Master Degree Project

UNIVERSITY OF SKÖVDE

Information Security in Healthcare

Security challenges and opportunities within integrated electronic health record systems

Erna Burdžović

Supervisor: Ali Padyab
Examiner: Rose-Mharie Åhlfeldt

Master Degree Project (60 ECTS) in Informatics
with a specialisation in Data Science/
Privacy, Information and Cyber Security
15 ECTS
Spring term 2022

ABSTRACT

In recent years healthcare industry has been rapidly changing towards digital solutions and migrating from paper-based systems to electronic health records (EHR) systems. Digitalisation within healthcare and EHR systems has brought many improvements in healthcare. However, digitalisation has also brought a lot of challenges and security risks. In 2017, the Region of Västra Götaland in Sweden decided to reorganise healthcare with an integrated healthcare record system, Millennium. As a result, patient information will be managed and communicated between various healthcare actors and organisations. Therefore, it is crucial to investigate the security challenges and opportunities with integrated patient record systems. To get insight into the security challenges and opportunities of an integrated patient record system, the following research question was formulated for the study: *What information security challenges and opportunities are there with an integrated electronic health record system on a regional level?*

To answer the research question and achieve the purpose of the study, a qualitative method with semi-structured interviews as a collection technique was chosen. The interviews were conducted with people responsible for the implementation of Millennium, a program owner, and a Data Protection Officer. As a result, the empirical data identified new opportunities and challenges. The conclusion drawn from the result is several security challenges and opportunities within integrated EHR. For example, some identified opportunities are easy to access medical data, equal healthcare, and improved healthcare patient safety. Finally, some identified challenges are a compromise of confidentiality, integrity, availability, and security breaches like hacking and unauthorised access.

Table of Contents

1 Introduction

In recent years healthcare industry has been rapidly changing towards digital solutions and migrating from paper-based systems to electronic health records (EHR) systems (Kandasamy et al., 2022). Digitalisation within healthcare and EHR systems has brought many improvements in patient care, for example, improvements in the diagnosis of diseases, accessibility of information, and even improvements in medical practices (Cresswell & Sheikh, 2015). However, digitalisation has also brought a lot of challenges and risks like information loss or disclosure and other types of cyberattacks and security breaches (Kandasamy et al., 2022). Even if healthcare digitalisation offers many advantages, as with any other digital solution, breach of privacy and violation of integrity, confidentiality and availability of health information are some of the risks associated with healthcare digitalisation (Madhavi & Lincke, 2018).

Information is critical in supporting healthcare providers to deliver care and carry out their activities. Therefore, it is crucial to keep this information safe and minimise security risks. Information security in healthcare is extremely important. In healthcare, sensitive personal data is handled, and knowledge about information security is needed to protect confidential and sensitive data from unauthorised access (Åhlfeldt, 2008).

As previously mentioned, the healthcare industry has been rapidly changing towards digitalisation, which is also the case in the Region of Västra Götaland in Sweden. In 2017 the regional council decided on a common strategy for reorganising healthcare with integrated systems where patient information will be managed and communicated between various healthcare actors and organisations, called Framtidens vårdinformationsmiljö, FVM (Eng. The healthcare information environment of the future). Today's healthcare environment contains many different systems that cannot communicate with each other, which causes problems with sharing information between specialist healthcare, primary care, municipal healthcare, and private care providers. As a result, the information is available but cannot be accessed by everyone who needs it. The objective of FVM is to offer accessible healthcare with high quality and to enable patient participation. The central part of FVM is the new integrated electronic health record system Millennium, which will contain all vital patient information and allow access to the information to all necessary actors (Vårdskiftet, 2021b).

An electronic health record (EHR) system is defined as "an electronic record of healthcare information of an individual that is created, gathered, managed, and consulted by authorised clinicians and staff across multiple healthcare organisations" (Jacob, 2020, p. 37). EHR contains a lot of information generated by one or more healthcare providers, including information regarding patients' medical history, physical examinations, treatments, patient demographics, progress notes, problems, medications, vital signs, past medical history, immunisations, laboratory data, etc. (Alshalali et al., 2018; Menachemi & Collum, 2011).

1.1 Problem Description

When the new integrated electronic health record system Millennium is established, as much patient information as possible will be shared, and Millennium will deal with highly sensitive information. Therefore, the work with patient information needs to meet information security requirements to reduce the risks associated with healthcare digitalisation. According to Haggerty (2017), increased healthcare digitalisation has made preserving data and information security challenging. Security breaches in the privacy of patients' medical records can result in multiple negative impacts. Therefore, patients' information must always be adequately protected, and information security must be considered. Despite these challenges, as FVM and integrated healthcare systems are developing, new opportunities arise, such as the availability of information and easy access (Vårdskiftet, 2021b). A wide range of research studies focus on data and information security, identifying security and privacy challenges (Cresswell & Sheikh, 2015; Kandasamy et al., 2022; Shrivastava et al., 2020). Despite the extensive research in the field, implementation of digital technology in healthcare often fails due to various security challenges, especially when involving patients. These challenges should be acknowledged to preserve patient security (Rachmani et al., 2021).

"Electronic medical records and patient data sharing are critical and considered core healthcare issues. How to store patient's information securely, how to access the information and how to ensure the privacy of patients when sharing medical data among several health service providers or agents are critical considerations." Electronic medical record systems face several security issues that need to be addressed (Alshalali et al., 2018, p. 760). According to Vårdskiftet (2021a), patient safety is the focus of FVM and Millennium, and continuous work with information security is in progress to preserve it. Therefore, for FVM, it is crucial to get a proper insight into information security aspects to implement the integrated patient record system Millennium in a patient-safe manner. Millennium is interesting to study because it brings new aspects such as integrating all relevant systems. In addition, Millennium will contain all vital patient information and allow access to the information to all necessary actors, which brings new security challenges and new opportunities.

It is important to study opportunities with integrated electronic healthcare record systems as well. For example, Alshalali et al. (2018) explain that electronic health records provide opportunities to enhance patient care. Some of these opportunities include being able to access medical data needed for patients' treatments easily and being able to share and exchange health information with necessary actors. In addition, Cashman et al. (2021) explain that integrated electronic health record facilitates a safer and more efficient healthcare service.

According to the mentioned problem description, this work aims to investigate the information security challenges and opportunities with an integrated patient record system on a regional level.

1.2 Research Question

To get insight into what security challenges and opportunities there are with an integrated patient record system, the following research question was formulated for the study:

What information security challenges and opportunities are there with an integrated electronic health record system on a regional level?

Healthcare information must be accessible to all necessary actors to provide qualitative healthcare, and at the same time, the healthcare information must be secured. Answering the research question, information security challenges and opportunities with an integrated electronic health record system will be provided. The expected answers to the research question can contribute to further research. Further, the answers can benefit the developers of integrated electronic health record systems to understand what challenges and opportunities related to information security exist. Moreover, the expected results can help developers know what to consider and focus on when developing integrated electronic health record systems. Finally, the answers can benefit the project Millennium to identify information security challenges and opportunities because Millennium is the primary example in the research.

1.3 Delimitation

To avoid the study becoming too large, it will be limited to examining only information security challenges and opportunities with an integrated electronic health record system on a regional level. The study will focus on integrated electronic health record systems, with Millennium as the leading example. The study will be limited to a regional level and will include opinions of security officers for municipality and region, system designers, security officers responsible for the planning, and likewise. In the study, the patients' perspectives will be excluded.

1.4 Thesis Structure

Chapter 1 introduces the chosen topic together with a problem description, research question and delimitations. In Chapter 2, the reader will find the research background about healthcare digitalisation and information security in healthcare and electronic health record systems. Further, in Chapter 3, the research method will be described, and the implementation of the selected research methods will be explained. In Chapter 4, the results from the implementation of the methods will be described and analysed. In addition, Chapter 5 will provide a discussion of the results concerning the previous research, implementation approach, and ethical and societal concerns. Finally, Chapter 6 will summarise and conclude the work.

2 Background

This chapter presents a scientific background about healthcare digitalisation and information security in healthcare and electronic health record systems. Key concepts of the chosen subject area are explained to provide a deeper understanding of the subject. Firstly, healthcare digitalisation is generally described, followed by a description of information security in healthcare. After that, information security in electronic health record systems, including security challenges and opportunities, is described. Finally, the Swedish Framtidens vårdinformationsmiljö with a focus on Millennium is explained.

2.1 Healthcare Digitalisation

In recent years healthcare industry has been rapidly changing toward digital solutions and mitigating from paper-based systems to electronic health records (EHR) systems (Kandasamy et al., 2022). According to Cresswell and Sheikh (2015), EHR has brought a lot of improvements in patient care, diagnosis of diseases, accessibility of information, and even improvements in medical practices. Digitalisation in healthcare can be applied to store, manage, and transmit data, including electronic and personal health record systems containing patient data. This data can be accessed by patients and professionals for several purposes and can support effective patient care. Further, healthcare digitalisation can be used for decision support, for example, electronic decision support systems that provide diagnostic and treatment advice. Moreover, healthcare digitalisation enables remote communication between healthcare professionals and patients (Cresswell & Sheikh, 2015).

Digitalisation in healthcare has increased notably, and the use of electronic patient record systems has become an everyday occurrence for healthcare providers (Blix & Levay, 2019, p. 8). Recently, the covid-19 pandemic has motivated healthcare to evolve towards digitalisation even more by enabling non-stop virtual care service and real-time support to minimise physical examinations. In addition, the increased digitalisation allows healthcare providers to be accessible remotely via webinars, hotlines, and even live video interactions (Maki et al., 2022).

However, digitalisation has also brought a lot of challenges and risks like information loss or disclosure and other types of cyberattacks and security breaches (Kandasamy et al., 2022). Even if healthcare digitalisation offers many advantages, as with any other digital solution, breach of privacy, confidentiality and availability of health information are some of the risks associated with healthcare digitalisation (Madhavi & Lincke, 2018). Healthcare digitalisation aims to improve the quality of medical treatments and patient care. In addition, the goal is also to improve the accessibility of patient care. One way to reach the mentioned goals is to implement electronic health record systems (Cresswell & Sheikh, 2015), which will be discussed later in this chapter.

2.2 Information Security in Healthcare

Information is critical in supporting healthcare providers to deliver care and carry out their activities. Therefore, it is crucial to keep this information safe. Whitman and Mattord (2011, p. 8) define information security as the protection of the "confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission". Further, the authors explain that it is achieved by applying policy, education, training and awareness, and technology. In addition, the National Encyclopedia explains that information security focuses on the information that data represents and the need for protection from that perspective. Further, information security refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection (Nationalencyklopedin, n.d.).

Further, information security ensures guidelines for organisational information security standards and information security management practices, including selecting, implementing, and managing controls considering the organisation's information security risk environment. Information security includes security issues in all sorts of information processing, and its goal is to protect information assets, aiming to achieve confidentiality, integrity, availability, and accountability. Confidentiality means that information should only be available to authorised users, but it should not be too difficult to access. However, it should still be protected from those who do not have access to it. Integrity is about ensuring that information has not been changed unauthorised, by mistake or due to a malfunction. Availability means that the information should be consistent and accessible for authorised parties when needed. Finally, accountability is the ability to trace performed activities to a user (ISO/IEC 27002, 2013).

Information security in healthcare is extremely important. In healthcare, sensitive personal data is handled, and knowledge about information security is needed to protect confidential and sensitive data from unauthorised access. "The main purpose of information security in healthcare is to achieve the two important aims, patient safety and patient privacy" (Åhlfeldt, 2008, p. 35). Further, Åhlfeldt (2008) explains that patient safety means giving patients the best care with the right information at the right time, and patient privacy means protecting sensitive patient information from unauthorised access. Therefore, preserving confidentiality, integrity, availability, and accountability is crucial for achieving patient safety and patient privacy (Åhlfeldt, 2008).

2.3 Information Security in Electronic Health Record Systems

An electronic health record (EHR) system is defined as “an electronic record of healthcare information of an individual that is created, gathered, managed, and consulted by authorised clinicians and staff across multiple healthcare organisations” (Jacob, 2020, p. 37). EHR contains a lot of information generated by one or more healthcare providers, including information regarding patients’ medical history, physical examinations, treatments, patient demographics, progress notes, problems, medications, vital signs, past medical history, immunisations, laboratory data, etc. (Alshalali et al., 2018; Menachemi & Collum, 2011).

According to Kandasamy et al. (2022), medical data collected in EHR has a great value on the black market, making it attractive to gain access to it. Medical data breaches are often caused by cyberattacks, which pose a danger to patient data, “leading to patient information leakage, patient misdiagnosis, and mistreatment. The most common attacks are phishing scams and other forms of e-mail fraud” (Kandasamy et al., 2022, p. 6). Security concerns arise because healthcare data is potentially accessible by different users, which poses a threat to privacy. When sensitive medical data is uploaded to EHR it becomes available for attackers. Therefore, security measures are essential to protect sensitive medical information (Alshalali et al., 2018). Information security in EHR is important, and many healthcare organisations have implemented security policies that define how to produce, store, and use sensitive healthcare information. Security policies for EHR specify the access and the authentication for requested data, which protects the security of sensitive data. Furthermore, other countermeasures to protect healthcare data are education, training and awareness, and technology (Smaradottir, 2018).

2.3.1 Security Challenges

Digitalisation has brought a lot of challenges and risks like information loss or disclosure and other types of cyberattacks and security breaches. For example, transferring or sharing sensitive health data can lead to data breaches (Kandasamy et al., 2022). Even if healthcare digitalisation and electronic health record systems offer many advantages, as with any other digital solution, violation of privacy, confidentiality and availability of health information are some of the risks associated with EHR. Furthermore, security breaches like hacking and unauthorised access to sensitive information are becoming the main issues for EHR. Also, poor usability, functionality, and performance are examples of security challenges within EHR. Because of the mentioned risks, it is a real challenge to ensure the safety of the sensitive information that EHR stores (Madhavi & Lincke, 2018). As previously stated, there are a lot of concerns and challenges regarding the privacy and security of sensitive health data, and these challenges are the most significant barriers to implementing electronic health records that could also be integrated (Keshta & Odeh, 2021).

The mentioned concerns and challenges negatively affect the trust in electronic health records. For example, some studies show that many patients worry about the security of their data because "it had to travel through the internet". In addition, some patients believe that exchanging their health information poses risks to their privacy, which has negatively impacted their will to share their health information online with healthcare providers. These concerns have also negatively impacted patients' choice to give access to personal health information (Keshta & Odeh, 2021; Perera et al., 2011). Another study showed that because of these concerns, patients responded by refusing to provide their personal information to healthcare facilities, fabricating personal information, and even requesting the removal of their personal information. Further, patients responded by issuing complaints either directly to the medical facilities or a third-party organisation (Kuo et al., 2014). In addition, Smaradottir (2018) explains that health information documentation is sometimes challenging. The reason is that a lot of free text is used when documenting, and the most critical patients' information is not visible in the documents' overview.

Summary of the most common security challenges within EHR:

- Compromise of confidentiality, integrity, and availability (Madhavi & Lincke, 2018),
- Security breaches like hacking and unauthorised access (Madhavi & Lincke, 2018),
- Poor usability, functionality, and performance (Madhavi & Lincke, 2018),
- Gaining patients' trust (Patients' acceptance of EHR) (Keshta & Odeh, 2021; Kuo et al., 2014; Perera et al., 2011),
- Medical data documentation in free text (Smaradottir, 2018).

2.3.2 Opportunities

Significant benefits and opportunities can be achieved with healthcare digitalisation and EHR systems. For example, EHR is the primary entity for sharing and analysing medical information for decision-making and medical treatment (Smaradottir, 2018). Further, Carey et al. (2016) explain that integrated electronic health records are effective and have benefits such as cost reduction and improved healthcare quality. Other benefits are that integrated

EHR systems promote evidence-based medicine usage and help record keeping. According to Keshta and Odeh (2021), integrated electronic health records can improve efficiency and patient safety by reducing medical or medication errors. Keshta and Odeh (2021) explain that HRs can also benefit from EHR by saving costs and having a central place for providing medical data.

According to Kuo et al. (2014), EHR can enhance the quality of care and increase patient satisfaction while assisting providers in delivering a higher quality of care to their patients. Furthermore, Menachemi and Collum (2011) argue that some of the opportunities associated with integrated EHR include being able to access medical data needed for patients' treatments easily and being able to share and exchange health information with necessary actors. Similarly, Keshta and Odeh (2021) argue that EHR increases efficiency in health care delivery, which means that resources are not wasted, including supplies, equipment, ideas, and energy. Moreover, Menachemi and Collum (2011, p. 50) explain that the benefits of EHR include "increased utilisation of tests, reduced staff resources devoted to patient management, reduced costs relating to supplies needed to maintain paper files, decreased transcription costs, and the costs relating to chart pulls".

Summary of the most beneficial opportunities with EHR:

- Improving healthcare quality (Carey et al., 2016),
- Improving patient safety (Keshta & Odeh, 2021),
- Reducing medical or medication errors (Keshta & Odeh, 2021),
- Lowering costs (Carey et al., 2016; Keshta & Odeh, 2021; Menachemi & Collum, 2011),
- Increasing patient satisfaction (Kuo et al., 2014),
- Easy access to medical data (Menachemi & Collum, 2011),
- Increasing efficiency (Keshta & Odeh, 2021).

2.4 Healthcare Digitalisation in Sweden

According to Blix and Levay (2018), healthcare is one of the most extensive sections of the public budget, and Sweden is one of the countries that invest most in healthcare. Swedish healthcare is taking advantage of digitalisation. One example is "digitalisation makes it easier to use a technology that already exists, such as the self-dialysis at the Ryhov regional hospital in Jönköping, where patients receive ID cards and can control the times of their visits, exercising greater control over their treatment". Another example is that patients can use several mobile applications (e.g. Kry and MinDoktor) to communicate with the various healthcare providers, which improves patients' ability to control their treatments (Blix & Levay, 2018, p. 18). In connection with digital healthcare meetings, public and private healthcare providers have opened up online clinics, which have been a time saver for healthcare providers (Ekman et al., 2019).

Furthermore, Åhlfeldt (2008) explains that many different actors conduct Swedish healthcare, for example, public and private healthcare actors and home healthcare. To provide effective healthcare, all these healthcare actors and organisations need to interact with each other, including the patients. Therefore, one of the most central parts of Swedish healthcare is electronic health records.

Information security in healthcare is extremely important. In healthcare, sensitive personal data is handled, and knowledge about information security is needed to protect confidential and sensitive data from unauthorised access. Therefore, security requirements need to be followed when handling sensitive personal data in Sweden. The Swedish Civil Contingencies Agency (MSB), Swedish Authority for Privacy Protection and National Board of Health and Welfare have presented a strategy for information security in healthcare. This strategy aims to create conditions for healthcare to be conducted with the right level of information security to meet the needs of citizens, patients, and society for transparency, participation, patient safety, and personal integrity. Examples of security requirements that need to be followed are The Health and Medical Service Act and The Patient Record Act (MSB, 2014).

2.4.1 Framtidens Vårdinformationsmiljö and Millennium

The healthcare industry has been rapidly changing towards digitalisation, which is also the case in the Region of Västra Götaland in Sweden. In 2017 the regional council decided on a common strategy for reorganising healthcare with integrated systems where patient information will be managed and communicated between various healthcare actors and organisations, called Framtidens vårdinformationsmiljö (FVM). Today's healthcare environment contains many different systems that cannot communicate with each other, which causes problems with sharing information between specialist healthcare, primary care, municipal healthcare, and private care providers. As a result, the information is available but cannot be accessed by everyone who needs it. The objective of FVM is to offer accessible healthcare with high quality and to enable patient participation. Information security must be preserved within FVM, and previously mentioned requirements must be met. FVM will introduce a new, modern and common healthcare information environment that makes it easier for all actors in healthcare to collaborate (Vårdskiftet, 2021b).

The central part of FVM is the new integrated medical record system Millennium, which will contain all vital patient information and allow access to the information to all necessary actors. Millennium is an international system used by healthcare in 24 countries worldwide. In Sweden, the system is adapted to the health care needs in the Region of Västra Götaland and the Region of Skåne. There are a lot of information security requirements that need to be met when implementing Millennium, which has been challenging. Further, Millennium aims to develop region-wide information management by standardising terms and concepts. All information needed for or created in healthcare must be available to those who need it. Millennium will use the possibilities of digitalisation to provide the patients with safe and secure care adapted to the needs of the patients (Vårdskiftet, 2022).

2.5 Related Research

Plenty of research has focused on healthcare digitalisation and electronic health record systems. For example, Winge et al. (2015) write about the increased complexity within healthcare. One challenge is that a single patient may receive care from several care providers, which can result in situations with potentially incoherent and uncoordinated information. In addition, multiple healthcare processes for investigating, treating, and assisting a patient can be involved. Further, Winge et al. (2015) propose a solution in the form of a Coordination Hub, an integrated software service that can make communication between different healthcare providers easy. The Coordination Hub enables exchanging information with all necessary healthcare providers.

Keshta and Odeh (2021) analyse the security and privacy of electronic health records and present concerns and challenges related to specifically integrated electronic health records. The research stresses that many governments have shown interest in using integrated electronic health records due to the expected benefits and presents these benefits. For example, the benefits are that integrated EHR increases efficiency in health care delivery, which means that resources are not wasted, including supplies, equipment, ideas, and energy. However, examples of the challenges presented in the research are security breaches like hacking, unauthorised access, and implementation costs.

Another research related to the study is by Adavi Madhavi and Susan Lincke from 2018. The research focuses on the advantages and challenges of digital electronic health records and presents a risk assessment of electronic health records. The authors claim that breach of privacy, confidentiality and availability of health information are some of the risks associated with EHR (Madhavi & Lincke, 2018). Next, Smaradottir (2018) presents some major benefits and opportunities with electronic healthcare records and explains that EHR is the primary entity for sharing and analysing medical information for decision making and medical treatment, which aligns with the study because opportunities within EHR are presented and explained.

Several researchers have addressed the issue of challenges and opportunities within healthcare, where electronic healthcare record systems are the main topic. For example, the research from, e.g., Keshta and Odeh (2021), Madhavi and Lincke (2018), and Smaradottir (2018) focus on the challenges and opportunities related to information security within electronic healthcare record systems. Further, the research from Winge et al. (2015) focuses on the communication needs and information sharing between various healthcare actors, which is the interest of this study. However, none has focused on investigating information security challenges and opportunities within integrated electronic healthcare record systems where different healthcare providers can collaborate by accessing and exchanging all patient information.

Various solutions for information sharing have been presented. For example, Winge et al. (2015) propose a solution in the form of a Coordination Hub, an integrated software service that can make communication between different healthcare providers easy. Furthermore, Neamah (2020) stresses the need to integrate electronic healthcare records to allow higher data availability and suggests a flexible data warehouse to build an integrated electronic health record. The research by Winge et al. (2015) and Neamah (2020) present solutions for integrating healthcare records. However, none has focused on investigating information security challenges and opportunities associated with integrated electronic healthcare record systems.

Cashman et al. (2021) explain that an integrated electronic health record system facilitates a safer and more efficient healthcare service and presents an example of the successful integration of two disparate healthcare records in Australia. The research also brings up the benefits of the integration, such as that all relevant patient information integrated into one system is accessible to multiple actors. However, Cashman et al. (2021) research does not explore information security challenges with these integrated electronic healthcare record systems and focuses only on opportunities.

In Sweden, the healthcare system is managed and run either by the regions, local authorities, or municipalities. In 2012, Swedish healthcare launched the service Journalen as the patient-accessible national electronic health record system. Journalen provides access to most of the various EHR systems used throughout Swedish healthcare organisations. Hence, the patients can access their health information regardless of which healthcare providers they have visited. However, the healthcare providers themselves do not see all the information that patients do (Hägglund & Scandurra, 2021). The approach made in Sweden to meet different care providers' needs for integrated information is the National Patient Overview. Authorised healthcare providers can access patients' information with the National Patient Overview. However, it only provides an overview, so all information about the patient is not there (Öström Zetterman, 2021). Furthermore, electronic healthcare records that enable information sharing between several healthcare actors have not been implemented sufficiently. The lack of integration within healthcare can result in missing the patient information, which can further lead to mistreatment. Challenges that remain in Sweden relate to differences in the implementation that lead to fragmentation and unequal access to information (Hägglund & Scandurra, 2017).

Although the Journalen interface is identical for all users, there are significant differences in how much information each healthcare provider gives access to, which causes that all relevant information may not be available to all necessary actors. Therefore, the ongoing project in the Region of Västra Götaland in Sweden, Framtidens vårdinformationsmiljö, FVM (Eng. The healthcare information environment of the future), is about reorganising healthcare with integrated systems where patient information will be managed and communicated between various healthcare actors and organisations. Today's healthcare environment contains many different systems that cannot communicate with each other, which causes problems with sharing information between different healthcare providers. The objective of FVM is to offer accessible healthcare with high quality and to enable patient participation. The central part of FVM is the new integrated medical record system Millennium, which will contain all vital patient information and allow access to the information to all necessary actors (Vårdskiftet, 2021b).

Another project, "Future Healthcare Information Systems" (FHIS), was carried out on behalf of the Region of Västra Götaland in Sweden, which recognised the current healthcare systems issues. For example, information systems used by different care providers do not communicate with each other, making it difficult for healthcare providers to fulfil their functions. The project's vision was that healthcare providers must have access to effective collaborative information systems that support process-oriented care where the patient is an active co-actor. Furthermore, the project aimed to develop a demonstrator that visualises a vision of how the information systems of the future should be designed. The demonstrator intended to show a new process-oriented way of working in healthcare where the patient's active participation and effective communication between different healthcare providers are central. The project also aimed to show how various healthcare providers can work together to achieve positive effects, like increased quality. Moreover, the FHIS project showed a need to integrate different systems. There are some prerequisites when implementing this kind of solution. For example, changes in governance and responsibility are required, extensive standardisation work is needed, and information security issues need special attention. This project laid the foundation for integrating different systems, including EHR (Åhlfeldt et al., 2016; Hedström et al., 2011).

Based on the analysis of prior research and the scope of the problem, the research about information security challenges and opportunities associated with integrated electronic healthcare record systems is lacking. Consequently, the solutions for existing healthcare challenges presented in the previous research focus on how to integrate electronic healthcare record systems. The previous research does not provide an insight into information security challenges and opportunities with integrated electronic healthcare record systems.

3 Method

When research and study are conducted, information and data within the field must be collected. To answer the research question, it is necessary to choose a method. Furthermore, a method enables to draw conclusions and present research findings. A method also enables analysis of the collected data, as well as an argument that new knowledge has been produced (Oates, 2006). This chapter presents the choice of method for the study and describes how the method will be implemented.

3.1 Research Method

When collecting information for a scientific study, there are two main methods: qualitative and quantitative methods. Data from direct field observations, open interviews, and written documents are analysed using a qualitative method. The qualitative method is based on unstructured and non-numerical data. In qualitative methods, the focus is on meaning and context, and the method aims to create a deeper understanding of attitudes and ideas that cause people's actions, formulations, and decision-making (Patton, 2015). On the other hand, the goal of a quantitative method is to test theories, models, and hypotheses about natural phenomena. Quantitative methods emphasise that measurements are fundamental because they connect observation and formalisation of the model, theory, and hypothesis (Berndtsson et al., 2008).

To get insight into the security challenges and opportunities with an integrated patient record system, the following research question was formulated: What information security challenges and opportunities are there with an integrated electronic health record system on a regional level? To answer the research question and achieve the purpose of the study, a qualitative method has been chosen because qualitative methods focus on meaning and context. The focus is to understand what security challenges and opportunities arise when using integrated patient record systems. This method was appropriate since qualitative research methods focus on creating a deeper understanding of the studied phenomenon. The healthcare industry includes many different actors that handle a massive amount of information, for example, patient information, which requires a deep understanding. Due to the gigantic information flow within healthcare, it is best to observe or question actors involved in the topic to get detailed insight into the studied phenomenon. Thus, the qualitative research approach has been chosen.

Qualitative methods use explorative strategies such as case studies and phenomenological studies. The case study focuses on a specific problem that needs investigation and aims to gain detailed insight into the problem (Oates, 2006). Hence, to achieve the purpose of the study, a case study has been chosen as the overall strategy for data collection. A case study focuses on what is to be investigated, and the case is analysed in detail using different data collection methods (Oates, 2006). Various aspects need to be considered when using case studies. One aspect that is important to consider is to go through existing research and literature to create an understanding of what is to be investigated before the work within the case study continues, as is the case with all research (Webster & Watson, 2002). Another aspect of the case study is conducting interviews, which are considered the most common step in the case study (Patton, 2015). The study focuses on getting insight into security challenges and opportunities with an integrated patient record system, which requires the case to be investigated in detail. Therefore, the case study was chosen as the research strategy. A case study is particularly suitable in situations where understanding the context is important. For example, a case study is preferred in areas with little knowledge of how and why something is important and where individuals' experiences are critical (Williamson et al., 2002). The new integrated electronic healthcare system Millennium has not been investigated in detail, and there is not much research focused on a regional level, therefore the case study was suitable to use. Other strategies were not appropriate to use. However, the survey could be used to obtain information about challenges and opportunities with integrated health record systems, but it would not result in the desired level of detail in the empirical data.

3.2 Data Collection

To address the problem and collect relevant data for the study, interviews have been chosen as a technique for data collection. There are several different types of interviews. Further, to get answers about security challenges and opportunities within integrated electronic health records, semi-structured interviews with security officers for municipality and region, system designers, and security officers responsible for the planning, and likewise, have been chosen as data collection methods. When collecting data about security challenges and opportunities, it is essential that the interview is open and experienced as a conversation to make respondents comfortable speaking about security challenges and opportunities. Semi-structured interviews also make the respondent feel safe and comfortable, which is appropriate for collecting information about security challenges and opportunities within integrated electronic health records.

To investigate what information security challenges and opportunities exist with an integrated electronic health record system on a regional level, semi-structured interviews with security officers for municipality and region, system designers, and security officers responsible for the planning, and likewise, were conducted. As a result, five respondents from the project FVM have been chosen to understand better security challenges and opportunities with integrated electronic health record systems. A selection has been made where the respondents must have been involved in the information security work with Millennium. All respondents are from the Region of Västra Götaland (regional level). The interviews lasted approximately 40 minutes to collect sufficient relevant data, and the interviews were recorded. Questions for the interviews were designed based on the literature search presented in the background. All interviews were conducted remotely using the meeting tools Zoom and Microsoft Teams.

The interviews were conducted using an interview guide (Appendix A), which served as a list of topics addressed during all interviews. The interview guide enabled flexibility and ensured that all main topics were addressed. Formulations of questions for the interview guide were not so specific to encourage flexibility and not limit new ideas that may arise from the collection of data during the interviews. To achieve the desired level of detail of the results, the interviews were conducted with five respondents on a regional level. All respondents are from the Region of Västra Götaland and are responsible for Millennium's information security. Table 1 provides an overview of respondents who have contributed to the study.

Table 1. Overview of the respondents.

Respondent	Work role and relevance to FVM
Respondent 1 (R1)	IT manager and implementation responsible
Respondent 2 (R2)	Doctor and program owner
Respondent 3 (R3)	Quality manager and implementation responsible
Respondent 4 (R4)	Digitalisation strategist and implementation responsible
Respondent 5 (R5)	Data Protection Officer and attends FVM meetings

Every respondent was chosen based on their work role within project FVM and Millennium. The selection that respondents must be involved in the project was made because the project Millennium is about an integrated electronic healthcare record system and is focused on a regional level. It was also important that respondents work with the information security part to have an opinion about security challenges and opportunities within the Millennium system. Respondent 1 (R1) is the IT manager and is responsible for implementing FVM. Next, Respondent 2 (R2) is the program owner for the FVM project. Furthermore, Respondent 3 (R3) is the quality manager and implementation responsible for FVM. Respondent 4 (R4) is the digitalisation strategist and implementation responsible. Finally, Respondent 5 (R5) is Data Protection Officer who attended FVM meetings.

The study focuses on collecting data and understanding what information security challenges and opportunities exist with an integrated electronic health record system on a regional level. The case study collected detailed data and gained deep insights into the chosen topic. Furthermore, with the help of the respondents who participated in the study, it was possible to collect deep insights and opinions about integrated electronic health record systems from the key people from the Millennium's team.

3.3 Data Analysis

To analyse the collected data, transcription of the interviews was chosen as the first step in preparing the data for analysis. The transcription provided an overall understanding of the collected data, which was further analysed using coding to identify themes and patterns in the data. Preece et al. (2016) suggest that the coding should be done iteratively by going through the material, and coding (marking, highlighting) is based on what is in the focus of the study. Open coding is a process where data is discovered through its properties or categories, and the process is similar to categorisation, which is suitable for finding details in the data. The purpose of the analysis is to identify properties of relevant categories and then use these as a basis for constructing a theory.

Data collected from the interviews have been further analysed based on a deductive analysis (Preece et al., 2016). Analysis processes began with transcripts of recordings from the interviews to get an overall impression of the data and look for patterns. Furthermore, the collected data was reduced to smaller and more manageable units by excluding things from the transcripts that were irrelevant to the study. The exclusion was made using open coding. The coding analysis began by going back to the purpose of the study and creating a coding scheme with predefined codes and themes such as *challenges, opportunities*, *integrated electronic healthcare record systems, healthcare digitalisation*, and *information security within healthcare*. The codes were identified according to different themes that emerged in the interviews. The goal of the codes was to find patterns in the data. When a code appeared in the collected data, the context was analysed. Then, a pattern was identified if similarities between these contexts were found. It was possible to get an overview and understand the collected data better by identifying patterns. Furthermore, the data from all transcripts were divided into specific themes to make it easier to compile a result. Figure 1 shows examples of the analysis with open coding, categories, and themes. Finally, the interview analysis was done by comparing existing and relevant research to the empirical data.

From the healthcare perspective, we have the opportunity to staff differently. For example, we can also get help from staff at a distance. For example, we can use staff who have retired and feel that they have the strength, energy and will to work and then they can work from home and take video patients, which can reduce the healthcare burden. So, this is a way for employers to offer opportunities for those who feel they could work remotely. It is a win-win situation for patients in general. When it comes to challenges with integrated EHR, it will be challenging to ensure good technical security solutions and administrative security solutions, i.e., assigning authorisations the right way and keeping track of our staff.

Codes	Themes
Advantages Opportunities Reduce the healthcare burden	Opportunity
Disadvantages Challenges Challenging to ensure …	Challenge

Figure 1. Example of the analysis with open coding, categories, and themes.

3.4 Research Ethics

When conducting research, there are guidelines and principles to follow. Research ethical considerations deal with principles related to data collection, mainly if the data collection contains information about people. In addition, research ethics requires openness regarding methods and results. There are four general ethical principles and main requirements for research: the information requirement, the consent requirement, the confidentiality requirement and the utilisation requirement (Vetenskapsrådet, 2017).

Before the interview, the respondents were informed about the purpose of the study and the purpose of the interview, which is to collect data and understand what information security challenges and opportunities exist with an integrated electronic health record system on a regional level. According to the information requirement, the respondents were informed that it is optional to participate in the study and that they have the right to cancel their participation. Vetenskapsrådet (2017) explains that it is important to inform all respondents about all study elements that may affect their willingness to participate in the study according to the information requirement.

Respecting the consent requirement, the respondents were informed about their rights, such as the right to anonymity, the right to cancel the interview, and the right not to answer questions that feel inappropriate. Further, according to the consent requirement, the respondents were informed about their right to decide about their participation and thus the right to withdraw from the study whenever they want, which means that all data collected about them will be deleted. Finally, the respondents were also informed that they have the right to receive the report when it is ready (Vetenskapsrådet, 2017).

Lastly, according to the confidentiality requirement and the utilisation requirement, participating respondents were informed that all data collected during the interview is confidential, i.e. the data will only be used for the purpose of the study and will not be published anywhere (Vetenskapsrådet, 2017). With the respondents' oral consent, the interviews were recorded and finally transcribed to be analysed. The recordings from the interviews were stored locally on the computer. Also, the recordings have not been used for purposes other than those specified in this chapter. After transcribing the interviews, the audio files were deleted to avoid saving personal data more than necessary.

4 Results

This chapter will describe and analyse the results of implemented methods. The study aims to get insight into the security challenges and opportunities with an integrated patient record system. Therefore, the following research question was formulated: What information security challenges and opportunities are there with an integrated electronic health record system on a regional level? To answer the research question and achieve the purpose of the study, a qualitative method has been chosen, and semi-structured interviews have been conducted to collect relevant data. Thus, the following subheadings are designed according to different themes that arose from the interviews and literature search from the background.

4.1 Identified Opportunities

With the help of the chosen method and the analysis of the results, several opportunities within integrated electronic healthcare records are identified. The opportunities are categorised as healthcare digitalisation, information security in healthcare and EHR, and Framtidens Vårdinformationsmiljö and Millennium.

4.1.1 Healthcare Digitalisation

According to the collected data, digitalisation within healthcare can be used to store and share patient information. As a result, all respondents believe that digitalisation contributes to better care. For example, Respondent 1 (R1) explains that the advantages of healthcare digitalisation are that the care becomes much more accessible, and healthcare providers are not dependent on time and space. Patients can request anything by contacting healthcare twenty-four-seven, and the healthcare providers can take care of that. Further, R1 explains that digitalisation also brings benefits to healthcare providers. R1 continuous:

"From the healthcare perspective, we have the opportunity to staff differently. For example, we can also get help from staff at a distance. For example, we can use staff who have retired and feel that they have the strength, energy and will to work and then they can work from home and take video patients, which can reduce the healthcare burden. So, this is a way for employers to offer opportunities for those who feel they could work remotely. It is a win-win situation for patients in general." (R1)

Respondent 2 (R2) describes digitalisation as everything from using technical solutions to defining a new way of delivering care. R2 explains that healthcare is an incredibly information-intensive organisation where information is handled and shared between many different actors, the patients themselves, their relatives, and care providers. Therefore, R2 argues that there is no possibility of creating safe healthcare without fully utilising digitalisation and technology. "Digitalisation is a prerequisite for me to receive sensible care when I get older and ill" (R2). Furthermore, Respondent 3 (R3) agrees with R1 by explaining that the advantages of digitalisation can be used to minimise the lack of competence within healthcare. R3 explains: "I see digitalisation as an enabler to sometimes replace a healthcare staff performing various activities, for example, administrative tasks." Respondent 4 (R4) also speaks about the advantages of digitalisation. R4 argues that healthcare, like most other industries, can benefit significantly from digitalisation. Digitalisation gives opportunities to deliver a high standard of care. The reason is that with more stored and analysed data, patients get better prevention and care. Respondent 5 (R5) adds that digitalisation means task simplification for healthcare providers and patients. For example, a digital medication dosage reminds and helps patients take their medication, which does not require help from medical staff. Another example where digitalisation can benefit is in hard-to-reach areas. R5 explains that camera surveillance can be placed in hard-to-reach areas to check when different alarms come. Using camera surveillance can prevent waste of resources in cases of false alarms.

4.1.2 Information Security in Healthcare and EHR

Information is critical in supporting healthcare providers to deliver care and carry out their activities. Therefore, it is crucial to keep this information safe. When discussing information security in healthcare, all respondents define information security as protecting and securing confidentiality, integrity, and availability of patient information. Furthermore, most respondents mention that patient safety and patient privacy must be preserved. R1 explains that healthcare takes information security seriously: "Today, there are logs and controls, so we have drastically increased security compared to before". R1 explains further that there is two-factor authentication for all healthcare providers and patients using BankID. Moreover, R2 thinks that "we must understand digitalisation's challenges. We must understand the system's construction in purely technical and programming terms while understanding legislation and regulations. The most important thing is to ensure that we use the available technology."

Regarding information security in healthcare, R3 agrees with R1 and believes that two-factor authentication for all healthcare providers prevents unauthorised persons from accessing patient information. In addition, R3 adds: "we must be aware that information needs to be protected. We must be careful how and where we use the information." However, R4 explains that healthcare must follow laws to ensure information security and protect patients' privacy, e.g., the Act of Patient Data, the Act on Healthcare Records and GDPR.

All respondents define electronic healthcare records (EHR) similarly. For example, R1 defines an EHR as a healthcare information system because "I think it should contain all the information about the patient and all this information must be possible to access when needed". Furthermore, R2 defines EHR as the total amount of information about an individual's health and care. In addition, R2 argues that electronic health records collect information and data about patients' health, illness, and care and then present it to different users.

Similarly, R3 explains that when healthcare switched to electronic records, old paper records were uploaded to different systems, making it difficult to read and find information. However, the advantages of EHR are that "you do not have to be physically where the patients' records are, and several actors can log in the same EHR simultaneously and use it." Furthermore, R4 explains that EHR is a system where all information about one patient is stored. This information can further be accessed by authorised healthcare professionals when needed.

Further, R1 explains that EHR contains sensitive information and to prevent unauthorised access, Swedish healthcare uses a SITHS card. Using a SITHS card when logging in to a computer system, the requirements for secure identification from the Patient Data Act are met. Also, patient information is encrypted when shared electronically between different healthcare actors.

4.1.3 Framtidens Vårdinformationsmiljö and Millennium

When discussing Framtidens vårdinformationsmiljö, FVM (Eng. The healthcare information environment of the future), all respondents see a lot of opportunities and benefits. For example, R1 argues that FVM, especially Millennium, can increase efficiency because different actors won't need to do the same analysis and examinations. R1 explains that every healthcare actor will have access to the same information, which will improve healthcare quality. FVM will include all health information like calendar, visit fees, health record documentation, etc. "The most important opportunity Millennium brings is access to all medical notes" (R1). All respondents agree with R1. For example, R2 explains that the most significant benefit is that every healthcare provider in the region will have the same system. "Today, we have one system in the hospitals and another in the health centres, our private providers have different systems, and our municipalities have other systems. Now we will all work in the Millennium, and the information will be gathered in one place", explains R2. Further, R3 agrees and explains that having the same system will simplify writing medical notes, and healthcare providers won't need to write the same notes in different systems, as is the case today.

R1 explains that what is especially good about FVM and Millennium is that all healthcare actors in the Region of Västra Götaland will share medical data. FVM will collect all patient documentation in the same system, and all healthcare actors will be able to read about all treatments that a patient did. Using Millennium, missing information that could lead to incorrect assessments and decisions will be avoided. R1 argues: "You get a complete picture of the patient. Due to patient safety, all healthcare providers need to have the same information when treating the patient, which will be enabled in Millennium" (R1). Additionally, R2 adds: "Millennium, the same system for all healthcare providers, will make manual information sharing disappear. The biggest opportunity is getting a total amount of patient information in one place".

Another opportunity with Millennium is simplifying contact with the patients when documenting. R3 explains that double documentation will disappear. The patients won't need to describe their issues several times to different healthcare actors because everything will be stored in the same system. Simplifying contact with the patients will make healthcare more secure because all critical information will be accessible for healthcare providers to complete their assessments of the patients. In addition, R3 argues that another opportunity with Millennium is standardisation. Every healthcare actor in the region will document in the same way; routines and guidelines for the documentation will exist to make healthcare more equal. Finally, R5 explains that involvement and communication will be uncomplicated with integrated EHR. R2 agrees:

"The overall opportunity for healthcare in the Region of Västra Götaland is offering the region's patients cohesive and more accessible healthcare with higher quality." (R2)

4.2 Identified Challenges

With the help of the chosen method and the analysis of the results, several challenges within integrated electronic health records are identified. The opportunities are categorised as healthcare digitalisation, information security in healthcare and EHR, and Framtidens Vårdinformationsmiljö and Millennium.

4.2.1 Healthcare Digitalisation

Despite all the opportunities with healthcare digitalisation, some respondents recognised several disadvantages. For example, R1 points out that certain patients today do not prefer digitalisation. The reason is that they may not be interested in digitalisation or have a disability or difficulties that make it challenging to understand. Further, R2 mentions that information security within healthcare digitalisation can be challenging to maintain. Another example that R2 mentions is that digitalising can make healthcare impersonal because most healthcare appointments will be online.

Moreover, R3 agrees with R1 and means that digitalisation can be challenging for some patients. Digitalisation does not suit everyone, and not everyone has the opportunity as a patient to use digital tools. R3 also believes that there are deficiencies in quality and patient safety in digital care as some doctors lack general IT skills. Further, R4 describes that some challenges within healthcare digitalisation can be information loss or disclosure and other types of cyberattacks.

"There are challenges with digitalisation in healthcare, for example, maintaining information security. But history shows that we as humans are good at adapting and learning to use advantages and avoid disadvantages." (R2)

4.2.2 Information Security in Healthcare and EHR

Most respondents recognised potential information leakage threats caused by cyberattacks regarding information security challenges in EHR. The reason is that information sharing between different healthcare providers today is managed both electronically and manually. R1 stresses: "When the medical information is shared manually, for example, via fax and letter, between different healthcare actors, the information security is not handled". R2 also explains that a lot of healthcare information is still shared manually via fax. According to R1 and R2, it is too difficult to maintain security when medical information is shared manually. In addition, R3 confirms that sending medical notes via fax is unsafe because fax machines are advanced, and the information may be stored in the fax machines. Contrary, R5 argues that sending patient information via e-mail can also be insecure depending on what e-mail servers are used. R5 explains that it is challenging to determine how patient information should be shared between healthcare providers to remain secure.

R1 explains that it is challenging to follow the Patient Data Act in today's electronic health records. According to the Patient Data Act, healthcare providers have permission to read medical notes from the same healthcare actor. But, if they need to read the health record's notes from other healthcare actors, they must ask the patient for permission. Getting the patient's consent takes time because healthcare providers must register that they have requested the patient's permission and explain how they have agreed to provide access to the notes.

"The biggest security challenge today is that we don't have access to all patient information. We don't share the same EHR system, but we all use different systems." (R3)

R2 agrees with R1 and explains that the most challenging part of information security in healthcare and EHR is following different laws and regulations. R2 describes that there are, for example, the Patient Data Act and GDPR that healthcare providers must follow. Further, R2 explains that following several laws and regulations is challenging and gives the following example: "If you come to the emergency room unconscious, according to the patient safety, a doctor needs to know what medication you are taking. But, on the other hand, medication can point to what diagnoses you have. Revealing these diagnoses can mean a breach of privacy and integrity". R2 stresses that laws and regulations must help maintain information security in healthcare and EHR and explains the issue: "As a doctor, I should have access to the information needed to provide safe care. But unfortunately, I have come across authorities who work with security legislation who think the opposite." R5 explains that law is challenging because there can be different assessments of the law. Furthermore, according to R5, the most significant information security challenge within healthcare today is the human factor. One challenge is to make organisations and the management understand that information security is ongoing work and that staff needs to be educated constantly.

Additional information security challenges that R5 mentions are ensuring that integrated electronic health record systems can prevent unauthorised access and that the correct permissions are assigned to the medical staff. It is challenging for everyone who uses the system to understand how to prevent unauthorised access and give permissions work.

Another aspect of information security in healthcare and integrated EHR that R3 describes is when there is a connection to Cloud services. Unfortunately, the Swedish laws and regulations make it challenging to use Cloud services. Furthermore, work overload within healthcare makes it challenging to bring awareness about information security. Therefore, healthcare providers must get educated about information security. It is essential to bring awareness and explain that information must be protected and carefully managed. Further, R4 explains the same aspect of information security challenges. For example, R4 mentions that it is necessary to use Cloud services to access patients' information through different devices. However, Cloud services can bring information security challenges like information leakage.

4.2.3 Framtidens Vårdinformationsmiljö and Millennium

When it comes to information security regarding FVM and Millennium, all respondents mention that it is complicated to follow Swedish laws and regulations. For example, R1 points out: "We have the same patients in the region, and all of us need to share the patient information, which the Patient Data Act does not accept". In addition, R1 explains that Millennium providers must follow Swedish laws and regulations, which has been challenging. Furthermore, R2 explains that following the Swedish laws and regulations is challenging for FVM and Millennium because there are many different interpretations of the existing laws.

According to R1, it can also be challenging to maintain information security in Millennium because healthcare providers will be able to read more medical notes than they have the right to do. Therefore, controlling who gets access to sensitive patient information and medical notes is not easy. R1 describes that Swedish legislation requires randomly checking 10% of all employees who access medical notes. In addition, R1 argues that in the Millennium, these check-ups should be increased to at least 50% because every healthcare provider in the region will have access to the Millennium. Furthermore, R2 thinks the same way and stresses a lack of educated staff that can take care of information security within Millennium. R2 explains that a massive amount of information will be stored in Millennium. Because of that, R2 discusses: "It will be challenging to ensure good technical security solutions and administrative security solutions, i.e., assigning authorisations the right way and keeping track of our staff". Maintaining patients' trust is also challenging because a single information leakage can sabotage the trust. In addition, R2 explains that ensuring guiding principles for healthcare providers and information security responsible, i.e., routines, guidelines, and policies is essential. The reason is that many information security risks are not in the system but in the people who use them, R2 explains. Moreover, R3 mentions the same challenge and explains that ensuring guiding principles and regulations is challenging. Defining these regulations is challenging because determining who can access what information and getting patients' consent is difficult and time-consuming.

R3 mentions other challenges with FVM and Millennium. For example, one challenge is using Cloud services. The reason is that an American supplier delivers Millennium, and it is not allowed by Swedish laws to have servers outside Europe. Further, it has been challenging to maintain information security within the Millennium and design the system according to Swedish laws, regulations, and even GDPR. Again, R3 and R4 explain that the reason behind this challenge is that Millennium servers are based outside of Sweden. An additional security challenge for FVM and Millennium that R5 mentions is ensuring that laws and regulations are clearly understood to be able to make demands for the system's supplier.

The FVM and Millennium will enable information access, and all patient information will be gathered in the same database. However, R5 points out that the most difficult challenge is ensuring that correct permissions to sensitive information are assigned. R5 also stresses that one significant challenge is making the management of FVM understand that information security is ongoing work and needs to be taken care of constantly.

4.3 Summary of the Results

From the analysis of the primary studies, several challenges and opportunities within integrated electronic health records were identified. Table 2 below summarises and compares identified opportunities from related research presented in the background and opportunities from the results of the empirical research. For example, opportunities identified in the existing research are improving healthcare quality and patient safety, reducing medical or medication errors, lowering costs, increasing patient satisfaction, easy access to medical data and healthcare, and increasing efficiency. Furthermore, some of these opportunities appear in the results of the empirical research. For example, easy access to medical data and improving healthcare quality are also frequently mentioned in the results of empirical research.

An additional opportunity from the results of the empirical research is equal healthcare for everyone, meaning that integrated electronic healthcare record Millennium can enable access to the same information to all necessary actors. Moreover, respondents of the empirical research mentioned an opportunity to staff differently, meaning getting help from retired staff at a distance. Furthermore, standardisation is also identified as an opportunity because every healthcare actor in the region will document in the same way, where routines and guidelines for the documentation will exist.

Table 2. Summary of the research results, opportunities.

Identified opportunities	Existing research	Empirical research
Easy access to healthcare	x	x
Easy access to medical data	x	x
Easy information sharing	x	x
Equal healthcare		x
Improving healthcare quality	x	x
Improving patient safety	x	
Increasing efficiency	x	x
Increasing patient satisfaction	x	
Lowering costs	x	
Opportunity to staff differently		x
Reducing medical or medication errors	x	x
Standardisation		x

Table 3 below summarises and compares identified challenges from related research presented in the background and challenges from the results of the empirical research. For example, challenges identified in the existing research are the compromise of confidentiality, integrity, and availability, security breaches like hacking and unauthorised access, poor usability, functionality, and performance, gaining patients' trust or patient' acceptance of EHR and medical data documentation in free text. In addition, using integrated electronic healthcare record systems and maintaining information security is seen as a challenge. Furthermore, as the table shows, some of the challenges appear in the results of empirical research. However, there are additional challenges identified in the results of empirical research. For example, one challenge is that some medical staff lack general IT skills making it difficult to use the systems correctly. When it comes to the integrated patient record system Millennium, the most complicated challenge identified is following the Swedish laws and regulations. Furthermore, using Cloud services for EHR is recognised as a challenge for Millennium.

Table 3. Summary of the research results, challenges.

Identified challenges	Existing research	Empirical research
Assigning correct permissions		x
Compromise of confidentiality, integrity, and availability	x	x

Following the Swedish laws (the Act of Patient Data and GDPR)		x
Gaining patients' trust	x	x
Getting management's support for information security		x
Lack of IT skills		x
Maintaining information security	x	x
Medical data documentation in free text	x	
Poor usability, functionality, and performance	x	
Security breaches like hacking and unauthorised access	x	x
Using Cloud services for EHR		x

5 Discussion

This chapter will discuss the results in relation to the previous research, implementation approach, and ethical and societal concerns. Identified opportunities and challenges will be compared and discussed. Furthermore, a discussion about how implementation and selected methods impacted the results will also be included. Finally, the research will be discussed in terms of ethical and societal issues.

5.1 Previous Research and Results

Analysing the primary studies and related research, several challenges and opportunities within integrated electronic health records were identified. For example, opportunities identified in the existing research are improving healthcare quality (Carey et al., 2016) and patient safety (Keshta & Odeh, 2021), reducing medical or medication errors (Keshta & Odeh, 2021), lowering costs (Carey et al., 2016; Keshta & Odeh, 2021; Menachemi & Collum, 2011), increasing patient satisfaction (Kuo et al., 2014), easy access to medical data and healthcare (Menachemi & Collum, 2011), and increasing efficiency (Keshta & Odeh, 2021). Furthermore, some of these opportunities appear in the results of the empirical research. For example, easy access to healthcare is also frequently mentioned in the results of empirical research by several respondents. Moreover, easy access to medical data and easy information sharing are explained by most respondents, which aligns with Menachemi and Collum's (2011) research.

Carey et al. (2016) explain that integrated electronic health records are effective and have benefits such as cost reduction and improved healthcare quality. Furthermore, Keshta and Odeh (2021) argue that integrated EHR increases efficiency in health care delivery, which means that resources are not wasted, including supplies, equipment, ideas, and energy. Similarly, R1 argues that FVM, especially Millennium, can increase efficiency because different actors won't need the same analysis and examinations. R1 explains that every healthcare actor will have access to the same information, which will improve healthcare quality.

An opportunity with integrated electronic health records is standardisation. R3 argues that every healthcare actor in the region will document in the same way; routines and guidelines for the documentation will exist to make healthcare more equal. Enabling equal healthcare does not appear in previous research. Other differences that are identified in empirical research when it comes to opportunities are standardisation and opportunity to staff differently. On the contrary, opportunities identified only in previous research are improving patient safety, increasing patient satisfaction, and lowering costs.

Challenges identified in the existing research are the compromise of confidentiality, integrity, and availability, security breaches like hacking and unauthorised access, and poor usability, functionality, and performance (Madhavi & Lincke, 2018). Furthermore, gaining patients' trust or acceptance of EHR (Keshta & Odeh, 2021; Kuo et al., 2014; Perera et al., 2011) and medical data documentation in free text (Smaradottir, 2018) are also identified as challenges. In addition, some of these challenges are identified in empirical research, for example, security breaches like hacking and unauthorised access. Most respondents recognised potential information leakage threats caused by cyberattacks regarding information security challenges in EHR. The reason is that information sharing between different healthcare providers today is managed both electronically and manually. Moreover, R3 explains that ensuring guiding principles and regulations is challenging. Defining these regulations is challenging because determining who can access what information and getting patients' consent is difficult and time-consuming. Gaining patients' trust and consent aligns with Keshta and Odeh's (2021) research, explaining that some challenges have negatively impacted patients' choices to provide access.

In healthcare, some laws and regulations govern how the information must be stored and handled. In Sweden, for example, there is the Patient Data Act that is applied to caregivers' processing of personal data in healthcare. Furthermore, GDPR also controls the handling of patient data. The Patient Data Act regulates how personal data must be handled in healthcare and complements the GDPR (Patientdatalag, 2008:355). All respondents categorised following the GDPR in the FVM project as challenging because the provider of Millennium is based outside of Europe. Moreover, some differences identified between empirical research and previous research regarding challenges are getting management's support for information security and assigning correct permissions. In addition, lack of IT skills is also a difference as it is mentioned only by some respondents. Furthermore, a difference in the result is that some respondents said using cloud services for EHR is a challenge, which does not appear in the previous research because this was excluded from the study.

5.2 Methods and Implementation

To get insight into the security challenges and opportunities with an integrated patient record system, the following research question was formulated: What information security challenges and opportunities are there with an integrated electronic health record system on a regional level? To answer the research question and achieve the purpose of the study, a qualitative method has been chosen because qualitative methods focus on meaning and context. The focus is to understand what security challenges and opportunities arise when using integrated patient record systems. This method was appropriate since qualitative research methods focus on creating a deeper understanding of the studied phenomenon. The healthcare industry includes many different actors that handle a massive amount of information, for example, patient information, which requires a deep understanding. Due to the gigantic information flow within healthcare, it is best to observe or question actors involved in the topic to get detailed insight into the studied phenomenon. Thus, the qualitative research approach has been chosen.

The case study collected detailed data and gained deep insights into the chosen topic. Furthermore, with the help of the respondents who participated in the study, it was possible to collect deep insights and opinions about integrated electronic health record systems from the key people from the Millennium's team. The study examined only information security challenges and opportunities with an integrated electronic health record system on a regional level. Further, the study focused on integrated electronic health record systems, with Millennium as the leading example. Even though the study used Millennium as the leading example, the results can generally be applied to integrated electronic health record systems.

The FVM is an ongoing project which made it challenging to get more than five interviews, but it was still possible to obtain sufficient information to answer the research question. Further, the FVM is still in progress and the interviews were conducted only with people who are involved in the implementation of the project, which affected the results of the study. The results are from the FVM's perspective, and it was not possible to include end-users' opinions. The results would have been different if the end-users' perspectives were included. For example, other possible opportunities and challenges related to the use of the Millennium system would be identified. Also, if more respondents were included, it would provide the study with much more detail. However, the collected data with the help of the interviews have been compared with existing research and this comparison means that the study is both empirically and theoretically based.

5.3 Ethical and Societal Aspects

When conducting scientific research and study, it is essential to think about ethical aspects and follow ethical principles. Since the study is primarily based on interviews, it was important to inform all respondents regarding their rights and about the study. The study has considered research ethics that deal with principles related to data collection because the data collection contains information about people and organisations. The study has been carried out in accordance with four general ethical principles and the main requirements for research that the Swedish Research Council recommends. The four applied principles are the information requirement, the consent requirement, the confidentiality requirement, and the utilisation requirement (Vetenskapsrådet, 2017). Before the interview, the respondents were informed about the purpose of the study and the purpose of the interview, which is to collect data and understand what information security challenges and opportunities exist with an integrated electronic health record system on a regional level. It was important to apply the research ethics principles because it created a sense of security among the participants in the study, which contributed to the participant's willingness to share their opinions.

All respondents categorised following the GDPR in the FVM project as challenging because the provider of Millennium is based outside of Europe. There are laws and regulations regarding storing and managing personal data, in this case, patient data, which FVM and Millennium struggle to fulfil. Healthcare and FVM should address these challenges in the way that serves the patients best. One respondent mentioned that FVM must think about whether to follow the laws or not because the benefits to the patients are many. However, choosing not to follow the laws can potentially bring ethical dilemmas. For example, one respondent mentioned that the laws exist for a reason and that healthcare must follow those because they ensure patient privacy. According to the respondent, Millennium can't follow the GDPR, and the system must be adapted to the Swedish legislation and the Swedish way of working. Since laws and regulations can change, ethical guidelines can help set the pillars for a successful transformation in the healthcare industry.

As the results show, there are many benefits and opportunities with Millennium, but there are also challenges which can potentially have consequences. For example, if Millennium fails to follow these laws, patient safety risks could arise. One example of these risks is incorrect medication dosage (Vårdskiftet, 2022). In this case, the FVM project and implementation of Millennium have come a long way, and the results show many benefits for the patients and healthcare. Therefore, it is important to make procurements and consider the benefits for patients. Changing the laws in the direction that is in the best interest of the patients can be one solution to the problem. The reason is that the law is sometimes not nimble enough to support patient-centred care and respect for patients' best interests.

From a societal aspect, the study has created benefits because the results are helpful in reality and can be used to develop an integrated EHR. In addition, the result gives a good overview of what is important to think about when implementing and using integrated electronic health records. The results are beneficial to a variety of parties. For example, the results can benefit the developers of integrated electronic health record systems in understanding what challenges and opportunities related to information security exist. Moreover, the results can help developers know what to consider and focus on when developing integrated electronic health record systems. Finally, the work can benefit the project FVM and Millennium. For FVM, it is crucial to get a proper insight into information security challenges and opportunities to implement the integrated patient record system in a patient-safe manner, which the results have provided.

6 Conclusion

The study aimed to investigate the information security challenges and opportunities with an integrated patient record system on a regional level. This study has contributed to an increased understanding of information security challenges and opportunities with integrated patient record systems. As a result, several challenges and opportunities were identified. Some of them were identified from the previous research, and some emerged from the empirical study. In conclusion, identified opportunities with integrated patient record systems are easy access to healthcare, easy access to medical data, and easy information sharing. Furthermore, other opportunities are equal healthcare, improving healthcare quality, improving patient safety, increasing efficiency, increasing patient satisfaction, lowering costs, the opportunity to staff differently, reducing medical or medication errors, and standardisation.

Digitalisation within healthcare and EHR systems has brought many improvements in patient care, for example, advances in the diagnosis of diseases, accessibility of information, and even improvements in medical practices. However, digitalisation has also brought a lot of challenges and security risks. Even if healthcare digitalisation offers many advantages, security challenges with healthcare digitalisation are common. In conclusion, identified challenges with integrated patient record systems are assigning correct permissions, compromise of confidentiality, integrity, and availability, following the Swedish laws, gaining patients' trust, getting management's support for information security, lack of IT skills, maintaining information security, medical data documentation in free text, poor usability, functionality, and performance, security breaches like hacking and unauthorised access, and using cloud services for EHR.

6.1 Future Work

The study focuses on integrated electronic health record systems, with Millennium as the leading example, making room for further research by including more examples of integrated electronic health record systems. However, the Millennium is still in the developing stage. Therefore, it would be interesting to have some examples of integrated electronic health record systems already in use, bringing new questions that can be answered through future research.

In the future, it would be interesting to address the patients' perspectives and understand how they think about integrated electronic health record systems. Furthermore, to increase the reliability of the result, the study can be expanded to more regions, not only the Region of Västra Götaland. It would be interesting to see a similar study done in several regions. In addition, to increase the reliability of the result, more respondents can be included in future work to ensure that the result applies. Further, the study excluded the perspectives of the future users of the Millennium, making room for further research. In the future, it would be interesting to apply the same study when the Millennium is in use and include the users of the system.

References

Alshalali, T., M'Bale, K., & Josyula, D. (2018). Security and Privacy of Electronic Health Records Sharing Using Hyperledger Fabric. *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 760–763. https://doi.org/10.1109/CSCI46756.2018.00152

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects: A Guide for Students in Computer Science and Information Systems*. Springer.

Blix, M., & Levay, C. (2018). *Digitalization and Health Care - a Report to the Swedish Governments Expert Group on Public Economics*. Minestry of Finance.

Carey, D. J., Fetterolf, S. N., Davis, F. D., Faucett, W. A., Kirchner, H. L., Mirshahi, U., Murray, M. F., Smelser, D. T., Gerhard, G. S., & Ledbetter, D. H. (2016). The Geisinger MyCode community health initiative: an electronic health record–linked biobank for precision medicine research. *Genetics in Medicine*, *18*(9), 906–913. https://doi.org/10.1038/GIM.2015.187

Cashman, H., Mayson, E., Kliman, D., Kesby, J., Bell, J., Vachalec, S., Withers, B., Lavee, O., Milliken, S., Moore, J., & Hamad, N. (2021). Integrated electronic health record facilitates a safer and more efficient rural outreach haematology service. *Internal Medicine Journal*, *51*(11), 1869–1875. https://doi.org/10.1111/imj.14973

Cresswell, K. M., & Sheikh, A. (2015). Health information technology in hospitals: current issues and future trends. *Future Hospital Journal*, *2*(1), 50–56. https://doi.org/10.7861/futurehosp.2-1-50

Ekman, B., Thulesius, H., Wilkens, J., Lindgren, A., Cronberg, O., & Arvidsson, E. (2019). Utilization of digital primary care in Sweden: Descriptive analysis of claims data on demographics, socioeconomics, and diagnoses. *International Journal of Medical Informatics*, *127*. https://doi.org/10.1016/j.ijmedinf.2019.04.016

Haggerty, E. (2017). Healthcare and digital transformation. *Network Security*, *2017*(8), 7–11. https://doi.org/https://doi.org/10.1016/S1353-4858(17)30081-8

Hägglund, M., & Scandurra, I. (2017). Patients' Online Access to Electronic Health Records: Current Status and Experiences from the Implementation in Sweden. *Studies in Health Technology and Informatics*, *245*, 723–727.

Hägglund, M., & Scandurra, I. (2021). User Evaluation of the Swedish Patient Accessible Electronic Health Record: System Usability Scale. *JMIR Hum Factors*, *8*(3), e24927. https://doi.org/10.2196/24927

Hedström, K., Jäger, K., Krasniqi, H., Linderoth, H., Nohlberg, M., Persson, A., & Åhlfeldt, R. M. (2011). *Vårdens framtida informationssystem – vision i form av en demonstrator*.

ISO/IEC 27002. (2013). *Information technology — Security techniques — Code of practice for information security controls*.

Jacob, P. D. (2020). Chapter 3 - Management of patient healthcare information: Healthcare-related information flow, access, and availability. In S. Gogia (Ed.), *Fundamentals of Telemedicine and Telehealth* (pp. 35–57). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-814309-4.00003-3

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST perspectives, and Recommendations. *IEEE Access*, 1. https://doi.org/10.1109/ACCESS.2022.3145372

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/J.EIJ.2020.07.003

Kuo, K.-M., Ma, C.-C., & Alexander, J. W. (2014). *How do patients respond to violation of their information privacy?* https://doi.org/10.12826/18333575.2013.0011.Ma

Madhavi, A., & Lincke, S. (2018). Security Risk Assessment in Electronic Health Record System. *2018 IEEE Technology and Engineering Management Conference (TEMSCON)*, 1–4. https://doi.org/10.1109/TEMSCON.2018.8488449

Maki, O., Alshaikhli, M., Gunduz, M., Naji, K. K., & Abdulwahed, M. (2022). Development of Digitalization Road Map for Healthcare Facility Management. *IEEE Access*, *10*, 14450–14462. https://doi.org/10.1109/ACCESS.2022.3146341

Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy*, *4*, 47. https://doi.org/10.2147/RMHP.S12985

MSB. (2014). *Strategi för stärkt informationssäkerhet inom vård och omsorg*.

Nationalencyklopedin. (n.d.). *IT-säkerhet* [online]. Available from: https://www.ne.se/uppslagsverk/encyklopedi/lång/it-säkerhet [Accessed 13 Mars 2022].

Neamah, A. F. (2020). Flexible Data Warehouse: Towards Building an Integrated Electronic Health Record Architecture. *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 1038–1042. https://doi.org/10.1109/ICOSEC49089.2020.9215433

Oates, J. B. (2006). *Researching Information Systems and Computing*. Sage.

Patientdatalag (2008:355). Patientdatalag [online]. Available from: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355 [Accessed 10 June 2022].

Patton, M. Q. (2015). *Qualitative research & evaluation methods: integrating theory and practice* (Fourth). SAGE Publications, Inc.

Perera, G., Holbrook, A., Thabane, L., Foster, G., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. *International Journal of Medical Informatics*, *80*(2), 94–101. https://doi.org/10.1016/J.IJMEDINF.2010.11.005

Preece, J., Rogers, Y., & Sharp, H. (2016). *Interaktionsdesign: bortom människa-dator-interaktion*.

Rachmani, E., Haikal, Mubarokah, K., Anjani, S., Handayani, S., Setyowati, M., Nurjanah, & Yanuar, A. M. F. (2021). Digital Transformation in Healthcare: Are patients ready to adopt eHealth in Primary Health Care. *Proceedings - 2021 International Seminar on Application for Technology of Information and Communication: IT Opportunities and Creativities for Digital Innovation and Communication within Global Pandemic, ISemantic 2021*, 273–279. https://doi.org/10.1109/ISEMANTIC52711.2021.9573228

Shrivastava, S., Srikanth, T. K., & VS, D. (2020). E-Governance for Healthcare Service Delivery in India: Challenges and Opportunities in Security and Privacy. *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, 180–183. https://doi.org/10.1145/3428502.3428527

Smaradottir, B. F. (2018). Security Management in Electronic Health Records: Attitudes and Experiences Among Health Care Professionals. In *2018 International Conference on Computational Science and Computational Intelligence (CSCI), Computational Science and Computational Intelligence (CSCI), 2018 International Conference on, CSCI* (pp. 715–719). IEEE. https://doi.org/10.1109/CSCI46756.2018.00143

Vårdskiftet. (2021a). *IVO granskar programmet FVM* [online]. Available from: https://www.vgregion.se/ halsa-och-vard/vardgivarwebben/vardskiftet/aktuellt-vardskiftet/aktuellt/ivo-granskar-programmet- fvm/[Accessed 7 February 2022].

Vårdskiftet. (2021b). *Vi ställer om vården* [online]. Available from: https://www.vgregion.se/halsa-och-vard/vardgivarwebben/vardskiftet/vi-staller-om- sjukvarden/[Accessed 27 January 2022].

Vårdskiftet. (2022). *Millennium* [online]. Available from: https://www.vgregion.se/halsa-och-vard/vardgivarwebben/vardskiftet/framtidens-vardinformationsmiljo/fragor-och-svar/millennium/[Accessed 20 Mars 2022].

Vetenskapsrådet. (2017). *God forskningssed*. Vetenskapsrådet.

Webster, J., & Watson, R. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*. https://doi.org/10.2307/4132319

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security Fourth Edition* (Fourth). Course Technology.

Williamson, K., Bow, A., Burstein, F., Darke, P., Harvey, R., Tanner, K., Johanson, G., McKemmish, S., Oosthuizen, M., Saule, S., Schauder, D., & Shanks, G. (2002). *Research methods for students, academics and professionals Information* (Second).

Winge, M., Johannesson, P., Perjons, E., & Wangler, B. (2015). The coordination hub: Toward patient-centered and collaborative care processes. *Health Informatics Journal*, *21*(4), 284–305. https://doi.org/10.1177/1460458214528822

Åhlfeldt, R.-M. (2008). *Information security in distributed healthcare : exploring the needs for achieving patient safety and patient privacy*.

Department of Computer and Systems Sciences, Stockholm University.

Åhlfeldt, R. M., Persson, A., Rexhepi, H., & Wåhlander, K. (2016). Supporting Active Patient and Health Care Collaboration: A Prototype for Future Health Care Information Systems. *Health Informatics Journal*, *22*(4), 839–853. https://doi.org/10.1177/1460458215590862

Öström Zetterman, I. (2021). *NPÖ, Nationell patientöversikt* [online]. Vårdgivarguiden. Available from: https://vardgivarguiden.se/it-stod/e-tjanster-och-system/nationell-patientoversikt-npo/[Accessed 25 April 2022].

Appendices

A - Interview Guide

Interview Guide

- Thank the person
- Introduce myself

Before we begin, I need to inform you about your rights and the ethical principles:

Ethics:

- My thesis aims to investigate the challenges and opportunities of information security with an integrated patient record system at the regional level, with the Millennium as the leading example.
- The interview aims to collect data and understand the challenges and opportunities of information security with an integrated patient record system.
- You have the right to cancel the interview, and you do not have to answer questions that feel inappropriate. Furthermore, you have the right to withdraw from the study whenever you want, which means I will delete all information I have received about and from you. You also have the right to anonymity and access to the study when it is ready.
- All data collected during the interview will be confidential, so the information will only be used for the purpose of the study and will not be published anywhere; no personal data will be processed during this study. I will not use your name in the study. I will only describe your work role.
- Do you have any questions or something you want to add?
- Am I allowed to audio record the interview?

Examples of questions that can be asked about the different themes:

1. We can start with you introducing yourself. What is your name? What is your professional role? How long have you worked in the role?
2. What is your relation to FVM? How long have you been involved in the work regarding FVM?

General questions - Digitalisation in healthcare:

1. What do you think about digitalisation in healthcare?
    a. Advantages
    b. Disadvantages

General questions - Information security in healthcare:

2. What should be done to maintain information security in healthcare?
3. What information security issues are there in healthcare?
4. What security measures do you think are important for maintaining information security in healthcare?

General questions - Information security in integrated EHR:

1. How would you define an electronic patient record?
2. Security measures are important to protect sensitive patient information. What security measures should be taken to safeguard integrated EHR systems?
3. In what way is patient information sent to other care providers today?

FVM and Millennium:

1. What opportunities are there with the new system Millennium?
2. What (security) challenges arise with the integration of systems (such as the Millennium)?
3. How is patient information stored within the Millennium?
4. How is information security met in the Millennium?
5. Does the Millennium comply with the laws?
6. What are Millennium's goals for information security?
7. How can information security be improved within the Millennium?

1. Is there anything you would like to add or something you would like to point out that I did not ask you during the interview?