

Exploring the value conflicts and supports of information security compliance in nursing practices

A case-study in the Hospital of Southern Norway (SSHF) Kristiansand

KAI HENRIK JORDALEN & TOBIAS STENSRUD LARSEN

SUPERVISORS

Polyxeni Vasilakopoulou & Devinder Thapa

University of Agder, 2020

Fakultet for Samfunnsvitenskap

Institutt for Informasjonssystemer

Preface

This master thesis is the result of work performed by two students from the master's degree program in information systems at the University of Agder (UiA).

In our work with this study, we have applied our own experience, theoretical knowledge from previous courses and literature, as well as research methodology. Writing the master's thesis has been demanding but, most of all, a gratifying and educational task.

First, we would like to address the health care personnel involved in our study; thank you for the vital work that you are doing in the light of the ongoing pandemic.

And, thank you to our main contact person at SSHF, the information security manager. Thank you for dedicating the time and for the supportive dialog throughout the project, and thanks for helping us facilitate interviews at the hospital.

In addition, this study would not have been possible without our fifteen interviewees who took the time to provide us with valuable insights despite busy workdays. Not to mention SSHF, thanks for letting two students conduct our small case study in your vast organization.

A special thanks go to our supervisors, Associate Professor Polyxeni Vasilakopoulou and Professor Devinder Thapa. Thank you for providing support and guidance from the project start to finish. Your encouragement helped us improve our academic work.

Kristiansand, June 4th, 2020

Tobias Stensrud Larsen

Kai Henrik Jordalen

"Seek First to Understand, Then, to Be Understood"
- Dr. Stephen R. Covey

Abstract

Background: Information and information systems are a vital resource for an organization. Data breaches cannot be prevented by technical measures alone, that is why this thesis looks at the human element in the search for understanding compliance with security policies. The context is the hospital sector with the aim of understanding the actual behavior of employees and the divergence of convergence with prescribed policies.

Theoretical lens: The study adopts the lens of Value-Based Compliance theory, which has its roots in the health care sector. This theory describes information security actions as 1) prescribed (the written policies), and 2) actual (the actual behavior of employees) and looks for goals and values associated with prescribed and actual information security actions to identify potential conflicts.

Method: This thesis follows a qualitative approach through a case study of SSHF Kristiansand with interviews and documents as the data sources. The interview data are collected from fifteen interviewees: nurses, unit leaders, and information security workers. The data analysis is performed following the value-based compliance method. This method is a development of the value-based compliance theory.

Results: Findings from the study indicate that both supports and conflicts are present at SSHF. Five situations are presented in tables and summary figures to give an overview of the goals and values linked to the actions of the prescribed rules. It is shown that the actual practice differentiates from the prescribed policies, which is not unusual. Based on the actual practice, we see that for nurses, efficiency (V5) stands out as a recurring value but also availability (V6) and quality of health care (V7). For the prescribed policies, confidentiality (V1) and privacy (V4) are the most recurring ones.

Implications: Our results provide insights about the rationalities behind the actual practices of nurses. We present patterns or situations that the management team is not always aware of today. We also present a set of underlying reasons for the choices that nurses have for their non-compliance. These insights can be further used when developing policies allowing the management to see the viewpoint of nurses for specific situations.

Keywords: *Information security, case study, compliance, value supports, value conflicts, hospital, nursing practices, information security actions, prescribed rules, actual practice.*

Table of Contents

Preface	3
Abstract	5
List of figures.....	8
List of tables.....	8
1. Introduction.....	9
1.1 Research context and motivation	10
1.2 Problem statement and research questions.....	10
1.3 Content and structure	11
2. Related literature	12
2.1 Literature search.....	12
2.2 Summary of literature review	12
2.3 Definitions of Concepts.....	14
2.3.1 User Values / User Rational	14
2.3.2 Security Culture	15
2.3.3 Policies.....	16
2.3.4 Behavioral	17
2.3.5 Compliance.....	17
3. Theoretical lens	19
3.1 Value-Based Compliance theory.....	19
3.2 Value-Based Compliance theory background.....	20
4. Method	21
4.1 Qualitative research.....	21
4.2 Research Approach.....	22
4.2.1 Case study.....	24
4.2.2 Interviews.....	24
4.2.3 Ethics	25
4.3 Data Collection.....	25
4.3.1 Decide on the demarcation.....	25
4.3.2 Collecting policy documents	26
4.3.3 Collecting data about actual actions	26
4.3.4 Interviews with the policy responsible.....	26
4.4 Data Analysis	27
4.4.1 Identifying prescribed actions.....	27
4.4.2 Identifying actual actions.....	28
4.4.3 Analysis of use and value rationale.....	28

4.4.4 Analysis of prescribed ISAs and value rationale	29
4.4.5 Value-Based Compliance analysis	30
5. Results	31
5.1 Authentication.....	31
5.2 Information Sharing	35
5.3 Reporting.....	37
5.4 Information Access.....	40
5.5 Information Protection.....	43
5.6 Summary of results	45
6. Discussion	47
6.1 Compliance - actual practices vs. prescribed policies	47
6.2 Differences across job roles.....	48
6.3 Continuing the work on Value-Based Compliance.....	50
6.4 Wrapping up the discussion.....	52
7. Implications and future directions.....	53
7.1 Implications for research	53
7.2 Implications for practice.....	53
7.3 Limitations.....	54
7.4 Future directions	54
8. Conclusion	56
9. References	57
10. Appendixes	60
10.1 Interview guide nursing personnel	60
10.2 Interview guide security manager	65

List of figures

Figure 1: UML representation of the VBC model (Hedström et al., 2011). 19
Figure 2: Value-Based Compliance method (Kolkowska et al., 2017). 23
Figure 3: Authentication. 34
Figure 4: Information sharing 36
Figure 5: Reporting. 39
Figure 6: Information Access. 42
Figure 7: Information Protection. 45

List of tables

Table 1: Overview of interviews 27
Table 2: A list of values derived from actual and prescribed ISAs 28
Table 3: A list of goals derived from actual and prescribed ISAs. 29
Table 4: Authentication (Prescribed) 31
Table 5: Authentication (Actual) 32
Table 6: Information sharing (Prescribed) 35
Table 7: Information sharing (Actual) 35
Table 8: Reporting (Prescribed). 37
Table 9: Reporting (Actual). 38
Table 10: Information Access (Prescribed). 40
Table 11: Information Access (Actual). 41
Table 12: Information Protection (Prescribed). 43
Table 13: Information Protection (Actual). 44

1. Introduction

In today's society, information, and information systems (IS) are vital resources for organizations. Data losses and security breaches can cause significant problems for organizations related to both economics and reputation. As technologies advance and mature, organizational information systems are starting to become more secure and robust. This has shifted the focus from just a technical perspective, to also include the human element, in other words, towards a holistic view on security (Herath & Rao, 2009). It is widely acknowledged in the literature that the human element is the weakest link in IS-security and, therefore, organizations focus on using tools to guide the employees. "*Security policies and codes of conduct are frequently the main, or only, tool used by managers to guide and control employees' security behaviors*" (Hedström, Kolkowska, Karlsson & Allen, 2011, p. 373). Security policies are introduced by information security managers and aim to guide employees into the same strategic path as the organization. Therefore, security policies are based on values at the management level of organizations (Hedström et al., 2011).

Nevertheless, there can be differences between the actual users of the policies and the policy creators. Interestingly, "*the design [of policies] is based on the creator's design rationale, while the use is based on the user's use rationale*" (Hedström, Karlsson & Kolkowska, 2013, p. 270). These different rationales indicate that there might be discrepancies between the designed policies and the actual use of them. Herath & Rao (2009) argue that if users do not follow the security policies, the policy efforts are in vain.

Several researchers have investigated employee divergence or non-compliance to security policies, using different theoretical models and testing them empirically. For example, prior research has used deterrence theory, which proposes that when punishment is a certainty, and the severity of punishment is increased, then; as a result, non-compliance is reduced (D'Arcy, Hovav, & Galletta, 2009; Herath & Rao, 2009). Other often-used theories are the theory of planned behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010), which evolves around that "*Intentions to perform behaviors of different kinds can be predicted with high accuracy from attitudes toward the behavior, subjective norms, and perceived behavioral control.*" (Ajzen, 1991, p. 179).

Another theory is neutralization, which is a summary of various techniques a person uses to justify actions deviant behavior (Sykes & Matza, 1957). An employee might justify their action based on that their deviant actions did not cause any harm; this technique is called denial of injury (Sykes & Matza, 1957). This prior research has a common orientation: the research aim is about shaping behavior and controlling the employees to ensure compliance with the information security policies. However, prior research by Hedström et al. (2011) showed that looking into examples where practitioners did not comply with policies can bring a new view of information security compliance. Instead of controlling employees into compliance, the research by Hedström et al. (2011) is oriented to creating an understanding of the underlying values that shape the non-compliance. The findings from that article have been developed over time from a theoretical framework (Karlsson & Hedström, 2008), to the value-based compliance (VBC) method (Kolkowska, Karlsson & Hedström, 2017).

1.1 Research context and motivation

We chose to conduct a study on information security compliance in the public Norwegian health care sector. This is a critical sector in the society, and IS-security becomes especially important because of all the sensitive patient information the hospital handles. Having data breaches or leaks of patient information can severely hurt the privacy of the affected individuals. Within the health sector, we decided to focus on the hospital segment as it represents large organizations with employee-numbers often in the range of thousands. The considerable size of hospitals, combined with the critical and confidential information they handle, makes it essential to ensure proper information security. After reviewing related research literature, we identified a gap related to actual practices in the Norwegian health sector: little is known about the reasons why employees comply or not with information security policies. However, we found studies (Hedström et al., 2011; Kolkowska, Hedström & Karlsson, 2009) conducted in our neighboring country, Sweden, and these motivated us to try similar research here in a Norwegian context. Our research aims to explore and get insights into actual day to day practices.

Not following policies in health care practices can have negative consequences for the patient, but also the health care personnel.

In any organisation that holds significant amounts of sensitive personal information, a data breach requires investigation which seeks to pinpoint the causes, and this often results in the identification of a culprit. Sometimes he/she becomes a focus of media interest. (Renaud & Goucher, 2012, p. 297).

We have seen cases in Norwegian media where health care workers are being blamed or accused of leaking patient information, and sometimes the media is exposing the identity of the health care worker. This can, of course, be a heavy burden to bear for the person being accused. Nursing personnel, in particular, have to work under significant time pressure while they also have to adhere to a multitude of rules and regulations. The Code of Conduct, “Normen” in Norwegian (The Norwegian Directorate of eHealth, 2020), is a collection of these laws, which aims to present them more understandably for the health care workers to read. For this master thesis, we decided to focus on the information security practices of nursing personnel.

1.2 Problem statement and research questions

Our initial thoughts were to look for threats associated with information security within the hospital sector, but not technical IS-security issues. This led us to look into the socio-technical perspective, looking for how individuals interact with technology and other individuals. After a small pre-study, we conducted at Hospital of Southern Norway (SSHF) Kristiansand the previous semester, we decided to focus our study on nursing personnel and how they relate to IS-security in their daily work. In order to get an understanding of this, we wish to look at the values that drive and affect the way nurses carry out their routines. With our research, we aim to bring up instances where nurses' values are in conflict with security policies and also instances where values are harmonious with security policies. This again led to our research question:

What are the value conflicts and supports of information security compliance in nursing practices?

We want to be exploratory in our study in order to identify the actual practices related to security policies. First, we need to find out what the prescribed policies are, and then what the actual practices are like at the hospital. To be able to answer the research question, we have to break it down into sub-questions:

- What are the goals and values behind information security policies at SSHF?
- What are the goals and values driving the actual practices of nursing personnel?

On the basis of, and to answer these questions, we conducted a qualitative study in the health sector with an explorative case study of SSHF Kristiansand. Prior to this thesis, we did a small pre-study at SSHF, focusing on insider threats. Insights gathered from the preliminary research helped us with the shaping of the research questions for this study.

1.3 Content and structure

The rest of the thesis is structured as follows; In chapter two, we include literature that forms the foundation for our research and introduce the main concepts that we explore. In chapter three, we introduce the value-based compliance theory, which guided this research. Chapter four summarized our method used throughout our thesis. In chapter five, our empirical results are presented; these are then discussed in the light of prior research in chapter six, discussion. In chapter seven, we elaborate on the limitations, future directions, and implications for both research and practice. Chapter eight is a conclusion of the thesis with references and appendixes following in the last chapters, nine and ten.

2. Related literature

In this chapter, we describe how we did the initial literature review and also how we extended our literature assessment at a later stage in our thesis. We present here both how we performed the literature review and also an overview of the concepts that were found and synthesized during the review process.

2.1 Literature search

For the literature review process, we used the structured approach provided by Webster & Watson (2002). The articles we ended up including were not only based on one journal, author, or geographic location but rather a variety of these variables. We argue that such a variety can give us insights from different perspectives, not limiting us to only using research from the US, for example. We followed the steps provided in Webster & Watson (2002) to determine the articles that we felt could help us in answering our research question.

For the first step, we started by searching for literature in the basket of eight for information systems journals, but due to our chosen theme, we had to expand our search. We decided to also include literature from other research domains, including research in the health sector, socio-technical security research, and organizational culture. This led us to an extensive literature basis to work on further. We also followed the second and third steps from Webster & Watson (2002), which included forward and backward searches for the given articles. This gave us insights from the past about employees' compliance and non-compliance with information security has been a big problem over time. As for our search criteria, we mainly wanted articles from the last twenty years. The reason to focus on the last twenty years is that we wanted relatively new findings, and most of the research on the domain has been conducted in this period with an increasing amount the last years.

During our preliminary research, we started with a focus on insider threat and related mitigation techniques. This search gave us solid insights into other lenses to look at the topic of non-compliance. The literature review gave us valuable insight and helped us take another angle of the topic, looking into the values of employees in relation to compliance. We identified a subset of research papers that fit well with our research interest. Specifically, these are the papers by Kolkowska et al. (2017), Hedström et al. (2011), and Bulgurcu et al. (2010). Moving on to the more fitting literature, we decided to do forward and backward searches on Kolkowska et al. (2017), Hedström et al. (2011), and Bulgurcu et al. (2010) in addition to general searches on information security compliance. These new searches gave us new insight into the topic of compliance. At the end of this process, we felt that we had a satisfactory overview of the topic, which is summarized in the next subsection.

2.2 Summary of literature review

Research on information system security is an essential and expanding topic that has shared a lot of different views and approaches to deal with the topic. On a more specific

level, the studies on non-compliance with policies have emerged. In prior research, there is a broad agreement that employees who violate or ignore the security policies create a significant problem, and reducing this is of interest. Deterrence theory is one of the most widely applied theories in IS-security research, particularly within behavioral IS security studies (D'Arcy & Herath, 2011). This theory was used back in 1990 with Straub Jr (1990) but also in newer articles (Cheng, Li, Y., Li, W., Holm & Zhai, 2013; D'Arcy et al. 2009). The theory has contributed with great insights, both theoretical and practical, but also had some inconsistent and mixed results (D'Arcy & Herath, 2011). As this topic is widespread between several disciplines, looking into the problem from several angles is needed.

Von Solms (2001) summarized information security as a multidisciplinary discipline, which he argued that looking into the strategic-, policy, ethical, human, awareness, technical dimensions to mention some and that each one is important. This has called for additional research from other perspectives. Siponen & Vance (2010) challenged the view of deterrence and introduced the neutralization theory into the information security field. This evolves around employees justifying their actions; For example, a person performing a deviant action justifies his/her behavior by claiming that no damage will really be done (Siponen & Vance, 2010).

Another regularly used theory is, the theory of planned behavior (TPB) is a theory that suggests that the intention to perform various kinds of behavior can be predicted with high accuracy using different factors (Bulgurcu et al., 2010). The results in the paper show that employee's compliance is affected by different factors such as attitude, normative beliefs, and self-efficacy to compliance (Bulgurcu et al., 2010). *"Success in information security can be achieved when organizations invest in both technical and socio organizational resources"* (Bulgurcu et al., 2010, p. 524).

Additional research has evolved around understanding each employee's behavior towards information security. The results from Pahnla, Siponen & Mahmood (2007) suggest that information quality has a significant effect on actual IS security policy compliance. Attitude, normative beliefs, and habits have a significant effect on the intention to comply with IS-security policies. This was further explored by Ifinedo (2012), as he viewed the theory of planned behavior (TPB) and protection motivation theory (PMT). The results showed that the intention to comply was positively influenced by self-efficacy, response efficacy, attitude towards compliance, perceived vulnerability, and subjective norms (Ifinedo, 2012).

Another viewpoint that has gotten attention is the topic of IS-security, and the conflicts security creates with other demands in an organization. *"In the set of demands for information security, functionality, usability, and efficiency, the users tend to prioritise the latter three ahead of information security, particularly if the information security workload becomes unacceptable."* (Albrechtsen, 2007, p. 285). Vaast (2007) also elaborates on this topic by looking into different occupational communities, and that conflicts are related to differences in perspectives. Albrechtsen & Hovden (2009), also shares this viewpoint in another context with information security managers versus users. User and information security managers have different responsibilities and rationalities, which creates a different understanding of information security between them. Information security managers have primary responsibility for information security, but the users also have

other tasks in addition to organization goals such as productivity and efficiency (Albrechtsen & Hovden, 2009). The users are aware of their role in information security; however, there is a gap between the intention of information security and the actual behavior of users regarding the topic (Albrechtsen, 2007).

This creates a field in information systems security of looking into the reasons for why these conflicts exist. "*The design [of countermeasures] is based on the creator's design rationale, while the use is based on the user's use rationale.*" (Hedström et al., 2013, p. 270). This study is based on Hedström et al. (2011), which presented a theoretical model where you investigate information security from another perspective rather than the typical control-based models. This view centers around the fact that practitioners base their actions on different value-rationalities when complying or not complying with information security guidelines (Hedström et al., 2011).

This model and the theoretical view have been even further developed into a method, named the Value-Based Compliance method (Kolkowska et al., 2017). In that paper, they address the problem of the lack of a way to analyze multiple rationalities that come into play when working with information security (Kolkowska et al., 2017). The empirical evidence from the article showed concrete situations where practitioners chose health care values over information security values. This view from health care workers is, however, not new, as Gaunt (2000) argues that "*the protection of information is less important than direct patient care, which is something that pervades clinical services in general.*" (p. 152).

We think this sizable literature review creates a good overall overview of the topic. This also helped us in identifying key concepts related to our research. These are defined and described in the following subsection.

2.3 Definitions of Concepts

In this subsection, we elaborate on our key concepts relating to our research questions. The concepts are a result from our literature review and have the intention to provide a foundation of knowledge on the topic. In the last part of this section, we explain how the concepts can be connected, and we present what areas we will focus on the study.

2.3.1 User Values / User Rational

"*There is widespread agreement that people's value priorities play an important role in predicting their attitudinal and behavioral decisions.*" (Myyry, Siponen, Pahlila, Vartiainen & Vance, 2009, p. 128). Schwartz & Bilsky (1987) distinct between different value contents is suggested by the idea that, because values are goals, they must represent the interests of some person or group. They were defining values as goals that give guidance and motivation and guiding individuals in a direction. The values are connected to an individual's identity both on a personal level and professional and that the values affect behavior, evaluations, and choice of actions (Myyry et al. 2009).

However, the view on value is not just on individual levels. Vaast's (2007) research shows that information security holds different meanings in different occupational communities. Looking at the hospital sector, Vaast (2007) argues that different communities such as nurses, physicians, and technicians view information security in unlike ways

even though they are all connected to patient care as a basis. Albrechtsen & Hovden (2009) share this view, which argues that information security managers and employees have different responsibilities as users have other important work tasks and information security, which is the main focus of information security managers.

Health care involves many different collaborating and communicating actors, such as politicians, civil servants, health care professionals, administrators, and managers on different levels. This complex structure leads to a varied and diverse work practice with many concurrent actors, actions, goals, and values. (Kolkowska et al., 2009, p. 2).

Weber (1978), elaborates on four different types of social actions: traditional, affectional, value-oriented, and instrumental. The traditional actions are carried out based on tradition; in other words, habits. The affectional actions are based on a person's feelings also sometimes without thinking of the consequences. The value-oriented actions are based on "*conscious belief in the value for its own sake of some ethical, aesthetic, religious, or other form of behavior, independently of its prospects of success*" (Weber, 1978, p. 24-25). The last type of social action, instrumental, is based on the "*expectations as to the behavior of objects in the environment and of other human beings ...*" (Weber, 1978, p. 24). In other words, the actors are basing the actions on the consequences. Weber (1978) also further divides the four types into two types: rational and non-rational. Two of the four are based on rationality, value-oriented and instrumental actions. While the other two, traditional and affectional actions, are based on non-rationality and does not include mental processes when carried out (Hedström et al., 2013).

Based on the original view from Weber (1978) and the theory of organizational learning (Argyris & Schön, 1996), Karlsson & Hedström (2008) created the value-based compliance theory. The VBC theory, which consists of a set of concepts, can be depicted as Unified Modeling Language (UML) classes: information security action (ISA) (prescribed and actual), actor, goal, and value (Hedström et al., 2011). "*Practitioners base their actions on different value rationalities when complying or not complying with information security guidelines.*" (Hedström et al., 2011, p. 375). A concrete example from Hedström et al. (2013) is that an employee fails to log out of the computer system because the employee rushes off to an emergency, which can be connected to affectional actions from Weber (1978) as the action is based on feelings. These types of situations are situations where the value conflicts between different values might arise. "*By viewing information security actions as social actions, it is possible to gain awareness of the underlying reasons for users' compliance and non-compliance without any a priori assumptions about user intent.*" (Hedström et al., 2013, p. 284). As the actions of employees often are shared between occupational communities, looking into the concept of security culture is also needed.

2.3.2 Security Culture

Security culture, in this context, is the culture among the employees when focusing on security. "*Organisational culture comes into being in the gaps within and between formal business processes and takes the shape of employee values, beliefs, and assumptions about what are acceptable short cuts, workarounds, or informal ways of working in the organisation.*" (Ashenden & Sasse, 2013, p. 396). The culture is something that affects how security is handled in the organization. In the context of different values between different

groups of employees, we see security culture as a middle ground between the prescribed and actual actions. Connecting the actions based on non-rationality with security culture, we see, for example, deeply rooted habits that employees may just perform without thinking of the consequences behind them can be connected to the accepted informal ways among a group of employees. If these types of actions are based on deeply rooted habits that are based on unhealthy values, they might harm the organization, a change, or at least an understanding of why this happens might be needed.

Having proper training and awareness programs might increase the culture in organizations. *"The organisational culture should be considered when cultivating an information security culture to ensure that the most appropriate controls are identified and deployed in a successful manner."* (Da Veiga & Eloff, 2010, p. 198). An essential role of the policies and underlying values is to make sure that the actions taken are following the correct pathway. Therefore, looking into the values of actual actions and creating an understanding will help the organization to create a thriving security culture.

2.3.3 Policies

The policies in an organization are the given rules that employees must or at least should follow to every given time at work. Are the policies in the organization clear and easy to understand? Do the policies act as an obstacle for daily work because they are too strict?

The first step to preparing the organization against these threats is the development of a systems security policy which provides instruction for the development and implementation of a security posture, as well as provides guidelines for the acceptable and expected uses of the systems. (Whitman, Townsend & Aalberts, 2001, p. 10).

We define information security policy, like Bulgurcu et al. (2010), *"as a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations."* (p. 526-527). However, creating these policies is a good starting point; it is not enough to make the employees comply with them (Bulgurcu et al., 2010). They further argue that creating an understanding of what motivates employees to comply with the information security policies and to solve issues regarding them (Bulgurcu et al., 2010).

"There is often a misunderstanding between the policy writer and the reader so that the reader is unable to understand what is required or how to achieve it." (Renaud & Goucher, 2012, p. 299). This shared view is something that Vaast (2007) also found in the research of different healthcare communities, where the different groups had different understandings. This is where the connection to values comes in to play; previous research has focused on how to make the employees adhere to policies. However, we argue that creating an understanding of why these misunderstandings and differences happen rather than control-approach might be more helpful.

"... managers need to be very cautious in choosing the manner, medium, and method of introducing new ISPs and organizational policies." (Lowry & Moody, 2015, p. 450). Another factor is the way these policies are presented, ISPs should be formal written controls, but presented in a respectful manner that softens or eliminates imperatives and provide

options (Lowry & Moody, 2015). Albrechtsen & Hovden (2009) argue that both security managers and users call for more significant interaction and dialogue from both sides. This is in line with our thoughts, and we see that understanding the value behind actions of non-compliance by employees could be a good starting point of this dialogue. We, therefore, argue that looking into values, policies, and behavior together might be suited.

2.3.4 Behavioral

This concept is connected to both security culture and policies. How does the employee behave in a work context? Do they follow the security policies, or do they find workarounds? Creating an understanding of behavior in an information security context has been on the agenda for some time in diverse contexts. Research has shown that individuals with different dispositional factors (internal factors) react differently to similar situational factors (external factors) in the context of security-related behavior (Johnston, Warkentin, McBride & Carter, 2016). An example from the hospital sector might be a nurse goes for a coffee and locks the computer while another nurse might not lock the computer. Creating understandings of why individuals and groups act differently in the same situation is something that understanding the values behind these actions can help us with. The action of not locking or locking the computer when leaving might be due to it being a habit (irrational) or even based on a rationality that the computer can get compromised by an unauthorized person. This diversity in actions is of interest; in addition, we also include the concept of compliance.

2.3.5 Compliance

How do you get employees to follow regulations and policies? There is a multitude of motivations behind people's intention to adhere to rules, and different personalities may also affect how people choose to comply. These actions can be based on irrationality and rationality, which has raised a research agenda with a focus on non-compliance. If employees' compliance benefits the organization, they are more likely to have positive attitudes towards compliance (Herath & Rao, 2009). We also see that deterrence can be used to deter employees from non-compliance (Bulgurcu et al., 2010; Herath & Rao, 2009).

We also see a connection to the information security culture. *"For example, peers or mentors often inadvertently empower an employee to neutralize and violate policy by saying in passing, for example, that "few people actually follow this password policy.""* (Barlow, Warkentin, Ormond & Dennis, 2013, p. 154). These are situations where non-compliance with policies might get out of hand and that groups of employees create procedures that conflict with the policies. This can, for example, happen when employees feel that the policies act as a hindrance to work and therefore are less likely to have a favorable view of the policies (Herath & Rao, 2009). This calls for better communication between information security managers and employees when creating policies (Albrechtsen & Hovden, 2009).

The overall view on information security compliance research has been with a focus on the shift from non-compliance to compliance. The results from Barlow et al. (2013) suggest that neutralization techniques are just as effective as deterrence approaches to shift the view. For example, employees might feel not comply with a policy because they feel like the actions do not hurt anyone. This can be linked to individuals creating un-secure passwords on systems even though the policies say they must create secure passwords.

The individual's actions are then neutralized by having this password on a system without sensitive information. This might be the case sometimes, that actions that violate policies are not actually harming the information security. We argue that you can not look at compliance as black and white and that there will be situations in the grey area.

All these concepts are selected from literature related to our topic. Many of these concepts do have a direct or indirect relationship together. Looking into the policies and the behavioral aspect of the actual behavior and what is behind those actions are our core interest. These similar topics have all been in the research radar for information security and are rich in data; however, looking into them together in a Norwegian hospital context has not yet been done to the best of our knowledge. In the next chapters, we will go deeper into the value-based compliance theory, and the value-based compliance method, which we followed for our case study.

3. Theoretical lens

This chapter explains the Value-Based Compliance (VBC) theory and why we chose to use this lens for our thesis. Because we decided to focus on compliance, it became natural for us to look for theories that try to elaborate on said topic. When we, in our literature assessment, came across the VBC theory, we felt this would be a fitting way forward as this theory is specific about compliance. Also, the VBC theory has its roots in health care, which fits the context of our study. Since this theory matches both our aim and context, we went with this specific theoretical lens.

3.1 Value-Based Compliance theory

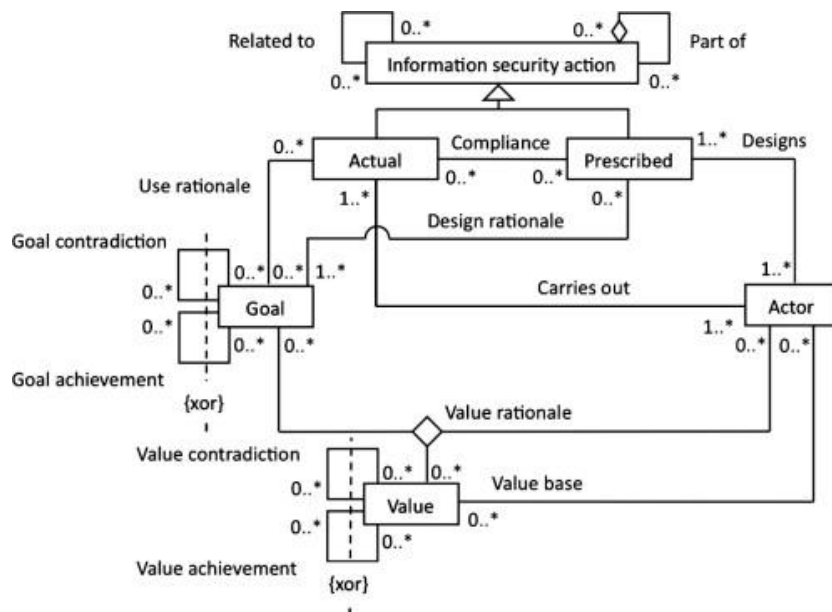


Figure 1: UML representation of the VBC model (Hedström et al., 2011).

The UML model above is a representation of the value-based compliance theory. This theory was a result of a longitudinal case study of information security practice conducted at a hospital in Sweden (Hedström et al., 2011). An actor in this model can be anyone, but in our study, actors are specifically nurses and information security workers. We look at the information security workers as the ones designing the prescribed Information Security Actions (ISAs) and nurses as the actor that carries out the actual ISAs in general. An Information Security Action (ISA) can be 1) prescribed, or 2) actual. Prescribed ISAs refer to the written policy and guidelines of how to act and behave. Meanwhile, the actual ISAs represent the way individuals actually behave in carrying out their daily work.

We see possibilities for nurses to take part in the design process of prescribed rules, but in our study to simplify, we distinguish between the two groups. One or more information security managers design the prescribed ISAs with value rationale as a foundation. Besides, one or more goals related to the design rationale of the prescribed ISAs. As Hedström et al. (2011), we can only assume that there is a rationale behind the designing of the prescribed ISAs.

One or more nurses might carry out one or more actual ISAs. The nurse either has zero or more goals that they want to achieve by performing the actual ISA. As opposed to the

prescribed rules, there might not be a goal with the actual ISA (for example, leaving the computer screen unlocked) but, such actions can also have a reason (for example, time-saving as the login process takes some time). According to the value-based compliance theory, goals and actions have an underlying foundation of values, with a value-rationale and base.

The nurses base their actions on their goals and values, and these are manifested in actual ISAs, and the information security management bases their design of prescribed ISAs on their goals and values. This can lead to either compliance or non-compliance; in other words, we can find divergence between the actual and prescribed actions. Looking into the different value-rationales behind each action can help in the understanding of how the value rationales can contribute to conflicts or supports.

3.2 Value-Based Compliance theory background

The VBC theory is based on the theory of organizational learning (Argyris & Schön, 1996) and the notion of Social Action Theory (Weber, 1978). Weber (1978) differentiates between direct observational understanding and explanatory understanding. This is exemplified with $2*2=4$. In direct observation, we understand the meaning of this when we read it or hear it; on the other hand, with the explanatory understanding, you look into what made the actor solve this math problem under these circumstances with precisely that movement. This can be connected to our research question: *What are the value conflicts and supports of information security compliance in nursing practices?* As we want to create an understanding of the values and tensions and not just find situations where the problem exists.

Weber (1978) also sees social actions as not solely individual actions and that others can influence actions. In our case at the hospital, seeing other colleagues locking the computer might influence your actions of locking the computer. The nurses act as members of a bigger group, and therefore exploring the group in total is a way of exploring the culture. As mentioned in Kolkowska et al. (2017), Weber also distinguishes between rational and irrational actions. This is one of the benefits of this theory, which evolves around values, that the rationality can easily be addressed as well as irrational actions with observations, which we will further elaborate in the method chapter.

This type of theory basis fits well with the aim of our study. By digging deeper into the underlying values of both the prescribed- and actual ISAs, we are likely to be able to find value related conflicts and supports. Our theoretical lens has a focus on compliance with security policies bringing into attention the comparison between the actual practice with the written policies. Using the theory of value-based compliance, we will be able to look into specific actions and create an understanding of the behavior based on the underlying values. By using the VBC theory on a role-level instead of a personal level, we can look at the nurse group's values together and compare them with the policies which will give an overview of the nursing personnel values as a group.

4. Method

In this chapter, we introduce our qualitative research approach. First, we describe the general advantages of doing qualitative research. Second, we present the method we planned to follow. Third, is how we gathered the data. Finally, we present how we did our data analysis.

4.1 Qualitative research

Qualitative studies are designed to help researchers understand people and the social or cultural contexts where they live (Myers & Avison (Eds.), 2002).

Qualitative research is exploratory and is useful when the researcher does not know the important variables to examine. This type of approach may be needed because the topic is new, or the topic has never been addressed with a certain sample or group of people (Creswell, J. W & Creswell, J. D., 2017, p. 22).

Looking into nursing personnel at SSHF and creating an understanding of how information security is handled in daily work is what we want to explore. As this is a context we have limited knowledge about, we chose to go onward with a qualitative explorative approach.

Interpretive studies generally attempt to understand phenomena through the meanings that people assign to them (Myers & Avison 2002). Trying to identify, explore, and explain how all the factors in a particular social setting are related and interdependent (e.g., an organization) (Oates, 2006 p. 292). Looking at the phenomena of information security compliance through the perceptions and meanings of nurses and information security managers. *“Different groups or cultures perceive the world differently.”* (Oates, 2006, p. 292). By looking at the perspectives of the respective groups, we get knowledge of how both groups view information security. An interpretive approach is appropriate in studies of organizational culture as culture is a part of the organizational phenomena studied (Dubé & Robey, 1999).

Oates (2006) argues that researchers are not neutral and that they have their assumptions, beliefs, values, and actions, and this will shape the research process. He also argues that the same criteria can not judge an interpretive and positivist study (Oates 2006 p. 292). Lincoln & Guba (1985) proposes a set of criteria for interpretivism research: trustworthiness, confirmability, dependability, credibility, and transferability. Instead of validity in positivist research, they argue that you look at trustworthiness and how much trust we can place in the research (Oates, 2006). In our study, looking at the trustworthiness, we had to assume that the information revealed in interviews is reflective in the reality of actual practice. However, during the interviews, we got similar information from nurses working in the same department, which is an indication that the information is valid. We also felt that the nurses were open to elaborate about the negative sides as it might be hard to speak about those as you do not want to expose the organization.

“Interpretivists, however, believes that there will always be bias.” (Oates, 2006, p. 293). When talking about confirmability, another researcher can look at the raw data, analysis,

research notes, for example, and put themselves into our shoes (Oates, 2006). In general, have we been told enough about the study that the results can confirm the results? (Oates, 2006). We have tried to include citations from the actual interviews to show where our results are coming from in addition; we also include interview guides in appendices, and anonymized raw data are available by request.

Regarding dependability, how well can this study be replicated? We present our planned research on a general basis in chapter 4.2, with a more detailed step by step way forward in actual research in chapter 4.3 and 4.4. Based on this, other researchers should be able to trace our steps backward and be able to follow them. Oates (2006) argues that for interpretivists, what is being studied is a social construction by individuals, which is short-living and changing, so the same results are unlikely to be met for a repeated study. This is something to keep in mind as there is interpretation included in the results, and another researcher could have interpreted the same empirical material in another way.

Lincoln & Guba (1985) argue that you cannot look at internal validity in interpretivism and instead look at credibility. In other words, making sure that the information from interviews was accurately identified, so the findings are credible (Oates, 2006). During our interviews, we made sure to ask follow-up questions if there was any insecurity about what they meant. As we also wanted to find more about the values, we asked nurses to summarize what the goal and/or value behind their actions was. In that way, we could make sure that what they elaborated on for three minutes was correctly understood instead of speculating. This is also a method of checking the internal validity of the results.

“Credibility ... can be achieved by ... checking for descriptions and interpretations, where researchers go back to their informants to check that their write-up is correct.” (Oates, 2006, p. 294-295). Also, by having two researchers in the room for the interview makes sure that we agree with what was actually said in the interview (Johnson, 1997). A strategy used in this case is investigator triangulation, with both of us taking place in all the interviews. We also used the strategy of data triangulation with the use of multiple data sources (Johnson, 1997). We did this by using both documents and interview data to understand the phenomena.

The last criteria are transferability, can the findings in this case transferred to another case? The case is unique in one way but also similar to other hospitals. There will always be local differences at hospitals; however, we look at most Norwegian hospitals as similar. There will perhaps be different situations with other systems, size-differences, or other challenges related to different hospitals. A way forward at another hospital could be to validate the situations that we present at their hospital in a test interview to check the relevance.

4.2 Research Approach

For our planned research, we wanted to follow the Value-Based Compliance method. The VBC method is presented in Kolkowska et al. (2017) as an information security analysis method (ISAM). An ISAM has the purpose of acting as a tool to analyze the current situation regarding information security, also to provide an indication to where the focuses for improvement should be planned for in the future (Kolkowska et al., 2017).

Moreover, the VBC method is a result of the further development of the VBC theory. The VBC theory has its roots in a longitudinal case study conducted in a Swedish hospital (Karlsson & Hedström, 2008).

The VBC method encompasses collecting data on the actual behavior of employees and analyzing it to compare it to the prescribed information security policies. “Identifying actual ISAs is seen to be one of the greatest challenges for behavioral information security researchers.” (Kolkowska et al., 2017). The method is consistent with the theoretical lens and aims to help researchers apply the theoretical lens in empirical studies. We will, in the following paragraph, briefly describe the nine steps of the VBC method.

The first step in the method in Kolkowska et al. (2017) is to determine the scope, aim, and focus of the study (1). You then move on to collecting policy documents (2) and identifying prescribed actions based on these documents (3). Moving on, you interview the policy designers about policy designers to get an understanding of the values and goals behind the policies (4). The analysis of the design and value rationale behind these actions are then grouped into tables with a linkage between prescribed actions, goals, and values (5). Then you move on to collecting data about the actual actions with both interviews and observations of employees as policy users (6). In the next step, you group the actual ISAs into tables with a linkage between the actual ISAs, goals, and values related (7). Analysis of the collected data by looking into the goals and values that are underlying each ISA (8). Finally, in the last step, you compare the prescribed and actual actions and the goals and values related to each (9). Analyzing the compliance and non-compliance and conflicts between practice and the written down rules. This process, with all of the steps, is shown below in figure 2.

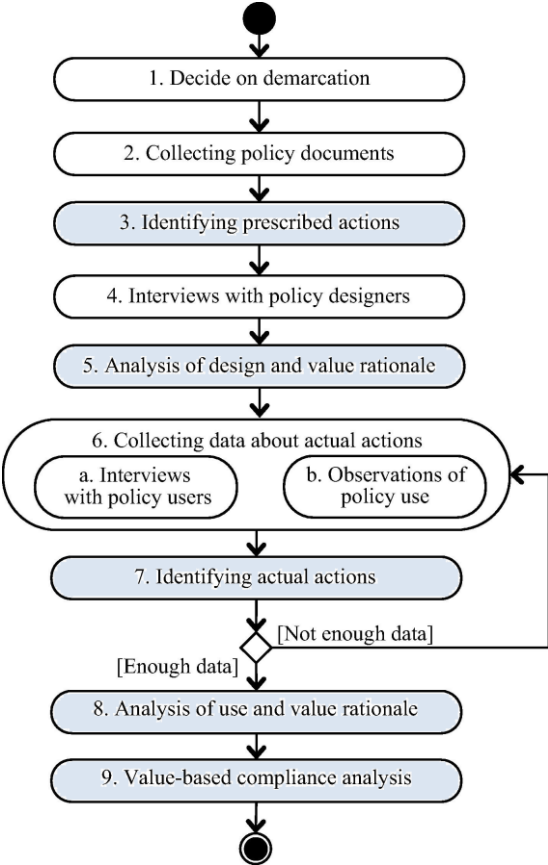


Figure 2: Value-Based Compliance method (Kolkowska et al., 2017).

Note: The authors of this thesis have colored the steps that involve analyzing for clarification that analysis takes place at several stages in the method.

4.2.1 Case study

A case study focuses on one instance of the 'thing' that is to be investigated, for example, an organization (Oates, 2006). This instance is studied using various data generation methods to obtain a rich and detailed insight of that case (Oates, 2006). For our case-study of SSHF, we used two methods: interviews and document analysis. The use of multiple sources and a wide range of data sources is something that characterizes case studies, for example, interviewing as many people as possible (Oates, 2006). This is an exploratory case-study with the focus of understanding the research problem using and testing an existing theory. *"A researcher could take an existing theory and use a case study to see if the empirical evidence gained confirms the theory, implies necessary modifications to it, or contradicts it."* (Oates, 2006, p. 146).

At SSHF, there are over 7000 employees with over 550 000 patient treatments every year (Hospital of Southern Norway, 2019) This shows how complicated and huge the organization is and how much information is located at the hospitals. The hospitals are located in Kristiansand, Arendal, and Flekkefjord, but we only focused on the hospital in Kristiansand. We look at SSHF as a typical hospital and that our findings can also apply to other Norwegian hospitals. After the health reform in 2002, the specialist health service was organized into four regional health enterprises: Northern Norway-, Central Norway-, Western Norway-, and South-Eastern Norway Regional Health Authority, which SSHF operates under (South-Eastern Norway Regional Health Authority, 2019).

In the Norwegian health- and care sector, more and more of the communication is electronic. Due to the challenges this brings to privacy, The Norwegian Directorate of Health started working on rules for safe information handling in 2002 and formally introduced in 2006 (The Norwegian Directorate of eHealth, 2020, 21. April).

4.2.2 Interviews

According to Myers & Newman (2007), a qualitative interview is used in all kinds of qualitative research; case studies, action research, ethnographies, and grounded theory. Interviews are a type of conversation between people with one person undertaking the interview and want to gain knowledge about the other(s) (Oates, 2006). Interviews are a suitable data generation method when researchers want to gain detailed information and questions that are open-ended (Oates, 2006). We used a semi-structured approach with a set of situations and themes we wanted to cover. In semi-structured interviews, you are willing to change the order of questions and ask additional follow-up questions (Oates, 2006). This was indeed the case for us, we had a set of situations ready, but the nurses could elaborate freely and introduce new topics of interest during the interviews. Before the interviews, we planned the questions and the topics based on literature and a validation process. Oates (2006) also argues that you should gather background information about your interviewees and their context. This is something we did, we gathered information about the departments we interviewed, as we did not have much knowledge about the nurse work or departments beforehand. In addition, we also asked the interviewees about intro and basis information and what was typical about their

department compared to others. We followed the same semi-structured approach for information security managers as well but focused more on the prescribed rules as of the actual practice.

4.2.3 Ethics

Informed consent is one of the underpinnings of doing research; this consent evolves around the person(s) being studied and that they are participating in their own free will (Jacobsen, 2015). This is something we took seriously during our interview process; we made sure that every participant had signed the agreement, which was approved by the Norwegian Centre for Research Data (NSD). In the agreement, we informed the participant about this being a voluntary study and that they could interrupt the agreement at any point along with information about the study and what kind of data we stored.

All the data collected in our data collection was anonymized using N1-N12 for nurses and A1-A3 for the administrative workers. We did not collect any private information from the personal life of the respondents but rather related to the work in a department with several employees. However, we put a disclaimer that specific statements could possibly be traced back to the respondent. This is a challenge you must take into account when working with small sample sizes (Jacobsen, 2015).

In addition to the NSD approval, we also signed a non-disclosure agreement, a data processing agreement to be able to carry out the data collection at the hospital. Before we got approval by the hospital, we also had to send in information about the project we proposed. In this process, we had to fill out an application with information about the project, send them the informed consent, the approval from NSD, and a project outline. In addition, the data collected during our thesis will only be held until the project is finished, after the thesis is delivered and evaluated, all the data will be discarded. The following subsection will elaborate on how we did this data collection.

4.3 Data Collection

In this subsection, we present the actual steps for data collection that we followed. This is based on steps 1,2,4 and 6, of the Value-Based Compliance method from Kolkowska et al. (2017).

4.3.1 Decide on the demarcation

We started by defining our scope, this being a master thesis, we knew the deadline for delivery, and this became the natural time-range of our study. In the previous semester, we had a course where we did a preliminary study of information security at SSHF. This helped us in getting in touch with the responsible persons at the hospital. Also, during the preliminary study, we did two interviews to get an understanding of the nursing personnel's relation to information security and to gather knowledge about the information security manager's responsibilities.

We initially wanted to do observations; however, after some discussion with our contact at the hospital, we decided to drop it as it would require approval on a higher level, which can be challenging to get. Given our limited timeframe, we could not afford to wait for such approval that might end up not been accepted after all. Doing observations in the hospital is considered by the management to be quite an intrusion of the employee's

and the patient's privacy. If our study had a broader scope, it could more likely be feasible, but for two master students with a five-month timeframe, we quickly realized that such an undertaking might be too ambitious.

So instead, we asked the hospital for twenty nurses to interview. We received contact information to eight and recruited four more during our visits to the hospital. The nurses varied from several departments, such as intensive unit, day-surgery department, patient hotel, post-surgery, surgical bed station, and orthopedic/geriatric department. As for the administrative workers, we interviewed three in total. Two of them, the ones working with information security, we planned to have several rounds of interviews with them.

4.3.2 Collecting policy documents

As we had familiarized ourselves with the hospital the previous semester, we knew where to look for background material. Most of it was open for public access on the hospital's webpages. The information security manager assisted us in finding the relevant documentation. We had also asked the nurse we interviewed the previous semester, what documents she used to keep updated on rules and regulations related to information security. Later in our study, we choose to limit ourselves to Normen (The Norwegian Directorate of eHealth, 2020, 21. April), along with its supporting factsheets (The Norwegian Directorate of eHealth, (n.d.)), as these contained the information we needed.

4.3.3 Collecting data about actual actions

This is step six in the Kolkowska et al. (2017) paper. However, we decided to gather and analyze data from actual actions before returning to investigate further the values behind the prescribed ISAs (steps six & seven). In hindsight, it was a wise move to prioritize gathering data from the nursing personnel as early as possible in our study, as the outbreak of the Covid-19 virus pandemic would most likely put a severe halt to our data collection past March 12th.

This step ideally consists of two substeps, (a) and (b), but since we were not doing observations, our only goal here was step (a), interviews with policy users. From our initial interview with a nurse, the previous semester identified important tasks and daily routines and what they want to achieve by doing it. In early 2020 we made many visits to the hospital in Kristiansand and interviewed our candidates from late February to early March. Our intension was to try and capture the user rationale behind their actions. The semi-structured interviews lasted between 30 to 45 minutes and were conducted with both of us present in the room. One of us was leading the interview, and the other was taking notes and keeping an overlook of the session as a whole. In addition to keeping the time and taking notes, this supporting interviewer helped by providing follow-up questions and making sure the main interviewer did not forget or dwell on any topic. All twelve interviews were recorded and transcribed.

4.3.4 Interviews with the policy responsible

After completing the data collection from nursing personnel on March 10th, we focused mainly on doing the analysis of the previous step (6). During this time, we were in contact with the information security manager at the hospital, and we planned for a Skype meeting to get a better understanding of the intentions and goals of the prescribed policies and the underlying values they are based on. For this virtual interview, we discussed policies related to the five situations we present in this master thesis. The interview consisted of both researchers, the information security manager (A1), and an ICT-

advisor (A2), and lasted for 50 minutes. We had previously met both interviewees at their offices in Kristiansand and done a small pre-study the prior semester, and this helped ensure the virtual meeting run smoothly as our professional relationship was already established. This interview was semi-structured but with plenty of room for discussion planned. We established an open dialog and discussed prescribed ISA to the related situation, before moving on to the next ISA for discussion. The Skype interview was audio-recorded, and later it was transcribed.

Subjects	Duration
A1	1:04:29 48:18 1:01:04
A2	47:42 48:18 1:01:04
A3	28:24
N1	44:28
N2	39:38
N3	42:35
N4	35:55
N5	30:00
N6	42:56
N7	45:46
N8	46:53
N9	33:26
N10	30:05
N11	33:01
N12	31:00

Table 1: Overview of interviews

The table above shows all the interviews that were conducted during this study. A total of fifteen individuals participated. We did three rounds with interviewees A1 and A2, as these were the ones working with the information security policies. This data collection process created a sound basis for further analysis of the empirical data gathered. The process of analysis is shown in the following subsection, 4.4 data analysis.

4.4 Data Analysis

In this subsection, we present how we analyzed the data collected from the previous chapter. This is based on steps 3, 5, 7, 8, and 9, of the Value-Based Compliance method from Kolkowska et al. (2017).

4.4.1 Identifying prescribed actions

As we investigated the collected documents, we took notes of concrete guidelines and paired them together with other texts and policies describing similar topics. A list of “do’s and don’ts” was assembled. It took some analyzing to understand and differentiate between the ISAs on our complete list. Around thirty prescribed actions were first identified before we grouped them into what we called “situations.” A situation could, for example, be related to “users sharing passwords.” Then we put the ISAs regulating password sharing into this group. This situation-based later helped us when we were interviewing the persons responsible for the policies. A total of fifteen situations were developed and became instrumental in conducting the interviews. Lastly, we translated the situations into English, with support from the hospital’s webpages and online

dictionaries. See Appendix 10.2 for the interview guide that led our dialog with the information security manager.

4.4.2 Identifying actual actions

For this step, we analyzed the data gathered from nursing personnel, comparing and grouping findings into a list of actual ISAs. The qualitative data analysis software, NVivo, was used to code and assisted us in keeping a systematic record of all the gathered data. While the transcribing of the recorded interviews was done individually, the coding and analysis were done with both of us present. When doing analysis, we quickly noticed that sometimes we looked at the same thing, but had a different view, a different interpretation. We then discussed and re-listened to the recording of the interviews in question. A lot of the times, we uncovered additional meanings or interpretations by paying careful attention to the little things like the interviewee’s cadence, when re-listening to our recordings. From identifying the prescribed ISAs in step three, we already had a set of fifteen situations with prescribed policies, that we now could line up to fit with the actual user actions findings. See Appendix 10.1 for the interview guide on how we presented the situations to the nursing personnel.

4.4.3 Analysis of use and value rationale

This is where we derived goals and values from the identified ISAs. We re-read the transcripts and did further coding in NVivo, discussing between us two along the way. In our work, we looked for where the users chose to follow or ignore policies. Furthermore, we tried to uncover the reasons why or patterns for their actions based on the explanations provided during the interviews. Identifying user rationale was possible for most ISAs, but sometimes we encountered actions that were not related to specific rationales, like forgetting to lock a workstation when leaving it. Sometimes leaving a workstation unlocked was explained to be a rational decision (when the nurse planned to return to it shortly after leaving it), when this was mentioned, we could extract the goal of time-saving from the action as was often indicated during interviews. During interviews, we would follow-up on examples like this and get an answer to why the workstation was left unlocked. We did not get to conduct follow-up interviews to investigate further some of the actions that were not discussed enough in the interviews to derive something from them. Efficiency, quality of health care, and availability were the two values that we encountered to most in our analysis.

Code	Value
V1	It is important that information is confidential (Confidentiality)
V2	It is important to ensure accountability (Accountability)
V3	It is important to ensure information integrity (Integrity)
V4	It is important to protect the privacy of patients (Privacy)
V5	It is important to be efficient (Efficiency)
V6	It is important to have information available (Availability)
V7	It is important to ensure a high quality of health care (Quality of health care)
V8	It is important to be aware (Awareness)

Table 2: A list of values derived from actual and prescribed ISAs

The process from the empirical data based on interviews with nurses to the actual goals and values behind them can be described by an example below.

We started by presenting the situation, in this example, the shared user accounts and what we meant by this. We started with open questions such as “*is shared user accounts*

something that is in use here? Usernames and passwords that several employees have knowledge about.” This open-ended question made sure that the nurses could elaborate on whatever system they wanted. For example, regarding shared user accounts, we got information regarding a shared user account for surgery planning. *“In postoperative, we have a shared password for surgery planning, because the patients change so often that there is no time to log onto your computer, it is not enough computers for that either.”* (Interviewee, N3). Already based on this statement, we could extract the fact that there is no time to log onto your computer, which can be linked to the fact that it is not efficient to change users every time (V5).

However, we also included follow-up questions such as *“Can you say something about the goal, why the shared user is there?”*. That way, we could make sure that what was said earlier was what the nurse meant and if there were more reasons for the actual practice. In addition to the time-saving, there was also a vital purpose in coordinating the patients. *“The surgery rooms are not coordinated, so you need to monitor several patients at the same time, to know who is coming next and that it is enough nurses who can receive the patients.”* (Interviewee, N3). Based on these statements, we also included the value of having information available (V6), as the nurses valued having an easily available overview of the information of the patients they were taking care of, in this surgery planning system.

4.4.4 Analysis of prescribed ISAs and value rationale

Here we derived goals and values from the collected policy documents along with our transcribed interviews with the persons working with information security. We looked for confirmation or indicators in the text related to what the policies want to achieve. During our interviews, the three principles of the CIA triad (confidentiality, integrity, availability) were sometimes referred to by the information security manager. When this was the case, we then looked for other statements that could further confirm the statement. The result of this step was a list of goals and values that we grouped together with the existing list of situations and goals and values from the actual actions.

Code	Goal
G1	Knowing who documents what
G2	Only authorized personnel with access
G3	Limit registering errors and missing information
G4	Protect sensitive patient information
G5	Easy access to information
G6	Time-saving
G7	Improve future treatment and systems
G8	Learning from past mistakes
G9	Increased visibility
G10	Handle emergency

Table 3: A list of goals derived from actual and prescribed ISAs.

We include here an example of how we moved from the transcripts to goals and values. The example relates to our first situation, which is about authentication (Chapter 5.1). We presented our interviewees of statements from Normen, such as *“Do not share your password or username with anyone else”* (The Norwegian Directorate of eHealth, 2019, 16. August) and *“Lending the password to other people is not allowed.”* (The Norwegian Directorate of eHealth, 2019, 20. May).

We then asked our interviewees to elaborate on these statements and why these policies are in place and essential. Interviewee A1 stated that “*all actions performed must be linked to an authorized user; we must know that you are authorized.*” Moreover, that the employees can be held responsible for what is done on your behalf; “*we should have traceability.*” (Interviewee, A1). Based on these statements, we could extract the goals of knowing who does what (G1) and only authorized personnel with access (G2). Furthermore, we could link those goals to the value of confidentiality (V1) and accountability (V2).

4.4.5 Value-Based Compliance analysis

In this final step, we analyzed our data to understand compliance and/or non-compliance. First, we compared the actual ISAs with the prescribed ISAs to identify situations where there was a conflict. Then we compared the values and goals (rationality) behind the ISAs. This was presented in tables for details, and in figures for a visualization of the areas of conflict and support.

The outcome of these steps is presented in the following chapter, 5. Results.

5. Results

In this chapter, we present our empirical results based on interviews with nurses and information security workers as well as our document analysis. We organize the results around five key situations (authentication, information sharing, reporting, information access, and information protection). For each of the situations, we present a table that includes the prescribed ISAs with the source and the goals and values behind them based on empirical data from interviews. We also present a table of the actual ISAs of employees, along with their goals and values with connected interviewees who elaborates on the specific ISA. Furthermore, for each situation, we present a figure which shows how the prescribed and actual ISAs are connected to each goal and value and the supports and conflicts between them. However, the prescribed and actual ISA do not necessarily have a 1:1 relation. (e.g., P4 might not be related or the opposite to A4). At the end of this chapter, the results are summarized in a concluding subsection. In Appendix 10.1, you can get a glimpse into the other situations we investigated in our data collection.

5.1 Authentication

Table 4 below presents three prescribed ISAs; these have been included because of their importance. The prescribed ISAs are meant to cover shared user accounts for a variety of systems, like Windows login, DIPS, surgery planning, and others.

Prescribed ISA	Source	Goal(s)	Value(s)
P1: Do not share your password or username with anyone else	Normen Factsheet 27	G1: Knowing who documents what G2: Only authorized personnel with access G3: Limit registering errors and missing information	V1: It is important that information is confidential (Confidentiality) V2: It is important to ensure accountability (Accountability) V3: It is important to ensure information integrity (Integrity)
P2: Lending the password to other people is not allowed	Normen Factsheet 31	G2: Only authorized personnel with access	V1: It is important that information is confidential (Confidentiality) V2: It is important to ensure accountability (Accountability)
P3: Shared user accounts should not be used in applications with health and personal information	Normen Factsheet 31	G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)

Table 4: Authentication (Prescribed)

For this situation, we distinguish between sharing passwords and usernames at all times and lending it to a colleague for a one-time job. We also differentiate between Microsoft Windows login and other systems that contain sensitive patient information. All of the accounts are supposed to be personal for every system so that you can trace the actions back to a user and log the data. Interviewee A1 also stated that this applies when lending away accounts, *“You get can be held responsible for what someone else does on your behalfs.”* (Interviewee, A1). In general, the purpose is to make sure only authorized personnel can read and register information, meaning a basis of treatment. This is especially prohibited for systems that contain patient information, such as DIPS. However, the use of shared user accounts for Windows login is something that is used, as you don’t get access to sensitive information. *“There is a possibility that they have a collegial acceptance as the computer already was open, but formally it is a deviation.”* (Interviewee, A1).

In table 5 below, we present findings from our interviews with nursing personnel. The actual ISAs describe situations where shared user accounts are used. We also show the goals and values behind the non-compliance of the prescribed ISAs.

Actual ISA	Interviewee(s)	Goal(s)	Value(s)
A1: Shared user account for surgery planning	N3, N6, N7 & N8	G5: Easy access to information	V5: It is important to be efficient (Efficiency) V6: It is important to have information available (Availability)
A2: Shared user account for MetaVision in the medicine room	N9 & N10	G5: Easy access to information	V5: It is important to be efficient (Efficiency) V6: It is important to have information available (Availability)
A3: Lending user-login for the patient transport booking system	N2 & N4	G6: Time-saving	V5: It is important to be efficient (Efficiency) V7: It is important to ensure a high quality of health care (Quality of health care)

Table 5: Authentication (Actual)

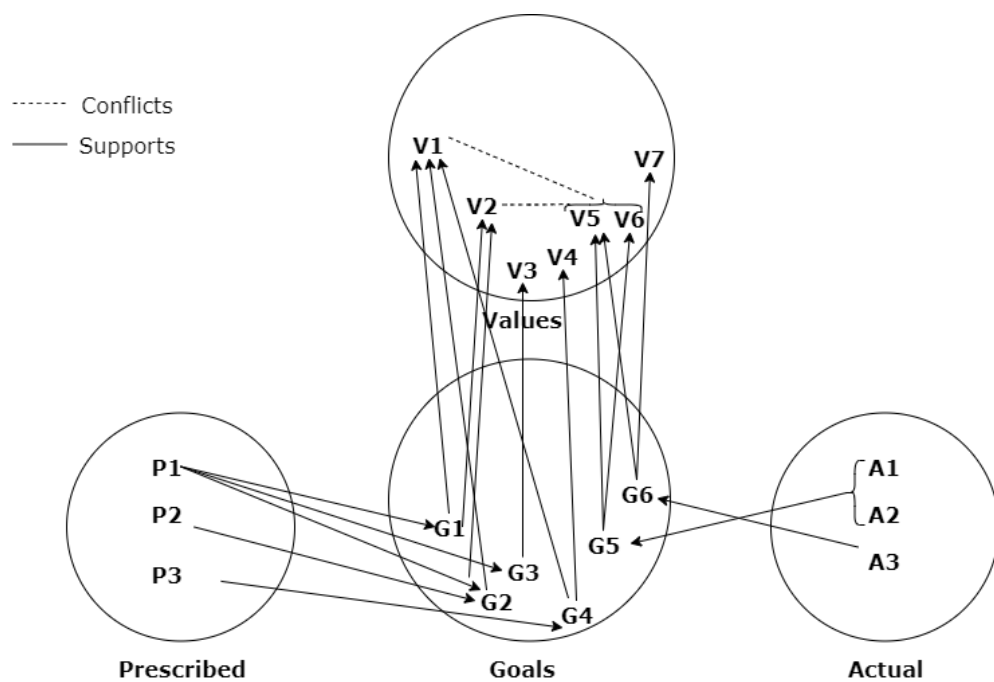
When interviewing the nurses about the shared user accounts, there were three areas that used shared accounts; surgery planning, MetaVision, and patient travel booking. In the postoperative department, several nurses told us that a shared user is used for surgery planning. This account has limited access, however earlier, they had more access and could look up sensitive information. The access has recently been more restricted, which has had a negative impact on the practical nurse work (Interviewee, N6). This was further confirmed: *“I can only see the surgery planner, but I can’t check information on the*

individual patient and read information about them. Then I must log in to my personal account." (Interviewee, N8).

Interviewee N3 also confirmed the use of shared users and added that this computer is located behind the reception desk, so it is not easily accessible for patients, next of kin, or any other visitors. Furthermore, in the postoperative department, there is a rapid patient flow of patients coming in and out that changing user accounts takes up too much time. Having easy access to the surgery planner also helps the coordination of the patient flow (Interviewee, N3).

The situation with MetaVision was also like the use of shared accounts for surgery planner. The computers which were used for this were behind locked doors in the medicine rooms where only authorized personnel has access. MetaVision was introduced 24 hours before our interview, so it was challenging to have a definite opinion on this system yet. However, the first impression for the use of shared accounts was to ensure easy accessibility and to save time (Interviewee, N9, and N10).

Regarding the third situation, ISA A3, this is a system that nurses use to book travel to get patients home from the hospital. Unless the user does not change its password within 90 days, the account gets locked. Interviewee N2 states: "*Then it's like we ask if anyone has an active user, e.g., at a hectic evening shift, it takes time to call the office and get it fixed.*" In the patient travel booking system, just basic information about the patient is disclosed, like name, address, and if the patient has an exemption card for public health services. Getting the patient home, after finished treatment, is the intension for why nursing personnel might borrow each other's log-in (Interviewee, N2).



- Prescribed ISAs**
- P1:** Do not share your password or username with anyone else
 - P2:** Lending the password to other people is not allowed
 - P3:** Shared user accounts should not be used in applications with health and personal information.

- Prescribed ISA Goals**
- G1:** Knowing who documents what
 - G2:** Only authorized personnel with access.
 - G3:** Limit registering errors and missing information.
 - G4:** Protect sensitive patient information.

- Prescribed ISA Values**
- V1:** It is important that information is confidential (Confidentiality)
 - V2:** It is important to ensure accountability (Accountability)
 - V3:** It is important to ensure information integrity (Integrity)
 - V4:** It is important to ensure patient's privacy (Privacy)

- Actual ISAs**
- A1:** Shared user account for surgery planning
 - A2:** Shared user account for MetaVision in medicine room
 - A3:** Lending user-login for the patient transport system

- Actual ISA Goals**
- G5:** Easy access to information
 - G6:** Time saving

- Actual ISA Values**
- V5:** It is important to be efficient (Efficiency).
 - V6:** It is important to have information available (Availability)
 - V7:** It is important to ensure high quality of health care (Quality of health care)

Figure 3: Authentication.

Figure 3 shows the different prescribed- and actual ISAs, along with the connected goals and values for each. This figure shows the healthcare values such as efficiency (V5) and availability (V6), which tend to be prioritized over information security values such as confidentiality (V1) and accountability (V2) for given situations. The prescribed policies are created to know who documents what (G1), to make sure only authorized personnel has access (G2) and protect sensitive patient information (G4). As mentioned earlier in practice, nurses use shared user accounts for surgery planning and MetaVision. For these systems, several nurses use the same accounts, which conflicts with the prescribed ISAs (P1, P3). These solutions are related to having easy access to information and not login time with login and logout of systems. Another actual practice is related to lending user-login for patient transport systems to save time (G6), be efficient (V5), and ensure

high quality of health care (V7). After the treatment of patients, the nurses just want to make sure that the patients get home safely and efficiently, as this is the interest of the patients as well. This action is similar to shared user accounts for the other systems, that it also conflicts with confidentiality (V1) and accountability (V2).

5.2 Information Sharing

Table 6 below displays two prescribed ISAs that we found essential to cover situations where uncritical sharing of information might occur.

Prescribed ISA	Source	Goal(s)	Value(s)
P4: Professional secrecy also applies between health personnel	Normen Factsheet 27	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)
P5: Make sure that unauthorized persons do not listen when talking about patients with a colleague, on the phone or in a public place	Normen Factsheet 27	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)

Table 6: Information sharing (Prescribed)

At the hospital, there are policies to protect the patient information, precisely; the policies are about the protection of unauthorized access and the privacy of patients. The rules apply independently if the information is revealed through a computer screen, via verbal communication face-to-face or by a phone call (Interviewee, A1). A notable clarification here is that the professional secrecy also applies between health personnel, as you need a basis of treatment for the patient before you can discuss or reveal any related information (Interviewee, A1). *“After all, you can discuss on a general basis, and you can also present a picture, curve or graph and discuss with a colleague because you need a “second opinion”.”* (Interviewee, A1).

Actual ISA	Interviewee(s)	Goal(s)	Value(s)
A4: Nurses discuss patient information so other patients can easily listen to information	N2, N4, N5, N6, N7, N8, N10, N11 & N12	G6: Time-saving	V5: It is important to be efficient (Efficiency)
A5: Phone calls in the hallway or patient rooms	N2, N7, N8, N9, N10, N11 & N12	G6: Time-saving	V5: It is important to be efficient (Efficiency)

Table 7: Information sharing (Actual)

The actual practice of ISA A4 is one of the most acknowledged practices because of its natural appearance with double rooms, and even bigger groups of patients gathered together. As this is how the hospital organizes, other patients can listen to the information

this particular situation, there is tension with the time spent, for example, when moving the patient to another location (Interviewee, N8).

The same applies to phone calls in the hallway or patient rooms where the nurses just want to be efficient (V5) and not walk the extra steps needed to safeguard the information (Interviewee, N2). As a summary, this situation sums up as both a layout of the hospital and a decision problem. The layout makes it more challenging; however, there are still possibilities available for most of the specific situations.

5.3 Reporting

The following table nr. 8 shows two prescribed ISAs related to discrepancy reporting.

Prescribed ISA	Source	Goal(s)	Value(s)
P6: Discrepancies and incidents shall be reported in the discrepancy processing system	Normen Factsheet 27	G7: Improve future treatment and systems G8: Learning from past mistakes	V7: It is important to ensure a high quality of health care (Quality of health care)
P7: Look at discrepancy reporting as an improvement measure that allows you to learn from mistakes and change routines	Normen Factsheet 27	G7: Improve future treatment and systems G8: Learning from past mistakes	V7: It is important to ensure a high quality of health care (Quality of health care)

Table 8: Reporting (Prescribed).

We learned from studying Normen, along with the supplying factsheets, that discrepancy processing has the intension of being a tool for improvement by learning from prior mistakes (The Norwegian Directorate of eHealth, 2019). This was also the impression we were left with after our interview with administrative workers A1 and A2. When we asked the information security manager about what the goal behind the deviation reporting was, he stated: *“Yes, it is primarily for learning and improvement, and not expose employees non-compliance.”* (Interviewee, A1). In discrepancy reporting, it is essential to distinguish between reporting and the immediate action taken with the actions in the long run. For example, if the problem is recurring, you can change routines, procedures, or work methods (Interviewee, A1). *“... the sum of the little things, individually, it might not be a big deal.”* (Interviewee, A1). If there is a small problem recurring, this might end up being exposed as a big problem in the end. If these small discrepancies are reported several times, the sum of those might lead to changes and, hopefully, improvement.

Table 9 below contains the actual ISAs regarding reporting that was revealed to us during our interviews. This table shows the actual ISA along with the goals and values that relate to each ISA.

Actual ISA	Interviewee(s)	Goal(s)	Value(s)
A6: Not reporting small discrepancies	N2, N5, N6 N7, N8 & N9	G6: Time-saving	V5: It is important to be efficient (Efficiency)
A7: Claims to have good discrepancy reporting culture	N5, N7, N9, N10, N11 & N12	G7: Improve future treatment and systems G8: Learning from past mistakes G9: Increased visibility	V7: It is important to ensure a high quality of health care (Quality of health care) V8: It is important to be aware (Awareness)
A8: Just fix the incident rather than reporting	N2, N4, N7 & N9	G6: Time-saving	V5: It is important to be efficient (Efficiency)

Table 9: Reporting (Actual).

The use of the discrepancy reporting system had a variety of different answers and views during our interviews. One of the leading practices is that small discrepancies might get down prioritized due to time constraints (Interviewee, N2, N6, N8, N9). “[It is] often a lot easier to just fix the problem rather than writing discrepancy reports” (Interviewee, N9). Actual ISA A6 and A8 are connected as there are often the small and the not that severe discrepancies that are just being fixed. “My perception is that if the patient is injured, the vast majority report. If there is no harm to the patient, then I think some people spend time on it, but most do not.” (Interviewee, N6).

An important factor regarding discrepancy reporting was to increase the visibility of the busyness in daily work (Interviewee, N9, N10). “When we are busy, that is when the mistakes happen. To make that more visible, we should report, so that management notices this” (Interviewee, N9). Besides, reporting unwanted actions (discrepancies) has led to many improvements for the systems (Interviewee, N11).

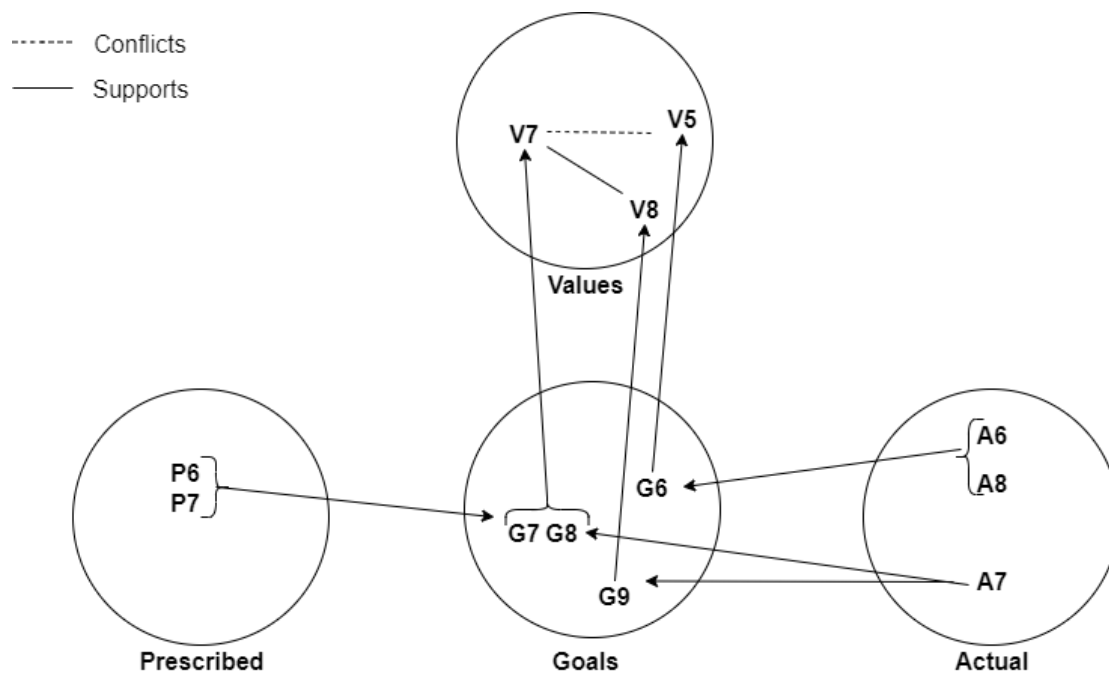


Figure 5: Reporting.

Figure 5 shows an overview of the situation called “reporting.”. The prescribed ISAs (P6 & P7) are created with the goals of improving future treatment and systems (G7) and learn from past mistakes (G8). These are both connected to an overall value at the hospital of ensuring high-quality health care (V7). “*Excellent and proper patient care is our most important task*” (Hospital of Southern Norway, 2016). On the other hand, we have the actual ISAs (A6 & A8), which are connected to time-saving (G6) and efficiency (V5). The practice of not reporting small discrepancies (A6) and just fixing it without reporting (A8) to be efficient (V5) conflicts with the value of high-quality health care (V7). The prescribed policies encourage you to report every discrepancy, but the actual practice is different as small discrepancies get skipped as the nurses want to be as efficient as possible.

For the last actual ISA (A7), this is connected to the same goals (G7 & G8) and value (V7) as the prescribed rules. Several of our interviewees said that the reporting culture was good at their department, which had resulted in changes and improvements in the systems (Interviewee, N11). This means that the actual practice (A7) and the prescribed rules (P6 & P7) support each other for this given situation.

Furthermore, this good reporting culture (A7) is also connected to increased visibility (G9) as one of the goals for the actual practice is to make the workload more visible for the management (Interviewee, N9, N10). This goal of increased visibility is created on the foundation of raising the awareness of various possible discrepancies and incidents. The increased awareness value (V8) is supported by the high-quality of healthcare (V7). We can, therefore, draw the conclusion that when you develop improved systems and learn from past mistakes, you create an environment with a higher quality of healthcare. Additionally, you also increase the awareness of the situations reported in on all levels in the organization.

5.4 Information Access

The following table 10 contains three ISAs that regulate the information access at SSHF, with the focus of always being authorized when you get access to information.

Prescribed ISA	Source	Goal(s)	Value(s)
P8: It is prohibited to read, search or acquire or use the information without justifying the patient's health care treatment	Normen Factsheet 27	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)
P9: All processing of personal data must have a legal basis	Normen (6.0)	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)
P10: You are not allowed to open your spouse, relatives or your own journal for no reason	Normen Factsheet 27	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)

Table 10: Information Access (Prescribed).

The prescribed rules are unambiguous for this particular situation as the hospital rules are clear and take care of the patient's privacy (Interviewee, A1). This was also further exemplified and clarified: *"You can not work in the maternity ward and search up information about a psychiatric patient."* (Interviewee, A1). Moreover, *"You can not search for a relative who is hospitalized in psychiatry, as you have no rights for that"* (Interviewee, A1). You need to have authorization and a legal basis to search for information about patients. These rules also apply for employees that want to search for their journal, as they have no rights for that either (Interviewee, A1). This is also a part of the training for DIPS, which is mandatory for everyone who uses it, and they get introduced for it from day one (Interviewee, A2).

The health worker's awareness regarding prying was further commented on by administrative worker A1.

It is a part of the training, it is a part of the Agreement of Confidentiality, and it is a part of the computer user agreement you sign, that you have read and understood it. And it is stated crystal-clear. (Interviewee, A1).

Being caught snooping can have severe consequences for your employment relationship. “We have had physicians that have been let go because of snooping.” (Interviewee, A1). With this seriousness in mind, we present our actual findings in table 11 below.

Actual ISA	Interviewee(s)	Goal(s)	Value(s)
A9: Very conscious of not to snoop or pry	N1, N6, N7, N8, N9, N10 & N11	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)
A10: Prepare for possible new patients	N3, N4, N5, N6, N7 & N8	G5: Easy access to information	V6: It is important to have information available (Availability) V7: It is important to ensure a high quality of health care (Quality of health care)

Table 11: Information Access (Actual).

Overall there was a mutual understanding across the hospital’s employees that snooping is not okay (Interviewee, N6, N9, N10, N11). We were also told that tales circulated the hospital, that might scare employees into compliance (Interviewee, N9, N11) along with the awareness of traceability and consequences (Interviewee, N6, N9, N10). This was a part of the foundation stones of duty of confidentiality and the job for health workers (Interviewee, N10). Besides, relatively recently, the patients can also check for who has read their journal, so it is even more transparent (Interviewee, N11).

Regarding ISA A10, there were quite a few of our respondents that noted that the strict rules on prying had some drawbacks when it came to not being able to prepare for new incoming patients. A common practice for patient logistics between departments is to read up on possible incoming patients to be prepared (Interviewee, N3, N6, N8). Searching for information about patients that have not been formally transferred to your department is not allowed, as you do not have the basis of treatment. On the other hand, knowing information about the patient beforehand is beneficial (Interviewee, N6 & N8) even if the patient is not transferred yet and might get canceled (Interviewee, N6).

The preparation part. i.e., if I know my patient is number six in the queue for surgery today, I can only access my patient, I can not see if surgery has started on patient number four ... So if my patient requires medicine administered one hour before surgery, I do not know when this “one hour before” is supposed to be. (Interviewee, N5).

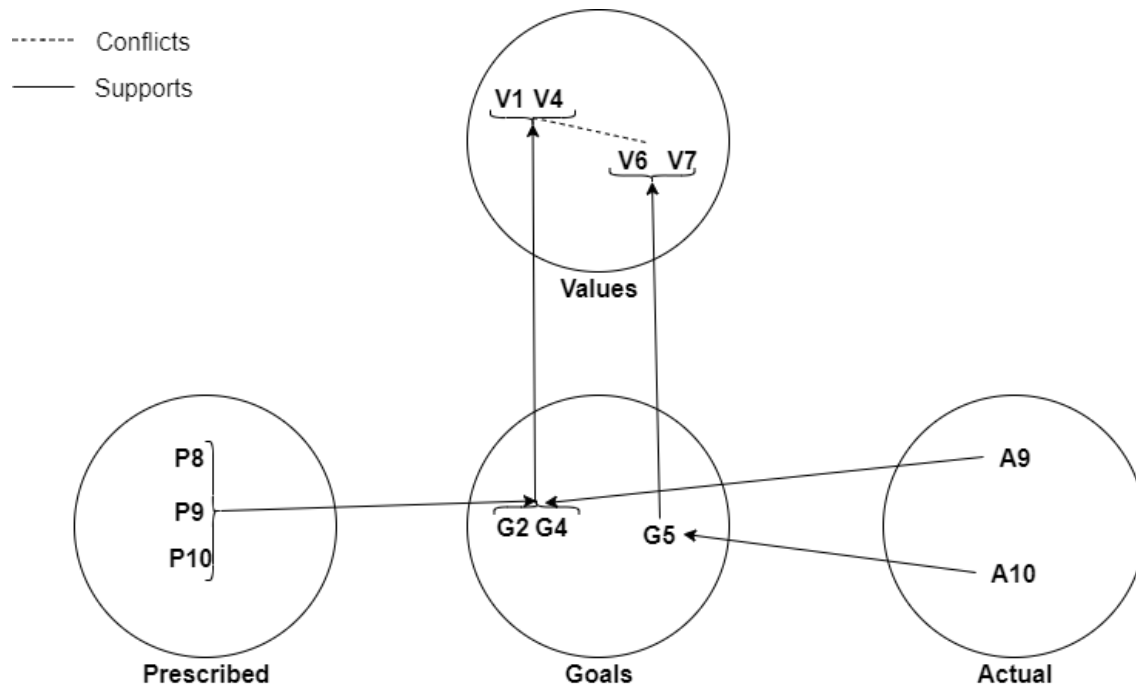


Figure 6: Information Access.

For the hospital, confidentiality (V1) and the privacy of patients (V4) are two essential building blocks. Consequently, the prescribed policies (P8, P9, P10) are created to protect the privacy of patients (G4) and make sure that only authorized personnel have access to information (G2). Based on our interviews, we also see that this is a part of the actual practice as well, and it is a part of the work responsibility (Interviewee, N10). Accordingly, the awareness of this topic shows that the prescribed- and actual ISAs are homogenous, with one exception: preparation (A10).

As mentioned above, preparation is a common practice among nurses. The nurses want easy access to information (G5) before the patient is transferred, to prepare for the treatment. That is based on the value of availability (V6) and the quality of health care (V7). The nurses want to be prepared when the patient arrives to deliver the highest quality, which is the best for both sides (Interviewee, N6). The actual practice of looking up patients not transferred (A10) and the prescribed policies create a conflict. However, this practice is not prying and just practical preparation (Interviewee, N8). We understand that this is just practical; however, according to the policies, this practice is in a gray area.

Lastly, we identified that actual ISA A9 has the same goals (G2 & G4) as the prescribed ISAs in this situation. Hence, support of the associated values V1 & V4 is then assured.

5.5 Information Protection

In the following table nr. 12, we showcase two prescribed ISAs that regulate information protection at SSHF.

Prescribed ISA	Source	Goal(s)	Value(s)
P11: You should always log off your PC, always lock the computer when you leave the workstation	Normen Factsheet 27	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)
P12: In case of absence from the workstation, and at the end of the workday, the user must log out of every system	Normen Factsheet 27	G2: Only authorized personnel with access G4: Protect sensitive patient information	V1: It is important that information is confidential (Confidentiality) V4: It is important to protect the privacy of patients (Privacy)

Table 12: Information Protection (Prescribed).

The prescribed rules of always locking computers (P11) were created to make sure only authorized personnel had access (G2). This applies when leaving the workstation (P11) and also at the end of the workday (P12). This is all connected back to always having an authorized user who performs the action (Interviewee, A1).

"... the policy's intension is that the PC shall be locked, having a screensaver that requires a password prompt before allowing the user back into the system." (Interviewee, A1).

We see the shared user-login (Information sharing) as a situation where the employee is more aware of the actions while leaving the PC unlocked (Information protection) is more a subconscious action. We can also differentiate the two situations by looking at the shared user accounts as a more organization-wide culture, while information protection is more on a personal scale. This distinction was also exemplified during the interviews with leaving the computer for a coffee- or toilet break, related to information protection.

Table 13 below shows the actions we uncovered while interviewing nursing personnel about their actual practices regarding information protection.

Actual ISA	Interviewee(s)	Goal(s)	Value(s)
A11: Patient journal system left unlocked	N1, N2, N3, N4, N6, N7, N11 & N12	G5: Easy access to information G6: Time-saving G10: Handle emergency	V6: It is important to have information available (Availability) V5: It is important to be efficient (Efficiency) V7: It is important to ensure a high quality of health care (Quality of health care)
A12: Using another colleague's (unlocked) user-session	N5 & N12	G6: Time saving	V5: It is important to be efficient (Efficiency)

Table 13: Information Protection (Actual).

We found numerous reasons why actual ISA A11 happened at the hospital. When the alarm bell sounds and calls for attention during an emergency situation, nursing personnel leave their workstations, to prioritize handling the emergency (G10) (Interviewee, N2, N3, N4 & N6) - in the heat of the moment, forgetting or not minding taking the time to lock the PC, leaving the patient journal system open. *“Usually, if I plan to leave, I lock it. But if the alarm sounds or someone asks me for something, I turn around and walk. Not logging out, so it happens quite often.”* (Interviewee, N4).

Actual ISA A12 can be exemplified as a worker using another colleague's user-session, typically when the colleague is not around but has left the system unlocked (Interviewee, N5 & N12). This is generally related to time-saving (G6) as our interviewee N12 told us: *“But of course, if you are just checking a quick small matter, it does take some time to log in. Then it is tempting to use an unlocked PC for just checking this one matter.”*

This was a practice that also the physicians practiced when they came for their doctor's round. Our impression was that the employees had some mixed feelings about this as they saw the practicality behind it, but also the risk of information being exposed to unauthorized personnel.

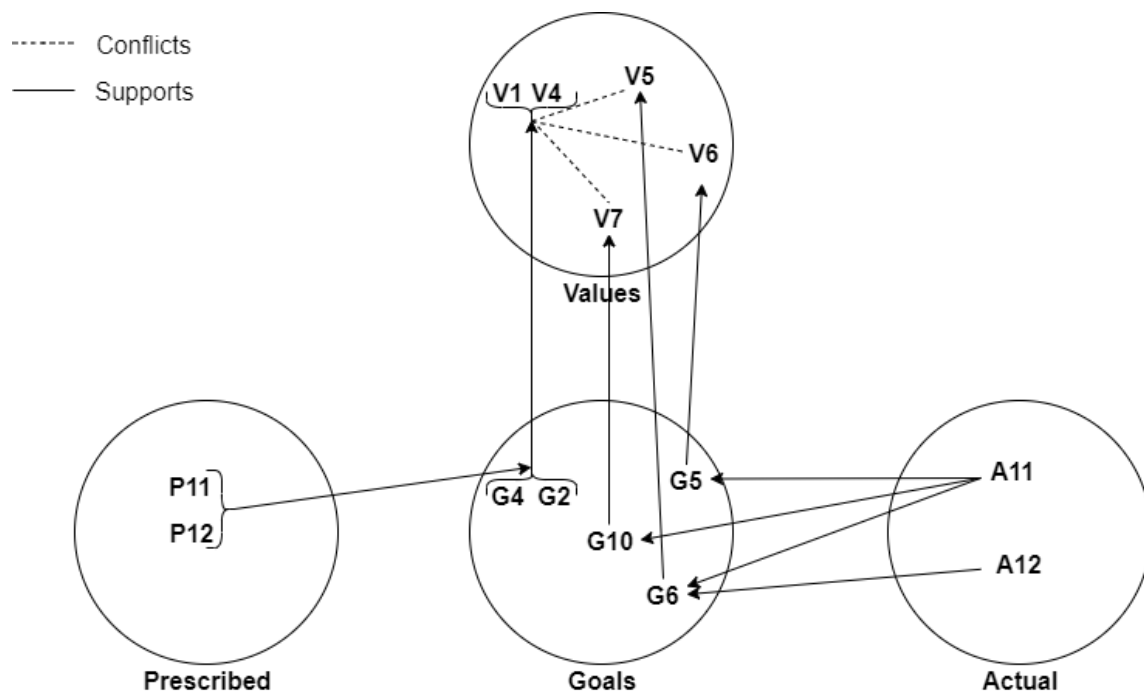


Figure 7: Information Protection.

Again we see the values of confidentiality (V1), and privacy of patients (V4) come forward as the values for the prescribed policies (P11 & P12). This emphasizes the importance of those and that all actions performed must be linked to an authorized user (Interviewee, A1). This situation is diverse and can have many different underlying values. Possibly the main reason is handling time-saving (G6) and the elemental value of efficiency (V5). Signing out of your colleague's account and signing in to your own user takes too much time (Interviewee, N6, N8, N11 & N12). "When the computer is unlocked, it is tempting just to check a small thing; but then, we often tell our colleague that we checked something on their login." (Interviewee, N12). This practice was also elaborated on by interviewee A1:

... due to the time aspect, it is easy to leave the computer without thinking twice. They probably have such a collegial acceptance that "I just used your login since it was already signed in." Formally, it is a deviation from the prescribed policies.

This creates a conflict between being efficient (V5) and having information available (V6) with the values of confidentiality (V1) and the privacy of patients (V4). Another detail that plays a significant role in the time aspect is emergencies and handling them (G10). When there is an emergency happening, it is easy to leave the computer and forget the buttons to lock the computer and rush to the location (Interviewee, N3, N4). The underlying value behind this is the importance of high-quality health care (V7). Leaving the computer unlocked and vulnerable, conflicts with prescribed policies' values of confidentiality (V1), and the privacy of patients (V4).

5.6 Summary of results

Our study focused on the understanding of underlying goals and values related to information security compliance in the hospital sector. The findings from the interviews were

categorized into 12 prescribed ISAs and 12 actual ISAs. These ISAs have been the basis for our result chapter and will be further discussed in the following chapter. We found that the hospital has strict policies to ensure high-quality health care and the protection of patient rights and privacy. Nursing personnel is overall very inline and compliant, and as such, support the value of high quality of health care (V7). However, we identified a recurring conflict between confidentiality (V1) and efficiency (V5). These results are in line with previous literature on the topic, which has looked into the values of different workgroups; we discuss this topic in chapter 6.2. We presented five specific situations related to health care practices and what type of actual ISAs that conflict with the associated prescribed policies. We present data about the rationality behind the actions of non-compliance with policies. In general, we see that the actual practice differentiates from the prescribed policies, which is not unusual. Based on the actual practice, we see that especially efficiency (V5) stands out as the most recurring value but also availability (V6) and quality of health care (V7). For the prescribed policies, confidentiality (V1) and privacy (V4) are highlighted. We see the nurses often want to be efficient and spend time with the patient to perform the treatment or service.

When exploring the value conflicts of information security in nursing practices, we also came across a couple of supporting values. In our situation related to reporting (chapter 5.3), we drew the conclusion that the prescribed ISA P6 & P7 had the same goal (G8) as we extracted from the actual ISA A7. This shared understanding of learning from past mistakes (G8), made for native support of the same value that it is important to ensure high quality of health care (V7). We also see support between awareness (V8) and ensure a high quality of health care (V7). Learning from past mistakes and being aware of them can influence the quality of the health care practice in the long run. Also, support was identified in chapter 5.4, when both prescribed and actual ISA had the same goals relating to information protection. This finding signals support with values V1 & V4 in relation to snooping.

At the hospital, different people work with different professions, in different phases with different intensity (Interviewee, A2). This reflects the information security awareness among employees (Interviewee, A2). This is also something we observed during interviews; some of the employees were slightly skeptical of being a part of the study, while others were quick to sign the agreement. After all, there is a shared goal of patient treatment, even for employees working with the economy, IT, or HR (Interviewee, A2). Overall, our impression is that the actual practices that violate the policies always have the intention to do what is best for the patient.

6. Discussion

In this chapter, we present lessons learned and discuss them with pre-existing literature. We choose to work with established theory, but we will compare results against other prior research that we also found to be relevant. The results from interviews will be discussed in light of previous literature and our research questions. We start by discussing the actual practice versus the prescribed policies with a focus on compliance. Next, we go on to debate the difference in view on information security between different groups. Third, we elaborate on how our findings and our modification on the Value-Based Compliance method compare with the original work on Value-based Compliance by Kolkowska et al. (2017) and Hedström et al. (2011). Finally, we end this chapter with a short concluding paragraph.

6.1 Compliance - actual practices vs. prescribed policies

The results from Bulgurcu et al. (2010) show that attitude, normative beliefs significantly influence employee's intention to comply with information security policies, along with self-efficacy to comply. We can draw lines to our findings and relate our results with their study. In our results, we interviewed each nurse alone and presented the situations and asked for actual practice. Based on the answers we got, we could compare goals and connect those with underlying values. The nurses interviewed do have a specific attitude, normative beliefs, and self-efficacy, which creates a basis for the goals and values in each situation. Based on our findings, we also see that the same values often are connected to the same group of employees. For example, prying, where next to all nurses told us this is not allowed and that prying is not a part of their job.

Using scenarios can help to reveal the differences in an employee's intention to comply with specific rules and regulations since these scenarios can provide detailed explanations about specific policies (Bulgurcu et al., 2010). In our study, we followed the VBC-method from Hedström et al. (2017), and we provided a detailed description of situations that were validated through information security managers and the first interviews with nurses. We presented the questions on a higher level with, for example, asking about the department as a whole and not on a personal scale. We did this to minimize the risk of employees concealing the truth because they see non-compliance as socially undesirable (Bulgurcu et al., 2010). Employees holding back the truth is definitely a possibility as talking about situations where they stray away from policies can be felt like exposing colleagues, themselves, or the department as a whole.

Bulgurcu et al. (2010) look at work impediments as a detriment for daily job-related tasks and that work impediment caused by compliance with ISP is positively associated with the perceived cost of compliance. This is in line with our findings as the nurses use shared user accounts under circumstances where the cost of compliance by, for example, waiting for the system to log out of their colleague's session and then relog into their user (Interviewee, N3, N5, N6 & N12). The nurses perceive the cost of being compliant with the related policies of not sharing accounts is high and that it acts as a hindrance. On the other hand, information security awareness has a negative influence on work impediments (Bulgurcu et al., 2010). When awareness is raised among the employees, the employees might not look at the policies as a work impediment anymore, because they now see the reasons behind it or the need for it. This result strengthens the importance

of creating a security-aware culture within the organization, which improves information security (Bulgurcu et al., 2010).

Routines for monitoring and controlling information security compliance is often developed on a top-down-approach, without sufficient inclusion of daily work practices (Hedström et al., 2011). Following the VBC method implicates that security officers should shift focus from looking for expected use and misuse of information systems, to focus on finding the actual use and misuse. People have been viewed as a problem in the information security context for a long time, which has led to the development of measures to enforce policies. We see, for example, Boss, S. R., Kirsch, Angermeier, Shingler & Boss, R. W. (2009), who argue that mandatoriness is effective in motivating the employees to follow the policies. Furthermore, Herath & Rao (2009), explores the role of penalties, pressures, and perceived contribution as motivating factors in information security behaviors. The results show that the normative beliefs regarding expectations of superiors or managers play an essential role in employees' behavior along with the behavior of other colleagues as well. They also argue that managers need to adopt mechanisms to investigate and evaluate the security performance of their employees by, for example, monitoring (Herath & Rao, 2009). A common denominator in these studies is the role of control-based compliance with sanctions and regulations to motivate the employees. We see the value of this type of approach; however, in the hospital sector, we argue that deterrence techniques might not be the best approach and that understanding the values and a more open dialogue might be more suited. Based on our empirical data, we can, for example, see that employees got scared away from prying into patient journals as "...We have probably been sufficiently frightened away from it" (Interviewee, N8), and "I think people are very conscious of not snooping because they know they can get tracked" (Interviewee, N11). On the other hand, nurses might end up in situations where workarounds might be appropriate as "*things work differently in practice.*" (Interviewee, N6). In total, having authority as a basis with an open dialogue that non-compliance might be accepted in some scenarios where severity is low or the health of patients is at risk.

6.2 Differences across job roles

In the article by Vaast (2007), "*Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare,*" a study was conducted at a hospital in a northeastern US city, with the goal of describing IS security from the point of view of different communities. "*Investigations aimed at studying the similarities and differences of representations of IS security by different occupational communities.*" (Vaast, 2007, p. 134). This is similar to what we did in a Norwegian context. Our selected two different professional communities were one, the nurses, and two, the information security officers in charge of enforcing the policies. We choose only two communities because of time constraints, and we managed to get an understanding of the ideas and concepts from the point of view of the persons involved. The health care sector includes many different occupational communities, like, physicians, nurses, technical workers; their training and daily practice vary, but they are still involved with patient care in one way or another (Vaast, 2007). From our study, we identified different underlying values between nurses' practice and the information security policies that are the responsibility of another occupational community, the information security workers. The tasks these two different groups perform on a daily basis vary to a large degree because of their

different job descriptions. We found that both groups value information security; however, the deeply-held health care values of the nurses will often take precedence within this particular professional community. The results from Hedström et al. (2011) also show that health care professionals choose to prioritize health care values over information security values under certain circumstances. This is also supported by our findings, which shows that the five situations presented, all have at least one conflict.

Vaast (2007) states that: *“Members of different occupational communities, faced by different contexts, engaging in various activities, and interacting with various parties, represent IS security in different ways.”* (p. 133). While we do agree with this statement, we find it to be a bit vague. Nurses and information security workers have different educational backgrounds, and we think a lot of the professional values are being shaped during those educational years of an individual. These occupational values are likely to be amplified when surrounding yourself with people with a similar background, peers, at a workplace. In our time at the hospital, we noticed a physical distance between the two groups, nurses in the treatment areas of the hospital, and the security officers in the more administrative offices. It seems natural to us that these different groups will have different values and representations of information security because of their diverse circumstances. Besides, not all groups perceive information security the same way, and health care practitioners base their actions on different rationalities when complying and not complying with information security policies (Hedström et al., 2011). In our results, we have shown that time-saving and the need to be efficient, could affect the information security negatively. By advocating the information security managers to include actual compliance actions will possibly lead to the health practitioners feeling like they are not just a part of their own occupational community but rather the whole organization's information security culture.

The view on differences between groups is also shown in the results from Albrechtsen & Hovden (2009) as they did a study on the different understandings between information security managers and users in regards to information security. They argue that from a socio-technical perspective, the difference in security skills, knowledge, perceptions of information security, social norms, and interpersonal relationships can result in differences (Albrechtsen & Hovden, 2009). This is something that reflects in our results by looking at individuals at SSHF; we got different answers from the interviews. This could be due to each individual having different security skills, knowledge, perception of information security, social norms, and interpersonal relationship.

In the study of Albrechtsen & Hovden (2009), they also found that the users did not realize the benefits of information security and that practicality and efficiency were more important for their work. This is indeed also supported by our results; we found results that showed that efficiency (V5), availability (V6), and quality of health care (V7) were valued over more information security-related values such as confidentiality (V1) and privacy (V4). The prioritization of health care workers' values over more information security values is shown in our results with specific examples and circumstances. Related to realizing the benefits of information security, an excellent example from our study is prying into patient journals. Based on our interviews, we found that prying is not accepted and that the nurses are very conscious of this topic (Interviewee, N1, N6, N7, N8, N9, N10 & N11). On the other hand, they also had a specific situation with preparation where the practicality trumps information security (ISA A10).

Albrechtsen & Hovden (2009) also argue that organizations and their stakeholders are living organisms and not stable, efficient, and predictable systems. They further elaborate on do not take into account human resources and values (Albrechtsen & Hovden, 2009). We see this as relevant for our study by taking into account the values of the actual practice in situations where non-compliance to policies are based on different values. It is essential to look into the reasons for non-compliance and not look at the policies as black and white. For example, in the hospital sector, the situations might vary each day, and the nurses might have good reasons based on values, for not complying with the more static policies. In practice, things work differently (Interviewee, N6). The policies will not be able to cover every possible scenario that nurses might end up in. We also saw based on our results that such differences exist.

They [policy workers] have no idea what an intensive care unit is... they do not have a real picture of how things are handled. I also think that we do not quite understand what they are thinking and why either. (Interviewee, N8).

As the results of Albrechtsen & Hovden (2009), we propose more significant interaction and dialogue between the groups to obtain this understanding.

6.3 Continuing the work on Value-Based Compliance

We will now look at Hedström et al. (2011) and Kolkowska et al. (2017) and point to similarities and differences with our own findings. The purpose of the 2011 paper was to create a new conceptual and practical tool to manage the tension between information security policies and the daily practice of information security by its employees (Hedström et al., 2011). It is argued that looking into and understanding the values and reflecting on those creates a secure information security environment. This is further exemplified with the situation of protecting and securing passwords, which are based on the prescribed values of confidentiality (V1), accountability, and integrity. However, the actual practice conflicts as the health care workers value care productivity and easy availability under these circumstances Hedström et al. (2011). These findings are also similar to our findings and support those. We found that making sure only authorized people had access to information (G2) and protecting the privacy of the patients (G4) were important in, for example, “uncritical of sharing information.” These goals belonged to the prescribed rules created by information security management, which was created on the values of confidentiality (V1) and protecting privacy (V4). On the other hand, based on our interviews, we found that under some circumstances, the goal of time-saving (G6) and the value of efficiency (V5) were prioritized. These findings go into detail on each situation and compare the prescribed and the actual ISAs. Overall based on our results, we see that confidentiality (V1) and privacy (V4) are the most dominant for the prescribed rules. For the health care workers' actual practice, we saw that efficiency (V5), availability (V6), and quality of health care (V7) were the dominating values. This is consistent with prior research by Hedström et al.: “*The prescribe rules related to patient information protection are based on confidentiality (v1), as found in the CIA-triad, while maximizing patient time (v3) and accessibility to information (v2) are values prioritized in daily health care practice.*” (Hedström et al., 2011, p. 381).

Our findings indicate that nursing personnel prioritizes their deeply-held professional values like ensuring a high quality of health care and maximizing time with patients. This aligns very well with Hedström et al. (2011). We interpret that the goal of time-saving (G6) and the value of efficiency (V5) are done in order to be able to spend the maximum amount of time with patients. This increased time dedicated to patients will likely lead to a higher quality of health care. Furthermore, we found that nurses are cautious about what they tell other colleagues regarding patient information; they might discuss cases but are careful not to reveal sensitive information. Also, nursing personnel is wary of not prying into patient journals that they do not have any legal treatment basis for doing. What is interesting is that the value of being effective does happen to come into conflict with the privacy of patients. As an example: a nurse is quick to respond to an emergency situation because she/he wants to ensure a high quality of health care. But in the process of getting to the action, leaves the workstation and patient journal system unlocked. In this situation, patient privacy is compromised. Now the likelihood of someone abusing this unlocked user-session is somewhat low, but nevertheless, the risk is still there. However, there are rules in the workstation system that ensure a lockdown of an inactive user account after a short period. So nursing personnel might argue and say that this is a risk they are willing to take. An important thing to keep in mind is that people react instinctively in the case of an emergency, and as such, nursing personnel might leave a workstation unlocked by a subconscious act.

The work of health care personnel is a highly time-critical practice, and the personnel holds strong professional values (Hedström et al., 2011). This can furthermore create an environment where the information security rules can operate under the risk of being ignored or the users create their own practice that is not that safe (Hedström et al., 2011). An example from Kolkowska et al. (2017) is: *"The pressure to treat as many patients as possible and the lack of technical solutions to support the pre-scribed ISAs means that staff felt justified in developing their own information-handling routines."* (p. 49). For our study, we found various actual practices that differ in safety level. For example, the use of shared user accounts in systems with a small amount of sensitive information (ISA A1, A2 & A3) or just fixing the incidents rather than reporting (ISA A8) is not really hampering the security. On the other hand, discussing information about patients over the phone or in hallways (ISA A4 & A5) or leaving the computer unlocked in the patient journal system (ISA A11) could have some more negative consequences. These practices created by health care professionals is based on the values of efficiency and availability, which can put the confidentiality and accountability at risk and indeed, the safety and privacy of patient information.

We distinguish our work from Hedström et al. (2011) in a way that, in their study, the focus was on conflicts only. *"We have chosen examples that, in a very clear way, illustrate value conflicts between prescribed and actual ISAs."* (Hedström et al., 2011, p. 377). In our work, we choose to also look into the supporting values as we think it is important to point to areas of alignment where the organization is doing good, not just show areas for improvement. We found three circumstances which had direct support, based on our empirical data. Giving credit where it is due will hopefully make the nursing personnel positive to be a part of organizational improvement programs. Furthermore, it is crucial to identify these supporting values to ensure that they will be preserved. Our study shows that the method and theory can be used for supports as well as conflicts.

6.4 Wrapping up the discussion

Overall, we found that the findings of our study are very much aligned with prior research. We see that nurses base their decisions on typical health care values and that the policies are built on security values. Under certain circumstances in specific situations, efficiency and time-saving are valued over confidentiality and privacy. When comparing the results to Hedström et al. (2011), we see many similarities, but we also show that the theory can be used for supports as well. We see comprehensible differences between the groups of professions and that the actual practice can vary from the written policies. There are indeed differences on individual levels because of security skills, social norms, perceptions of information security policies; however, employees from the same occupational communities are on the same wavelength. Creating an environment where both communities understand each group's values could improve the overall information security as well as open up for more cooperation. Following the VBC method could help get such insights into underlying values and goals.

7. Implications and future directions

In this section, we present the potential impact of the findings from our study. The first two subsections propose implications for research and practice. Then, the study's limitations are discussed. Finally, we conclude this chapter by showing possible directions for future research.

7.1 Implications for research

In the method chapter, we showed how we modified the method as we did not have access to observations. We developed the interview guides by adding detailed descriptions and examples of the situations we presented to the interviewees. Our results indicate that the method can be used without observations as a complementary part of the data collection. This shows that the VBC method can be used by other students who might not have the access level as for example, researchers or information security managers would be able to get. Nevertheless, as we also note in the limitations subsection (7.3), by not including observation as a data source, it is possible to miss out on some actual actions, and this is a drawback.

The VBC method was created as a tool for investigating the underlying values of why employees comply or not comply with information security policies (Kolkowska et al., 2017). For our study, we found it is natural to include supports as well as conflicts expanding the scope of VBC. Emphasizing supports could make the employees feel more positive towards revealing their actual ISAs when the VBC method is being used for internal assessments. Our expansion of the method can be further explored in future empirical studies that take such an inclusive approach covering both value conflicts and value supports.

Our interviewees confirmed all the situations that we developed as relevant situations in daily practice. By using the VBC theory, we showcase a rich approach to understanding the rationale behind employee compliance. We have provided insights that call for further exploration and explanation for understanding the employee's compliance rationale.

7.2 Implications for practice

Our results provide insights about the rationalities behind the actual practices of nurses. We present patterns or situations that the management team is not always aware of today. We also present a set of underlying reasons for the choices that nurses have for their non-compliance. These insights can be further used when developing policies allowing the management to see the viewpoint of nurses for specific situations. More interaction and dialogue are likely to improve each group's understanding of the work the other does and bridge the divide between them, making the security measures more effective (Albrechtsen & Hovden, 2009). Hopefully, our study will allow accessing the untapped potential of a better understanding of information security in the everyday practice of nurses by seeing users as resources instead of problems. Leading to a change in the old ways of thinking: *"Employees are still seen as the biggest obstacle to information security."* (Kolkowska et al., 2017, p. 51). Also, following the VBC method implicates that

security managers should shift focus to looking for the actual practices. Routines for monitoring and controlling information security compliance is often developed on a top-down-approach, without sufficient inclusion of daily work practices (Hedström et al., 2011). In our results, we have shown that time-saving and the need to be efficient, often affects the information security negatively. By advocating the information security managers to include actual compliance actions will possibly lead to the health practitioners feeling like they are not just a part of their own occupational community but rather the whole organization's information security culture.

7.3 Limitations

By using the VBC method without including the complementary observations, we base our results on documents and interviews only. By not including observations as a data source, it is possible that we missed out on additional ISAs, as some actual actions can be hidden or that the employees are reluctant when it comes to self-reporting. The natural scope-limit and time-constraint of doing a master thesis, combined with the sensitive hospital sector, made it necessary to exclude observations from our study. Moreover, our results are based on the interviewee's opinions and interpretations, with us as researchers added as an extra layer of interpretation.

In our study, we wanted to include a variety of nurses from various departments to get an overview of the hospital as a whole. This means that we included 2-3 participants from each respective department, which might not be sufficient to reflect the actual practice as a total. If we were to include more participants, we could be more sure that the results actually reflect the situation in the whole hospital. Following the VBC method, we provide a status, as per now, of the organization. We do not show how to improve information security practices. Nevertheless, as we identify areas where the actual actions of employees are in conflict with the prescribed policies, organizations get an overview of where to focus their efforts. We, as researchers, met little resistance in conducting our research at the hospital. All our interview candidates were forthcoming and seemed content to be a part of the study. However, security managers might find it harder to do such an investigation internally since the employees might feel like they are being "investigated" and therefore withhold some of the actual actions.

7.4 Future directions

Hedström et al. (2011) conducted their empirical study in the Swedish health sector and encouraged future research using the VBC in other countries. To our knowledge, this is the first time this method has been used in the Norwegian health sector, so we suggest that comparing the results from SSHF with other Norwegian hospitals would give fruitful results. This could be done by presenting the situations we used at another hospital and see if the values and actual practice presented matches. Another future direction could be to go deeper into SSHF and expand the participants to see if the results are current at the hospital as a whole. This could also further explore even more actual practice at SSHF, and here it would be vital to have access to do observations.

As proposed in Kolkowska et al. (2017), to have a look into if employees are willing to reveal their actual ISAs when information security managers collect the data as opposed to external researchers, and to see the VBC method used as an internal training

program, would be exciting. In order for this, an organization would have to carry out the VBC method on its own.

Another way forward would be to investigate how the new digital health-care system MetaVision that was implemented in early March 2020 has affected some of the ISAs, or to see if it has created new ones. During our interviews, we discovered that several of the candidates had experienced that this new solution requires several additional steps before registering patient information than the previously existing system. This type of registering is done many times a day and could possibly take up more time than the pen & paper system the hospital used before MetaVision. So it might be that the employees create some kind of workaround that could be in conflict with the prescribed ISAs in this situation.

For this study, we collected rich empirical material that we analyzed using the VBC theoretical lens. An interesting direction for future research would be to analyze the empirical material through dialectics. Dialectics are useful for understanding contradictions that pull in opposite directions (Moe, Newman & Sein, 2017) and can bring useful insights into the resolution of the challenging situations identified.

8. Conclusion

This study contributes to research on information security practices and builds upon the already existing stream of research of value-based compliance with a contribution of knowledge about the Norwegian health sector and its values. Our results are compatible with the findings in Hedström et al. (2011), as we find several conflicts between practice and actual ISAs. However, we did not only focus on conflicts but deemed identifying supporting actions as equally important in order to get a holistic view.

Our study shows empirical evidence that the VBC method can be used to look into conflicts and supports in concrete situations between prescribed and actual practice. We have furthermore explored the understanding of information security between health care professionals and information security management and that there is a difference in underlying values, based on job roles. Our results show that health care values, such as efficiency (V5), availability (V6), and quality of healthcare (V7), are predominant in the actual practice. Moreover, the typical information security values such as confidentiality (V1) and privacy (V4), are the underpinnings of the prescribed policies. The most recurring conflict is between confidentiality (V1) and privacy (V4), against efficiency (V5). Furthermore, we identified support between the goals and values of actual and prescribed actions in the situations of reporting (chapter 5.3), and in information access (chapter 5.4).

We want to point to implications for the practice of information security management and encourage the utilization of the VBC method for uncovering actual usage and misuse of information systems. Understanding the values of employees will help get insights into compliance with IS-security. Furthermore, we recognize that it could be a demanding task to carry out VBC in the organization, but we propose the method can be scaled down or adapted in order to be more accomplishable. The first execution of the VBC method could leave out doing observations, then at a later point, it then would be interesting to do a second execution where you include observations, and see if it has uncovered previously hidden ISAs.

After conducting this case study, we are left with the overall impression that the actual practices that violate the policies always have the intention to do what is best for the patient. Though, it is not ideal to live in contradiction, should you seek to resolve, or continue to live in conflict? To answer this, we have proposed different ways to do research on this topic in the future.

9. References

- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2), 179-211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289. <https://doi.org/10.1016/j.cose.2006.11.004>
- Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28(6), 476-490. <https://doi.org/10.1016/j.cose.2009.01.003>
- Argyris, C., Schön, D.A., 1996. *Organizational Learning 2. Theory, Method, and Practice*. Addison-Wesley Publishing Company, Reading, Mass.
- Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, 39, 396-405. <https://doi.org/10.1016/j.cose.2013.09.004>
- Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39, 145-159. <https://doi.org/10.1016/j.cose.2013.05.006>
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164. <https://doi.org/10.1057/ejis.2009.8>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548. <https://doi.org/10.2307/25750690>
- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, 447-459. <https://doi.org/10.1016/j.cose.2013.09.009>
- Creswell, J. W., & Creswell, J. D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage publications.
- D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658. <https://doi.org/10.1057/ejis.2011.23>
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98. <https://doi.org/10.1287/isre.1070.0160>
- Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207. <https://doi.org/10.1016/j.cose.2009.09.002>
- Dubé, L., & Robey, D. (1999). Software stories: Three cultural perspectives on the organizational practices of software development. *Accounting, Management and Information Technologies*, 9(4), 223-259. [https://doi.org/10.1016/S0959-8022\(99\)00010-7](https://doi.org/10.1016/S0959-8022(99)00010-7)
- Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics*, 60(2), 151-157. [https://doi.org/10.1016/S1386-5056\(00\)00115-5](https://doi.org/10.1016/S1386-5056(00)00115-5)
- Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user

- rationale. *Information Management & Computer Security*, 21(4), 266-287.
<https://doi.org/10.1108/imcs-08-2012-0043>
- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373-384. <https://doi.org/10.1016/j.jsis.2011.06.001>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125. <https://doi.org/10.1057/ejis.2009.6>
- Hospital of Southern Norway (2016, 30. November) Kvalitet og pasientsikkerhet. Retrieved from URL: <https://sshf.no/helsefaglig/kvalitet-og-pasientsikkerhet>
- Hospital of Southern Norway (2019). Om oss - Helseforetaket. Retrieved from URL: <https://sshf.no/om-oss#om-helseforetaket>
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.
<https://doi.org/10.1016/j.cose.2011.10.007>
- Jacobsen, D. (2015). *Hvordan gjennomføre undersøkelser?: Innføring i samfunnsvitenskapelig metode* (3. utg. ed.). Oslo: Cappelen Damm akademisk.
- Johnson, R. B. (1997). Examining the validity structure of qualitative research. *Education*, 118(2), 282.
- Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, 25(3), 231-251.
<https://doi.org/10.1057/ejis.2015.15>
- Karlsson, F., & Hedström, K. (2008). Exploring the conceptual structure of security rationale. In *WISP 2008, Dec. 13, Paris, France*.
- Kolkowska, E., Hedström, K., & Karlsson, F. (2009). Information security goals in a Swedish hospital. In *8th Annual Security Conference, 15-16 April 2009, Las Vegas, USA* (Article no. 16).
- Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, 26(1), 39-57.
<https://doi.org/10.1016/j.jsis.2016.08.005>
- Lincoln, Y.S., & Guba, E.G. (1985). *Naturalistic Inquiry*. Beverley Hills, CA: Sage.
- Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, 25(5), 433-463.
<https://doi.org/10.1111/isj.12043>
- Moe, C. E., Newman, M., & Sein, M. K. (2017). The public procurement of information systems: dialectics in requirements specification. *European Journal of Information Systems*, 26(2), 143-163. <https://doi.org/10.1057/s41303-017-0035-4>
- Myers, M. D., & Avison, D. (Eds.). (2002). *Qualitative Research in Information Systems: a reader*. Sage.
- Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17(1), 2-26.
<https://doi.org/10.1016/j.infoandorg.2006.11.001>
- Myyry, L., Siponen, M., Pahlila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An

- empirical study. *European Journal of Information Systems*, 18(2), 126-139.
<https://doi.org/10.1057/ejis.2009.10>
- Oates, B. (2006). *Researching Information Systems and Computing*. London: Sage Publications.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE.
<https://doi.org/10.1109/hicss.2007.206>
- Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership?. *Information Management & Computer Security*.
<https://doi.org/10.1108/09685221211267666>
- Schwartz, S. H., & Bilsky, W. (1987). Toward a universal psychological structure of human values. *Journal of Personality and Social Psychology*, 53(3), 550.
<https://doi.org/10.1037/0022-3514.53.3.550>
- Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 487-502.
<https://doi.org/10.2307/25750688>
- South-Eastern Norway Regional Health Authority (2019). Om oss. Retrieved from URL: <https://www.helse-sorost.no/om-oss#om-helse-sor-ost-rhf>
- Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276. <https://doi.org/10.1287/isre.1.3.255>
- Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22(6), 664-670. <https://doi.org/10.2307/2089195>
- The Norwegian Directorate of eHealth (2019, 20. May). Faktaark 31 – Passord og passordhåndtering. Retrieved from URL: <https://ehelse.no/normen/faktaark/faktaark-31-passord-og-passordhandtering>
- The Norwegian Directorate of eHealth (2019, 16. August). Faktaark 27 - Retningslinjer for daglig informasjonssikkerhet. Retrieved from URL: <https://ehelse.no/normen/faktaark/faktaark-27-retningslinjer-for-daglig-informasjonsikkerhet>
- The Norwegian Directorate of eHealth (2020, 21. April). Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. Retrieved from URL: <https://ehelse.no/normen/normen-for-informasjonsikkerhet-og-personvern-i-helse-og-omsorgssektoren>
- The Norwegian Directorate of eHealth (n.d.). Faktaark – ehelse. Retrieved 21.05.2020 from URL: <https://ehelse.no/normen/faktaark>
- Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of information systems security in healthcare. *The Journal of Strategic Information Systems*, 16(2), 130-152. <https://doi.org/10.1016/j.jsis.2007.05.003>
- Von Solms, B. (2001). Information Security—a multidimensional discipline. *Computers & Security*, 20(6), 504-508. [https://doi.org/10.1016/s0167-4048\(01\)00608-3](https://doi.org/10.1016/s0167-4048(01)00608-3)
- Weber, M. (1978). *Economy and Society: An outline of Interpretive Sociology (Vol. 1)*. Univ of California Press.
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii-xxiii.
- Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In *Information Security Management: Global challenges in the new millennium* (pp. 9-18). IGI Global. <https://doi.org/10.4018/978-1-878289-78-0.ch002>

10. Appendixes

10.1 Interview guide nursing personnel

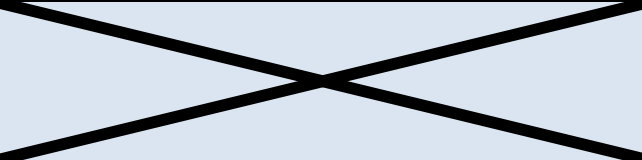
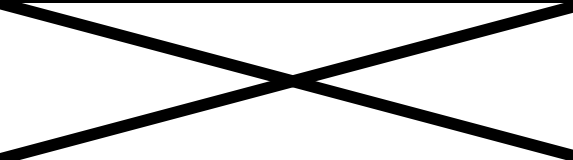
Jobb/Stilling	
Kandidat	
Dato	
Deltakere	

A. Oppstart av samtalen (5 min.)	
Spør om de har lest informasjonsskriv. Opplyse om prosjektet, spør om de lurer på noe?	Signer!
Forklare hva målet vårt er. For å lære. Hva vi har funnet fra litteratur når vi snakker om informasjonssikkerhet.	Infosystems. Digitalisering. Hvordan bruke teknologi på en best mulig måte. Vi er ute etter svar basert på din erfaring og hvordan du og dine kollegaer forholder dere til informasjonssikkerhet i hverdagen.
Kort om deg selv: Hvor lenge har du jobbet her?	

B. Spørsmål til kandidaten (20 min.)

<ul style="list-style-type: none"> a) Kort om hvordan er et skift organisert b) Hvem holder "morgenmøte" c) Er det en leder på hvert skift? d) Hvem er din nærmeste leder? e) Hvordan får du oversikt over hva som skjer, hvilke pasienter du skal behandle per. dag? f) Hvordan vil du beskrive informasjonssikkerheten blant ansatte her? 	<p>Spørsmål a – d, ble kun brukt i de innledende intervjuene.</p>
<ul style="list-style-type: none"> ▪ Sensitiv informasjon på lapp <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Enkle notater i lommen</p>
<ul style="list-style-type: none"> ▪ Lister med pasientinformasjon <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Henger til info på behandlingsrom. Lunsjrom. Med intensjon.</p>
<ul style="list-style-type: none"> ▪ Delt brukerinlogging <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Delt passord/brukernavn. DIPS</p>

<ul style="list-style-type: none"> ▪ Ikke logge ut/låse brukerkonto <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Kopp kaffe, toalettbesøk. Gå fra PC ulåst.</p>
<ul style="list-style-type: none"> ▪ Ikke godkjenne egne dokumenter før hjemreise <ul style="list-style-type: none"> ▪ Skjer dette? Ofte? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Godkjenne notater til en pasient.</p>
<ul style="list-style-type: none"> ▪ Godkjenne andres dokumenter ved vaktstart <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Henger sammen med den over.</p>
<ul style="list-style-type: none"> ▪ «Snoking» (informasjon om seg selv, eller familie) <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	
<ul style="list-style-type: none"> ▪ Behandle 2 pasienter før man registrerer informasjon i EPJ. <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Utsetter å registrere. Huske i hodet, eller lapp i lommen.</p>
<ul style="list-style-type: none"> ▪ 2 sykepleiere behandler samme pasient, på en samme bruker. <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Fører inn data om pasient samtidig.</p>

<ul style="list-style-type: none"> ▪ Ikke rapportere avvik <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Hvor lite avvik er det snakk som eventuelt ikke blir rapportert inn?</p> <ul style="list-style-type: none"> - F.eks. finne et ark på feil sted, legger det kanskje tilbake igjen bare
	
<ul style="list-style-type: none"> ▪ Ikke makulere sensitiv informasjon <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>F.eks. kastes i vanlig søppel</p>
<ul style="list-style-type: none"> ▪ Ukritisk deling av informasjon slik at andre kan overheøre (andre pasienter, kollegaer f.eks. på venterom). <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	
<ul style="list-style-type: none"> ▪ Bruke personlig mail til jobb relaterte dokumenter <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Er det mulighet for dette?</p>
<ul style="list-style-type: none"> ▪ Lagre sensitiv info i uautoriserte lokasjoner <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Legger igjen på møterom/behandlingsrom. Ikke på dedikert plass. Ulåst rom.</p>

<ul style="list-style-type: none"> ▪ Forsendelse av informasjon til feil person <ul style="list-style-type: none"> ▪ Skjer dette? ▪ Hvorfor? Målet bak dette? ▪ Hvorfor ikke? 	<p>Internpost, feil hylle.</p> <p>Tror du dette hadde blitt rapportert?</p>
---	---

<p>Avslutning (5 min)</p>	
<p>a) Er det noe som vi ikke har spurt om, som du mener vi bør vite før vi går videre i prosessen?</p> <p>b) Info om veien vår videre:</p> <ul style="list-style-type: none"> ▪ Tilgjengelig for spm. på mail ▪ Forslag til andre å intervju? 	<p>Var situasjonene greie å forstå?</p> <p>Selg prosjektet. Snowball.</p>
<p>Tid til spørsmål fra intervjuobjektet</p>	

10.2 Interview guide security manager

This guide was used for identifying goals and values from the prescribed ISAs. We asked the security manager to elaborate and explain the intention of the following policies.

S03 Delt brukerinnlogging

- Du skal ikke dele brukernavn og passord med andre (Ref. Faktaark 27)
- Alle brukere skal ha eget brukernavn og passord til alle systemer (Ref. Faktaark 27)
- Felles bruker-ID og passord skal ikke benyttes i applikasjoner med helse- og personopplysninger.
Med felles menes at to eller flere brukere deler den samme bruker-ID og passord. (Ref: Faktaark 31)
- Utlån av passordet til andre personer er ikke tillatt (Ref: Faktaark 31)
- Passordet er personlig og skal ikke deles med andre personer (Ref: Faktaark 31)

S04 Ikke logge ut av brukerkonto

- Man skal alltid logge av PC, lås alltid når du går i fra. Tips er også å bruke «Windows + L» (Ref. Faktaark 27)
- Ved fravær fra arbeidsplass og ved arbeidstidens slutt skal bruker logge ut av alle systemer (Ref: Faktaark 27)

S07 Snoking

- Du vet hva du kan og ikke kan lese (Ref: Faktaark 27)
 - Det er forbudt å lese, søke eller på annen måte tilegne seg eller bruke opplysninger uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift (Ref: Faktaark 27)
 - Ikke lov å åpne i ektefelles, slektningers eller din egen journal, uten grunn. (Ref: Faktaark 27)
- Det er ikke tillatt å søke etter informasjon man ikke har behov for eller ikke er autorisert for (Ref: Faktaark 27)
- Personopplysninger kan bare behandles når lovgivningen tillater det. All behandling av personopplysninger skal ha et lovlig grunnlag. I personvernforordningen kalles dette et behandlingsgrunnlag (Ref: Normen v.6)

S10 Ikke rapportere avvik

- Jeg vet hvordan jeg melder avvik (Ref. Faktaark 27)
 - Bruk avvikssystemet (Ref. Faktaark 27)
 - Se på det som et forbedringstiltak som gjør at man lærer av feil og kan endre rutiner (Ref. Faktaark 27)
- Avvik skal rapporteres i avvikssystemet (Ref. Faktaark 27)

S12 Ukritisk deling av informasjon

- Du vet hva og med hvem du kan dele pasientinformasjon (Ref. Faktaark 27)
 - Taushetsplikt gjelder også mellom helsepersonell (Ref. Faktaark 27)
 - Pass på at ikke uvedkommende lytter når du snakker om pasienter med en kollega, i telefon eller på offentlig sted (Ref. Faktaark 27)
 - Når du deler pasientopplysninger med andre må du forsikre deg om at vedkommende du kommuniserer med har rett til å få opplysningene. Mottar du f.eks. telefonsamtaler om pasienter, og du er i tvil om identiteten til innringer, kan du be om å få ringe vedkommende tilbake. (Ref. Faktaark 27)

- Vær forsiktig og ikke røp sensitiv informasjon (Ref. Faktaark 27)