Computer Science and Artificial Intelligence Laboratory

Technical Report

MIT-CSAIL-TR-2018-001 January 24, 2018

Privacy and Security Risks for National Health Records Systems

Ahmed Alawaji and Karen Sollins

massachusetts institute of technology, cambridge, ma 02139 usa — www.csail.mit.edu

Privacy and Security Risks for National Health Records Systems

by

Ahmed S. Alawaji
B.S., University of Bradford (2010)

Submitted to the System Design and Management Program and
the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degrees of
Master of Science in Engineering and Management
and
Master of Science in Electrical Engineering and Computer Science
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
February 2018

Author . . . . . .
System Design and Management Program and
the Department of Electrical Engineering and Computer Science
January 15, 2018

Certified by. . . . . .
Karen Sollins
Principal Research Scientist, Computer Science and Artificial Intelligence Lab
Thesis Supervisor

Certified by. . . . . .
Chintan H. Vaishnav
Senior Lecturer, MIT Sloan School of Management
Thesis Supervisor

Accepted by . . . . . .
Joan S. Rubin
Executive Director, System Design and Management

Accepted by . . . . . .
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

This page intentionally left blank

Privacy and Security Risks for National Health Records Systems

by

Ahmed S. Alawaji
B.S., University of Bradford (2010)

Submitted to the System Design and Management Program and
the Department of Electrical Engineering and Computer Science
on January 15, 2018 in partial fulfillment of the
requirements for the degrees of
Master of Science in Engineering and Management
and
Master of Science in Electrical Engineering and Computer Science

Abstract

A review of national health records (NEHR) systems shows that privacy and security risks have a profound impact on the success of such projects. Countries have different approaches when dealing with privacy and security considerations. The aims of this study were to explore how governments can design secure national health records systems. To do that systematically, we developed a framework to analyze NEHR systems. We then applied the framework to investigate the privacy and security risks in these systems. The studied systems demonstrate that getting privacy and security right have a considerable impact on the success of NEHR projects. Also, our study reveals that the healthcare system structure has a substantial impact on the adoption and usage rates of the system. The studied cases uncover many opportunities for improving privacy and security measures in future projects. The framework demonstrates the utility of applying it to the three cases.

Thesis Supervisor: Karen Sollins
Title: Principal Research Scientist, CSAIL

Thesis Supervisor: Chintan Vaishnav
Title: Senior Lecturer of Management Science

This page intentionally left blank

Acknowledgement

This long journey would not have been successful without the many people that have supported me throughout my time at MIT.

First, I would like to express deep gratitude to my advisor, Karen Sollins, for stimulating my research direction and keeping me on course during the past two years. Karen was always available to answer my questions and helped me brainstorm solutions to difficult problems. Her ingenious creativity and relentless optimism have pushed me to achieve more than I ever thought possible.

I would also like to thank Chintan Vaishnav for agreeing to be my co-advisor during the last year. Chintan helped me navigate the difficulties of structuring the thesis and was never short on great advice.

Thanks to all my friends who have made my time here more enjoyable, my SDM core team in particular!

Finally, and most importantly, I would like to thank my wife, Rawan. Her support, encouragement, quiet patience and unwavering love were undeniably the bedrock upon which the past few years of my life have been built. Rawan has been my best friend and great companion, and helped me get through this period in the most positive way. I thank my parents, Suliman and Amal, for allowing me to realize my own potential. The support they have provided me over the years was the greatest gift anyone has ever given. Also, I thank my siblings who offered invaluable support and humor over the years.

Contents

List of Figures

List of Tables

1 Introduction

The thesis explores the privacy and security risks of national electronic health records (NEHR) systems. The scale of NEHR projects and the sensitivity of health data increase the chances of privacy violations. One of the thesis aims is to outline how a government can design a secure and private national health records systems. The second objective is to explore and investigate the current security and privacy controls used in implemented systems.

The thesis studies the national health record systems of Australia, Denmark, and France using a proposed framework. It outlines the most crucial components of the privacy and security of NEHR systems including both the healthcare and NEHR systems. Although our target is the NEHR of a country, we must consider that the NEHR is only one part of a country's overall healthcare system. Hence, our analysis begins with an overview of the healthcare system and then considers the requirements and design constraints that places the NEHR. In the healthcare system, the framework tries to capture the structure, stakeholders, and the healthcare goals of the country. This includes identifying the direct and indirect stakeholders' relations to understand the influence of each of the stakeholders on the NEHR system. The framework also explores how the healthcare system of the selected countries is financed to measure the effect of the financial structure on the NEHR.

The framework was used to study three cases in Australia, Denmark, and France. All the chosen countries have already implemented an NEHR system. We applied the framework to each of the selected countries. Applying the framework to the cases unlocked many lessons and insights that can be utilized for future NEHR systems implementations.

Finally, the framework results and conclusions were discussed to outlines some recommendations on the privacy and security tradeoffs of NEHR systems.

Contribution: The thesis provides the following contributions:

1. The NEHR framework: we present a framework to analyze the privacy and security of national health records systems. The framework was used to analyze the NEHR systems of Australia, Denmark, and France. The framework investigated both the healthcare and NEHR systems. It also provides a common comparison structure even when the NEHR systems of the studied countries are not alike.
2. Three NEHR case studies: The thesis outlines the different elements of the NEHR system in each of the studied countries. The work summarizes the healthcare structure and goals of each of the studied countries. It also identifies the existing controls used to secure NEHR systems. Followed by a discussion on the potential risks of the existing security mechanisms.
3. NEHR System Implementation Questions: The thesis provides a list of questions derived from these cases for each of the system development stages. The developed stages considered are analysis, design, and evaluation.

4. NEHR privacy and security tradeoffs: The framework and the studied cases provide a plethora of lessons that can be used as guidelines for future NEHR projects. The last chapter summarizes these findings along with questions that can help system designers to build a secure NEHR system.

2 Background and Motivation

The use of Electronic Health Records is critical to the future of healthcare management. Many nations have developed NEHR in response to this. The rise of these systems necessarily invokes issues surrounding data security and the privacy of individuals. This research is a comparative study of the security and privacy issues in the following NEHR systems: Australia, Denmark, and France. The privacy and security issues of national health record (NEHR) systems cannot be analyzed without examining the building components of NEHR systems. In most cases, electronic health record systems are the primary data source for NEHR systems. The background chapter summaries the various functions and processes carried out in both EHR and NEHR systems. The chapter's goal is to provide sufficient background to understand these systems' goals and functions. Subsequently, the privacy and security definitions are discussed and aligned to justify the scope and motivation for the thesis. Moreover, the section explores the current privacy and security solutions in the context of healthcare based on the current literature.

2.1 Electronic Health Record System

Electronic health records (EHR) systems have become an indispensable part of the healthcare processes and procedures. These systems maintain patients' records and facilitate information exchange between departments. In the past, paper records were used to maintain patients' records in a central department that specializes in

managing patients' records. Every medical folder contained one of the patient's records including demographic data, medical history, family history, x-ray images, and medications history. Until recently, paper-based records were the only approach used to collect and maintain patients' records. However, the use of paper medical records has shown many limitations. Paper records are prone to human errors and inconsistencies because content cannot be quickly checked. Furthermore, as a patient gets older or sicker, his medical folder becomes large and hard to track. Also, manual folders are passive in their natures which can limit how the records can be utilized to prevent health issues or plan for care [1]. Further, papers cannot be easily summarized and analyzed to track and investigate changes to a group of patients that have similar characteristics or health conditions. Sharing paper medical records across providers is costly and prone to privacy violations.

Advances in information technologies, the decreased cost of data storage, and increased citizens expectations about public health have accelerated EHR adoptions considerably. The first EHR systems appeared in the late 1960s in the United States. Following that, more than 70 hospitals started medical records databases projects by 1969 [1]. Although the components that define EHR system varies from hospital to another, the Healthcare Information and Management Systems Society (HIMSS) defines an EHR system as:

> "a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problem, medications,

vital signs, past medical history, immunizations, laboratory data, and radiology reports. The EHR automates and streamlines the clinician's workflow. The EHR has the ability to generate a complete record of a clinical patients encounter, as well as supporting other care-related activities directly or indirectly via interface-Including evidence-based decision support, quality management, and outcomes reporting [2]"

In most cases, EHR systems have five main functional components including an integrated view of patients data, clinical order entry, clinical decision support (CDS), knowledge repository, and integrated communication and reporting support [1]. The *integrated view* of patient data show patient's data coming from all the systems and databases. The component allows physicians and nurses to view medical data of different types ranging from text summaries to video files. Moreover, physicians can access data coming from other departments like viewing lab results and x-ray images. *Clinical order entry* allows doctors to issue medical requests to other entities inside or outside the health entity. For instance, a doctor can request x-ray test for a specific part of the body. The request goes to the responsible person in the radiology department to carry out the scan whenever the patient comes. The *clinical decision support* (CDS) component is used to help the care team members in making better decisions for the patients. This function encompasses many tools including alerts, notifications, suggestions, and templates. For instance, CDS shows and sends automatic reminders about immunization and appointments for both physicians and patients. CDS is also used to suggest tests

and scans according to some specified criteria. Another component that most EHR systems have is the *knowledge repository*. Although physicians can access knowledge instantly from browsers to find answers to clinical-related questions, some EHR systems show summarized information about medical cases when the physician makes an entry order. Accessing relevant clinical knowledge and literature can improve doctors' efficiency. It can also increase patients' safety because physicians can verify conditions with a reliable source of knowledge.

Finally, physicians have to communicate with other departments and entities inside and outside the healthcare organization. *Communication and reporting* is another key component used in many EHRs. The function enables general practitioners to submit referrals to specialized doctors while attaching important information needed by the specialist.

The use of EHR has shown many advantages regarding reducing cost, improving patients' safety, and increasing physicians' efficiency. According to Ball and Lillis, EHR systems have transformed the patient/physician relationship in five major areas including health education, disease management, clinical decision support, physician/patient communication, and other administrative processes [3]. Several studies reported that EHR systems decreased conducting unnecessary or repeated tests in many settings during the health delivery process. In one study, EHR has shown to reduce diagnostic tests per visit by 14%. Also, the same study found that the system was responsible for reducing tests cost by 12.9%. Another study found 18% reduction in ordered tests in an emergency department after implementing an

EHR solution. Furthermore, the use of EHR systems increases patients' safety through checking order entries and computerized alerts. The clinical order entry component has shown to reduce adverse drug events and medication errors by 55% [4].Several studies have examined the impact of computer alerts on the delivery of healthcare and patients' health. One study found that computer alerts have increase immunizations by 35%-50%. Another study found that alerts have contributed to improving treatments by 11% for hypertension patients in primary clinics [5]. For physicians, historical records can be obtained quickly to make faster healthcare decisions. For health organizations, automatic alerts and reminders increase revenues because they increase patients visits. Also, a study found that hospitals that use EHRs effectively have better operational performance than those that do not [5].

2.2 Health Data Network

Computer networks allow systems to share resources or exchange files. Networks are used not only inside health care facilities but also outside the facility. The use of networks allows sharing resources and exchanging information between computers and health systems. Inside the health facility, a hospital or a clinic can print documents using one printer. Outside the healthcare facility, networks allow computers to exchange important information and data about patients. NEHR systems rely on networks to exchange data between providers. The design of the NEHR network depends on many functional, organizational, and technical factors. The network architecture can be either centralized or de-centralized. In the

centralized network, all EHR systems communicate to a single database instance. In the de-centralized network, systems can communicate directly to each other. Also, the network can support different healthcare functions and process including prescriptions, referrals, or billing. Moreover, some networks use the Internet to exchange data, whereas other networks are built in a private network infrastructure [6]. Networks also can be built and maintained by government entities or by private companies. While networks can save millions by utilizing existing resources and exchanging data between stations, there are some potential risks of using networks. Networks are susceptible to DDoS attacks which can hinder connectivity between systems for a while.

2.3 National Electronic Health Records System (NEHR)

Although healthcare organizations have realized some of the benefits of EHR systems, other benefits can be realized with national health records systems (NEHR). Researchers have predicted that EHR systems' use cases and scope will evolve from serving a single health entity to a network of entities [3]. In most cases, the building foundation for national electronic health records systems is hospital electronic health records systems.

There is no universal definition for national health records systems mainly due to the variations in the architecture and functions of these systems. The key function of an NEHR is to allow patients and health providers to view health records that are important for caring for the patient. Nevertheless, countries may define other secondary goals that solve public health issues specific to the country or the region.

In Australia, for example, one of the NEHR system's objectives is to improve health outcomes for indigenous Australians [7]. Other countries have defined objectives related to specific health problems that are rampant in the country like smoking. These variations in secondary goals have resulted in wide range of systems components implemented according to the needs and priorities of the nation. Nonetheless, the single most important system component is the database that can feed the NEHR system with accurate, relevant, and reliable data. This component stores patients' records and information that come from different sources of data depending on the availability of records and data extraction processes. For instance, some countries start the system with initial records extracted from Medicare, whereas other countries build the system with data extracted from hospitals EHR systems. In most cases, the most important source of data is hospitals or clinics EHR systems. As a result, interpretability between EHR systems and the national system is one of the pre-requisites for building a centralized electronic health records system [8]. Like in most national systems, implementing an NEHR is a challenge due to the high number of stakeholders involved in the project. Successful implementation of an NEHR requires the involvement and collaboration of regulators, insurance providers, pharmacies, laboratories, and healthcare providers.

Current NEHR implementations have revealed that technical issues are not the most challenging aspects of the systems. Instead, social and organizational barriers are the hardest issues to tackle and manage [9]. A recent study explored NEHR

implementations in five countries found change management, doctors' acceptance, organizational change, and data controls are the most critical areas when designing these systems. For change management, the lack of proper collaboration and communication between government entities can lead to system's failure. Instead, many researchers debated that the success of nationwide systems projects cannot be realized without meaningful collaboration between private and public entities. Collaboration should not only be present during the system design stage but also during policies and regulation formulation [9].

2.4 NEHR Privacy and Security

The success of NEHR projects depends on many legal, technical, organizational, social, and economic factors. NEHR systems encompass a large volume of sensitive data that is extracted from various sources. As a result, designing NEHR systems to handle and avoid privacy violations is one of the most important factors for NEHR success. In this section, we attempt to define the boundaries of privacy and security for national health record systems is discussed. Also, the section discusses the history of privacy and security risks that led to the introduction to many of the current regulations and policies in the healthcare sector. The purpose of the section is to summarize privacy and security arguments especially those related to healthcare data. Finally, the last section explores potential privacy and security solutions implemented in the healthcare industry.

2.4.1 Privacy

Data privacy in healthcare is one of the most challenging issues due to the sensitivity of medical data. The need for data privacy laws, regulations, and principles was triggered by advances in information technologies. The backbone of many of the current privacy laws in the United States and other countries was the Fair Information Practice Principles (FIPPS). The principles were developed as a result of the proliferation of personal records databases in federal agencies. They were formulated in 1973 to handle privacy concerns about data use cases and collection processes. These are FIPPS principles with brief descriptions:

1. **Transparency:** Organizations should be transparent with consumers about what data is being collected and how this data is handled. This includes providing users with a clear privacy policy statement that explains all the data related aspects.
2. **Individual Participation:** In this principle, organizations should allow people to know what the organization knows about them. This also includes giving individuals the opportunity to correct any errors in the collected data.
3. **Purpose Specification:** Organizations must specify the purpose of collected data. They also should get permission from individuals to use the data for the specified purpose.
4. **Data Minimization:** The data collected has to be relevant to the task specified earlier. Organization should ensure that the specified task cannot be accomplished without the collected data. Otherwise, the data should not be stored.

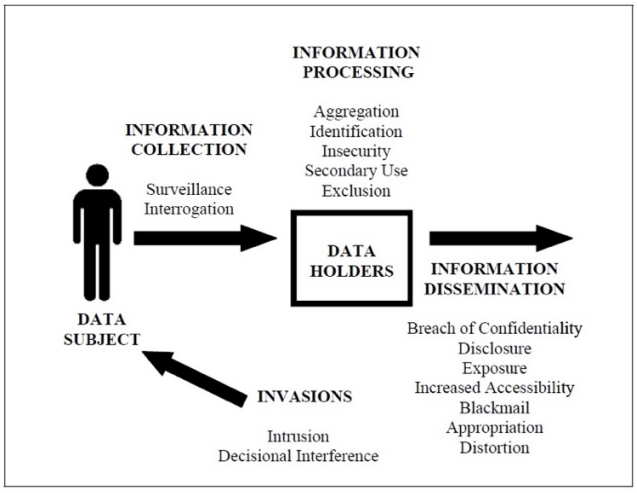
5. **Use Limitation:** The data cannot be used for other than the specified purpose(s). Organization should ensure that collected data used in the purpose identified in the previous principle. Otherwise, they have to inform users of other uses and only if users accept the data can be used.
6. **Data Quality and Integrity:** Organizations are responsible for the quality and integrity of the data. This includes avoiding collecting inaccurate data.
7. **Security:** An organization has to ensure the security of the data. This includes defining different access levels based on the complexity of the system and the structure of the organization.
8. **Accountability and Auditing:** Organizations should be accountable for complying with the laws and regulations. This includes auditing activities for the collected data in order to keep track of the uses and misuse of the collected data.

These principles have become the founding ground for many laws and regulations formulated in the United States. The Privacy Act of 1974 was one of the first regulations driven from these principles. The act defines the practices that govern the collection, use, dissemination of personally identifiable information. Following this act, many regulations were introduced for protecting data privacy in other industries and domains. For example, the Children Online Privacy Protection Act was introduced to protect children data online, whereas the Health Insurance Portability and Accountability Act (HIPAA) specifies the conditions and requirements for protecting and sharing medical data. Other countries have

granted privacy rights according to what is considered a privacy violation within the nation. In Europe, the Data Protection Directive defines a similar set of policies that protect the right to privacy for Europeans.

While the FIPPS define important aspects of data privacy, they fail to define the boundary of data privacy. Solove defined data privacy by categorizing the issues that can occur as a result of violating privacy [10]. His privacy taxonomy framework classifies privacy violations based on four main activities: information collection, information processing, information dissemination, and invasion. The diagram below was derived from his privacy taxonomy paper which shows the different sub-activities under the categories identified earlier.

Figure 1: Privacy Taxonomy [8]



Although these activities define privacy abuses in different domains, only some activities within the information processing, dissemination and invasions groups are relevant to NEHR systems. Another issue with the framework is that it derives many of the examples and arguments based on laws and cases from the United

States. Studies have shown that the value of data varies significantly between nations. One study used a conjoint analysis method to measure data value for people in different countries. The research surveyed over 900 people in the United States, India, China, Great Britain, and Germany. The result shows that people from different countries have a different value for data. For instance, the data value for people from China was low across all domains. On the other hand, people from India valued financial information compared to other data types. For health records, Germans assigns the highest value compared to people from all other countries [11].

The Fair Information Practices Principles were the main sources of many of the laws developed in different domains including the Health Insurance Portability and Accountability Act (HIPAA). HIPAA consists of five titles all of which are related insurance and fraud protection except for the second, known as the administrative simplification provision. It defines procedures and guidelines for maintaining and protecting the security and privacy of health information. The title also details the criminal penalties for violating any of the defined procedures. HIPAA regulates the use and disclosure of protected health information (PHI) regarding privacy and security. It also specifies the cases in which PHI can be disclosed like in court orders.

These policies and regulations have increased the cost of privacy violations dramatically. For instance, a record loss in the healthcare industry cost about $233, compared to $136 on average for losing a record in other industries [12].

Further, privacy violations can negatively impact users' participation and registration in NEHR systems which lead to low adoption rate from health providers. The low adoption rates could cause project failure which can cost countries billions of dollars. Thus, countries have to invest heavily in understanding privacy risks before implementing NEHR systems. This requires countries to formulate and implement policies, tools, processes, and entities that can reduce privacy violations.

2.4.2 Security

Defining security is complex because the definition varies based on the system and the stakeholders that use the system. Security is about protecting users' data in national electronic health records systems. HIPPA's second title has outlined many measures on how an organization must protect protected health information (PHI). The act requires organizations to perform risk analysis, administrative, technical, and physical activities to ensure data security. For the risk analysis, the health organization is required to evaluate likelihood and impact of any risks to health data and to implement security measures required to address these risks. For the administrative side, organizations have to define appropriate security policies and processes to secure the system's data. Also, organizations are responsible for the training and development activities of employees to ensure compliance. From the technical side, systems must implement the right access control and auditing procedures. The security of NEHR systems relies on the tools, methods, and processes required to design, implement, and test the NEHR system. Many studies

have discussed and tested security and privacy factors of EHR including system architecture, access control, emergency, data sharing, search, and data anonymizations techniques. However, limited studies have explored security and privacy issues for national health records systems. One of the aims of this work is to define security risks of NEHR systems. Finally, some recommendations are made to help countries in securing these systems.

2.4.3 Current Solutions

The increased number of security and privacy violations and high cost of violations have motivated health entities to implement security solutions to mitigate these risks. Some of these solutions are used in many systems to improve privacy and security, others are implemented only in the healthcare sector. EHR systems' requirements share many similarities with NEHR systems. The overlap in the system requirements of both systems makes some of the privacy and security solutions in EHR effective in NEHR systems. To ensure privacy and security, an organization requires a blend of technical solutions, governance procedures, administrative processes, and employees' capabilities.

From the technical side, system architecture, authorization methods, authentication techniques, data encryption tools, and audit logs are some of the most fundamental techniques. There are many system architecture designs, but the two most common approaches are central and distributed architectures. The central design stores patients record in a single database that handles all systems related operations. On the other hand, the distributed architecture allows systems

to exchange records while maintaining appropriate security and data integrity measures. Access control or authorization models are used to restrict and control access to the system's data. There are three methods to define access controls: role-based, attribute-based, and identity-based [13]. These measures are not only applied to the systems level but also to the different layers of systems including application, middleware, operating system, and hardware [14]. Due to its simplicity, the most popular access method in EHR systems is role-based access control (RBAC). The method gives access to users based on their role. For instance, physicians can access all the patients' data unless restricted by the patient. On the other hand, administrative departments can only access a high-level overview of the billing data. Authentication is another major research area which is concerned with verifying the identity of users. There are many authentication techniques used in EHR including users' credentials, smart cards, telelogin, biometric, and digital certificates. In most cases, security, usability, and economy are the most important comparison factors when choosing the optimal authentication method. For instance, if security is the most important factor and the cost is not an issue, biometrics scan is used for authentication [15]. For data encryption, most systems apply SSL-encryption during data transfer.Secure Sockets Layer (SSL) is a security standard used for establishing an encrypted link between a web server and a browser. Other systems apply encryption on different elements like for passwords or shared documents. Audit logs store information about access and medical records changes [16]. Further, Since EHR systems are connected to

other systems using computer networks, they are vulnerable to networks attacks that are caused by network protocols and topology [14]. For example, DDoS attacks on the network can hinder the system which can lead to either losing data or inaccessible systems. Having inaccessible medical systems can cause serious safety issues especially during emergencies.

Furthermore, organizational procedures are another important dimension which can ensure the sustainability of processes and tools used to protect privacy. Governance procedures include formulating policies that create incentives for departments to ensure compliance. Also, key performance indicator (KPIs) are used to monitor logs and abnormal activities across the system. Security processes are another important organizational element to ensure compliance. This includes establishing a department responsible for information privacy and security. The team responsibilities and goals should be mapped to the security and privacy requirements and needs of the organization. Finally, training and development activities is another essential element to protect users' private data.

3 A Framework for NEHR Privacy and Security

There are two central questions this work tries to tackle:

1. How can governments design a secure and private national health records system?
2. Why some countries are more successful than others in enforcing security and privacy measures in their NEHR systems?

The choice of research methods depends on many factors including what kind of questions the research is answering and how much control on the behavioral event the work requires. In theory, this thesis questions can be answered by either experiments or case studies. In the case of national electronic health systems, privacy cannot be easily measured by experiments. Also, experiments require extensive system design and implementation efforts to validate and test different considerations for an NEHR system. While both experiments and case studies focus on analyzing contemporary events, they require different ways of controlling events. In experiments, researchers have to manipulate behavior systematically to observe reactions. However, the extent of this work cannot be tested easily through experiments. The work requires finding links between the different system factors to understand what works and what does not for NEHR security considerations [12]. These considerations motivated the use of the case study methodology to

analyze the factors that countries have to consider in NEHR systems. Yin defines a case study according to both its scope and features. Regarding scope, a case study is an empirical inquiry that "Investigates a contemporary phenomenon in depth and within the real-world context" [12].

A case study relies on numerous sources of evidence and previous theoretical work to guide the data collection and analysis processes and can be answered by single or multiple cases. Multiple cases can provide better analysis and depth to the conclusions. Hence, the thesis studies the implementation of NEHR in Australia, Denmark, and France. These countries were selected because they already have implemented an NEHR system and it is currently operational. Another factor was the availability of reliable data sources that can be used to validate and understand the different elements of the NEHR system. The studied cases are used to draw appropriate conclusions and recommendations for future projects.

3.1 NEHR FRAMEWORK

In this work, we define and use a framework to analyze the current landscape of NEHR privacy and security issues in the three countries. The framework intentionally does not try to capture all the elements involved in the healthcare delivery process but rather the main components that are essential in securing NEHR systems. The framework uses a top-down approach to examine each of the countries: healthcare system, NEHR system, and the security controls. In the framework, we begin with an analysis of a country's overall healthcare system

including goals, structure, stakeholders, and the users. Then, the NEHR system is analyzed in all the relevant areas.

3.1.1 The Healthcare System

One of the essential framework components is understanding the healthcare system. Understanding the healthcare system requires analyzing all stakeholders involved in the healthcare delivery process and their objectives. NEHR success depends on the acceptance and collaboration of every stakeholder in the healthcare delivery process. Securing these systems requires the cooperation of many of the healthcare system stakeholders including government entities, healthcare providers, patients, and industry partners. In this section, the framework tries to capture how the government governs and finance the healthcare system and how the healthcare is delivered. Government is not only responsible for forming regulations and policies but also allocating financial and human resources to manage the NEHR system. Furthermore, states form entities that enforce privacy and security compliance. Some of these entities handle privacy complaints filed by any of the involved stakeholders. In most countries, the healthcare process starts with a visit to the primary care physician or general practitioner. There are many variations in how primary care is delivered which affect the adoption and usage of NEHR systems. Another major area is how the healthcare system is financed and covered. This determines how much influence the government has on healthcare providers. These elements have been studied in the context of each country to understand

how government can align the right incentives and governance structure to ensure NEHR privacy and security.

NEHR systems are not just a central database of patients' medical records. They are formed based on many other systems. Therefore, the success of NEHR projects depends on the readiness of the country for such projects. Eysenbach has articulated a broad definition of e-health that captures most of what the framework tries to tackle regarding e-health. He defined e-health as:

> "An emerging field in the intersection of medical informatics, public health, and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and commitment for networked, global thinking, to improve healthcare locally, regionally, and worldwide by using information and communication technology" [13].

Building NEHR systems requires an e-health mindset which requires time to build. In most cases, a government formulates a long-term e-health strategy with multiple initiatives. Every initiative includes several planned projects to solve some of the country health-related issues using technology. However, delivering successful e-health systems takes time because the country has to develop its technical skills and capabilities. From the technical side, exploring operational e-health systems can help understand how the NEHR will get data. The goal of this section is

capture the most relevant policies, capabilities, and systems that have an impact on the security and privacy of NEHR systems.

3.1.2 The NEHR System

After analyzing the healthcare system, the NEHR system is analyzed. This section answers few questions including: (a) why the system was designed in the first place; (b) what stakeholders are involved in the planning and implementation phases; and (c) how the system works, and what is the current state of the system. It also tries to explore the building components of the NEHR system in various countries. Another important aspect is understanding data sources for these systems. Moreover, analyzing the history of implementing the system is explored especially when there were previous failed system implementations. Also, this section tries to explore the extent in which systems vendors are involved in delivering the NEHR system.

3.1.2.1 NEHR Goals

Countries have different goals when it comes to implementing an NEHR. However, the following are some of the important goals for an NEHR:

1. Improve healthcare outcomes for citizens.
2. Reduce healthcare cost by reducing repeated tests.
3. Increase healthcare efficiency by improving coordination between healthcare providers.
4. Facilitate public health policy planning by utilizing health data.

5. Develop industry capabilities by ensuring industries are built around electronic healthcare solutions.

3.1.2.2 NEHR Stakeholders

In this section, the stakeholders involved in the different stages of the NEHR project are listed. Moreover, the stakeholder's analysis can reveal the architectural decisions that are central to NEHR security in some of the studied countries. The potential list of NEHR stakeholders may contain the following entities:

- Government: It is responsible for developing policies to start the NEHR project. It also formulates policies to protect patients' records. The government structure varies based on the country's governance system. Policies are developed either locally (city or district based) or on the national level.
- Healthcare standards authority: Countries either develop standards from scratch or use existing standards. Standards are vital to store the integrity of health data across various systems. Health standards are used for storing data, reporting, and exchanging information between systems. HL7 is one of the most popular standards and is used to facilitate the exchange of health data between electronic systems. ICD standards are also used for diseases and health problems classifications [1].
- Data protection agency: This agency main responsibility is to enforce regulations for protecting data in various industries. The agency monitors data issues like quality issues, data breaches, and users' complaints.

- Systems provider: Technology companies develop most of the infrastructure and standards used for public and private entities. The use of existing solutions can reduce time required to implement systems. In addition, it allows government entities to utilize the expertise of such outside companies.
- Users: This category is concerned only with patients whose medical records are stored online in the NEHR system. Different systems provide different ways of controlling the system's data.
- Healthcare providers: This category includes entities that are part of healthcare delivery process. The entities under this category varies in different countries based on the healthcare system. Health providers include primary care clinics, dentist, hospitals, labs, or pharmacies.
- Health insurance providers: In most countries, there are public and private health insurance providers. In the public insurance, the schema is used for a specific subset of the population like the elderly. The private is supplied and paid for by private companies and may provide more coverage than public insurance.
- Research and academia: These organizations use the data for research purposes.

The table below summarizes the roles played by each of the stakeholders concerning NEHR systems. Regarding privacy, stakeholders may have one of the following roles: data protection, data generation, or data consumption.

Entity	Privacy and Security Role		
	Data Protection	Data Provider	Data Consumption
Government	✓		✓
Hospitals		✓	✓
Labs		✓	
Data protection agency	✓		
Health insurance provider		✓	✓
Research			✓
Patients	✓	✓	
Physicians		✓	✓
System developer	✓		

3.1.2.3 NEHR Architecture

In this section, the architecture of the system is summarized. The architecture lists all the system's components with relation to its potential users. This section is useful to understand the features and functions delivered by the system for each of the identified stakeholders. It can also help in identifying the tradeoffs for the different design decisions.

3.1.2.4 Health Data Network

As discussed earlier, health data networks are used for many processes in the healthcare system. This section analyzes the network implemented in each of the

studied countries. From the technical side, the network's architecture, security, and design are discussed. From the operation side, the network processes, functions, and procedures are examined.

3.1.2.5 NEHR State

Finally, the current state of the NEHR system is examined. This section compares some of the important performance indicators including the number of registered users and the number of uploaded documents. The number of registered users provides a clue about the acceptance rate of the system. Further, the number of uploaded documents provides a clue about how the system is used.

3.1.3 NEHR Privacy and Security

After analyzing the NEHR system, this section dives into the privacy and security components of the system. This section discusses the authentication, authorization, and governance techniques used in each of the case studies. The goal of exploring these elements is to understand what works and what does not in enforcing privacy and security in NEHR. For authentication, the framework explores the authentication tools used in NEHR systems. One major authentication area in NEHR is the use of unique national identification numbers. Moreover, the framework tries to analyze the different layers of authentication used for both patients and healthcare providers. The second area is medical records authorizations elements. This includes understanding how authorization works in the current NEHR implementations. One major area is how authorization to patient records is granted during emergencies. Finally, the last section deals with

issues related to enforcing privacy and security. This includes how NEHR systems implement logs auditing and data breach notification features. Moreover, the section tries to explore how NEHR government entities deal with data integrity and breaches matters.

4 NEHR Case Studies

This chapter outlines the Australian, Danish, and French case studies. We analyzed the healthcare systems of these countries. Then, the security and privacy controls for the NEHR systems have been discussed. Furthermore, the current states of NEHR systems are examined.

4.1 Australia

This section discusses the major components related to the NEHR system including the health care system and the current NEHR implementation in Australia. Australia has implemented "My Health Record" to improve the healthcare quality of Australians. Currently, more than 22% of the Australian population is registered. The primary data resources for the case are My Health Record website, the digital agency reports, and government reviews. There are other references that will be included throughout the reporting on that country as well.

4.1.1 The Health Care System

The Australian health care system is managed and governed across three levels: the national government, the state government, and the local government. The responsibilities of each of the government levels are explored in the stakeholders' section. Australia has six states and two territories which can increase the complexity of managing healthcare systems across government entities. Australia's healthcare system employs over 850,000 people and provides services to over 22 million. The central government is responsible for financing states and territories

governments. Moreover, it formulates and establishes healthcare policies and regulations. The government also funds and manages the national medical insurance scheme called “Medicare”. The program provides basic public health services for all citizens and permanent residents free of charge. Medicare funding comes from the general tax revenue. Health expenditure constituted about 10% of the GDP spending in 2017 and projected to reach 20% in 2045 [17]. The federal government also regulates medicines, devices, and other related medical products.

On the other hand, state governments own and manage public hospitals and license private hospitals. According to the Ministry of Health’s latest reports, there are in total 1331 hospitals, 52% of which are public and 48% are private hospitals. Also, the state governments are responsible for handling public health complaints to improve healthcare quality and efficiency. Also, local governments are responsible for community-related activities like public health campaigns.

More than two-thirds of the health care financing comes from the central government, and the rest comes from private insurance companies. Private health insurance is either funded by citizens or employers. Citizens pay for private insurance to get extra coverage that is not included in the public health insurance scheme. Primary care health delivery is provided by both general practitioners and specialists. Patients cannot go to specialists without referral letters from general practitioners. Primary care constitutes about 38% of Australia health expenditure, and the rest of spending goes to hospitals.

In 2008, Australia launched a national e-health strategy to improve the quality, safety, and sustainability of health systems by utilizing healthcare information and data. The project identified several challenges to the use of information technology in healthcare. The project report indicated that IT utilization in the healthcare industry was lagging compared to other sectors. One of the main identified challenges was the lack of investments in information technology solutions and infrastructure. This lack of investment resulted in limited sharing of information between different providers in the healthcare industry. To tackle these challenges, the government introduced a healthcare transformation project with five working streams: foundations, e-health solutions, change and adoption, e-health strategy, and governance. The first two working streams are the most relevant to the NEHR system.

The foundations working stream objective was to create standards, protocols, and rules for exchanging healthcare information electronically. Another primary goal was to standardize medical letters and terminology to ensure patients' safety and data accuracy. The foundation's work stream focused on five areas including identification and authentication, information protection and privacy, national e-health information standards, investment in computing infrastructure, and national broadband services.

The e-health solutions working stream objective was to build e-health solutions that could scale to eliminate redundant efforts and implementations [7]. As part of this work stream, a new national electronic health record system project was

launched in July of 2012. The system was named PCEHR “Personally Controlled Electronic Health Records” to show users that health records are entirly controlled by themselves.

A year after the launching of PCEHR, the number of registered users from health providers and patients was lower than anticipated. As a result, the Ministry of Health conducted a comprehensive review to assess the state of the system and to make recommendations for the future [18]. The committee made 38 recommendations of which twelve are related to governance, eight are related to privacy and security concerns, and four are related to technical problems.

The first recommendation was to change the system’s name from “Personally Controlled Electronic Health Records” to “My Health Records”. The committee stated that using the word “electronic” is not necessary because of the proliferation of digital government services.

Another crucial recommendation was to establish a new organization responsible for all digital health projects. The body named the "Australian Digital Health Agency” was to be accountable for all the activities and projects related to the NEHR system. Before the new agency was established, the operations and planning were conducted by two different groups: The National E-Health Transition Authority (NETA) and the PCEHR group. The new agency is responsible for all national digital health services and systems with a focus on utilizing data and technology to help patients and healthcare professionals.

4.1.2 National Health Records System

This section reviews the major component of the Australian NEHR system. The first section outlines the goals defined for the Australian NEHR system. The following section lists the stakeholders relevant to the NEHR system. It also discusses the tasks and responsibilities of each of the stakeholders. Finally, the system components are discussed and analyzed, followed by a discussion of privacy and security controls.

4.1.2.1 NEHR Goals

There are primary and secondary goals for the system design. Some goals are related to patients and others related to health providers. The Digital Health Agency defined the following goals for the current NEHR system:

- Provide access to people's health information to help overcome the fragmentation of health information. One of the government's goals is to have all Australians health records online in the NEHR system by 2018. Health providers and patients should be able to access files through mobile apps which can be built on top of the NEHR system.
- Improve the availability of health information. Interoperability between EHR systems and NEHR is one of the most technically challenging aspects of online systems especially in health due to the sensitivity of the data. The government is working on interoperability standards to enable the exchange of data between hospitals and the NEHR system. It will test the proposed

standard by 2022 in one region and then apply to the other areas if successful.

- Improve the coordination of healthcare provided to patients by healthcare providers. This goal can be achieved by different components including the secured messaging system. The system allows exchanging letters between different health providers. For example, a general practitioner can send a prescription request to a pharmacy or a referral letter to a specialist online.

4.1.2.2 NEHR Stakeholders

- Government
    - Federal Government: The federal government has formulated several laws to initiate the NEHR project. The first introduced law was the Health Identifiers Act which provides a legal framework for the use of health identifiers for both patients and health providers. My Health Records Act was the second law that was developed to support the implementation of the NEHR system.
    - State\Territory Government: The states and territories enforce the laws and regulations formulated by the federal government. States administer public hospitals, community health services, and mental health care services. Every state is responsible for the implementation of "My Health Records" in the hospitals located in the state.

    - Local Government: The local government is responsible for carrying out community-related activities and campaigns. This includes conducting trainings sessions for both citizens and health providers on how to register and use My Health Records system.
- Ministry of Health: The entity's primary goal is to improve the health of current citizens and future generations. The ministry has many divisions including health systems policy and primary care, health financing, health products regulations, population health, and other corporate divisions. Moreover, the ministry funds and manages the Australian Digital Health Agency which manages the NEHR system.
- Medicare: Medicare provides universal healthcare insurance for all Australians. It is the primary funding party for Australia's healthcare system for both citizens and permanent residents. The scheme gets its funding from the federal government which gets its funding from the general income tax.
- Australian Digital Health Agency: This agency is responsible for all digital health-related projects. The office gets its funding from the federal government, and it now administrates Australia's NEHR system. The agency supports system developers to integrate healthcare IT solutions with My Health Record system.
- Australian Information Commissioner: The agency acts as the national data protection authority and reports directly to the Prime Minister. The

agency has three main tasks that are related to privacy, freedom of information, and information policy. For privacy, the agency conducts periodic privacy assessments for any projects that handle private citizens data. The agency also monitors government agencies and report violations to ensure compliance with privacy regulations.

- System Developers: There are two main system developers' categories. The first type implemented and maintains the existing NEHR system and infrastructure. The second category is responsible for developing technical components that integrate with "My Health Record" system. The Australian Digital Health Agency provides a knowledge portal for vendors to develop, test, and deploy technical health record solutions that can work with My Health Record system.
- Patients: There are two options for patients to register to the NEHR system. Patients can either register by themselves using the official single sign-on service MyGov or get registered by health providers. Once registered, a patient can add some basic information or view medical records added by health providers.
- Healthcare Providers: There are different health providers that have different tasks including hospitals, clinics, pharmacies, and aged care providers. Each of these providers have different goals, requirements, and needs. It takes few days to implement and configure the NEHR system

for a small general practitioner clinic, whereas it may take more than a month to do the same for a hospital.

- Private Insurance Providers: Non-government sources provide about 30% of financing for health care. The use of NEHR might reduce the expenses on private insurance companies' due to the reduction of repeated tests and consultations.

4.1.2.3 NEHR Architecture

My Health Record is a centralized database for storing electronic medical records uploaded using either the official web portal or EHR systems. The system gets data from consumers, health providers, or other government systems like Medicare. This section details consumers and health providers key processes.

- **Consumers:** Consumers are individuals that will use the system to view their records or other processes. These are the main processes:
  - Manage and add a personal health summary: The system allows consumers to add several types of data including information about medicines, allergies, and adverse reactions. Consumers also can add personal health notes that can be viewed by the account holder only.
  - Manage access to documents: By default, every document stored in the system can be accessed by authorized health providers. Further, the system allows users to restrict access to certain documents.
  - Remove a document: Users can remove any of the documents added to the system. However, it is unclear if deleting the document in the system,

removes the file permanently from the database. It is also unclear if this action results in deleting the record in the hospital or the clinic EHR system.

- Manage Medicare data consent: By default, users' data is extracted from Medicare to populate the medical health record system with the latest information. The data extracted from the Medicare system includes data about medications, immunizations, organ donations, and past Medicare claims. Users have the option to stop showing these records in the system.
- View the list of people who accessed a record (Audit log): The current system component allows users to view access history, documents viewed, and view time.
- Setting up notifications: Users can get notification about who has accessed their medical records. Notifications can be sent to a mailbox, email address, or mobile phone.

- Health Providers
  - General Practitioners and Specialists:
    - View a medical record: doctors can view discharge summaries, prescription and dispense records, shared health summaries, event summaries, specialist letters, and referral letters.
    - Upload a shared health summary: The shared health summary is the patients' summary at a point in time. A doctor or a nurse can

upload this document to the system either from the online portal or the hospital's EHR system.

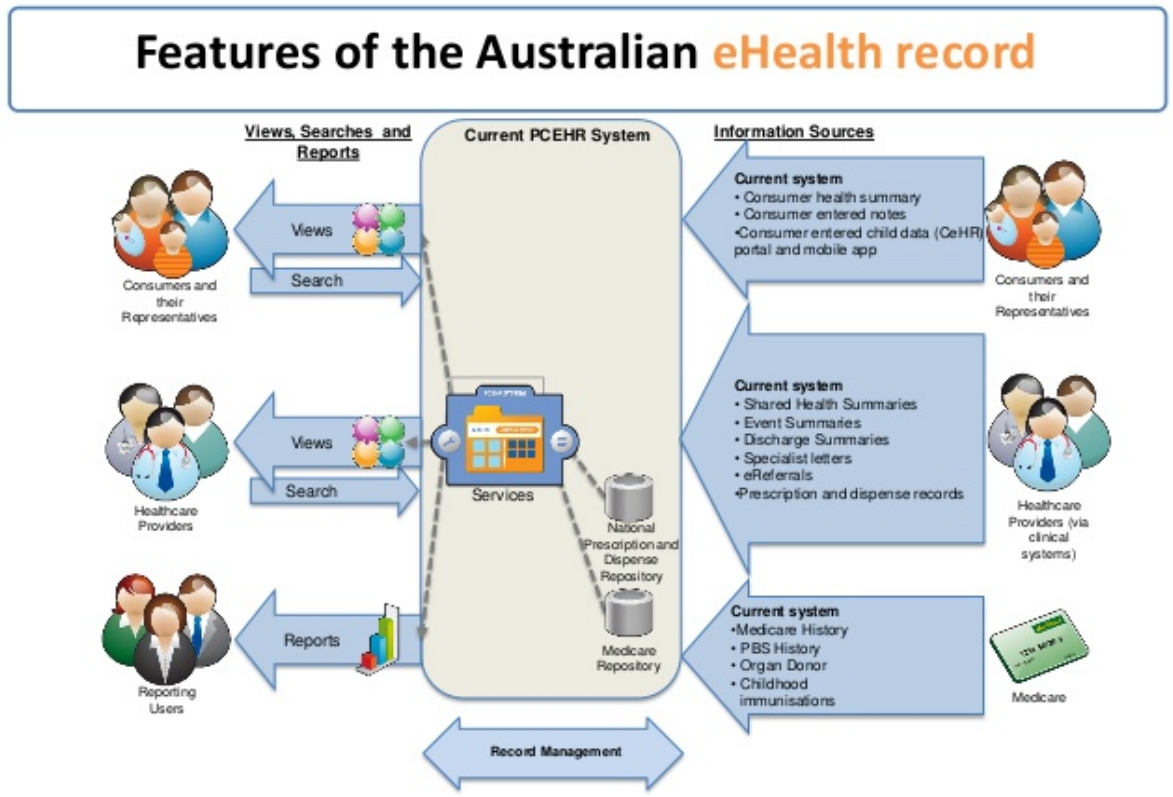
        - Upload an event summary: The event summary records important information about the patients that are related to the healthcare process.
        - Upload a prescription: Prescriptions can be uploaded through another software to My Health Record system. Then, the prescription can be viewed by pharmacist and other health providers.
    - Pharmacist:
        - View a medical record: A pharmacist can view discharge summaries, prescription and dispense records, shared health summaries, event summaries, specialist letters, and referral letters.
        - Manage the medication process: The system allows pharmacists to manage the process of prescribing, dispensing, and administering of medicines.

My Health Record system maintains a central database for all health-related records provided by different entities in Australia. The system data is entered by either account holders or healthcare providers. Furthermore, the system extracts data from the official Medicare system to reduce the time required to add some basic information. Individuals or their representatives can add information about allergies and adverse reactions. Also, they can add healthcare emergency

information in case patients are not able to communicate because of health conditions. Healthcare providers can add and see information about patients' medical history, conditions and treatments, discharge information, diagnostic imaging reports, pathology reports, and specialist letters. Physicians can access patients' medical records either through the official online portal or the hospital EHR system. Accessing the records from the online portal allows the doctors to see the latest systems' updates and data.

The third source of information is the Medicare system which contains patients' medicines, claims history, organ donation decision, and immunizations history. Figure 2 shows a high-level overview of the system design as described earlier.

Figure 2: My Health Record Architecture [19]



During the first release of the NEHR system (PCEHR), registration in the system was optional. In the opt-in model, both patients and doctors had the choice to register in the system. Patients had more control over their health records and freedom to register whenever needed. However, this mode resulted in a limited number of registered patients and doctors. Only 400,000 patients registered from 2012 to 2013 (2% of Australia's population). This negative network effect reduced the amount of investment and the number of registrations from the healthcare providers side. Many doctors had not registered nor invested time in adoption to the system due to the low patients' number [18].

The limited adoption from patients' and doctors' sides initiated some reviews and experiments to understand the cause of the issue. In 2013, the government conducted a comprehensive review of the system to answer questions related to the benefits, privacy and security concerns, and the governance of NEHR. One of the review topics was to explore the benefits and the risks of moving to an opt-out model in which patients are registered to the system by default. The review concluded that an opt-out model would drive registrations and records creation because it could reduce the time required for enrolling in the system. The report argued that the opt-out model would be helpful for specific groups that have limited access to the internet. Furthermore, this approach would increase health care providers' investment in learning and adopting to accommodate a larger patient base [18]. A trial was conducted in 2016 to evaluate the opt-in and the opt-out approaches. The experiment's goal was to understand public opinion about the opt-out mode, measure the impact of network effects, and find implementation issues before rolling out the opt-out method. The study compared the results of two opt-outs and two opt-ins implementations in different regions in Australia. Then, the researchers surveyed more than 4000 patients and 8000 health providers in the selected areas. The study found that the opt-out approach is the preferred approach for various stakeholders. The approach achieved higher participation numbers and higher understanding of the system's objectives and uses. Also, many of the stakeholders supported the creation of health records from other data sources if adequate education and training are provided [19]. On the other hand,

the opt-out approach has triggered negative responses around the country. Some argue that changing to an opt-out model might not be a solution to the registration problem due to the lack of quality data records obtained from other systems like Medicare. Transparency was another concern as some researchers argued that system design documentation should be shared to allow the public to critique and analyze the system architecture and security [20]. The agency responsible for My Health Record shares only high-level design documents of the system. The current documents do not have information about the system's infrastructure like the server, databases, network, or the encryption methods.

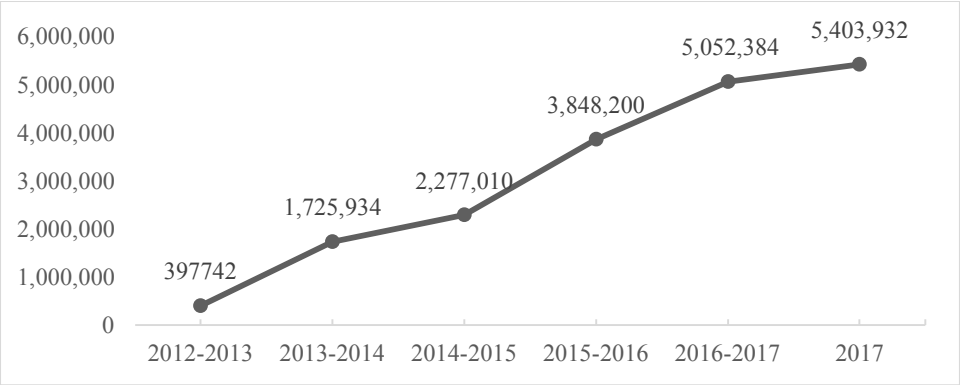
4.1.2.4 Health Data Network

Australia launched a health data network before launching the first NEHR system implementation. The current network is called "Secure Messaging" and aims to support the delivery of messages and data between different health providers. The network supports referrals, specialist letters, and discharge summaries only.

4.1.2.5 NEHR State

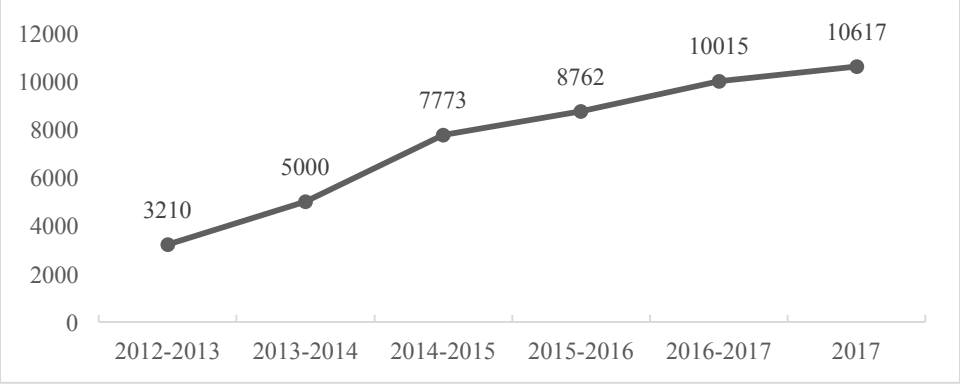
The recommendations and changes to the Australian NEHR have increased users' and health providers' registrations and activities considerably. Now, over 5 million people which are about 22% of the Australian populations have registered in My Health Record system. The majority of the registered individuals are under the age of 39. Figure 3 shows the change in the number of registered consumers over time. The figure shows that government changes to the program and additional budget allocations have augmented registrations number since 2015.

Figure 3: Consumer's Registrations in The Australian NEHR System



On the other hand, a total of 10,617 health providers have registered in the system as of December 2017. About 60% of the enrolled organizations are general practices, 7% are public hospitals, 1.6% are private hospitals, and 13% are pharmacies. Figure 4 shows the number of healthcare registrations over time. The line shows modest growth in the number of registrations health providers. About 73% of all Australia's general practitioners' clinics have registered in the system.

Figure 4: Health Providers' Registrations in My Health Record System



4.1.3 NEHR Privacy and Security

In this section, some of the most essential privacy and security components are reviewed. This includes discussing the laws and regulations that regulate the

security and privacy of My Health Record. Then, a discussion about the security and privacy elements of the system is analyzed and discussed.

4.1.3.1 Laws and Regulations

This list contains a list of rules and regulations that are vital for sustaining the privacy and security of "My Health Record", the NEHR system of Australia.

- Privacy Act 1988

  The Privacy Act 1988 regulates how public and private organizations must handle personal information. The act introduces 13 information principles for specifying how information can be secured and protected. The principles are similar to US Fair Information Practice Principles (FIPPS) in determining how information should be collected, processed, secured, and finally deleted [21]. The act also explains the Information Commissioner's responsibilities and reporting requirements. The Information Commissioner is responsible for enforcing the privacy and security laws. The agency's tasks vary from investigating data breaches to publishing annual reports on the activities carried out by the agency. The bill also explains the various issues that must be considered with specific data types like credit reports and tax numbers data. Furthermore, the act requires an extra layer of protection for health-related data. It requires health providers to obtain patients' consent before storing and using any of their health data and information.

- Healthcare Identifiers Act 2010

Australia does not have a unified national identification number. Several laws were introduced for the creation of a national identification number, but they were abandoned because of privacy and identity theft concerns. For off-line authentication purposes, government and private entities use one of the following: Medicare number (for health purposes), tax file number (TFN), or driving license number. However, the growing use of various unique identifiers caused inconsistencies in matching people with health records. As a result, the Health Identifier Act was introduced to formalize the process of creating unique health identifiers. The law defines health identifiers for health recipients, health providers organizations, and individual healthcare providers. It also outlines situations in which the healthcare identifiers can be disclosed and shared with other healthcare entities. The act also describes how the law interacts with the Privacy Act 1988. For example, it details the cases in which sharing healthcare identifiers constitutes a privacy breach. Following the ruling, health identifiers were created for all citizens. These health identifiers are used in the registration process for authenticating both patients and health providers.

- My Health Records Act 2012

The law was formerly called "The Personally Controlled Electronic Health Records Act 2012" and renamed after the system name was changed. It outlines the legal framework of the system converging many essential governance considerations. The first part of the law describes the roles and

responsibilities of the system operator. The system operator is responsible for all system related issues including data sources, access management, and data privacy. The second part of the law details registration requirements for different stakeholders including consumers, health providers, and contractors. Furthermore, the law goes into details on how to handle membership cancellation and suspensions.

4.1.3.2 Technical and Operations

- Authentication

  In 2013, the Australian government launched the universal login service called MyGov. The service's primary goal is to become a centralized login platform for all government-related services. My Health Records system cannot be used without a MyGov account. After registering with MyGov, a user can login using the registered email and password. The service is linked to many government services and systems. The single sign-on service is integrated with My Health Records, Medicare, child support, veteran affairs, disability insurance claims, and taxation office digital services. To connect other services to their MyGov accounts, users have to authenticate through two options: membership details of the other service or questions related to the service. The first option is used when the user already has another membership in the other service and wants to migrate his account to the MyGov platform. It is unclear how MyGov can ensure and enforce security over memberships in other systems. The second option is used when users do

not have a membership, and the system validates membership through questions specific to the users. For instance, questions about transaction numbers for previous health claims.

The MyGov platform improves efficiency in reducing the time required to maintain and register for eleven digital government services. On the other hand, having all these services and information under a single log-in platform can increase security risks especially when data breaches or identity theft occur. Moreover, the login process does not verify users through other authentication methods like mobile or email verification codes. Thus, it makes identity theft easier for adversaries.

- Authorization

One of the main features of the NEHR system is sharing information with other entities. The sharing of documents within the system is governed by various authorization and access management approaches. The system has two types of access control on records; general and restricted. In the general access, health providers can access any of the patient's information and records, and it is the default viewing setting for all entered records. Users can restrict access to records using the restricted access approach by defining which files cannot be viewed. In the case of an emergency, a health provider can view both the general and restricted files.

- Audit Log

One of the system's main privacy and security components is the auditing access feature. It allows patients to review the access history to the medical records. Users can view what records have been viewed, what has been added to their profiles and by whom. This gives users a detailed view of all types of activities performed before, during or after visiting health providers. In the same section, users can revoke any providers' access to certain information. Besides, users can set alerts to get messages in email and mobile whenever their profiles have been accessed.

- Data Breaches and Quality:

Following the My Health Records Act 2012, the government established the Information Commissioner office to review digital health compliance and enforcement activities. The office is responsible for many of the privacy, security, and compliance issues. The office also handles and investigates data breaches in digital health projects. The office received 35 data breaches notifications that occurred between 2013 and 2016 affecting over 100 health recipients. Most of these data breaches were caused by a technical issue allowing health recipients to obtain access to other users' records. This issue resulted in uploading users' records to other users. This violates the privacy of patients especially if there is sensitive information. It also can trigger safety problems especially if a physician makes a decision based on an inaccurate data.

Table 1: Data Breaches Notifications Received

Year	2013-14	2014-15	2015-16
Data breaches notifications	2	7	16
Number of healthcare recipients affected	-	1	103

4.1.4 Conclusion

My Health Record system provides a remarkable example of building a secure NEHR system. The failure of the first system has provided many lessons to redesign the system with the right processes, regulations, procedures, and IT tools. From the technical side, the government has engaged private companies in the design and implementation processes. On the security side, the government has tested several authentication options before building the national single sign-on platform. The platform can help citizens to login to different services quickly but increases the risk in case of identity theft.

4.2 Denmark

Denmark is one of the leading countries in providing quality health care services. It is also one of the first countries that implemented a healthcare network that allows health providers to exchange messages and information electronically. This network enabled the country to implement many solutions including the NEHR system discussed our case study. The primary data resources for the case are official NEHR website, and MedCom reports and statistics. Other references will be included throughout the reporting on that country as well.

4.2.1 Health Care System

Denmark provides a universal health care system for all citizens. As per law, residents receive all healthcare treatments free of charge and non-residents can receive care for critical conditions only. Total health expenditure is about 11% of the GDP. Health-related projects are planned at the central government and managed and enforced at the regional level. Five regions govern and manage public health care systems. All the public system financing comes from earmarked income taxes [22]. For primary care, all general practitioners are self-employed and paid by regions in which rates are defined by national agreements with doctors' associations. Patients cannot be admitted to hospitals without referrals from general practitioners.

Denmark is considered one of the most advanced countries in e-health solutions. The government's success in e-health projects was a result of many e-health vision strategies that were formulated over the years from 1996 to 2003. The first e-health vision strategy was developed in 1996 to define an overall strategy, goals, plans, and challenges for transforming the Danish health care system. The latest national strategy report was developed in 2007 to adjust strategies and plans according to the existing state of e-health. One of the most important success factors was establishing MedCom which is a government organization that manages the health data network. It also developed the rules, standards, and protocols for electronic communication between healthcare providers. The network project was launched in 1994 after defining electronic document interchange (EDI) standards and protocols including health providers letters [23]. The network is used for exchanging many

types of letters including prescriptions, referrals, lab results, and discharge. Following this project, many regulations and projects were introduced to increase EHR systems usage in hospitals and GP practices. In 2004, the health ministry launched an e-health portal for providing all health-related information. In 2004, a law was introduced making the use electronic health records for GP practices mandatory which increased EHR adoption to 93% for all GP practices [24]. Then, the government introduced a law to enforce the use of EHR systems for specialists in 2006. Although these laws increased adoption of EHR, most of these systems are isolated and do not exchange data with other systems [25]. The fragmentation of EHR systems across entities increased the cost of sharing information, delays of appointments, and safety risks in some cases [25]. These concerns led the government to initiate projects to consolidate and standardize electronic health records across regions. The first project was initiated in 2001 to standardize all EHR systems specifications to facilitate the exchange of information between health providers. However, the proposed changes were too risky to implement in the existing systems, and the project was decommissioned in 2006. Then, another project was initiated to integrate all medical records in a single database. However, the project was abandon due to technical and coordination complexities.

4.2.2 National Health Records System

This section reviews the major component of the Danish NEHR system. The first section reviews the goals assigned for the NEHR system. The following section lists the stakeholders relevant to the NEHR system. It also discusses the tasks and

responsibilities of each of the stakeholders. Finally, the system components are discussed and analyzed. Followed by a discussed of privacy and security considerations.

4.2.2.1 NEHR Goals

The Ministry of Health identified the following goals for the current NEHR system:

- Provide reliable information related to the use of the healthcare services. The type of information provided varies from health records, to treatment information, to drugs reviews.
- Provide a communication medium between the patient and the healthcare provider. The portal allows a secure communication between patients and health providers through the secured network defined for this purpose. For instance, patients can schedule an appointment using the portal. Also, they can check the waiting times for all the hospitals that use the system.
- Establish a private patients network to communicate about common diseases and health issues. This allows patients to talk with patients who have similar diseases to understand treatments, outcomes, and other relevant information.

4.2.2.2 NEHR Stakeholders

- Government
    - National Government: The national government is responsible for setting the legal regulations for healthcare services. It also

supervises regions to make sure that they are following the formulated laws and regulations.

    - Regional Government: The national government funds the government of the five regions. Hospitals and clinics are managed and owned by the regions' government. Also, the regional government is responsible for conducting quality checks to ensure patients' satisfaction.
    - Municipal Government: Municipalities are responsible for financing and delivering nursing home care, home nurses, health visitors, some dental services, school health services, home help, and treatment for drug and alcohol abuse. Some municipalities play a role in training and development activities for the different e-health solutions.

- Ministry of Health: The primary goal is to improve the health of current citizens and future generations. The ministry has many divisions including health systems policy and primary care, health financing, health products regulations, population health, and other corporate divisions.
- The Danish Health Data Authority: This agency is responsible for generating health-related data for different stakeholders. It also cooperates with other Danish entities to build e-health solutions for patients and health professionals. The agency collects health data from

various government databases and provides the data to health professionals, policymakers, and citizens.

- Medcom: A private organization owned by government, regions, and municipalities. The organization was founded to manage and implement IT projects within hospitals. Further, it designs standard solutions to be used by clinics and other health providers with a focus on national implementation. Medcom developed and maintained the network that is currently used to exchange data between health providers.
- The Danish Data Protection Agency: The agency acts as the national data protection authority and enforces the regulations specified the Personal Data Processing Act. The agency is responsible for advising public and private organizations on the use of personal data. It also receives citizens' complaints on data issues to investigate violations and other matters. The agency also conducts annual inspections on public and private entities to ensure they are not violating any of the country's regulations.
- Patients: Patients can get the latest information about doctors and treatments. They also can access health records since 1977.
- Healthcare Providers: The current system provides access to patients' records and information. It also gives health providers access to medical handbook to get the latest updates on treatments and technologies.

- Private Insurance Providers: Non-government sources provide about 14% of financing for health care. The use of NEHR might reduce the expenses on private insurance companies' due to the reduction of repeated tests and consultations.

4.2.2.3 NEHR Architecture

Sundhed.dk is the national portal for health services in Denmark. It allows patients and health providers to find relevant health information. Patients and health provider can access medical records dating back to 1977 [26]. Health records can be read only by patients because the portal does not store the records in a central database. The Danish government built a network to exchange letters and messages between health provider in the 1990s. The exchanged messages were stored in a central database. These letters use common industry standards to exchange information between different health providers. The portal uses the database to extract patients' records and information. The current portal extracts patients' data from over 85 databases. This section outlines consumers and health providers functions to show the key design elements of the system.

- **Consumers:** Consumers are individuals that will use the system to check and update health records system. These are the main functions:
    - View a medical record: Patients can view all the details of medical records to 1977. Most of the information is extracted from hospitals EHR systems.
    - Request a medicine: A patient can access prescription information to order a medicine and to renew prescriptions. Further, the portal provides

information about available drugs to allow patients to compare between drugs in terms of effectiveness, quality, and price. The reimbursement rate depends on the price of the drug. For instance, if the drug costs less than $150, the reimbursement rate is 0%. On the other hand, if the drug's price is between $150-$250, the reimbursement rate becomes 50%.

    - Find relevant health information: the portal provides various types of data related to treatments, regulations, medications, and doctors.
    - Network with other patients: the portal allows patients with similar pathologies to discuss issues and treatment in the online forum section of the portal.

- General Practitioners and Specialists:
    - View a medical record: doctors can view discharge summaries, prescription and dispense records, shared health summaries, event summaries, specialist letters, and referral letters.
    - Access medical handbooks: this allows doctors and consumers to view the medical handbook in order to update knowledge or verify information.

After several failed projects, the Danish government managed to successfully deliver two national health records systems: the shared medication record (FMK) and the national health records (E-Journal) systems. The shared medication record system project started in 2008 and was completed by mid-2014. The system was built to give general practitioners an overview of patients' prescriptions and

medication history within the last two years. It also allows practitioners to submit prescription electronically which increased adoption considerably because many GPs did not have technical capabilities to use the e-prescription systems. The shared medication record system usage rate varies by regions at an average of 60% [27].

The government launched another NEHR system called E-journal the system which gives healthcare providers access to all patients' health records. It extracts patients' data from all public and private hospital data databases. Patients can access their data through the central health portal (sundhed.dk). The portal allows patients to access their medical records, refill prescription drugs, make an appointment with general practitioners. The system contains about 85% of the Danish population health records. For health professionals, the portal gives access to patients' medical records and historical medications information. It also provides a trusted knowledge of medical articles, studies, videos, and tests. GP clinics access patients records directly from the web portal (sundhed.dk), while hospitals integrate their EHR systems with the NEHR database.

4.2.2.4 Health Data Network

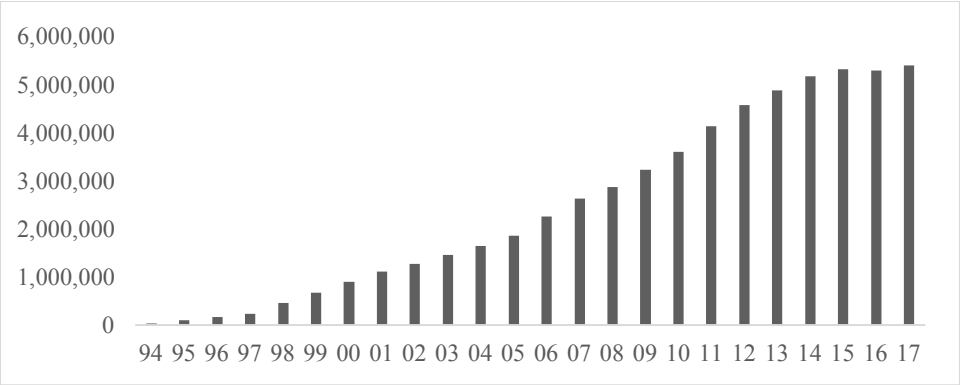
Denmark is one of the first countries in the world to launch a successful country-wide network for health data. The network design and implementation were carried out by Medcom in the 1990s. The organization defined the network's standards, protocols, and procedures for the use of the health data. The network links secure local networks in a shared infrastructure and used by many current services.

Connection to the network requires either using multiprotocol label switching (MPLS), fixed link (through private MLPS or fiber optic), or the internet (using IPSec-encrypted VPN link). The current network handles different types of messaging between providers including prescriptions, referrals, discharge summaries, laboratory requisitions, digital images, and health insurance reimbursements [24]. Although the letters were based on EDI standards, the government initiated a new project to convert all messages standards to XML. Currently, the network handles over 6 million message every month send by over 6000 organizations. The messaging system is supported by over 60 vendors and 100 IT systems. The potential saving of the current health data network was over $100 million in 2008.

4.2.2.5 NEHR State

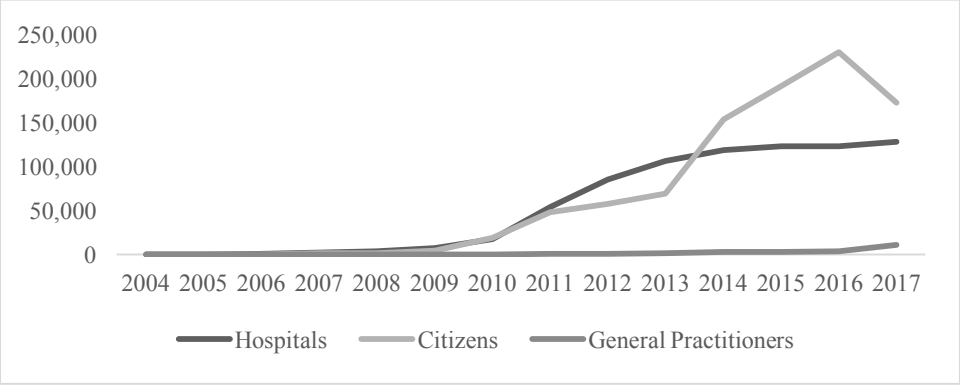
Since most of the financing of health care comes from the government, the government contract requires health providers to use EHR systems. It also requires them to use the electronic network to exchange messages and letters. The government shares the statistics on the number of messages exchanged. According to the Ministry of Health, all GP clinics use electronic health record (EHR) systems and 98% exchange messages via the network. Moreover, all laboratory tests produced by hospitals and labs are sent and received electronically by GPs. Figure 5 shows the number of messages (excluding prescription) sent in the network from 1994 to 2017.

Figure 5: Messages sent from 1994 to 2017



The launch of sundhed.dk has increased the number of medical record lookups. Figure 6 shows the increase in the number of lookups done by citizens as a result of integrating the health portal. The low number of GP look-ups might be because of the nature of GP work or because people do not change clinics. Therefore, the original patients' records are stored in the GP local system.

Figure 6: Number of EHR Look-ups



4.2.3 NEHR Privacy and Security

In this section, some of the most essential components of privacy and security are reviewed. This includes discussing the laws and regulations that regulate the security and privacy of health record in Denmark. Then, a discussion about the security and privacy elements of the system is analyzed and discussed.

4.2.3.1 Laws and Regulations

- Processing of Personal Data Act

The Processing of Personal Data Act is similar to many countries' laws on how personal information should be handled. However, the Danish regulations are longer and more specific on the various cases in which data must be protected. There are certain data types that are protected by the laws including credit information and video surveillance. The law also specifies the entities that can access the personal data outlining all required conditions. Chapter 11 of the law outlines the regulations required to secure personal data. The act also defines the role and function of the data protection agency.

- Health Act

The main health act in Denmark has been amended several times to support IT innovation and patients' rights in the health sector. In 2011, the act was amended to allow patients to access national health records online. Also, patients' rights were restricted to maintain patients' privacy in 2013. Another amendment was about financing, planning, and coordinating IT projects in the healthcare sector [28].

4.2.3.2 Technical and Operations

- Authentication

The Danish government assigns a unique identifier number called central personal registration (CPR) from birth. Accessing health records online for patients and health providers can be done through the official health portal

Sundhed.dk. The portal relies on a sign-on service called "NemID" in which the CPR is used to verify the identity of the user. The service was launched for login to online banking services and later was used for other online public services. NemID uses a two-factor authentication approach to verify logins before allowing the user to access the service. The use of a single login service for several entities can bring many advantages as users do not have to remember membership details for different providers. For entities, the use of this service reduces cost because they do not have to manage infrastructure and customer service. However, there are several risks associated with using a single sign-on service including having a single point of failure. Firstly, any technical issue can lead to a complete blockage to accessing various important services. NemID has experienced several technical difficulties in which users were not able to access public nor banking related information. In some cases, users were not able to log in for over 20 hours. A similar issue occurred when a new update of Java was released. NemID users downloaded the update without realizing that it was not compatible with NemID login technology. As a result, users who updated Java were not able to access portals and had to downgrade to overcome the issue [29].

- Authorization

Patients can access medical records and information from the main online portal (Sundhed.dk). It takes 3-5 days for new records to be extracted from

hospital databases to the NEHR databases. By default, any health record is accessible by all health providers including general practitioners and specialists. Patients have limited control over health documents but they have the option to restrict access to some records. Moreover, records entered by public hospitals cannot be accessed by general practitioners without authorization from the patient. Another essential authorization feature is the user's ability to give access to other registered people. For instance, a patient can authorize a relative to access her medical records.

- Audit Log

Auditing access helps users know any activities that occurred in their online health profile. This improves the system accountability as users can monitor their accounts and report any inaccurate data. The existing NEHR system gives patients ability to track who added any medical records based on login details. However, the record logs details for health professionals in most cases are inaccurate. The working nature of health professional requires a continuous moving within the same hospital or clinic. This requires physicians to log in many times in different workstations. Since the authentication process requires a second authentication, this increases the time required for signing in. As a result, general practitioners started sharing login details to reduce the time required to login. This unanticipated behavior led to limited data accuracy for auditing purposes and increases the chances for violating patients' privacy and security [25].

- Data breaches and integrity

  In 2000, the Danish government introduced laws to protect personal data and information. Following these regulations, the government established an agency responsible for enforcing these rules called the Danish Data Protection Agency. The agency is not only responsible for enforcing data protection laws but also in monitoring all stakeholders involved in which personal data is processed or shared. Further, the agency publishes an annual report regarding both the agency's activities and the received complaints.

Table 2: Number of Complaints

Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Cases	4368	5492	5042	4859	5665	5442	5166	6118	5904	5461	4427

Table 2 shows a summary of the number of complaint cases recorded by the agency. It is unclear why the number of cases fluctuates but latest recorded year showed 19% in the number of processed cases. The top three categories for the reported cases are in complaints on private entities, reviews for the private sector, and legislative work. The report provides a summary of the private sector complaints in which the number of complaints is low. On average only 3.5% of complaints were related to the health sector. The low number of complaints results from the low number of private sector hospitals and clinics. In Denmark, most of the healthcare services are state-owned. No records or information about malicious behavior was found in the studied documentations.

4.2.4 Conclusion

The Danish case shows that successful NEHR projects require government commitment and years of planning. Denmark spent many years developing the health data network infrastructure, standards, and protocols. The healthcare system structure, regulations, and financing sources accelerated the adoption and usage of this network. The Danish case shows another approach on building NEHR system where the design is optimized for health providers. This increases the health providers trust about the system data and records. This architecture limits users' ability to control the data found in their medical health records.

4.3 France

This section summarizes the components that are relevant to the French NEHR system "DMP". The system was introduced in the past few years and has been redesigned to improve privacy and security mechanisms. The primary data resources for the case are the NEHR official website, the digital agency reports, and government reviews. There are other references that will be included throughout the reporting on that country as well.

4.3.1 Health Care System

The central government is responsible for provisioning the French health care system across regions. It also plans and controls budget spending to control and maintain health cost. Health expenditure constituted about 9% of all GDP spending in 2015. Health care coverage is funded through statutory health insurance (SHI) funds which provide a compulsory health coverage for all citizens

and residents. The statutory health insurance covers many of the health providers services in public and private hospitals and practices. On average 64% of statutory health insurance financing comes from employers and employee payroll taxes, and the rest comes from earmarked taxes and voluntary health insurance companies. Health care is delivered by general practitioners and specialists. Patients can visit specialists without general practitioners' referrals.

4.3.2 National Health Records System

4.3.2.1 NEHR Goals

The initial goals for the NEHR projects were defined prior to the project start as follows:

- Enhanced coordination between health professionals through exchanging information between the different stakeholders.
- Provide real-time access to the latest health information which can lead to better quality of care provided by health providers.
- Provide accurate health information to make people more responsible for their health.
- Reduce health insurance expenses due to the reduction of redundant tests

4.3.2.2 NEHR Stakeholders

- Government: The national government is responsible for all the healthcare-related policies. Most of the planning and enforcement of healthcare policies is conducted by the Ministry of Health and Solidarity.

- Ministry of Health and Solidarity: The primary goal is to improve the health of current citizens and future generations. The ministry is responsible for defining the national healthcare strategy. The various departments in the Ministry are responsible for executing the defined strategies.
- National Commission of Computing and Freedoms (CNIL): CNIL agency has many roles including informing individuals about their privacy rights, protecting the rights of citizens, regulating data processing laws, and inspecting any personal data-related violations.
- Statutory Health Insurers (SHI): Healthcare funding comes from statutory health insurance funds. About 80% of health care coverage comes from these funds.
- Share Health Information Systems Agency (ASIP): A public agency under the Ministry of Health responsible for all information system projects in the health sector. The agency builds and maintains health information systems including the current NEHR system (DMP). It also provides a smart card system for the authentication used in health information systems. Another important responsibility is maintaining the national directory of health providers.

4.3.2.3 NEHR Architecture

The French government announced the creation of a national health records system in 2004. The system was named “Dossier Médical Personnel” (DMP) which means “Personal Medical Records”. However, the system name was later changed

to become “Shared Medical Records” to emphasize collaboration between health providers and patients. These are the processes that can carried out by patients and health providers:

- **Consumers:** Consumers are individuals that will use the system to check and update health records system. These are the main functions:
    - Manage access to documents: By default, every document stored in the system is accessed by authorized health providers. The system allows users to restrict access to certain documents.
    - Remove a document: Users can remove any of the documents added to the system. However, it is unclear if deleting a document in the system, removes the file permanently from the database. It is also unclear if this action results in deleting the record in the hospital or the clinic EHR system.
    - View the list of people who accessed a record (Audit log): The current system component allows users to view access history, documents viewed, and view time.
- Health Providers
    - View a medical record: doctors can view all the patient’s record stored in the system.
    - Upload a shared health summary: The shared health summary is the patient’s summary at a point in time. A doctor or a nurse can upload this

document to the system either from the online portal or the hospital's EHR system.

- Upload a prescription: Prescriptions can be uploaded through another software to My Health Record system. Then, the prescription can be viewed by the pharmacist and other health providers.

Before starting the NEHR project, the Ministry of Health formed an interest group within itself to carry out the design and implementation activities. After the system was developed, a plan was carried out to test the system in different regions. Unfortunately, most of the testing experiments failed due to security and confidentiality issues. Consequently, the ministry decided to suspend the project until a full assessment of the system's requirements is conducted. The lessons learned in the failed implementation have shaped many of the legal and design aspects of the new DMP system. The government formed a new agency responsible for managing and maintaining the system. The agency has introduced several regulations to facilitate the adoption of the system by health providers and patients. It relaunched the new system in 2009. The new DMP system allows patients to create their profile directly from the online portal. Moreover, the medical profile can be created in primary insurance and health providers facilities. Although regulations helped in solving previous system patients' rights concerns, the adoption rate was slower than anticipated. In 2012, a government report indicated that the project cost €200 million while maintaining only 150,000 profiles. At the end of 2016, only 590,000 medical profiles were created which

represents 1.5% of the targeted population [30]. Besides the low adoption rate, researchers found that most of the medical profiles lack useful medical records. For instance, more than 41% of the created DPM profiles did not contain medical records. Moreover, only about 14% of the medical records were accessed by health providers [30]. This indicates that health providers were not utilizing the system to consume medical records and information either because of trust, accuracy, or usability issues.

4.3.2.4 Health Data Network

Besides the NEHR system, ASIP has launched a secure messaging system called MSSanté (MS Health). The system was launched in 2016 and it allows health professional and institutions to send and receive encrypted and secured messages from the system. Health professional use a web portal to login to the platform. The platform has a list of trusted health providers directory list to ensure that message do not go to untrusted parties. Unlike the other systems, it does not use standard message formats and layout but instead it allows senders to send any type of messages and content.

4.3.2.5 NEHR State

The first version of the DMP system managed to get about 500,000 registered users. However, this number was insufficient to realize the benefits of using the NEHR system. Also, the number of documents uploaded to the DMP was about 2,390,123. However, most of these documents were never viewed on the system

[31]. Moreover, the study found that 41% of all the created profiles contained no records.

4.3.3 NEHR Privacy and Security

4.3.3.1 Law and Regulations

- Data Protection Law (1978)

  France is one of the first countries in Europe to introduce a data protection law. The law dates back to 1978 and has been amended several times based on European regulations. The following rights are granted for data subjects: the right to consent, right to be informed, right to object, right of access, right of indirect access, right to correct and delete, and right to be forgotten. The law outlines the obligations from the data controller side in which privacy and security of the data must be ensured.

- National Personal Health Record (DMP) Law

  The act introduces the NEHR goals and design principles. It outlines the different aspects in which the data should be processed and handled. The law also goes through requirements for creating medical records for patients. No online medical record can be created without patients' consent and knowledge. The law also briefly goes through the use of national patient identifiers to connect users with their health data.

4.3.3.2 Technical and Operations

- Authentication - Smart Cards

For patients and health providers' authentication, the DMP requires the use of the official insurance smart card "Carte Vitale" details for registration. The smart card was first introduced in 1998 to facilitate insurance claims between doctors and health insurance funds. The use of the card eliminated the long reimbursement process between patients and the health insurance fund. The card is free of charge and issued for citizens above the age of 16. Parents' cards will contain information about related beneficiaries under the age of 16. Advances in healthcare have triggered the need to update the smart card to include more data and functionalities. As a result, health authorities have introduced the second generation of the card "Carte Vitale 2". One of the most critical aspects of the card is the personal photo. Health providers can use the card not only to authenticate patients but also to verify the identity from the photo. Although the card is used primarily for insurance claim process, it is currently being used for patients' authentication and identification when visiting health providers.

Patients cannot register with the DMP system without the information found on the insurance card including the social security number and card serial number. Also, health providers cannot register with the DMP without smartcard readers and the professional health smartcard (CPS). The smartcard readers are used to authenticate and identify patients using the insurance card. The professional health smart card is used to submit patients' insurance information to the insurance providers electronically. It is

also the main card used for creating, sharing, and viewing patients' electronic records from the DMP system. The professional health smart card has been utilized for other purposes including access management to facilities and restricted areas.

- Authorization

One of the most important features that were developed to manage authorization is the "Health Professional Enabling Matrix". The matrix is used to define authorization and access settings for various health providers based on the position and document type. On the y-axis, the matrix has many types of reports and MRI images. On the x-axis, the matrix has health providers positions including general practitioners and pharmacist. The matrix shows what documents are accessed by whom. The system allows hiding sensitive information that has to be reported directly by a doctor. This feature allows doctors to publish the document and hide it unless communicated verbally to a patient.

- Audit Log

The system provides two main features to improve governance: access history and alerts. Access history allows patients to view all added and viewed medical records history with times and names. This allows patients to get insight into accessed their records which help them revoke access to certain documents if not needed. The system also has an alert function that sends emails whenever a document was added or accessed.

4.3.4 Conclusion

The French case shows that the lack of appropriate governance structure and procedures can limit the uptake of the NEHR system. The usage and registrations rates of the system were limited. The case does not reveal any significant privacy and security risks due to the inadequate adoption of the system.

4.4 Discussion

This section revisits and analyzes the sections discussed in the case studies chapter. The goal of this section is to compare the health care system and the NEHR of Australia, Denmark, and France. It begins with an analysis of the healthcare systems in the selected countries. Then, a discussion about the state of e-health in these countries is reviewed. Finally, a comparison between the NEHR state is conducted. Followed by a summary of the privacy and security risks found in each of these systems.

4.4.1 Healthcare Systems

Healthcare systems are one of the most complex systems in the world. There are many legal, social, financial, and technical factors that involve in determining the state and the quality of health care. This section briefly compares some of the essential healthcare indicators that are used to compare the quality of healthcare. Table 3 shows the average life expectancy in the studied countries. The life expectancy average is similar in all the selected countries. Despite the lower health spending per capita, Australia and France have higher life expectancy than in Denmark and the rest of OECD countries.

Table 3: Life Expectancy for the Total Population

Indicator	Country	2006	2016
Life expectancy, Total population at birth, Years	Australia	81.1	82.5
	Denmark	78.4	80.8
	France	81	82.4
	OECD Avg	78.6	80.6

Another important factor in determining the state of the health care system is health care spending trends. Health expenditure as a percentage of the gross domestic product (GDP) does not vary greatly between the reviewed countries. Although France allocated the most percentage of GDP for health, health spending per capita is smaller than in the other countries. Table 4 shows that Australia and Denmark expenditure on health per capita grew by more than 50% between 2006 and 2016. Nevertheless, Denmark spent the highest on health per capita at about $5205.

Table 4: Healthcare Spending

Indicator	Country	2006	2016
Current expenditure on health, % of gross domestic product	Australia	7.9%	9.6%
	Denmark	9.2%	10.3%
	France	10%	11%
	OECD Avg	8%	9%
Current expenditure on health, per capita, US$ purchasing power parities (current prices, current PPPs)	Australia	$3023	$4708
	Denmark	$3422	$5205
	France	$3279	$4600
	OECD Avg	$2651	$4003

Financial sources are one of the essential factors in successful NEHR implementations. It increases governments leverage over other stakeholders, especially health care providers. Table 5 shows that government sources constitute about 84% of health expenditure in Denmark. The amount of spending gives the Danish government control over stakeholders involved in the system implementation process. For example, Danish general practitioners are required to use EHR systems and the health data network to be eligible for government reimbursement process. Another important indicator is out-of-pocket spending as a percentage of health. Table 5 indicates that all the average out-of-pocket spent on the health of studied countries is lower than in other OECD countries. The table shows that both France and Denmark managed to reduce the out-of-pocket spend for patients. On the other hand, Australia out-of-pocket spending share increased slightly.

Table 5: Healthcare Financial Sources

Indicators	**Country**	**2006**	**2016**
Government and compulsory health insurance schemes, % of current expenditure on health	Australia	68.3%	67.8%
	Denmark	83.9%	84%
	France	78.7%	78.8%
	OECD Avg	71.8%	72.5%
Out-of-pocket expenditure, % of current expenditure on health	Australia	19.2%	19.6%
	Denmark	14.9%	13.7%
	France	7.2%	6.8%
	OECD Avg	21%	20.3%

4.4.2 Health Data Networks

Each of the studied countries developed a network for exchanging data between health providers. The networks' functionality and maturity level vary between them. Medcom, the Danish data network, was launched in 1994 and it is the most developed data network. The network was adopted by a wide range of health providers due to regulations, technical, and financial factors. GPs regulations stipulate the use of the network for exchanging some prescriptions and reimbursement letters. Moreover, the company responsible for maintaining the network has developed many messages standards and formats that were widely accepted by health providers. On the other hand, the messaging platforms developed by Australia and France were launched for the same purpose in 2016 and 2014 respectively. Australia's network is integrated with the NEHR system to allow health provider to exchange data uploaded to the NEHR system. On the other hand, the French communication network is built on a separate portal that allows health providers to find other verified health providers and send messages securely. Table 6 shows a summary of the data networks.

Table 6: Health Data Networks Summary

Dimension	**Australia**	**Denmark**	**France**
Name	Secure Messaging	MedCom	MSSanté
Launch Year	2016	1994	2014
Messages	Standard Only	Standard Only	Free Text
NEHR Integrated	Yes	Yes	No
E-Referrals	In-development	Yes	No
E-Prescriptions	In-development	Yes	No

4.4.3 NEHR Systems

There are some variations in the architecture of the studied NEHR systems. Both the Australian and the French systems store data in the primary NEHR databases. On the other hand, the Danish NEHR system reads the data from other databases used for the data network. There are also differences between the studied countries in how patients are enrolled in the system. Australia implemented an opt-out registration mode which means patients are registered in the system by default. Denmark follows a similar approach as it records all patients' data and users' can access them from the official health portal. On the other hand, registering in the French NEHR system is still optional which have caused a low participation number. The first version of the NEHR system built by the Australian government was opt-out. However, this led to low participation numbers from both patients and health providers. As a result, the new system shifted to an opt-out model. Moreover, the NEHR system built by the French government had a small participation number. One of the causes of the low participation is the opt-in model [31]. Governments have to study the impact of opt-in and opt-out modes on the number of participants.

Table 7: NEHR Systems Summary

Category	Australia	Denmark	France
Controller	Digital Health Authority Agency	Medcom	Share Health Information Systems Agency (ASIP)
Launch Year	2012	2004	2010
Registrations	Opt-in	Opt-in	Opt-out
Patient Control	Read, Write, and Delete	Read Only	Read and Write

The current state of the system varies between the studied countries. In Australia, the number of registered users exceeded 5 million consumers, about 22% of the Australian population. Denmark does not publish the number of registered consumers mainly because the data and the network are built and optimized for health providers use. France has the lowest registration number among the studies countries with only about 1.5% of France population as shown in table 8.

Table 8: Number of NEHR Users

Indicator	Country	Registrations	% of Population
Number of registered users in the current NEHR system and % of the total population	Australia	5,403,932	22%
	Denmark	N/A	N/A
	France	583,997	1.5%

The number of uploaded documents is Australia has reached over 19 million documents as shown in table 9. In France, more than about 2.4 million documents were uploaded. On the other hand, the Danish system contains over 60 million

messages mainly because the system started back in 1994. It can also be a result of the proliferation of EHR systems in general practitioners' clinics.

Table 9: Number of Uploaded Documents

Indicator	**Country**	**Documents Uploaded**
Number of uploaded/sent documents by health providers	Australia	19,000,000
	Denmark	60,000,000
	France	2,400,000

4.4.4 NEHR Privacy and Security Summary

The studied countries have implemented different privacy and security techniques and methods. For unique identifiers, Denmark is the only country that uses a unique national identification number which is issued for every citizen at birth. Australia and France use health identifiers that connect patients with their health records. The use of national identifiers for health and non-health related identifications can increase the risk of identity theft. Therefore, using a unique health identifier provides more security because it limits the use of identifiers for other services. For authenticating users to the NEHR systems, the governments of Australia and Denmark use single sign-on platforms. However, every country has implemented the single sign-on platform differently. In Australia, the government platform is used for all digital government services. In contrast, Denmark utilized a platform that was developed for online banking purposes. Public and private Danish entities use the same platform to login in digital services. On the contrary, France does not have a single sign-on platform to login to the current NEHR system. Both Australia and France use two-factor authentication techniques to

verify the identity of the user. The NEHR platforms send either short codes to mobile or email to verify the verify of the users. Moreover, Australia adds an extra layer of protecting by asking users some security questions to verify users' identities. There are security, usability, and economy tradeoffs in using each of the authentication methods. Regarding security, the use of passwords only is inadequate to prevent identity theft. As a result, adding extra layers of protecting like security questions or two-factor identification used in Australia can reduce the risk of identity theft. For usability, the use of a password and two-factor authentication decrease efficiency especially for elderly or inexperienced users [15]. Australia and France implemented access notification and audit logs to keep track of online medical records. The access notification feature sends mobile or email messages to users if someone accessed their medical profiles online. Furthermore, NEHR systems in both Australia and France allow users to track access history. This function is technically not possible in Denmark due to the way in which the system was designed.

Table 10: NEHR Security Summary

Area	**Australia**	**Denmark**	**France**
Personal Identifier	Individual Healthcare Identifier (IHI)	Personal Identification Number (CPR)	Social Security Number
National Single Sign-On (SSO)	Yes (MyGov)	Yes (NemID)	No (Smart-card)
Two-Factor Authentication	Yes	No	Yes
Security Questions	Yes	No	No
Access Notifications	Yes	No	Yes
Audit Log	Yes	No	Yes

The current cases had several privacy and security issues. In Denmark, the use of a single authentication platform caused two major issues. The first problem was caused after a new release of Java was released, and users' computers were updated. The update prevented many users from accessing the NEHR system for up to 24 hours because the login technology was not compatible with the latest version of Java. The other issue was caused by the long duration of the authentication process which produced many health providers to share login details to shorten the time required to use the workstations. In Australia, extracting data from Medicare system resulted in over 100 data integrity issues in which users' records were shown for other users. In France, the limited legal framework around the NEHR systems lowered the number of participants from the patients and

health providers sides. This legal issue caused lower adoption and ultimately the failure of the first NEHR project in France.

Table 11: NEHR Security Issues Summary

Area	**Country**	**NEHR Privacy and Security Issues**
Single sign-on	Denmark	Updated version of Java caused precluded users from using the official login portal
Two-factor Authentication	Denmark	Physicians in the same clinic/hospital share login information to reduce time required to login
Data Integrity	Australia	Extraction of data from Medicare system resulted in exposing over 100 users' records due
Legal	France	The first version of the NEHR was decommissioned due to the limited legal framework for dealing with private data

5 Conclusions and Recommendations

This chapter summarizes some of the most important lessons learned from the studied cases. The selected cases show that the privacy and security of NEHR systems require different approaches. The sensitivity of health data, the high number of stakeholders, and the complexity of the systems increase the chances of privacy and security violations. However, some of the approaches shown in cases in dealing with these issues proved to be useful for future NEHR implementations. The chapter summarizes the most fundamental conclusions that can be taken into account when developing NEHR systems. The findings are preceded by a list of recommendations to summarize the security and privacy tradeoffs in NEHR systems.

5.1 NEHR Development

The development of nationwide digital systems requires extensive analysis and planning to achieve the desired outcomes. The cases show that NEHR systems are more complicated than the average national system because of the sensitivity of data and the high cost of the project. The following sections outline some inquiries that countries have to examine before starting NEHR projects. Figure 7 outlines some of the critical steps in developing the NEHR system. The following sections describe the details that should be carried out at every stage.

Figure 7: NEHR Development Stages

5.1.1 NEHR Analysis

One of the first steps in the NEHR system development is planning e-health solutions on the national level. To achieve that, all the studied countries had developed national e-health strategies before implementing NEHR systems [32][17][31]. The e-health strategy of each of the countries served as a guideline for the NEHR system designers and developers. It provided a reliable source of data on healthcare issues that can be solved using e-health solutions. Also, these strategies provided system designers with a comprehensive overview of the country's e-health solutions landscape which can have a profound impact on the architecture of the NEHR solution. Table 12 outlines a selected set of questions for the stakeholders involved in the analysis process.

Table 12: NEHR Analysis Questions

Category	Questions
Legal	• What data privacy and security regulations exist for protecting patients' electronic records? Are they comprehensive? • Does the country have any laws on the role and responsibilities of the NEHR system operator?
Governance	• Does the country have an independent organization to monitor privacy and data issues? • Does the country have a dedicated agency responsible for the NEHR system?
Technical	• Does the country have data and network infrastructure, standards, and protocols? • Does the country have a dedicated agency responsible for the NEHR system?

Stakeholders' trust cannot be gained without the existence of a comprehensive legal framework to protect users' data as seen in the Australian and the French NEHR cases [31][18]. Further, the Danish case shows that having an independent organization to manage government e-health solutions can increase the probability of success [25]. This governance structure limits finger-pointing during government projects failure and develops the organization technical skills and capabilities. Moreover, the Danish case shows that investments in health data network standards and protocols produce significant returns in the long run [24][26].

5.1.2 NEHR Design

The design phase of the NEHR system depends on many of the elements articulated in the analysis phase. Table 13 outlines a selected set of questions for the stakeholders involved in the design process.

Table 13: NEHR Design Questions

Category	**Questions**
Legal	• What are the legal implications when shifting from paper to electronic-based health records? • What incentives and legal structures that can be used to involve health providers in the design and testing processes?
Governance	• Are the stakeholders involved in the testing and review processes of the NEHR system?
Technical	• Should the architecture of the NEHR system be centralized or decentralized? • What are the details of NEHR processes, functions, and procedures? • What are the current data sources for the NEHR system and how to integrate them electronically? • Should the NEHR system use an existing authentication platform or develop in-house platform?

In the design phase, the main goal is to evaluate the system choices which will have a key influence on the NEHR project. From the legal side, the current healthcare processes and procedures have to be adjusted to incorporate future NEHR processes. Both Australia and France developed regulations that detail the functions and processes expectations of NEHR systems [33][34]. For incentives, Australia developed a financial incentives program for general practitioners that use the NEHR system meaningfully [35]. Further, the involvement of stakeholders

in all the system development processes can increase users' acceptance which reduces the time required for adoption [8].

5.1.3 NEHR Assessment

The assessment and evaluation of NEHR systems can be challenging due to the structural variations of these systems. The cases provide a broad set of metrics to measure the impact and outcomes of NEHR systems. Table 14 summarizes some of the typical key performance indicators used in the studied countries.

Table 14: NEHR Key Performance Indicators

Category	**Key performance indicator examples**
Enrollment	• % of the adult population registered in the system • % of health providers registered, per type (GP, Hospital, ...) • % of public and private health providers registered in the system
Usage and productivity	• Number of health documents uploaded per user • % of the uploaded documents accessed by health providers • % of users that access their health records online • % of referrals sent via the NEHR system network • % of prescriptions sent via the NEHR system network • % of tests and x-ray requests sent via the NEHR system network
Security and privacy	• Number of security claims opened (per type) and severity level • Number of data breaches (per type) and severity level • Number of system audits completed

Table 14 shows an example list of some of the key performance indicators (KPI) used in measuring enrollment, usage, and security. For enrollment, keeping track of changes in the number of registered health providers is significant to the success of NEHR projects. It allows the government to adjust policies to encourage and help

health providers to use the system. For usage, the KPIs depend on the architecture, functions, and processes of the NEHR system. Since the Danish NEHR system relies heavily on the data network, the KPIs used are related to the number of exchanged documents electronically [36]. On the other hand, the Australian system used only the number of uploaded documents to measure the usage until discovering that this metric is insufficient for understanding the utility of the system [37]. Finally, the privacy and security measures are not used by system operators but mainly for data protection authorities [38], [39].

5.2 NEHR Privacy and Security Tradeoffs

The way in which the NEHR is built can have a major impact on the privacy and security of the system. In Denmark, the data network was built to facilitate the exchange of messages between health providers. Then, users were given access to the stored messages and records. This gave health providers confidence on the stored data because users were not allowed to change records. In contrast, users were not able to see the access history. On the other hand, Australia allows doctors to upload records and give users the ability to change or delete any of the uploaded records. This gives users more control over data and who can access records. One of the major questions is whether to give users more control over data and logs with the expense of limited functionality (utility) for health providers. Table 15 summarizes some of the main questions system designers have to think about. It also categorizes the questions based on the stakeholders involved in the system design and development processes.

Table 15: NEHR Stakeholders' Questions

Solution Area		**Ecosystem**	
EHR	What are standards and protocols that have to be implemented in the industry provided EHR systems?	Industry	How to collaborate with industry to build secure and private add-ons and industry solutions?
Data Network	How will health providers be authenticated, authorized, and monitored on the access and usage of network data?	Government	How to foster collaboration between government entities to increase NEHR adoption while maintaining privacy and security?
NEHR	How much control users will be given over data?	Users	How to educate and train users on accessing, securing online records?

5.3 Future work

The importance of healthcare systems has encouraged countries to take charge of improving healthcare services including developing e-health solutions. As many countries are working toward similar solutions, the number of issues will increase in probability and frequency. Therefore, our work can be extended in numerous ways. Firstly, our analysis framework can be extended to analyze the technical details of integrating NEHR with local EHR systems. Furthermore, additional cases can be added to show and compare the utility of the analysis framework in various system architectures. Moreover, the healthcare structure should be studied to understand the most important factors in maintaining the privacy and security of records not only in NEHR but also in in-house EHR systems.

6 Bibliography

[1] E. Shortliffe and J. J. Cimino, *Biomedical Informatics*. 2014.

[2] N. Institutes, "Electronic Health Records Overview," no. April, 2006.

[3] M. J. Ball and J. Lillis, "E-health: Transforming the physician/patient relationship," *Int. J. Med. Inform.*, vol. 61, no. 1, pp. 1–10, 2001.

[4] R. Jolly, "The e health revolution — easier said than done," no. 3, 2011.

[5] N. Menachemi and T. H. Collum, "Benefits and drawbacks of electronic health record systems," *Risk Manag. Healthc. Policy*, vol. 4, pp. 47–55, 2011.

[6] A. Sheikh, T. Cornford, N. Barber, A. Avery, A. Takian, V. Lichtner, D. Petrakaki, S. Crowe, K. Marsden, A. Robertson, Z. Morrison, E. Klecun, R. Prescott, C. Quinn, Y. Jani, M. Ficociello, J. Paton, B. Fernando, A. Jacklin, and K. Cresswell, "Implementation and adoption of nationwide electronic health records in secondary care in England : final qualitative results from prospective national evaluation in ' early adopter ' hospitals," pp. 1–14, 2011.

[7] "National E-Health Strategy," no. December 2008.

[8] L. L. Fragidis and P. D. Chatzoglou, "Development of Nationwide Electronic Health Record (EHR): An international survey," 2017.

[9] A. Geissbuhler, "Lessons learned implementing a regional health information exchange in Geneva as a pilot for the Swiss national eHealth strategy," *Int. J. Med. Inform.*, vol. 82, no. 5, pp. e118–e124, 2013.

[10] D. J. Solove, "A Taxonomy of Privacy," *Calif. Law Rev.*, vol. 90, no. 4, pp. 1087–1155, 2006.

[11] A. Schoop, "Customer Data : Designing for Transparency and Trust," no. May 2015, 2016.

[12] Ponemon Institute LLC, "2017 Cost of Data Breach Study," no. March, 2017.

[13] B. Yüksel, A. Küpçü, and Ö. Özkasap, "Research issues for privacy and security of electronic health services," *Futur. Gener. Comput. Syst.*, vol. 68, pp. 1–13, 2017.

[14] R. J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems," *Security*, vol. 50. pp. 1–12, 2008.

[15] H. Fujii, N. Shigematsu, H. Kurokawa, and T. Nakagawa, "Telelogin: A two-factor two-path authentication technique using caller ID," *NTT Tech. Rev.*, vol. 6, no. 8, 2008.

[16] J. L. Fern??ndez-Alem??n, I. C. Se??or, P. ??ngel O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013.

[17] Australian Digital Health Agency, "Australia's National Digital Health Strategy," p. 63, 2017.

[18] A. G. D. of H. and Aging, "Review of the Personally Controlled Electronic Health Record December 2013," no. December, 2013.

[19] F. Report, "Evaluation of the Participation Trials for the My Health Record," no. November, 2016.

[20] A. P. Foundation, "Feedback on the PCEHR/IHI Legislation Discussion Paper This," 2015.

[21] A. G. of the Commonwealth, "Privacy Act 1988," no. 119, 1988.

[22] E. Mossialos, M. Wenzl, R. Osborn, and C. Anderson, "2014 International Profiles of Health Care Systems," *Commonw. Fund*, no. January, p. 163, 2015.

[23] T. Danish and H. Data, "Medcom in 20 Years," no. May, 2014.

[24] S. Cannaby, D. Westcott, C. D. Pedersen, H. Voss, and C. E. Wanscher, "The cost benefit of electronic patient referrals in Denmark: summary report.," *Stud. Health Technol. Inform.*, vol. 100, pp. 238–245, 2004.

[25] P. Kierkegaard, "EHealth in Denmark: A case study," *J. Med. Syst.*, vol. 37, no. 6, 2013.

[26] D. M. of Health, "E-health in Denmark," *Agenda*, 2012.

[27] P. Kierkegaard, "Interoperability after deployment : persistent challenges and regional strategies in Denmark," vol. 27, no. February, pp. 147–153, 2015.

[28] A. Lantieri, F. Pelsy, and Milieu Ltd, "Overview of the national laws on electronic health records in the EU Member States. National Report for France," no. January, pp. 1–49, 2014.

[29] "NemID dur ikke med seneste opdatering." [Online]. Available: https://www.b.dk/tech/nemid-dur-ikke-med-seneste-opdatering. [Accessed: 27-Jul-2017].

[30] B. Seroussi and J. Bouaud, "Use of a Nationwide Personally Controlled Electronic Health Record by Healthcare Professionals and Patients: A Case Study with the French DMP," *Stud. Health Technol. Inform.*, vol. 235, pp. 333–337, 2017.

[31] B. Séroussi and J. Bouaud, "Adoption of a Nationwide Shared Medical Record in France: Lessons Learnt after 5 Years of Deployment.," *AMIA Annu. Symp. Proc.*, vol. 2016, pp. 1100–1109, 2016.

[32] "National Strategy for Digitalisation of the Danish Healthcare Service," 2012.

[33] Commonwealth Government of Australia, "Healthcare Identifiers Act 2010," no. 72, 2010.

[34] J. Rahbek, "E-Record – Access to all Danish Public Health Records," p. 2013, 2013.

[35] A. Government, "Practice Incentives Program." [Online]. Available: https://www.humanservices.gov.au/organisations/health-professionals/services/medicare/practice-incentives-program.

[36] D. Healthcare Denmark and D. Ministry of Health, *Healthcare in Denmark*. 2016.

[37] C. Pearce and M. Bainbridge, "A personally controlled electronic health record for Australia," *J. Am. Med. Informatics Assoc.*, vol. 21, no. 4, pp. 707–713, 2014.

[38] Australian Government Department of Health and Aging, *Annual Report 1 July 2012 to 30 June 2013*, no. June. 2013.

[39] I. Commissioner, "Annual report of the Information Commissioner ' s activities in relation to eHealth," no. June, 2013.