> "A style of computing where scalable and elastic IT capabilities are provided as a service to multiple customers using Internet technologies" [9].

This means that the capacity of the resources needed of a cloud service is easy to scale according to demand. With the understanding of cloud computing, the same service is delivered to multiple consumers, using the same amount of resources as the traditional single-consumer application [10]. The users of cloud services no longer need the infrastructure or resources in their own network, they use the services offered by the cloud provider.

The National Institute of Standards and Technology (NIST) cloud computing reference model shows the different participants and roles that interact in the cloud ecosystem, as illustrated in Figure 2.1 [11]. A cloud consumer is a person or an

[1] Big Data is the collective term for describing enormous and complex data sets that exceeds the normal processing capabilities of traditional database systems.

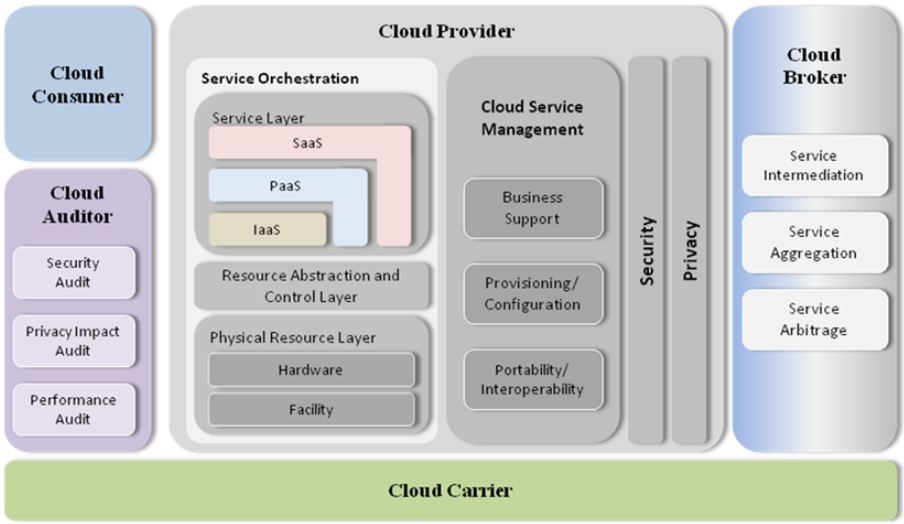

Figure 2.1: The (NIST) Conceptual Reference Model is an overview of the cloud architecture that identifies the major actors and their roles in the cloud ecosystem [11].

organization, and is the user of the service provided in the cloud. A cloud provider is an entity that offers a service to the consumer and makes the arrangements for the service deployment. The provider is responsible for supplying the physical resources needed to run the service, and also to manage the infrastructure required. The exact role of a cloud provider depends on the service model it offers. There are three different models in the cloud computational stack. The first one is Infrastructure as a Service (IaaS) [12]. Here the provider offers virtualized hardware and infrastructure, like storage, servers and network. For Platform as a Service (PaaS), the provider offers a computing platform that consists of development software that let consumers execute their applications. The Software as a Service (SaaS) is a software application that a consumer can access, which runs in the provider's infrastructure, like an email application or a file sharing tool. Cloud providers also often combine services, for example, a SaaS is executed on the PaaS, which run on an IaaS. Figure 2.2 illustrates the three service models in a layered notation, with the respective amount of responsibility regarding security controls for the consumer and the provider [11]. In a SaaS environment, the cloud provider has the responsibility for implementing the security controls, but the consumer must ensure that all these issues are addressed in the cloud service contract. The provider is responsible for securing the infrastructure, operating system and middleware in a PaaS, while the consumer must ensure to secure both application deployment and access to the application [13]. For a IaaS, the provider is responsible for securing the operating system layer, while the consumer is

accountable for the rest of the software stack [14].

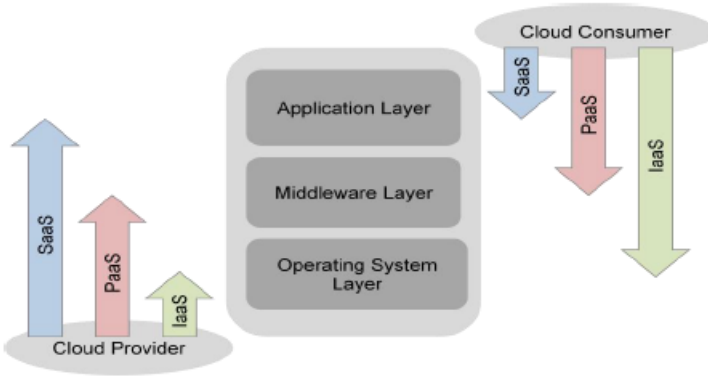

Figure 2.2: The accountability of security controls distributed between the consumer and the provider vary depending on the cloud service model [11].

A significant paradigm shift has been introduced with the cloud computing technology, both concerning distribution and utilization of applications and services [15]. The cloud entails obvious benefits like major cost savings for both consumers and providers regarding infrastructure, installations and IT maintenance [1]. Other advantages offered by the cloud are mobile access to content and responsive services that are easy to scale on demand - which provides a more efficient use of computing resources [16].

Contrarily, there are some considerable issues with cloud solutions that impair the consumers' trust in these services. A transfer to the cloud denote an important alteration for the consumers; from being in direct control of their own IT environments they must now administer their assets through the cloud provider [17]. With this change it is necessary to build competence regarding the new management style, together with addressing the new challenges that arise like data location, availability and performance of the service. One of the absolute main concerns around the cloud service adoption regard the privacy and security of the services [18].

Several models are defined for deployment of the cloud infrastructure, each representing the exclusivity of computing resources made available for the cloud consumer [19]. Figure 2.3 provides an overview of these models [20]. In a public cloud environment, the service is delivered to a consumer by an external cloud provider. The service is made available to the general public and is potentially deployed to multiple consumers over the Internet. A private cloud is a model of which the computing environment is available and custom-made for a single consumer only. The management and hosting of the resources can be done by the consumer or by a

third party. Community cloud serves as a private cloud, but for a group of consumers with common concerns [21]. A hybrid cloud is a combination of public, private and/or community cloud services, either on-site or outsourced. The public cloud model will be explained in more detail in the next section, as it is the main target for the security checklist that will be presented in this thesis.

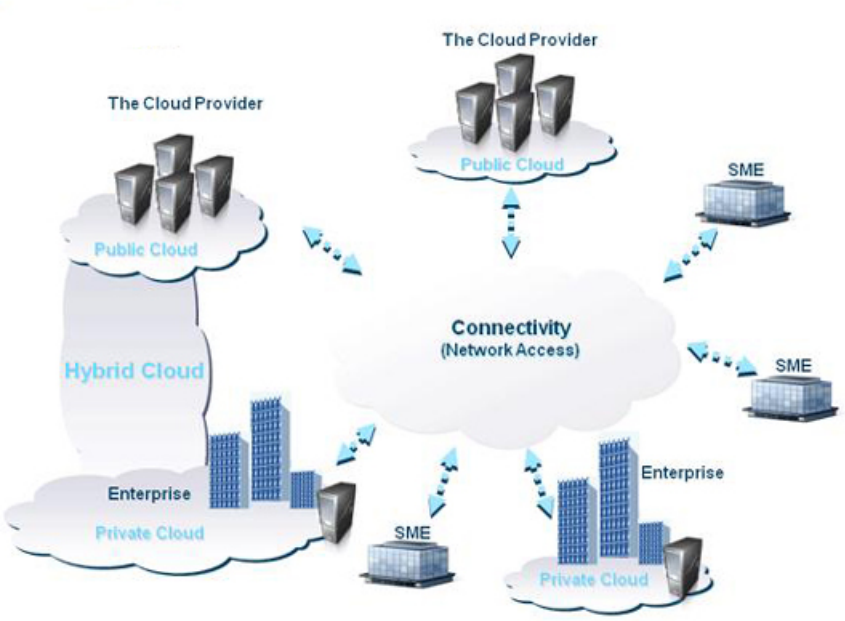

Figure 2.3: The cloud deployment models defined for the cloud infrastructure, illustrating the differences between public, private and hybrid cloud models [20].

2.2 Public Cloud

A definition of the public cloud deployment model is given by Gartner:

> "A style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies - i.e. public cloud computing uses cloud computing technologies to support customers that are external to the provider's organization" [22].

The public cloud is the model closest to the definition of cloud computing and refers to services available to the general public over the Internet. The services are easy to access, it is easy to increase the capacity when desired, and the consumer only pays for the resources used [23].

The public cloud services can be divided into three main classes. The first class represents the services that are at no cost for the consumer, and supported by advertisement instead. Examples of such services are Google mail, Facebook and Spotify. This class often represents the basic version of a service, and the Terms of Service (TOS) are non-negotiable. The second class includes the services that are fee-based, and normally these services do not contain any advertisements. The types of services are often equal to those of the first class, but the consumer normally have the opportunity to upgrade the service to an advertisement free version by paying a fee. An example is Spotify, who let the consumer upgrade to a version free of advertisements by paying a monthly fee. Another example is Dropbox who offers a basic version for free with access to a minimum amount of storage space, and another version with more space for a monthly fee. The TOS are non-negotiable for these services also. The services of the third class are also fee-based and free of advertisements, but their TOS are negotiable between the consumer and the provider[2] [24]. An example of such a service is Microsoft Office 365. Another difference between these classes in addition to the subscription fee is the degree of protection mechanisms offered by the provider, increasing from first to third class [19].

This thesis has a focus on the public cloud model more than the other deployment models, because of the security and privacy issues related to this deployment model. For the private, hybrid and community models these issues are not that extensive since these issues can, to some extent, be prevented by the consumers in their own private networks or in collaboration with the providers. For the other models the consumers can also have a relation to the service provider, and contracts can be negotiated.

2.3 Security and Privacy in Public Clouds

A transition to a public cloud environment brings along new challenges regarding security and privacy. These challenges prevent many organizations from adopting the public cloud model, but there are also important security benefits due to the cloud characteristics [25]. The large scale of service let the cloud providers specialize staff regarding security and privacy, which in turn will lead to improvements due to much more experience and expertise. It allows for greater availability, fast restoration of data, off-site backup storage, redundancy and disaster recoveries. Also the economic benefit of the scalability as the security measurements are cheaper in a larger scale [25]. The cloud computing platforms are much more homogeneous, which makes updates more efficient, plus the management controls for privacy and automation of security is much easier and faster with this uniform model. On the other hand, with

[2]Business consumers might manage to negotiate service agreements with the cloud provider. It might depend on factors like the service offered, the influence the consumer has on the provider, and if it involves any advantages for the provider.

the uniform model a single flaw could impact every tenant and all services in the environment [19]. In the cloud architecture, the cloud provider processes most of the data in their infrastructure locally, which leads to the mobility of the cloud solution; the consumers can access their data from both their laptops and their embedded devices, securely - given the right set up and protection. Security is a top priority for the consumers in a decision of moving to the cloud, which makes a strong motivation for cloud providers to improve their security practices and obtain a good reputation in the cloud market.

Along with the potential upsides a consumer could achieve by adopting to the cloud, there are severe risks to be cautious about as well [19]. The cloud computing environment is very complex with many components, which leads to an increased vulnerability to attacks. The fact that multiple tenants share the provider's resources and infrastructure form another challenge; controlling the resources logically instead of physically. In the public cloud, the consumer's data is delivered over the Internet, which leads to new threats from the network. Remote access, performance and quality of service might also be affected over the Internet. When transitioning to the cloud, the consumer cedes control of its assets to the provider. The management and control that was under the consumer's direct control before is now the provider's responsibility [19]. Neither the physical location of data is under the consumer's direct control in the cloud. Cloud providers often have multiple locations for storage of consumer data, both domestic and abroad, which leads to concerns about the valid legislations of the current state or country. Examples of such concerns are confidentiality of consumer data[3] [26], or the legal actions a cloud provider is obligated to comply to - like delivering supporting evidence in case of security incidents regarding any of their consumers [15]. For public cloud services there might not exist a direct contact between the consumer and the provider, which leaves the consumer compelled to trust that the provider comply to both agreed terms and data protection laws and regulations. There are few procedures and standards for defining security measures that would give guarantees to the consumer about e.g. data portability, migration and deletion of data [25]. In addition, there are no standards[4] that determine what cloud providers must describe in their service SLAs regarding the security measures implemented for their service. This is a challenge for the consumer, as information regarding security for a service might be difficult to find; security measures are often described differently for various services, or even non-existent [27].

[3]Like the PRISM program run by the U.S government where the amount of data collected by the NSA is of a much greater extent than previously known, as revealed by Edward Snowden in 2013.

[4]There are standards in progress. In December 2013, the EU launched their Research and Innovation programme, Horizon 2020, where one of the topics concern "support to the definition of common reference models for SLAs (service provider contract) in the cloud" [27]. Meanwhile, no defined standards are available.

As illustrated in Figure 2.2, the degree of responsibility for security controls differs between the consumer and the provider in the computing stack. The level of control depends on the service model and is also determined by which party is best suited for implementing proper security measures in their environment [11]. Nevertheless, the accountability for protecting data in the cloud environment ordinarily remains with the consumer [13]. It is recommended for the consumer to ensure that a lawful agreement is established with the provider that precisely specify roles, expectations, and assign the accountabilities of each party [14].

2.4 Related Work

Throughout the work with this thesis, several relevant documents and papers about security and privacy in cloud computing have been studied. Both guidelines, recommendations and other checklists have been examined to acquire knowledge about existing studies and previous results. The selected literature for this thesis will be presented in this section, but first an introduction to the security checklist made by SINTEF referred to in the problem description.

1. The *"Security Obligations for Cloud SLAs"* (2012) [28] is a security checklist developed by SINTEF. The checklist consists of 101 specified security requirements for a cloud consumer to use when examining the contract of a cloud service. The checklist includes details about technical controls which are feasible for a cloud provider to implement, and also possible for the consumer to monitor.

The creation of the new security checklist in this thesis will be based on the security checklist by SINTEF ('the old security checklist')[5]. 'The old security checklist' was created a few years ago, and it is assumed that several changes have occurred in the cloud environment since then, as it is a dynamic environment that evolves rapidly. This implies that 'the old security checklist' is out of date, and the purpose of this thesis is to contribute to reflect the changes. Before creating the new security checklist, a research project that applied 'the old security checklist' on existing cloud services will be described, as the results of that research is essential for the new security checklist.

The research project *"Security Requirements for the Cloud"* was conducted as a specialization project at the Norwegian University of Science Technology (NTNU) in December 2013 [29]. The research utilized the security checklist created by SINTEF

[5]Throughout the report, this checklist will be referred to as 'the old security checklist', for simplicity.

[28], paper number 1 presented above, to examine the security and privacy requirements described in documentation made publicly available by the service provider, like SLAs, TOS and Privacy Policies. The aim was to investigate how much the cloud providers describe in their publicly available documents about their implementations of security and privacy protection mechanisms. By utilizing the security checklist, and applying the information found, a list of relevant requirements for the cloud services investigated were made. The resulting lists of relevant requirements for the services examined consisted of very few requirements. The conclusion of this research was either that the security checklist was too detailed, or that the security information made publicly available by the service provider was too limited. As this is a research recently conducted, it can be assumed that the amount of information the providers supply is relatively unchanged. Hence, this thesis will assume that the security checklist was too detailed, and that this was the decisive factor for the results of the research project just reviewed.

The results of the research project demonstrated that 'the old security checklist' was not applicable to existing cloud services based on the publicly available information, the requirements in the checklist were too specifically defined. This indicates that a more general checklist would be a better solution, in order to assess the security and privacy protection mechanisms offered by the cloud provider. But before creating the new security checklist, it is crucial to investigate if such security checklists already exists. The literature examined to acquire knowledge about existing checklists and recommendations will now be presented.

First, a presentation of the documents reviewed that consists of descriptions and best-practices regarding security and privacy challenges. No specified recommendations or requirements are defined in these papers, rather thorough descriptions of threats and guidelines on approaches to properly manage these issues.

2. The *"NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing"* (2011) [19] is a report that provides an overview of security and privacy issues related to the public cloud environment, which the consumer should be aware of. The document presents the most important issues and threats to consider when transitioning to a public cloud, and outlines a set of general guidelines to considerations an organization should take into account when outsourcing its applications or infrastructure.

3. The paper *"Procure Secure - A guide to monitoring of security service levels in cloud contracts"* (2012) [18] was published by European Network and Information Security Agency (ENISA), and is a practical guide to security requirements meant for procurement teams to apply when considering to outsource their data to the public cloud. It provides recommendations on questions to ask the

provider related to the monitoring of security service levels of the service. The aim is to give guidance for monitoring continuously throughout the duration of the contract.

4. The document *"Cloud Computing - Benefits, risks and recommendations for information security"* (2012) [25] is another report published by ENISA, and is a cloud security risk assessment study. It presents a security guidance both for potential and existing users in the cloud ecosystem, that also provides specific practical recommendations.

5. The report *"Cloud Standards Coordination (CSC) Final Report"* (2013) [30] is launched by European Telecommunications Standards Institute (ETSI) and presents an overview of existing standards and specifications defined for cloud computing. It is a mapping of critical areas and addresses subjects like security, interoperability and SLAs. It includes definitions of roles in the cloud ecosystem, a collection of use cases related to cloud computing, relevant specifications and white papers and categorization of activities based on roles. It reflects the dynamic nature of cloud computing, and states that the findings of the report is only temporary and needs to be updated periodically.

In addition to the documents presented above, existing security checklists were examined. They all contain specific formulations of requirements and concrete recommendations for managing security issues in the cloud. Hence, these studies contain descriptions of a greater level of detail than the previous documents 2-5.

6. The *"Cloud Security Alliance Cloud Controls Matrix(CCM)"* (2013) [31] is a controls framework that specify essential security principles to guide cloud consumers with evaluating the security risk of a cloud provider. The documentation for the framework is also examined, the *"Security Guidance for Critical Areas of Focus in Cloud Computing V3.0"* [14]. The framework provides detailed descriptions and extensive recommendations within 13 security domains. It is based on several other standards and regulations such as ISO 27001, PCI and NIST.

7. *"Security for Cloud Computing - 10 steps to ensure success"* (2012) [13] is a paper released by Cloud Standards Customer Council (CSCC) that aims to guide IT and business leaders when they consider a transition to the cloud environment. The guide contain concrete steps and strategies for evaluating cloud provider security, covering threats, risks and safeguards.

8. The *Federal Risk and Authorization Management Program (FedRAMP) Security Controls Baseline* (2012) [32] is a document that provide a set of security

controls that are necessary to implement in order to satisfy the requirements of the FedRAMP. The security controls are based on the NIST SP 800-53 Revision 3 catalogue, and address cloud environment risks like control, responsibility and trust.

9. *"Cloud Security Principles"* (2014) [33] is a publication by the UK government's National Technical Authority for Information Assurance (CESG) that intend to provide guidance to public sector organisations concerning security features to consider when evaluating a cloud service. The guidance also include implementation recommendations for each of the security principles, together with risk management for cloud services.

The studies 1-4 described above are general descriptions of security and privacy issues for public cloud services, while the studies 5-9 present concrete recommendations for protection and management of security and privacy issues. The aim for the new security checklist is for it to be easily applicable for a cloud consumer when evaluating security risks associated with a public cloud service. The literature investigated for this thesis, as presented in this section, demonstrated that currently no such security checklist exist. None of the documents found in this investigation contains checklists with defined security requirements that can be directly applied to a public cloud service. This thesis desires to create such a security checklist.

Based on the literature investigated and the experiences from the research project, the decisive factor for the new security checklist was identified; the level of detail for the requirements to be defined in the checklist. The new security checklist aims to be a cross between the two groups, 2-5 and 6-9, regarding the level of detail. Specifically, it aims to contain specific requirements formulated as questions that a cloud consumer can ask a cloud provider, or find answers to in the cloud service contracts.

Recall from Chapter 2.3, a challenge with the cloud service contracts is that there are no standards that define how the service providers must describe their security and privacy protection mechanisms in their service contracts. This cause a variety in the security information made available by the cloud providers, which makes it difficult for a cloud consumer to get an overview of the risks to be aware of. The purpose of the new security checklist is to help the cloud consumer to manage the security and privacy risks with public cloud services. For public cloud services the contracts are normally non-negotiable, hence the level of detail of the new security checklist must reflect the information found in the contracts. The research project presented above [29] tested 'the old security checklist' on service information made publicly available by the service provider. Hence, when referring to the experience from the research project, this challenge is also included in this experience.

Taking all these precautions into consideration, the ideal level of detail to achieve the aim of the new security checklist is somewhat challenging to calculate. This thesis will attempt to attain the appropriate level of detail based on the eight reports, 2-9 presented above, together with the experience from the research project presented.

In addition, to demonstrate the relevance of defining security and privacy requirements for cloud services, some guidelines that are in progress will be briefly mentioned below.

The International Organization for Standardization (ISO) is currently working on guidelines and checklists for cloud services. These are not examined for this thesis as they are still in progress, but they are included in this section because they are presumed to affect the work with security checklists and requirements in the future.

The *ISO/IEC 27017* standard will provide a code of practice related to information security of cloud services, together with recommendations regarding security controls [34].

The *ISO/IEC 27018* standard will provide guidance to ensure that cloud service providers offer suitable privacy protection of the consumers' sensitive personal information [35].

And the *ISO/IEC 27009* is a standard that will define how to apply the *ISO/IEC 27001* standard in special domains, e.g. the cloud domain [36]. The ISO/IEC 27001 is a standard that specifies a suite of activities for managing information security risks in general information systems [37].

Chapter 3
Security Checklist

This chapter will present the new security checklist created in this thesis. The security categories covered in the checklist will be described, and the meaning of each requirement will be explained. First, the creation process will be presented.

The data acquisition process started by examining the documents described in Chapter 2.4, numbered from 2 to 9. These documents were thoroughly reviewed, to extract the important aspects of the security and privacy issues described. These aspects were collected into a spreadsheet and divided into security categories, to get an impression of the issues that were most frequently described through the eight reports. These issues were also interpreted to currently be the most important issues of public cloud services. This approach was anticipated to work, as the documents examined was carefully selected to be representative as state of the art. The spreadsheet now consisted of a mix of specific requirements and superior descriptions of security and privacy issues. At this stage, the level of detail of each category was evaluated. This particular process was somewhat difficult to perform, as the level of detail was so roughly defined, recall from the discussion in Chapter 2.4. An attempt to attain the appropriate level of detail was performed to the best of the author's judgement based on the experiences from utilizing 'the old security checklist' in the research project [29], and based on the new findings from the data acquisition. When this procedure was completed, the next step was to convert these descriptions into defined security and privacy requirements. The requirements had to be formulated as questions that it would be easy for a consumer to apply to a cloud service. When these formulations were ready, a cross-check was performed against 'the old security checklist' to examine if the most essential security categories were included in the new security checklist. In addition, the resulting lists of requirements that were created in the research project [29] were directly utilized. To clarify, the requirements represented in these lists are known to be present in current cloud service contracts, which is why they were considered to be important to include in the new security checklist. These requirements are identical to the correlated requirements of 'the old security checklist'.

The resulting checklist constitutes 35 security requirements formulated as questions, and consists of 9 security categories. The idea is for the cloud consumer to ask the public cloud provider these questions, or to apply it to the service contract, to discover the security measures offered for a public cloud service. Also, it is meant to raise awareness among the consumers of what security aspects to pay attention to regarding public cloud services. The requirements defined can be applied to any of the three service models; IaaS, PaaS and SaaS.

The new security requirements checklist will now be presented by category. Each security requirement defined for a category will be described, and the coherent requirement will be presented in a table at the end of each section. The new security checklist can be found in its entirety in Appendix A, which unifies all the requirements defined in this chapter. The resulting checklist in Appendix A is categorized differently than presented in this chapter. This is done for convenience; e.g. the requirements for data encryption in Appendix A are categorized by data in transit, in storage and in process. While for the descriptions in this chapter, it was better to present data encryption as a category, where data in transit, storage and process are represented. Each requirement presented in this chapter will have an ID, which correlate to the ID in the resulting checklist in Appendix A. The requirements that are directly derived from 'the old security checklist' are indicated with a star (*) added to the ID number. The other requirements defined in this chapter are derived from the findings in the data acquisition. Accurate references can be found in Appendix A.

3.1 Protection of data

Protection of data at every layer in the service is important; during transfer, in storage and when processed. Protection of data means to keep the data secure and to prevent unauthorized access to the data [19]. For a public cloud the environment is shared with many consumers, so protection of data is necessary from both unauthorized third-parties, and other consumers that are utilizing the service. Two measures to ensure protection are encryption of data and data isolation.

Encryption of data is essential to prevent intruders from reading the consumers data and to ensure confidentiality. Data in transit involves data moving at any layer in the service; from the infrastructure to cloud providers, from end user devices to the cloud service, from one instance to another within the cloud service, and data sent between different cloud providers [14]. Encryption of data in storage ensures that data will never be stored in clear text. To prevent data from being processed in clear text, data accessed by virtual machines has to be encrypted [14].

A very important aspect of data encryption in the public cloud is the cryptographic key management. For the consumer data to be adequately protected, the encryption

keys have to be stored and managed by the consumer or by a trusted third party. The risk by allowing the cloud provider to handle the keys is that the employees at the provider are able to decrypt the data, hence they have full access to the consumer's data [15]. It is recommended to store the keys at a location separated from the data [13]. Also a strong encryption algorithm following a validated standard is required [14].

Data isolation helps to ensure integrity of data and prevents intruders from tampering with or intercepting consumer data. Isolation is necessary both to separate consumers of the service from affecting another consumer's use of the service, and for protection against unauthorized third-party access [33]. A multi-tenant platform like public cloud services must ensure complete isolation for data in storage, so that no tenant can access another consumer's data [18]. The network must be isolated at every layer so no tenants can intercept another tenants data during transfer across the network. Processing of data in Random Access Memory (RAM) must also be isolated to ensure no tenants can read or modify any of the data in the RAM allocated for another consumer, and also prohibit that virtual machines interfere with each other [14].

An approach to validate integrity of data is to digitally sign the data using different techniques, e.g. hashing algorithms [13]. It is important that the provider has implemented such algorithms to ensure that consumer data is accurate and unaltered [28].

The lifecycle of consumer data in a public cloud service consists of one more phase that also needs to be carried out securely, the data deletion process. It is not sufficient to delete data from the storage media and backup media, it is also often necessary to make the data unrecoverable [14]. Resources in a public cloud service are reused by other tenants, so if a storage device is not securely recycled other tenants might access data previously stored on the device. If the consumer data is not properly sanitised, the provider could potentially retain the data indefinitely. It is important to require from the provider that data is properly deleted, both upon request and when the service contract is terminated [33].

Based on these security aspects, ten security requirements are defined for the new security checklist:

Category	ID	Requirement
Encryption		
	1	All consumer data will be encrypted during transfer at any layer?
	7	Encryption is employed to protect all data at rest?
	8	Encryption keys are stored and maintained by the consumer or a trusted key management provider(3rd party)?
	15	Data accessed by virtual machines is encrypted by using policy-based key servers that store the keys separately from the virtual machine and the data?
Isolation		
	2	Does the provider offer a sufficient level of network isolation between the tenants so that no tenant can see or interfere with other consumers' data in transit?
	9	For structured data held in databases within the cloud provider's environment, is there proper separation of data belonging to different consumers in a multi-tenant environment?
	16*	All consumer data in RAM will be isolated from other tenants' data?
	17*	The service provider has implemented mechanisms to ensure that virtual machines do not interfere with each other?
Sanitation		
	10	The consumer is aware of the amount of time it will take before all consumer data (and any backups) are securely sanitised?
	11	The service provider ensures secure disposal and complete removal of all consumer data from all storage media, making sure that no data is recoverable by any computer forensic means?

Table 3.1: Security requirements for data protection

3.2 Compliance

Compliance refers to the laws and regulations the cloud provider abide by [19]. There are differences in policies and procedures across countries, and it must be clear what regulations the provider comply to [13]. This is important for several reasons. In some countries the law enforcement agencies can access encrypted data in case of an illegal act, which directly impact the protection of Personal Identifiable Information (PII) [13]. Some law enforcement agencies may request information during civil lawsuits, and some might even demand hardware to be seized as evidence [25]. To predict the

legal risks, it is important for the consumer to know what laws that are applicable for the service [33]. It is common for cloud providers to outsource some specialised tasks to third-parties, and in these cases it is important that also they demonstrate compliance to the security policies that the provider claims to support [25].

Another important aspect to the differences in compliance of laws is the physical location of the consumer data. It is common practice for cloud providers to store a backup of data in multiple geographical locations. This makes it challenging to know which laws that apply, it might be the laws where the data was collected, processed or stored [19]. It is important that the provider inform the consumers about the location of their data, and about any planned changes to these [33].

Related to compliance and physical location of data, six security requirements where defined:

Category	ID	Requirement
Governance		
	20	The service provider's security governance framework is formally documented, as are policies governing key aspects of information security relating to the service?
	21	Third-party service providers demonstrate compliance with information security and confidentiality, service definitions, and delivery level agreements included in third-party contracts?
Physical location		
	5	Consumer data will be stored in (a) specific geographic location(s)? (specify country)
	6*	All consumer data will be stored in a country under a particular jurisdiction? (specify jurisdiction)
	18	Consumer data will be processed in (a) specific geographic location(s)? (specify country)
	19*	All consumer data will be processed in a country under a particular jurisdiction? (specify jurisdiction)

Table 3.2: Security requirements for compliance

3.3 Data Storage

Some security requirements are already defined for data storage in the cloud, as described in the previous sections. Those already reviewed are encryption, isolation and physical location. In addition to these, there are several other aspects to take into account when evaluating the security of a cloud service regarding data storage.

It is often desirable to have a backup of valuable data, both when storing it locally and in the cloud. It is important to know what the cloud provider offer regarding backup, if it is provided at all, how frequently a backup copy is made, the physical location of the backup and what kind of information the copies contain [15].

Before entering a cloud service it is essential that the consumer is aware of the exit process, both if a change of provider is desired or to get a hold of the consumer data after the contract termination. The awareness of data deletion after termination is already described in Chapter 3.1. Additional aspects of interest are the amount of time until the consumer can receive data after termination and the format of the data received [19]. The provider should offer the consumer to receive the data in an industry-standard format, like .doc or .pdf. The best solution to ensure portability would be if the provider offered an import and export function to convert data into standard formats [14]. This way the provider supports portability and prevents vendor lock-in. It would also enable the possibility to migrate any existing data the consumer would want bring into the cloud, e.g. a database of user data [13].

Another significant issue to pay attention to when storing data in the cloud, is the ownership of the consumer data. It is important that the ownership rights are clearly defined so the consumer can maintain exclusive rights over all data, also after termination [15]. This data should include data generated between users and applications stored in the cloud by the consumer [28].

The five security requirements for data storage are defined below:

Category	ID	Requirement
Back-up		
	3	The service provider maintains backup copies of the consumer's data at a specific time interval?
	4*	All backup data is stored in another geographical location?
Portability		
	12*	Consumer data can be exported and imported according to a specified standard?
Migration		
	13	Can the consumer integrate its existing database of internal information and assets within the cloud environment?
Ownership		
	14*	All consumer data stored in the cloud remain the sole property of the consumer?

Table 3.3: Security requirements for data storage

3.4 Access control

When moving data to the cloud, the consumer depend on the provider's ability to protect private data. In the cloud, the consumer data is no longer shared with only trusted people inside of the consumer's environment. Data can also be accessed by employees from the provider, for reasons like maintenance or support [15]. It is difficult for the consumer to keep track of the number of people that have access to their data, which makes it important to establish the routines of the provider regarding access control and the management of identities [19]. Access control should ensure that only authorized and authenticated users have access to the service [33]. Also, it is recommended to keep the access level at a need to know basis, hence the most sensitive data is shared with as few people as possible. These restrictions should be applicable both for users from the consumer, and for employees at the provider that have access to the system. The provider staff should be subject to a proper background check in accordance to their role in the service and the classification level of the data they can access [14]. Implementation of multi-factor authentication protocols is essential to decrease the chance of false identities, and to authenticate users before providing them access to the service [19]. A frequently used authentication protocol is the Security Assertion Markup Language (SAML) standard. This protocol also support Single Sign-On (SSO), which provide access to multiple related applications the provider offers by signing in to one of them once [13].

If the provider offer several software systems, it is useful to know if the consumer can access all of them across applications.

Protection of the premises where the consumers' data are stored is also of importance [33]. Physical access control mechanisms to authenticate users at the data centres should be required to avoid unauthorized interception or damage of consumer data. Other possible security actions that can be put into effect to protect the data centres are guards, surveillance cameras and fences [13]. Equipment and data centres should not be located in physical areas with a high risk of natural disasters or environmental damage [14]. Temperature, water and power are examples of environmental conditions that should be monitored, and redundancy of both equipment and data should be ensured.

Related to access control there are five requirements defined, as listed below:

Category	ID	Requirement
Data centre security		
	22	Physical infrastructure and facilities are held in secure areas with constrained access control?
	23	Physical protection against damage from natural causes and disasters are anticipated, designed, and the provider have countermeasures applied?
Personnel security		
	24	All employment candidates, contractors, and third parties are subject to background verification proportional to the data classification to be accessed?
	25*	The service provider supports multifactor authentication to ensure secure access to the cloud management interface (dashboard)?
	26	Does the service provider offer single sign-on for access across multiple applications offered or trusted federated single sign-on across applications with other vendors?

Table 3.4: Security requirements for access control

3.5 Incident management

Auditing is an approach to monitor and evaluate the security controls of the service. Audit information usually consists of events, logs and reports from the system. Audit information is important for the consumer to be able to evaluate the security of the

system, and to prove that the security controls implemented in the system works deliberately [13]. The service provider should define a set of events to be monitored, and provide the resulting logs to the consumer [33]. Information of interest is typically access information like authentication and authorization, e.g if an access attempt to the system fails [13].

Monitoring the activity in the system is important to gather statistics and maintain an overview of the security in the system. If an incident should occur, it is even more important that the provider alert the consumer about it. An incident report should contain details like severity of the security breach, the expected time to recover, the amount of time from the incident occurred until the consumer was notified, what kind of incident that occurred and what equipment and data that was affected [18]. Incident reports should be made available to all affected consumers. The provider should also notify all consumers about security breaches or incidents in their systems within a reasonable amount of time, even though the consumer is not directly affected [13]. The provider should have actions to deal with possible security breaches inherited from the third parties and their supply chains, as well as actions for their own vulnerabilities [14]. Examples of incidents the provider should notify consumers about are intrusions to the system, alarms from firewalls or detected malware [32].

If an incident occurs, the service provider is required to handle the situation and recover from the security breach. The provider is responsible for the operational security of the service by having procedures in place to prevent, detect and recover from incidents [33]. To prevent security incidents from occurring, the provider must implement precautions to detect attacks before they hit. Firewalls shall be configured, Intrusion Detection Systems (IDS) should be implemented, and regular malware scans should be performed [28]. To be well prepared against security attacks and threats, the provider need to stay up to date on new and evolving threats [33]. Training of employees and users to be conscious about security and aware of how to properly behave might be an underestimated, but valuable precaution against attacks [19].

It is important to know what laws and regulations the provider comply to, also for incident management. Some laws contain a clause that require the provider to hand over supporting evidence if an incident is severe enough to cause legal action. It is of interest to know if the provider facilitate forensic procedures [28].

Six requirements regarding incident management were defined for the new security checklist:

Category	ID	Requirement
Auditing		
	27	The service provider has made the consumer aware of what audit information that will be available?
	28	The provider makes security incident information available to all affected consumers?
Operational security		
	29*	The service provider has implemented firewalls and malware protection?
	30	Does the provider's network have intrusion detection and prevention in place?
	31	New and evolving threats are regularly reviewed and the service is kept up to date with the latest security patches?
Forensics security		
	35*	In case of a security incident that requires a legal action, the provider will collect and deliver supporting evidence?

Table 3.5: Security requirements for incident management

3.6 Transparency

Transparency is mostly a matter of trust and is a vital initiative to strengthen the relationship between the provider and the consumer [19]. Through visibility the consumer can be involved in the processes of the provider and maintain a certain amount of control, which will increase the comfort level about the cloud service for the consumer [14]. The provider has to inform the consumer about outsourced services to third party suppliers, and the impact it has on the system. The provider is required to provide details about the information shared with these parties. The consumer should be provided with information about the supply chain of both the service provider and the third parties. This is important since the security level of a service is always as strong as the weakest link [25].

One requirement is defined to ensure transparency in the cloud service:

Category	ID	Requirement
Transparency		
	32	The service provider informs consumers how much of their information is shared with, or accessible by, third party suppliers and their supply chains?

Table 3.6: Security requirements for transparency

3.7 Privacy policies

Protection of PII is a crucial measure that consumers need to be guaranteed by their providers. Examples of information characterized as PII are phone number, home address, email address or date of birth. The provider is in possession of an excessive amount of consumer data, both application data and PII. There are numerous compliance regulations defined to ensure that PII data is protected and remain private. These regulations vary from country and state, hence to learn which regulations the provider comply to is critical [19]. It is recommended to clarify what kind of PII the provider will collect and how this information will be protected. Consumer data must not be exposed to third parties, neither application data nor PII [28].

Two requirements are defined for personal identifiable information:

Category	ID	Requirement
Privacy policies		
	33*	The provider will not disclose any of the consumer's application data to any third party?
	34*	The provider will not disclose any of the consumer's PII to any third party?

Table 3.7: Security requirements for privacy

Chapter 4
Application of the Security Checklist

In this chapter, the security checklist presented in Chapter 3 will be applied to a cloud service in the healthcare domain. An analysis of the security and privacy requirements for this service will be performed. The resulting requirements from the analysis will be employed to the new security checklist, to evaluate the extent of which it manages to address the main security and privacy challenges of this particular service. It is important to mention that the healthcare system to be presented is still a theoretical research where nothing is yet implemented. However, if this system is to be a reality, an important prerequisite could be to identify the security and privacy requirements for the system.

4.1 The M Platform

The healthcare system will be described in further detail in this section.

The M Platform is a cloud-based solution in the healthcare domain and is illustrated in Figure 4.1 [38]. The system makes use of wireless network sensors, which in the latest years have become an increasingly useful way of monitoring and collecting data. By using these sensors, a considerable amount of data will be generated, which leads to the use of a cloud solution, as the cloud offer high capacity to store and process data, and the ability to adapt to expanding amounts of data at a low cost. These sensors can either be attached to the patient, or placed in the environment. The purpose of the platform is to be able to observe elderly people from their own homes instead of keeping them on the hospital for observation. There are several reasons for why this would be desirable. In some cases it can be difficult to diagnose a patient, which could result in a tedious process. Other application areas could be monitoring chronic diseases, analyse the response of a preventive treatment, or measuring values like blood pressure or heart rate. With this solution the patient can stay at home in familiar environments, following normal routines and be monitored carefully at the same time, instead of being at the hospital. It is also

practical to provide this service to patients that live in distant areas. This solution is cheaper for the hospital and more comfortable for the patient.

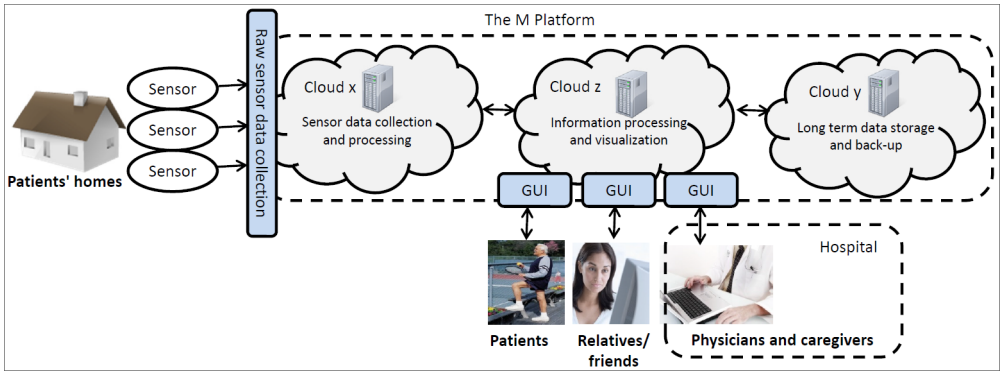

Figure 4.1: The conceptual model of the M Platform illustrates an overview of the actors and their functions for this healthcare cloud service [38].

From a technical point of view it is easy to recognize the advantages of a cloud-based solution like this, but there are numerous security and privacy concerns related to the processing of sensitive personal data in the cloud. Medical data is highly confidential that require strict protection, which will be reviewed in the next section. First, a description of roles and functionality of the system.

The M Platform consist of three separate cloud providers; one for collecting and processing the patient's medical data(Cloud x), one for visualizing the data to the users of the system(Cloud z), and one for long-term storage and back-up of the medical data(Cloud y), as illustrated in Figure 4.1. Medical data from the patient's sensor is registered and transmitted to Cloud x, where it is processed and stored temporarily. Cloud z offer the user interfaces, so it communicates with Cloud x to gather the patient information, process the data and visualize it to the users. The patient's medical data is now accessible by the patient itself, relatives or friends, and hospital staff like physicians, doctors and other caregivers. Cloud z also communicates with Cloud y to store and back-up data.

The identified roles in the system are as follows. The hospital is a cloud consumer in this cloud ecosystem. They have a contract directly with Cloud x, which is the hospital's cloud provider. Cloud z is also a consumer towards the cloud providers Cloud x and Cloud y, and have a separate contract with each of them. The hospital does not have any direct relation to neither Cloud x nor Cloud y. The hospital will provide and deliver the sensors to the patients, and make sure they are connected to the M Platform. The users of this system that have access to the data through

the interface provided by Cloud z are; the patients themselves, relatives or friends of the patient, and hospital staff like doctors, physicians and other caregivers. The patients have access to view the data collected about them, to see if data has been edited or accessed by others and who they are, and also the patient have every right to disengage from the service at any time, and require all data to be deleted. The relatives or friends of the patient have the exact same admission to the information as the patient itself, but in addition they have access to view their own personal data as well, which would mostly be login information and metadata used in access logs by the system. The third user of the system is the hospital staff, which will have complete access to the patient's medical condition. This means they have the same rights as the other users, and can monitor the patients vital signs in real-time. The system will log all accesses to the data, and all edits that are done to the patients data, which means metadata and personal information about every user in the system.

4.2 Security and Privacy Requirements for the M Platform

Protection and security of consumer data is the superior concern for a cloud consumer before subscribing to a cloud service, and is the foundation of the new security checklist presented in Chapter 3. It is important to establish the kind of consumer data to be processed in the cloud, as there are special regulations for some types of information. The M Platform presented in Section 4.1 is a cloud-based solution in the healthcare domain, which in addition to protection of consumer data need to properly handle information about the medical condition of patients. This type of information is classified as sensitive personal data, and is a special kind of PII of which there are additional regulations and laws for protection. The divergence between these two classifications will now be discussed.

Privacy protection refer to the rights each individual have to protect their private life, the ability to decide what personal data they want to share with others, and to be ensured of their information's integrity [39]. Personal data is defined as identifiable information related to an individual, such as national identity number, home address or phone number [40]. Such information are often collected by a cloud service to be able to identify and authenticate users. It is important that this kind of personal data is protected, as discussed in Chapter 3.7. Sensitive personal data is a designation for special sensitive information about an individual that require specific protection, such as ethnic background, political views, religion and medical condition [3]. The regulations for processing this kind of information are more strict, and defined by a set of laws and regulations, both national and international. The laws and regulations that apply for the M Platform will be reviewed shortly. An important precondition to clarify first, is that the M Platform must be assumed to be utilized by a Norwegian hospital, of which European laws and regulations for privacy protection apply. As

mentioned in Chapter 1.3.2, 'the Directive' is valid for members of the EEA and defines directions to protect processing of individuals' sensitive personal data. Hence, 'the Directive' apply for the M Platform.

In addition to 'the Directive', two documents that address security requirements in the healthcare sector are reviewed. Recall from Chapter 1.3.2, 'the Norm' [6] is a Norwegian standard that defines security requirements for information systems in the healthcare sector, to ensure privacy protection. Secondly, the paper "Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems" [7] addresses the risks with processing EHRs in the cloud. The paper directly suggest protection measures related to the confidentiality of the health records, together with some general issues related to the security of cloud services. The requirements for processing personal data in the healthcare sector based on these documents will be further discussed in this section.

'The Directive' [5] originally prohibit processing of information categorized as sensitive information, but exceptions exist. It is allowed, e.g. if the individual it regards specifically consent or if access to the information is determined by law [41]. For the M Platform to be allowed to process the medical information about a patient, the patient must give an explicit approval. Further, it is required that the patient is informed about the type of data that is to be collected about itself and how the information will be processed. It is important that sensitive personal data is collected only if truly necessary, and for a legitimate purpose. For the M Platform case, the information would be collected as a part of the process of diagnosing a patient, or other similar purposes. The information collected must be kept to a minimum, so unnecessary information shall not be obtained, and all information must be accurate and up to date, as decisions about the patient's health are made based on this data. If the information is no longer needed for any specific purpose, it must be archived. The M Platform is not supposed to hold the complete medical journal throughout the patient's life, so for this case the information shall not be archived, it must be erased [7]. Also, the patient is entitled to acquire full access to all information obtained in the system about itself, and rights to edit or delete this information. The patient must also be provided with an overview of every other person that can access its own information, and if anyone else edited, deleted or viewed the patient's information. In the case of the M Platform, the hospital is responsible for providing the patient with the appropriate access to have complete visibility of its own information in the system, and to have the opportunity to perform any of the actions mentioned above [38]. Permitting the relatives and friends to have complete access to the medical condition of the patient is a concern that might interfere with the patient's privacy policy, and must be mindfully considered.

Information security is another preventative requirement for processing personal

data in the healthcare sector. 'The Norm' [6] states that medical data is under obligation of professional secrecy, so when processing healthcare information it is critical to retain the confidentiality. This can be done by ensuring no access to the system or information by unauthorized people or other intruders outside the organizations. As for this case, no other than the authorised hospital staff, the patient and the relatives/friends of the patient should have access to the information. It is also important that the hospital restrict their policies of handing out access to patients' medical journals. The hospital staff should only have access to a specific patient's medical information if absolutely necessary for the patient's treatment. Also, the staff are required to keep their authorisation and not under any circumstance try to acquire information irrelevant to be able to carry out their tasks. Access accounts must be reviewed periodically, and withdrawn when it is no longer needed [7]. It is required to keep access logs with details of users that have accessed the system, users that have attempted to access the system and failed, if the users where authorised to access the specific information and how many times the authorised access have been used. A challenge in the healthcare sector is that one person at the hospital can have different roles depending on the case, which makes it important to associate the role with the appropriate authorisation and level of access to the system. In the healthcare sector there could be critical situations where it is necessary to access the system e.g. to save a patient's life, which means that emergency access to the system and a patient's medical journal must be possible, with the confidentiality and compliance to regulations is maintained. This type of emergency access must also be logged and traceable.

The hospital must ensure that vital information about the patients' medical conditions must be available at all time, even if system failure should occur. Back-up of patient data is absolutely vital, and must be securely stored in a different location that ensure an easy recovery and the accuracy of the patient information.

Proper security of the physical location and equipment is another requirement according to 'the Norm'. Security measures to assure that only authorised personnel will have access to equipment and proper procedures for managing keys and admission cards. Procedures to protect mobile devices and equipment that employees can bring home is also very important. It is relevant to configure equipment so that only activities related to the professional tasks will be performed. Any storage media like discs and flash drives that are no longer in use must be deleted and the content must be destroyed.

Communication through the system must be sufficiently protected to manage sensitive personal data. 'The Norm' define the roles of the actors in a system where sensitive personal data is transmitted. All communication through the system must be encrypted end-to-end. Sensor data sent through the network and the system

must be digitally signed to verify that the content has not been altered, and also to ensure that the originator can not deny having sent the data. It is important to register the arrival of sensor data, so the receiver can not deny the arrival of the data. Ensuring that no intermediary party can interfere with the information transmitted is essential, neither intruders, other tenants nor the cloud provider [7]. For the M Platform, personal data will be processed and stored at three different providers, Cloud x, y and z respectively. At Cloud y the personal data will not be processed, but stored for a longer period of time. This means that Cloud y does not need access to the personal data, so data must be encrypted before it is transmitted from Cloud x to Cloud y, and Cloud x must manage the encryption keys. To be confident that the intermediary party, which is the Cloud x in this case, will not interfere with or use the sensitive personal data processed through their service, the hospital must add this as a requirement in the service contract between the provider and the consumer.

To be able to address the security risks with a service, it is significant to understand the roles defined by the system and acknowledge the responsibilities each party have. It is the cloud consumer's responsibility to ensure that all of the cloud providers in the supply chain comply to the applicable laws and regulations. For the M Platform, it is the hospital that is accountable for ensuring that Cloud z comply to the legal regulations for processing sensitive personal data in the cloud, as well as ensuring that Cloud x and Cloud y comply. The hospital have a contract with Cloud z, but initially no direct connection to the two sub-providers Cloud x and y. Nevertheless, the hospital is responsible to ensure that the implementation of security measures is sufficient for all three services. It is recommended that the hospital seek to establish a contractual agreement with the sub-providers as well, before trusting the sub-providers with the sensitive personal data. An important term to include is to require that the providers will not, under any circumstance use patient data for their own purposes, or disclose any of the information to any unauthorised person. Also, as mentioned in the previous paragraph, it is recommended to require that no provider can interfere with the consumer data. Termination of the service must also be defined in the contract, assigning the owner of the information and the format of the retrievable patient records. By using the contract, the hospital can assign some of the accountabilities and restrictions to the providers.

The Norwegian Data Protection Authority[1] [42] require the parties, here Cloud z and the hospital to sign a predefined contract[2] [43] before they can cooperate about processing healthcare information about any patient. The contract cover many of the issues discussed in this section, like purpose of the information collected, both parties' obligations, considerations regarding the use of a sub-provider, and security

[1] In Norway this is Datatilsynet.
[2] The contract is in Norwegian, 'Databehandleravtale etter helseregisterloven'.

measures implemented in the service. The contract is a draft and can be expanded if desirable. It can be found in its entirety in Appendix B.

Other general security measures briefly mentioned in these regulations related to the providers obligations in the healthcare domain are; the implementation of intrusion prevention and detection systems to avoid malicious activity, audit information, supply the consumer with notifications and reports about security breaches within a particular period of time, and informing the consumer about the physical location of the consumer data.

4.3 Applying the Security Checklist

In this section, the security checklist presented in Chapter 3 will be applied to the healthcare system just reviewed, the M Platform. The security checklist will be evaluated based on the applicability on the M Platform.

To perform the application of the security checklist, the author of this thesis will act as the Information Technology (IT) Director at the hospital, considering to cooperate with the M Platform to process their patients' medical records in the cloud. The security and privacy requirements recommended for the M Platform examined in the previous section will be registered in the security checklist, and the result will be a list consisting of the matching requirements. The resulting list of requirements can be found in Appendix C.

In addition to this list, there were some requirements identified for the M Platform that were not represented in the security checklist. These requirements had to be additionally defined. From the analysis of security and privacy requirements for the M Platform in the previous section, 11 requirements were extracted from the analysis, that were not defined in the security checklist applied. These requirements concern; the patients' consent to allow the hospital to process their clinical information, the management of the patients' information regarding the type of information collected and for what purpose, stricter requirements for access control, and requirements concerning configurations and protection of mobile devices. These requirements are additionally defined and presented in Table 4.1.

Through the application process, some requirements in the security checklist were found to be too superficially defined. Six requirements were identified from the analysis of the M Platform, that were more detailed than the corresponding requirements in the security checklist. These six requirements are considered important for the security and privacy protection of the M Platform, which made it essential to define these requirements in more detail. Table 4.2 contain these specified requirements.

In total, these two tables constitute 17 requirements it was necessary to supple-

mentary define for the M Platform. Each requirement in these two tables have an ID from A to Q. These IDs are meant to simplify the referring to the requirements in the discussion of these results. The discussion will be provided in Chapter 5.

Category	ID	Requirement	Reference
Patient's consent			
	A	According to legislation, patients must allow the hospital to process their clinical information, except in emergency situations	[38] [7]
Information management			
	B	The patient must be informed about the type of data that is to be collected and how the information will be processed	[38]
	C	Sensitive personal data must only be collected if truly necessary and for legitimate purpose	[38]
	D	Information must be accurate and up to date	[38]
Access			
	E	The patient is entitled to acquire full access to all information obtained in the system about himself/herself, and rights to edit or delete information	[38] [6]
	F	The patient must be provided with an overview of every other person that can access its own information, if anyone edited, deleted or viewed information	[38] [6]
	G	The hospital staff should only have access to a specific patient's medical information if absolutely necessary for the patient's treatment	[6]
	H	Staff are required to keep their authorisation and not under any circumstances try to acquire information irrelevant to be able to carry out their tasks	[6]
	I	Emergency access to the system and a patient's medical journal must be possible	[6]
Mobile devices			
	J	All equipment must be configured so that only activities related to the professional tasks can be performed	[6]
	K	There must be procedures in place to protect mobile devices and equipment that employees can bring home	[6]

Table 4.1: Security requirements additionally defined for the M Platform that were not present in the new security checklist.

Category	ID	Requirement	Reference
Access control			
	L	Role-Based Access Control should be deployed in order to allow authorized personnel access to specific data based on their role	[6]
	M	Every employee's access account must be reviewed by the hospital every 90 days to ensure only authorized employees have access to the system	[7]
	N	Every employee's account is automatically revoked when initial reason for authorized access is no longer valid or the treatment is completed	[7]
Auditing			
	O	An audit register should include all accesses to the information and all the changes that have taken place to the health records	[7]
Deletion			
	P	Medical records should be archived for a set period of time, according to legislation of the respective country. After this period of time, the medical data must be deleted	[7]
Integrity			
	Q	Ensure that no provider or third-party can interfere with the consumer data	[7]

Table 4.2: Security requirements defined in more detail to address the details that were important for the M Platform, but not present in the new security checklist.

Chapter 5
Discussion

This chapter will discuss the resulting security checklist presented in Chapter 3, and the findings of the evaluation process conducted in Chapter 4. The discussion will link the results to the research questions defined in Chapter 1.2.

As reviewed in Chapter 2.4, a great variation in the level of detail was observed when examining the guidelines, standards and existing checklists. Some of the documents were very specific, from details in formulations of requirements and implementation proposals, to overall descriptions of security and privacy issues in the cloud environment. For instance, the guidance provided by the UK government on security principles [33] was thorough and included both a guidance to the main security issues with public cloud services, together with explicit recommendations for implementation strategies to ensure that these issues are managed by the cloud providers. Similarly, the security checklist constructed by SINTEF [28] consists of detailed requirements for security and privacy issues that are possible to implement in a public cloud service. On the other hand, some of the documents reviewed describe aspects of security issues on an informative level rather than defining specific requirements, like the NIST guidelines [19] and the Cloud Standards Coordination report [13].

To be able to make a decision on which requirements to include in the new security checklist to address a suitable level of detail, a more tangible factor than the impression of the related studies was essential. Utilizing the results of the research project [29] recently performed, as presented in Chapter 2.4, were expected to be of significant value as they were based on practical experience. The research project made use of 'the old security checklist' created by SINTEF [28] by applying it to current cloud service contracts, to evaluate the extent of information cloud providers describe security requirements in their contracts. The research project evaluated the contracts of six cloud providers, and 'the old security checklist' consists of 101 security requirements. The number of security requirements found in these service contracts by applying the checklist varied from 3 to 32, and 5 of the providers described less

than 15 requirements in their contracts. For this thesis, these results were assumed to be reasoned by the fact that 'the old security checklist' is too detailed.

As discussed in Chapter 2.4, the decisive factor for developing the new security checklist was identified to be the level of detail for the content of the security checklist. This factor is further divided into two sub-factors based on the related work as discussed above:

1. The experiences gathered from the previous research project.
2. The level of detail of the most common security issues extracted from the eight documents in Chapter 2.4, numbered from 2 to 9.

Revisiting the first research question defined in Chapter 1.2, these two sub-factors decided what this security checklist should contain to address the security and privacy guarantees offered for public cloud services. The creation of the new security checklist was performed to the best of the author's judgement, attempting to attain the appropriate level of detail based on these two factors.

The resulting security checklist presented in this thesis consists of 35 requirements regarding security and privacy for public cloud services. The checklist was applied to the M Platform to evaluate the applicability of the list on an actual cloud service, and determine to what degree it encompasses the main security and privacy challenges. The analysis of the M Platform was performed to derive the required security and privacy requirements for the service. Out of the 35 requirements defined in the security checklist, 28 of them where represented by the requirements derived from the analysis, and constituted the resulting list of requirements that should be defined between the hospital and the M Platform. In addition, the analysis identified 11 requirements of great importance that were not present in the security checklist, of which it was essential to define additionally, as shown in Table 4.1. There were also 6 requirements that were insufficiently defined in the security checklist, that it was necessary to specify in further detail. These requirements are presented in Table 4.2.

Considering these numbers in isolation it appears as the checklist covers the main security and privacy issues, with 28 out of 35 requirements represented in the resulting list of requirements for the M Platform. This validates the checklist to be applicable and highly relevant regarding security categories to be addressed when considering a transfer to the M Platform. On the other hand, it was necessary to additionally define 17 requirements to acquire a complete coverage of the essential data protection issues for the healthcare service. The matter of interest for the evaluation of the checklist is if these requirements are specific for the healthcare domain only, or if they are vital to define for the general cloud service as well. All the requirements that were

specified in further detail, hence all the requirements in Table 4.2, are obligations it could be desirable to apply to any other cloud service. For example, the requirement with ID L is a specific demand from the consumer regarding the implementation protocol for managing access control. It is a requirement that could be adopted to cloud services in general. The requirements additionally defined from Table 4.1 address the special measures necessary to protect sensitive personal data, which are extraordinary actions for the healthcare domain. Exceptions are the requirements with ID J and K, which would be applicable for most cloud services as well. These are recommendations about configuration and management of equipment associated with the service, to ensure safe usage of the service with these devices. In total, there are eight requirements that it might be important to add to the security checklist, based on the analysis of the healthcare service. These are:

J: All equipment must be configured so that only activities related to the professional tasks can be performed

K: There must be procedures in place to protect mobile devices and equipment that employees can bring home

L: Role-Based Access Control should be deployed in order to allow authorized personnel access to specific data based on their role

M: Every employee's access account must be reviewed by the hospital every 90 days to ensure only authorized employees have access to the system

N: Every employee's account is automatically revoked when initial reason for authorized access is no longer valid or the treatment is completed

O: An audit register should include all accesses to the information and all the changes that have taken place to the health records

P: Medical records should be archived for a set period of time, according to legislation of the respective country. After this period of time, the medical data must be deleted

Q: Ensure that no provider or third-party can interfere with the consumer data

A public cloud service normally offer a non-negotiable contract to the service consumers, which means that there are most likely no room for special treatment regarding system requirements. The purpose of the security checklist created in this thesis was for a cloud consumer to use it as a template for questions to ask a service provider, or find answers to in the cloud service contract, to discover the security measures implemented for a public cloud service. When reviewing the results

of the evaluation, it appears as the new checklist was too superficial, as the eight requirements listed above might be relevant to add. Reviewing the security categories defined in the new checklist, 8 out of 9 categories were covered by the requirements derived for the M Platform. The one that was not represented defines forensic procedures. In addition, one category must be added to the security checklist if it is decided that the eight requirements listed above should be added to the security checklist. This regards the category describing the requirements with ID J and K concerning mobile devices. The good coverage of categories indicates that the overall scope of security and privacy aspects is included in the new security checklist. The uncertainty still remains in the level of detail of the checklist, as it was necessary to additionally define 17 requirements for the healthcare service. If these supplementary requirements were related to the healthcare domain exclusively, the checklist would have fulfilled the purpose of being a general list to be applied to any public cloud service. This is known to be incorrect as eight of them are identified to be important for the general cloud service. Hence, this suggests that the checklist is too imprecise, that the security aspects addressed in this list cover many of the concerns, but is incapable of ensuring that the appropriate level of protection is obtained by applying the checklist only.

The IT Director in an organization, in this case at the hospital, should be an expert on the type of data processed within the organization and the characteristics of this data. Consequently, it would be reasonable to assume that the IT Director is knowledgeable about the regulations and laws for privacy protection of sensitive personal data, like a patient's medical records. The IT Director should also be well-informed about the procedures related to the obligations of the hospital staff and their authorizations, and the policies of maintaining the confidentiality of a patient's data. This insight might help the IT Director to communicate some of the desirable requirements a potentially cloud service has to offer. Assuming this scenario is sensible, the checklist could function as a tool to indicate the overall security aspects, of which it is important to acquire information about when evaluating a potential cloud service. It would have to be the IT Director's responsibility to ensure the details of the implementations of these security aspects, and the specifications of the requirements. One of the objectives with developing security checklists like the ones reviewed in this thesis, is precisely to give guidance regarding security and privacy to the IT Directors in organizations, to ease the tremendous responsibility it is to solely manage. Nevertheless, this thesis derived the security and privacy requirements for the M Platform based on the new security checklist, the laws and regulations related to privacy policies, and the description of the system. Competence about the two latter ones should be matters that are tied to the job description of an IT Director, which again leaves the security checklist to be of considerable help when evaluating the risks of a potential cloud service. Hence, the checklist can be applied as a recommendation that addresses the main security and privacy issues, under the

condition that additional domain specific descriptions are utilized.

Revisiting the second research question defined in Chapter 1.2, the security checklist created in this thesis manages to encompass the main security and privacy challenges of the M Platform. Though at a superficial level, as it was necessary to define additional requirements and categories to ensure that the security and privacy aspects for the M Platform was completely covered. The security checklist is imperfect, as applying the security checklist to the M Platform was insufficient to guarantee the hospital that the patients' medical data are securely protected.

Chapter 6
Conclusion and Future Work

The aim for this study was to develop a new security checklist based on existing best-practices and standards. The intention was for a cloud consumer to utilize this checklist to discover the security and privacy procedures the cloud providers implement for their public cloud services. A cloud-based healthcare service was studied to evaluate the applicability of the checklist, and to what extent it manages to encompass the main security and privacy issues in a public cloud solution.

An analysis of the security and privacy requirements for the M Platform was performed by reviewing national laws and regulations for protecting patients' medical health records, characterized as sensitive personal data. The evaluation was carried out by applying the new security checklist to the M Platform, using the requirements derived from the analysis. The results from the evaluation showed that the security checklist created in this thesis covers the main security and privacy issues of the M Platform to a large extent at a superficial level. The checklist is highly suitable as a guidance to the most essential security issues a cloud consumer should examine before embracing a potential cloud service. The checklist is also valuable for raising consciousness among cloud consumers about security elements to beware of regarding public cloud services. Though, it is not adequately detailed for a cloud consumer to utilize to be guaranteed that sufficient implementation of data protection mechanisms are provided for a cloud service. As the evaluation revealed, it was necessary to define supplementary requirements to the checklist, to ensure that all aspects necessary to protect the patients' medical data was addressed. This result demonstrates that the checklist was unsatisfactory for this particular cloud service concerning the level of detail. The security checklist developed in this thesis can act as a reliable guide for consumers to employ for discovering the overall security measures taken by the cloud provider. By applying this list, the consumer should additionally define specific requirements for each category that needs to be addressed for their particular system.

There are several opportunities for further development of this security checklist. The checklist could be improved for this particular healthcare service, by updating

it with the findings of the evaluation performed in this thesis, e.g. expanding the checklist with the 17 requirements identified, both Table 4.1 and Table 4.2. An essential prerequisite would be to perform an extensive assessment of the security checklist. This thesis has been conducted based on the author's knowledge only. An investigation of the value of a security checklist like the one created here should be conducted. How to conduct this investigation would also be future work, but it is essential to examine if such a checklist is applicable for an IT Director, if such a checklist is of interest and considered valuable for the user.

Further development of this security checklist could also consist of updating it to be utilized for general public cloud services, e.g. by expanding the checklist with the eight requirements listed in the discussion, with ID from J to Q. When the expecting standards and regulations for describing and implementing security measures in the cloud are published and in force, the checklist should be updated to reflect these obligations. The cloud technology is rapidly growing, and security issues will most likely be addressed to a greater extent in the future, and more requirements will be made. If the preconditions are still to keep the checklist applicable to the general public cloud service to the greatest extent possible, it must be updated periodically to adapt and follow current changes, both regarding level of detail and relevant categories.

Bibliography

[1] **European Commission's DG CONNECT**, *net-cloud future*. 2013. [Accessed: 11.02.2014.]. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/NET-CLOUD_DIGITAL-AGENDA_clickable_0.pdf.

[2] **Bhattacherjee, Anol**, *Social Science Research: Principles, Methods, and Practices*. 2012. USF Tampa Bay Open Access Textbooks Collection. Book 3.

[3] **Justis -og Beredskapsdepartementet**, *Om lov om behandling av personopplysninger (personopplysningsloven)*. (In Norwegian) Last updated: 01.06.2013. [Accessed: 05.06.2014.]. http://lovdata.no/dokument/NL/lov/2000-04-14-31.

[4] **European Parliament and the Council of 24 October 1995**, *Proposal of the European Parliament and of the Council - General Data Protection Regulation*. Dated: 12.03.2014. [Accessed: 06.06.2014.]. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.

[5] **European Parliament and the Council of 24 October 1995**, *Directive 95/46/EC*. Official Journal, 23.11.1995. [Accessed: 05.06.2014.]. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[6] **Helse-, omsorgs- og sosialsektoren, Helsedirektoratet**, *Norm for informasjonssikkerhet, 3. utgave*. (In Norwegian) Last updated: 05.12.2013. [Accessed: 27.05.2014.]. http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/Sider/default.aspx.

[7] **Rodrigues, Joel JPC and Torre, Isable de la and Fernández, Gonzalo and López-Coronado, Miguel**, *Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems*. Published: 21.08.2013. Published in Journal of Medical Internet Research. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3757992/.

[8] **Edd Dumbill, Forbes**, *Defining Big Data*. Last updated: 07.05.2014. [Accessed: 08.06.2014.]. http://www.forbes.com/sites/edddumbill/2014/05/07/defining-big-data/.

[9] **Gartner.**, *Cloud Computing*. [Accessed: 03.11.2013.]. http://www.gartner.com/it-glossary/cloud-computing/.

[10] **Salesforce**, *Sustainability.* [Accessed: 27.12.2013.]. http://www.salesforce.com/company/sustainability/benefits.jsp.

[11] **Liu, Fang and Tong, Jin and Mao, Jian and Bohn, Robert and Messina, John and Badger, Lee and Leaf, Dawn**, *NIST Cloud Computing Reference Architecture, Special Publication 500-292.* 2011. [Accessed: 20.02.1014.]. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

[12] **Gartner.**, *Platform as a Service (PaaS).* [Accessed: 18.12.2013.]. http://www.gartner.com/technology/research/cloud-computing/report/paas-cloud.jsp.

[13] **Cloud Standards Customer Council**, *Security for Cloud Computing - 10 Steps to Ensure Success.* Last updated: August, 2012. [Accessed: 08.04.2014.]. http://www.cloudstandardscustomercouncil.org/Security_for_Cloud_Computing-Final_080912.pdf.

[14] **Cloud Security Alliance**, *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0.* Last updated: 2011. [Accessed: 08.04.2014.]. https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf.

[15] **Jaatun, Martin Gilje and Meland, Per Håkon and Bernsmed, Karin**, *Cloud Security Whitepaper: A Briefing on Cloud Security Challenges and Opportunities.* 2013. [Accessed: 15.02.2014]. http://www.telenor.com/wp-content/uploads/2013/11/TelenorWhitepaperCloud-V_30_v.pdf.

[16] **Salesforce**, *What is Cloud Computing? - The Complete Guide.* [Accessed: 02.01.2014.]. http://www.salesforce.com/uk/socialsuccess/cloud-computing/what-is-cloud-computing.jsp.

[17] **Ernst and Young**, *Cloud computing issues and impacts.* 2011. [Accessed: 27.03.2014.]. http://www.ey.com/Publication/vwLUAssets/Cloud-computing_issues_and_impacts/$FILE/Cloud_computing_issues_and_impacts.pdf.

[18] **ENISA**, *Procure Secure - A guide to monitoring of security service levels in cloud contracts.* 2012. [Accessed: 04.03.2014.]. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts.

[19] **Jansen, Wayne and Grance, Timothy**, *Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144.* 2011. [Accessed: 15.02.2014]. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[20] **Hurwitz, Judith and Bloor, Robin and Kaufman, Marcia and Halper, Fern from Cloud Computing For Dummies**, *Comparing Public,Private, and Hybrid Cloud Computing Options.* [Accessed: 07.04.2014.]. http://www.dummies.com/DummiesArticle/Comparing-Public-Private-and-Hybrid-Cloud-Computing-Options.id-147134.html.

[21] **Mell, Peter and Grance, Timothy**, *The NIST Definition of Cloud Computing, Special Publication 800-145.* 2011. [Accessed: 21.02.2014].

[22] **Gartner.**, *Public Cloud Computing.* [Accessed: 09.04.2014.]. http://www.gartner.com/it-glossary/public-cloud-computing.

[23] **TechTarget, by Margaret Rouse**, *Public Cloud.* Last updated: 15.05.2009. [Accessed: 09.04.2014.]. http://searchcloudcomputing.techtarget.com/definition/public-cloud.

[24] **Mackie, Kurt**, *Gartner Offers Tips on Office 365 Negotiations.* Published: 11.05.2013. [Accessed: 07.06.2014.]. http://redmondmag.com/articles/2013/11/05/office-365-negotiations.aspx.

[25] **ENISA**, *Cloud Computing - Benefits, risks and recommendations for information security.* Last updated: December 2012. [Accessed: 12.04.2014.]. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.

[26] **Poitras, Laura and Greenwald, Glenn**, *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' - video.* 09.06.2013. [Accessed: 15.06.2014.]. http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

[27] **European Commission Decision C**, *HORIZON 2020 - WORK PROGRAMME 2014-2015.* 2013. [Accessed: 15.01.2014.]. http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-leit-ict_en.pdf.

[28] **Bernsmed, Karin and Meland, Per Håkon and Jaatun, Martin Gilje**, *Security Obligations for Cloud SLAs, version 1.0.* (Internal report) Date: 01.10.2012. [Accessed: 01.10.2013.].

[29] **Kosmo, Monika Katrin**, *Security Requirements for the Cloud.* 2014. (Internal report) Norwegian University of Science and Technology.

[30] **European Telecommunications Standards Institute (ETSI)**, *Cloud Standards Coordination Final Report Version 1.0.* Published: 27.11.2013. [Accessed: 30.04.2014.]. http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF.

[31] **Cloud Security Alliance**, *Cloud Security Alliance Controls Matrix (CCM).* Published: 26.09.2013. [Accessed: 15.03.2014.]. https://cloudsecurityalliance.org/research/ccm/.

[32] **FedRAMP**, *Federal Risk and Authorization Management Program (FedRAMP) Security Controls Baseline, version 1.1.* Published: 25.07.2012. [Accessed: 04.03.2014.]. http://cloud.cio.gov/document/fedramp-security-controls-nist-sp-800-53-rev-3.

[33] **CESG and Cabinet Office**, *Cloud Security Principles.* Last updated: 23.04.2014. [Accessed: 30.04.2014.]. https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles.

[34] **ISO**, *ISO/IEC 27017 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (DRAFT).* [Accessed: 09.05.2014.]. http://www.iso27001security.com/html/27017.html.

[35] **ISO**, *ISO/IEC 27018 - Code of practice for PII protection in public clouds acting as PII processors (DRAFT).* [Accessed: 09.05.2014.]. http://www.iso27001security.com/html/27018.html.

[36] **ISO**, *Sector-specific application of ISO/IEC 27001 - Requirements (DRAFT).* [Accessed: 09.05.2014.]. http://www.iso27001security.com/html/27009.html.

[37] **ISO**, *Information security management systems - Requirements.* 2013. [Accessed: 09.05.2014.]. http://www.iso27001security.com/html/27001.html.

[38] **Bernsmed, Karin and Hon, W. Kuan and Millard, Christopher**, *Deploying Medical Sensor Networks in the Cloud - Accountability Obligations from a European Perspective.* (Internal report). 2013.

[39] **Datatilsynet**, *Hva er personvern?* (In Norwegian) Published: 25.11.2011. [Accessed: 05.06.2014.]. https://www.datatilsynet.no/personvern/Hva-er-personvern/.

[40] **Datatilsynet**, *Hva er personopplysninger?* (In Norwegian) Published: 22.08.2012. [Accessed: 05.06.2014.]. https://www.datatilsynet.no/personvern/Personopplysninger/.

[41] **Justis -og Beredskapsdepartementet**, *Om lov om behandling av personopplysninger (personopplysningsloven) Kapittel V.* (In Norwegian) Last updated: 01.06.2013. [Accessed: 05.06.2014.]. http://lovdata.no/dokument/NL/lov/2000-04-14-31#KAPITTEL_5.

[42] **Datatilsynet**. (In Norwegian) [Accessed: 05.06.2014.]. http://www.datatilsynet.no.

[43] **Datatilsynet**, *Databehandleravtale om behandling av personopplysninger.* (In Norwegian) Published: 29.12.2011. [Accessed: 05.06.2014.]. http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/.

Appendix A - The New Security Checklist

ID	Category		Security Requirement	References[1]	Supporting references[2]
	Data in transit				
		Encryption		[33]	[25][13][32][31][30]
1			All consumer data will be encrypted during transfer at any layer?	[33]	[28]
		Isolation		[33]	[25][13][31][30][28][18]
2			Does the provider offer a sufficient level of network isolation between the tenants so that no tenant can see or interfere with other consumers' data in transit?	[18]	[13][33][28]
	Data in storage				
		Back-up			
3			The service provider maintains backup copies of the consumer's data at a specific time interval?	[32]	[28]
4*			All backup data is stored in another geographical location?	[28]	
		Physical location		[33]	[25][30][28]
5			Consumer data will be stored in (a) specific geographic location(s)? (specify country)	[33]	[28]
6*			All consumer data will be stored in a country under a particular jurisdiction? (specify jurisdiction)	[28]	[33]
		Encryption		[33]	[31][13][32][28]
7			Encryption is employed to protect all data at rest?	[13]	[32][28]
8			Encryption keys are stored and maintained by the consumer or a trusted key management provider(3rd party) ?	[31]	[13][32][28]
		Isolation		[33]	[25][13][31][30][18][28]
9			For structured data held in databases within the cloud provider's environment, is there proper separation of data belonging to different consumers in a multi-tenant environment?	[13]	[18]
		Data sanitation (deletion)		[33]	[25][13][31][18][30]
10			The consumer is aware of the amount of time it will take before all consumer data (and any backups) are securely sanitised ?	[33]	[18]
11			The service provider ensures secure disposal and complete removal of all consumer data from all storage media, making sure that no data is recoverable by any computer forensic means ?	[31]	[33]
		Portability		[25]	[28][31]

12*			Consumer data can be exported and imported according to a specified standard ?	[28]	[31]
		Migration		[13]	[30]
13			Can the consumer integrate its existing database of internal information and assets within the cloud environment?	[13]	
		Ownership			[13][31]
14*			All consumer data stored in the cloud remain the sole property of the consumer?	[28]	
	Data in processing				
		Encryption			
15			Data accessed by virtual machines is encrypted by using policy-based key servers that store the keys separately from the virtual machine and the data?	[31]	[13][33][28]
		Isolation			[30]
16*			All consumer data in RAM will be isolated from other tenants' data?	[28]	
17*			The service provider has implemented mechanisms to ensure that virtual machines do not interfere with each other ?	[28]	[30][31]
		Physical Location		[33]	[25][31][30]
18			Consumer data will be processed in (a) specific geographic location(s)? (specify country)	[33]	[28]
19*			All consumer data will be processed in a country under a particular jurisdiction? (specify jurisdiction)	[28]	[33]
	Governance			[33]	[25][13][31][30] [28]
20			The service provider's security governance framework is formally documented, as are policies governing key aspects of information security relating to the service?	[33]	[25][13][31][28]
21			Third-party service providers demonstrate compliance with information security and confidentiality, service definitions, and delivery level agreements included in third-party contracts?	[31]	[25][32][13][33]
	Access Control				[30]
		Data centre security		[33]	[13][31]
22			Physical infrastructure and facilities are held in secure areas with constrained access control?	[13]	[33][28][31]
23			Physical protection against damage from natural causes and disasters are anticipated, designed, and the provider have countermeasures applied?	[31]	[13][1]

		Personnel security		[33]	[25][13][32][31] [28]
24			All employment candidates, contractors, and third parties are subject to background verification proportional to the data classification to be accessed ?	[31]	[28]
25*			The service provider supports multifactor authentication to ensure secure access to the cloud management interface (dashboard)?	[28]	
26			Does the service provider offer single sign-on for access across multiple applications offered or trusted federated single sign-on across applications with other vendors?	[13]	[28]
	Incident management			[33]	[13][32][18][31] [28][30]
		Auditing			
27			The service provider has made the consumer aware of what audit information that will be available?	[33]	[18][31]
28			The provider makes security incident information available to all affected consumers?	[31]	[13][28][18][30]
		Operational security		[33]	[13][31][18][30]
29*			The service provider has implemented firewalls and malware protection?	[28]	[13]
30			Does the provider's network have intrusion detection and prevention in place?	[13]	[28]
31			New and evolving threats are regularly reviewed and the service is kept up to date with the latest security patches?	[33]	[28]
	Transparency			[25]	[30]
32			The service provider informs consumers how much of their information is shared with, or accessible by, third party suppliers and their supply chains?	[33]	[25][32][31][13] [28]
	Privacy policies			[28]	[30]
33*			The provider will not disclose any of the consumer's data to any third party ?	[28]	[31]
34*			The provider will not disclose any of the consumer's confidential data to any third party?	[28]	
	Forensics			[28]	
35*			In case of a security incident that requires a legal action, the provider will collect and deliver supporting evidence?	[28]	

1) Main reference to the defined requirement, can be found in the bibliography in the report
2) Additional reference that also discuss the problem of issue. Can be found in the bibliography in the report
*) Derived from 'the old security checklist'

Appendix B - Contract for Cloud Services in the Healthcare Domain in Norway

(In Norwegian)

Vedlegg B: Avtaleskisse – databehandleravtale etter helseregisterloven (NB – gjelder i hovedsak helse/forskning)

Databehandleravtale

I henhold til helseregisterlovens § 16, jf. § 18 og
personopplysningsforskriftens kapittel 2.

mellom

…….
databehandlingsansvarlig

og

…….
databehandler

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger (helseregisterloven) og forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften). Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer databehandlers bruk av personopplysninger på vegne av den databehandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

2. Formål

Her skal det redegjøres for formålet med databehandleravtalen. Herunder:

- hvilke personopplysninger som skal behandles
- hvilke behandlinger som omfattes av avtalen
- hva som er rammene for databehandlers håndtering av personopplysninger

3. Databehandlers plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som databehandlingsansvarlig til enhver tid har bestemt skal gjelde.

Databehandler plikter å gi databehandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at databehandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Databehandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

4. Bruk av underleverandør

Dersom databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal dette avtales skriftlig med databehandlingsansvarlige før behandlingen av personopplysninger starter.

Avtale med underleverandører
En slik avtale bør gjøres som et tillegg til denne avtalen.

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

5. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven og personopplysningsforskriften, herunder særlig helseregisterlovens §§ 16 – 18 og personopplysningsforskriftens kap. 2 og 3. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på databehandlingsansvarliges forespørsel.

Avviksmelding etter personopplysningsforskriftens § 2-6 skal skje ved at databehandler melder avviket til databehandlingsansvarlig. Databehandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet.

6. Sikkerhetsrevisjoner

Databehandlingsansvarlig skal avtale med databehandler at det gjennomføres sikkerhetsrevisjoner jevnlig for systemer og lignende som omfattes av denne avtalen.

Revisjon
Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

7. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av databehandlingsansvarlig.

eller

avtalen gjelder til _____

Ved brudd på denne avtale eller personopplysningsloven kan databehandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning

Avtalen kan sies opp av begge parter med en gjensidig frist på _____, jf. punkt 8 i denne avtalen.

8. Ved opphør

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den databehandlingsansvarlige og som omfattes av denne avtalen.

Tilbakelevering
Videre kan det avtales at det skal gis en utskrift og kopi av alt innhold i databaser og lignende med data som er omfattet. Kostnader ved dette, eller om opplysningene skal leveres i et særskilt format, kan også inngå i en slik avtale.

Det skal avtales at databehandler skal slette eller forsvarlig destruere alle dokumenter, data, disketter, cd-er mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Avtalen bør spesifisere på hvilken måte sletting og/eller destruksjon skal skje etter avtalens opphør.

Databehandler skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

9. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til: _____

10. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar XXXXXX tingrett som verneting. Dette gjelder også etter opphør av avtalen.

Valg av verneting kan avtales

***

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Sted og dato

Databehandlingsansvarlig	Databehandler
……..	……
(underskrift)	(underskrift)

Appendix C - Resulting List of Security Requirements for the M Platform

ID	Category		Security Requirement	Defined
	Data in transit			
		Encryption		
1			All consumer data will be encrypted during transfer at any layer?	X
		Isolation		
2			Does the provider offer a sufficient level of network isolation between the tenants so that no tenant can see or interfere with other consumers' data in transit?	X
	Data in storage			
		Back-up		
3			The service provider maintains backup copies of the consumer's data at a specific time interval?	X
4			All backup data is stored in another geographical location?	X
		Physical location		
5			Consumer data will be stored in (a) specific geographic location(s)? (specify country)	X
6			All consumer data will be stored in a country under a particular jurisdiction? (specify jurisdiction)	X
		Encryption		
7			Encryption is employed to protect all data at rest?	X
8			Encryption keys are stored and maintained by the consumer or a trusted key management provider(3rd party) ?	
		Isolation		
9			For structured data held in databases within the cloud provider's environment, is there proper separation of data belonging to different consumers in a multi-tenant environment?	X
		Data sanitation (deletion)		
10			The consumer is aware of the amount of time it will take before all consumer data (and any backups) are securely sanitised ?	X
11			The service provider ensures secure disposal and complete removal of all consumer data from all storage media, making sure that no data is recoverable by any computer forensic means ?	X
		Portability		
12			Consumer data can be exported and imported according to a specified standard ?	X

		Migration		
13			Can the consumer integrate its existing database of internal information and assets within the cloud environment?	
		Ownership		
14			All consumer data stored in the cloud remain the sole property of the consumer?	X
	Data in processing			
		Encryption		
15			Data accessed by virtual machines is encrypted by using policy-based key servers that store the keys separately from the virtual machine and the data?	
		Isolation		
16			All consumer data in RAM will be isolated from other tenants' data?	X
17			The service provider has implemented mechanisms to ensure that virtual machines do not interfere with each other?	
		Physical Location		
18			Consumer data will be processed in (a) specific geographic location(s)? (specify country)	X
19			All consumer data will be processed in a country under a particular jurisdiction? (specify jurisdiction)	X
	Governance			
20			The service provider's security governance framework is formally documented, as are policies governing key aspects of information security relating to the service?	X
21			Third-party service providers demonstrate compliance with information security and confidentiality, service definitions, and delivery level agreements included in third-party contracts?	X
	Access Control			
		Data centre security		
22			Physical infrastructure and facilities are held in secure areas with constrained access control?	X
23			Physical protection against damage from natural causes and disasters are anticipated, designed, and the provider have countermeasures applied?	X
		Personnel security		

24			All employment candidates, contractors, and third parties are subject to background verification proportional to the data classification to be accessed ?	X
25			The service provider supports multifactor authentication to ensure secure access to the cloud management interface (dashboard)?	X
26			Does the service provider offer single sign-on for access across multiple applications offered or trusted federated single sign-on across applications with other vendors?	
	Incident management			
		Auditing		
27			The service provider has made the consumer aware of what audit information that will be available?	X
28			The provider makes security incident information available to all affected consumers?	X
		Operational security		
29			The service provider has implemented firewalls and malware protection?	X
30			Does the provider's network have intrusion detection and prevention in place?	X
31			New and evolving threats are regularly reviewed and the service is kept up to date with the latest security patches?	
	Transparency			
32			The service provider informs consumers how much of their information is shared with, or accessible by, third party suppliers and their supply chains?	X
	Privacy policies			
33			The provider will not disclose any of the consumer's data to any third party ?	X
34			The provider will not disclose any of the consumer's confidential data to any third party?	X
	Forensics			
35			In case of a security incident that requires a legal action, the provider will collect and deliver supporting evidence?	