Project Number:
43-HXA-D101

Danish Healthcare Information Technology - An Analytical Study of Consumer Issues

Analysis of Issues Danish Consumers of Health IT Systems Face, Focusing on the Domains of Privacy and Interoperability

An Interactive Qualifying Project submitted to the faculty of Worcester Polytechnic Institute in partial fulfillment of the requirements for the Degree of Bachelor of Science

Submitted by:
Sahil Bhagat
Danielle Fontaine
Karl Gibson

Professor Holly K. Ault, Faculty Advisor

In Cooperation With:
Project Liaison:
Senior Health Advisor, Sine Jensen
Forbrugerrådet

May 11th, 2010

Abstract

Health information technology is a relatively new field that is advancing the quality of healthcare. Health IT systems are complicated and must address many issues in order to be effective – systems must ensure that patient data is kept private and that they are interoperable with other systems. This project assisted *Forbrugerrådet* (the Danish Consumer Council) in identifying issues that Danish consumers of health IT systems face, with a focus on the domains of privacy and interoperability. We conducted a general literature review of health IT systems and held 14 interviews with various health IT experts and stakeholders from different organizations in order to identify issues that affect both healthcare patients and providers. Our findings indicated that while Danish health IT organizations are highly focused on furthering the interoperability of systems, there is much less being done to ensure patient privacy. We identified five major privacy issues for patients, and four interoperability and legal issues that affect healthcare providers. This report provides eight recommendations that address all of these issues, including three technical systems that can greatly increase both privacy and quality of care. We compiled these findings and recommendations into a policy paper that Forbrugerrådet can distribute to Danish legislators.

Acknowledgements

We would first like to thank Prof. Holly Ault for reading our project proposal and final report several times and providing us with constructive criticism.

Prof. Scott Jiusto, for all his help with our proposal.

We would like to thank our liaison, Sine Jensen and our sponsor organization, Forbrugerrådet for providing us with resources and guidance.

Mogens Larsen, for being our guide to the city of Copenhagen.

To all of our interviewees: William Corbett, Bengisu Tulu, Kenneth Ahrensberg, Morten Godiksen, Anette Høyrup, Frederik Endsleff, Marianne From, Pia Jespersen, Stephen Engberg, Pernille Bjørn, Henning Mortensen, Jan Petersen, and Mette Hartlev, we would like to thank them for giving us their valuable time, ideas, and opinions.

Finally, we would like to thank Prof. Peder Pedersen and Mr. Tom Thomsen for supporting the Denmark Project Center and for giving us the opportunity to experience such a project.

We would also like to thank mindshift.com for the use of the image on our title page.

Authorship Page

Sahil Bhagat, Danielle Fontaine, and Karl Gibson
contributed equally to the creation of this report.

Table of Contents

List of Figures

List of Tables

Executive Summary

Healthcare information technology, or health IT, is the use of computers and electronic resources to manage data used in the healthcare industry. Health IT includes Electronic Health Record (EHR) systems that allow patient data to be stored and accessed easily throughout different healthcare institutions. Health IT is revolutionizing healthcare and greatly improving quality and ease of care. However, the widespread availability of sensitive patient data due to EHR systems leads to privacy concerns for patients. Many health IT systems also lack *interoperability*, which is the degree to which separate systems can share data. Furthermore, advances in either privacy or interoperability create a conflict, as the goal of privacy is to restrict data, while the goal of interoperability is to spread data.

Denmark has already taken steps towards improving its health IT infrastructure by creating a strategy for implementing health IT in the coming years. Many organizations are dedicated to developing health IT systems but tend to focus more on interoperability and less on ensuring patient privacy. This raises concerns for both patients, whose sensitive data are at stake, and healthcare providers, who have a responsibility to ensure privacy. *Forbrugerrådet* (the Danish Consumer Council), a non-profit organization devoted to consumers, is specifically interested in improving the quality of healthcare for the patient and the quality of systems for healthcare providers by addressing privacy and interoperability concerns.

This project was aimed to assist Forbrugerrådet in better understanding the issues of health IT systems that affect healthcare patients and providers. We accomplished our goal by conducting scholarly research, assessing EHR infrastructure in Denmark through interviews with experts in various fields relating to health IT, and analyzing the interaction between privacy and interoperability with EHR in different health IT systems. These methods helped us formulate suggestions for how to spread awareness on the effects of EHR implementation in Denmark.

Background Research

EHR systems are very complicated and take a long time to implement effectively. Effective EHR systems must ensure privacy of patient data, be interoperable with other EHR systems through the use of data exchange standards, and follow all of a country's healthcare laws and regulations. It is also critical that an EHR system is specifically customized for a hospital and its staff; otherwise, the system can actually decrease productivity. When properly

implemented, an EHR system offers significant advantages to both patients and healthcare providers.

Today, there is a push in many countries to implement EHR systems in hospitals, but many legal and technical obstacles impede its progress. In addition to following all of a country's healthcare laws, EHR technology also creates a need for legislation that specifically deals with electronic data rather than paper records. Technical issues with EHR technology include lack of a technical implementation plan, lack of proper IT personnel for support, healthcare providers' lack of technical knowledge, and technical failures inside the systems.

Denmark is considered to be a leader in health IT, and as of 2009, 95% of the country's general practitioners make use of EHR systems. However, only 35% of hospitals use EHR, leaving much room for improvement (Castro D. , 2009). Currently, many government organizations are working together to increase interoperability between the hospitals in the different regions and municipalities. There have been four national plans for the digitalization of medical data since 1995.

Methodology

Because health IT is an extremely broad topic, it was important for our project to concentrate on the issues that most affect the consumers of health IT systems, which includes both patients and healthcare providers. We focused our research on the issues surrounding patient privacy and interoperability of EHR systems in Denmark. With this in mind, we developed four main objectives to accomplish our goal.

The first objective was to identify technical, legal, and social issues of health IT faced in Denmark. A preliminary literature review revealed a variety of both potential and current problems and demonstrated how stakeholders in Denmark have dealt with the issues of privacy and interoperability.

The second objective was to identify the organizations involved in health IT in Denmark and to understand how they interact with health IT consumers and each other. This was accomplished by conducting interviews with key members of the different organizations. We used interviews in order to gain a deeper understanding of how the organizations interacted.

The third objective was to understand the social implications of privacy and system interoperability issues within health IT on Danish patients and healthcare providers. We again used interviews of health IT experts and stakeholders to better understand the issues. When choosing candidates to interview, we were careful to speak with both government and private organizations in order to get a balanced perspective of the problems.

The final objective was to organize and analyze our findings in a manner that allows Forbrugerrådet to make an objective and knowledgeable argument about EHR privacy and interoperability in the best interest of both healthcare patients and providers. We presented our findings in the form of a policy paper to be presented to Danish legislators. The policy paper addressed nine issues and recommended eight ways to address the issues, which can be found in the Conclusions and Recommendations chapters of this report.

Results and Analysis

Working in Denmark, the majority of our data came from our interviews with experts and stakeholders. The information gained from all 14 interviews helped us assess issues relevant to consumers of EHR systems in Denmark's health IT infrastructure, as well as strategies to improve these systems.

There is an overwhelming number of government and private organizations in Denmark involved in different areas of health IT, with complex interactions between them. Healthcare is funded by the Danish government and allocated through the Ministries of Finance, Science and Technology, and Health to each of Denmark's five regions. The regions control the state hospitals and decide on EHR systems and interoperability solutions within each region. Other organizations, such as Digital Health and Sundhed.dk, help connect the regions' EHR systems with each other, but do not have the power to make final decisions for the regions.

Privacy of medical information is a low priority in Denmark due to the generally trusting mindset of Danish society. Most Danes trust that the government protects their privacy and are unaware of personal data collection and access. Danes can also find it difficult to use privacy technology, discouraging its use. Currently, Denmark works on a terms-of-use, "trust" system that leaves the door open for data to be compromised. Any doctors can access any patient's data, and access is logged by the system and audited for illegal activity. However, only 1-10% of the logs are reviewed, creating large privacy risks for patients.

Denmark uses a digital signature system for user access into systems holding private data. The Danish CPR number is also used for identification. While the signature uses strong security technology, it also creates a centralized point of access that creates more privacy risks for patients. If an attacker compromises the digital signature or more easily finds a user's CPR number, they can gain access to all of a user's sensitive data stored in any system that also uses the CPR or digital signature, resulting in identity theft. Large, centralized systems are used often in Denmark, adding to this threat.

Each of Denmark's regions is responsible for creating an EHR system or interoperability solution for hospitals within that region. The primary solution for nation-wide EHR is currently sundhed.dk, the eHealth portal. Healthcare providers can use the portal to gain access to patient data, but this solution is not directly interoperable with region-wide systems and only provides limited data. Multiple organizations in Denmark are working on developing better interoperability solutions across the country.

Health data standards are critical in making systems interoperable. Most organizations agree that Danish standards are not strict enough in how they can actually be implemented in systems, resulting in poor interoperability between systems. The lack of acceptable standards means that large vendors in Denmark tend ignore standards, so that when hospitals buy their systems, they are "locked in" to that vendor and cannot use solutions from other vendors.

Danish laws on healthcare can be confusing for healthcare providers. Many different groups disagree on whether or not the current legislation for health IT is adequate. Conflicting laws on health and laws on service can simultaneously apply to the healthcare industry, raising a question of which law to follow during what times. There are also no organizations that help system vendors implement patient privacy according to legal regulations.

There are a handful of possible solutions that address both privacy and interoperability concerns. In place of the CPR number and digital signature, a pseudonym-based identification system would provide much greater security. In a pseudonym system, a user is given a different login identifier for each different system. An attacker must break into each system individually. In addition, data stored on servers is encrypted with a key held by the user, meaning only a user can give access to the data.

Role-based access control would also significantly improve patient privacy and make systems more usable for providers. Using role-based access control, a system would restrict providers'

access of data to only those patients they are currently treating, with an override that would allow doctors to access anyone's data in case of an emergency. This would reduce the burden placed on providers to decide whether or not they are legally accessing data.

Smaller, modular systems instead of larger systems would provide significant benefits for providers. Large systems that attempt to be "one-size-fits-all" solutions for health IT are slow to upgrade and cannot be customized to meet providers' specific needs. In a modular system, a number of small systems interconnect and work together. Different providers in the same hospital can choose the systems they prefer, and upgrades to individual systems can happen more quickly. Security systems in particular benefit, since security technology evolves rapidly and must be up-to-date to be effective.

Vendors could also conduct Privacy Impact Assessments when developing their systems. These assessments, performed at each stage of a system's development, involve identifying all potential privacy risks in the system. This way, countermeasures for each risk can be developed.

Conclusions

Danish EHR systems cause different problems for patients than those faced by healthcare providers. We identified five major issues that primarily concern patients and four issues that concern healthcare providers.

Patients face issues related to the privacy of their data. Danish patients are largely uninformed and unconcerned with the privacy of their data, leading to ignorance in the use and storage of their data. The Danish CPR number is widely used in many systems with sensitive data and is easily obtained, creating a large security risk. The large, centralized nature of these systems contributes to this risk by concentrating sensitive data into fewer systems. Currently used EHR systems have simplistic access control and do not prevent healthcare providers from accessing irrelevant patients' medical data. Finally, privacy technology can be complicated and difficult for patients lacking technical knowledge to use.

Healthcare providers face some issues with the interoperability of EHR systems. Data standards used in Denmark lack strict implementation requirements, reducing interoperability and restricting hospitals' choices when purchasing systems. The large systems often used in hospitals are too inflexible for providers' needs due to difficulties in customization and upgrading.

Providers face some legal issues as well, with regard to patient privacy legislation. Data accessibility laws can often contradict treatment requirement laws, preventing providers other than doctors from accessing data needed for effective treatment. Complicated laws can also cause confusion for providers and make them wary when accessing medical data.

Most of the issues found are related to a lack of patient privacy. Large security risks exist for Danish patients, who are both unaware and unconcerned. Systems are not built to take privacy into account and create issues and unnecessary burdens for providers. Denmark's government-based health IT organizations at large are more concerned with interoperability issues and believe that current systems for privacy of data are adequate.

Recommendations

To solve the issues for both patients and providers, we recommend eight general solutions to cover the nine problems. Most of these solutions address more than one issue.

Danish patients should be made more aware of the significant risks to their privacy so that they can take proper precautions. This will also motivate both the industry and legislators to focus on keeping patient data private. Raising awareness among patients is absolutely critical in furthering privacy, as they are the group actually at risk due to these systems.

The use of pseudonym-based identification would significantly improve patient privacy and grant users control over their data. Pseudonym systems would also decrease privacy risks to patients caused by the Danish CPR number, while still maintaining interoperability between systems. Implementing role-based access control in systems will also greatly improve patient privacy and reduce the burden placed on providers to decide whether or not they are legally accessing data.

Vendors should work more directly with users when creating systems intended for both patients and providers to ensure that they are easy to use and effective for their users. Vendors should also conduct Privacy Impact Assessments to properly secure their systems. Using smaller, more modular health IT systems instead of larger, universal systems will fit both healthcare practitioners' and hospital administrators' needs. Smaller systems will also aid vendors in designing small systems customized towards providers.

Stricter interpretation of standards would promote interoperability between systems and empower smaller vendors of health IT systems. Stricter standards will also facilitate the use of small modular systems, which require high levels of interoperability. An organization that

helps vendors properly adhere to data standards would help create stricter interpretations and encourage vendors to ensure that their systems are interoperable with other systems. Finally, a revision of the laws related to health IT issues to remove contradictions would reduce complicated situations in which a healthcare provider must decide which law to follow under differing circumstances.

These solutions vary in how long they will take to implement, and some rely on other solutions being finished first. Using pseudonym-based systems will require a fundamental paradigm shift in how Denmark deals with privacy. It will also likely be difficult to increase awareness on privacy issues due to the Danish mindset on trust. However, some solutions are closer -- there is already a push for better standards, and role-based access control is not as far away as pseudonyms. Both privacy and interoperability can be achieved in EHR systems, but Denmark's government-based health IT organizations must give more attention to privacy issues in order to accomplish this.

Chapter 1: Introduction

Healthcare information technology, or health IT, is the use of computers and electronic resources to manage the enormous amount of data used in the medical industry. The field of health IT includes Electronic Health Record (EHR) systems that provide a centralized database for individual patient records and useful websites such as ePrescription systems that allow patients to order prescription medicines online. The field of health IT is revolutionizing healthcare and in many cases has already greatly improved quality and ease of care. However, health IT systems are far from perfect – many challenges still exist, and new risks have emerged from the use of these systems that have not yet been fully identified and addressed. For example, the large scale and complexity of systems can cause unintentional violations of patients' privacy. Interoperability, or the exchange of data between different systems, is also a major concern in health IT. The point of health IT systems is to transfer information quickly and easily, and this benefit is greatly undermined if different systems cannot communicate with each other. These two goals naturally conflict – a system that has higher interoperability has data more freely available and must focus even harder on security to maintain an adequate level of privacy. These issues only begin to touch on the complex problems in health IT systems today, many of which are not yet well understood.

Many efforts have been made to assess the state of health IT on both national and global levels. Very recently, the EHR Impact study looked at a number of different hospitals in different countries to determine whether EHR systems provide the socio-economic benefits that they are predicted to deliver (Dobrev, Jones, & al., 2009). The study found that EHR systems do provide long-term, sustainable benefits, but at significant up-front cost, and that each country and organization must build EHR systems specialized for their own use in order for them to be most effective. The Information Technology and Innovation Foundation has also recently released a report detailing which countries are leading in health IT, which areas they lead in, and how other countries can improve their own performance (Castro D. , 2009). Many other studies have been done to analyze problems in specific countries (Hartlev, 2008). Sweden and Norway have world-class healthcare and have successfully implemented many health IT systems. Denmark is also considered to be a leader in health IT, but there are still many problems that exist in their systems (Jensen, 2010).

Patient privacy is an important aspect of health IT systems that Denmark has not yet fully addressed. In 2008, the Danish Health Act allowed the Danish Medicines Agency to keep a database of patients' personal electronic medicine profiles (The Danish Health Act., 2010). When a

new provider wishes to look at a patient's profile, patients are supposed to receive communication allowing them to give consent. However, many times the patients receive the communication some time after the provider has already looked at the profile (Jensen, 2010). This is just one specific issue – health IT is such a broad field that it requires extensive analysis in order to identify all of the possible problems. Furthermore, Denmark has many medical institutions, and the rules and regulations differ between the country's five regions. Solutions to problems can also have conflicting interests, such as the previously-mentioned clash between privacy and interoperability. Denmark has already taken steps towards the future of its health IT – it has created a plan for implementing health IT in the coming years (National Strategy for Digitalisation of the Danish Healthcare Service, 2007). Also existing in Denmark is the organization Connected Digital Health in Denmark (SDSD), which was created to analyze, facilitate, and improve health IT adoption throughout the country. Denmark has already focused efforts into improving health IT, but more limited effort in assessing what effects these improvements have had.

Forbrugerrådet, a non-profit organization devoted to consumers and their issues, has turned its interests towards the field of health IT. The Council is a research and advocacy group that helps to design policy and has politically motivated goals. It is specifically interested in improving the quality of healthcare for the patient by addressing privacy and interoperability concerns. The Council has recognized that there are some problems with the country's health IT systems, and is interested in gathering information about what these problems actually are from the consumer's point of view. The previously mentioned patient record consent issue is one such problem. There have been few comprehensive studies to analyze precisely what issues exist in currently-used health IT systems, which ones affect each other, and which ones are the most important to consumers. In addition, consumer opinion on the visible effects of health IT systems is not well known.

Our group used a four-step process to identify major issues affecting patients in Denmark's health IT, with a primary focus on privacy and interoperability issues. First, we analyzed the variety of legal, technical, and social issues that affect patients in health IT systems in Denmark to identify a large number of potential problem areas. We identified those issues that dealt specifically with the issues of privacy and interoperability that Forbrugerrådet is concerned with. Second, we identified the organizations involved in health IT in Denmark and gained understanding in how they interact with each other, patients, and healthcare providers. Third, we used these problems identified as well as our understanding of the health IT structure in Denmark as a starting point to search for issues in

Denmark's hospitals and clinics, primarily through the use of interviews and surveys. Finally, we used our findings to determine what the most pressing issues are in Denmark's health IT systems for Danish consumers and recommended which should first be addressed to the Forbrugerrådet and Danish legislators through our Policy Paper and "facts for patients" that will be featured on the Forbrugerrådet website.

Chapter 2: Background

The field of health IT is specialized and complicated yet very broad, with many parties involved in its implementation and usage. Health IT is a relatively new industry and is not yet well established, but extensive efforts have been made to study and advance the field. This chapter will provide a brief overview of health IT systems and focus on how the implementation of these systems affects the consumers who, in this project, are the healthcare providers and patients. This chapter will first examine what factors are the most important ones for an effective health IT system, who will benefit from it, and what some of the technologies actually are. Next, we will examine the various issues and risks that arise when systems are implemented, and who will be affected. Finally, we will investigate how Denmark and other countries have implemented health IT and compare the results these countries have had.

2.1 Health IT and Electronic Health Records

The introduction of electronic information systems, more specifically electronic health records (EHR), into the healthcare industry is projected to substantially improve healthcare in the near future. For the past two decades, there has been a push to implement EHR technology. Figure 1 shows how EHR has already been adopted among U.S. physicians and estimates how adoption will proceed. The upward slope presented in the graph is not specific to just to US, and the growth trend of EHR adoption is expected globally. This push has been attributed to both the benefits in improved quality of care and cost savings that EHR promises.

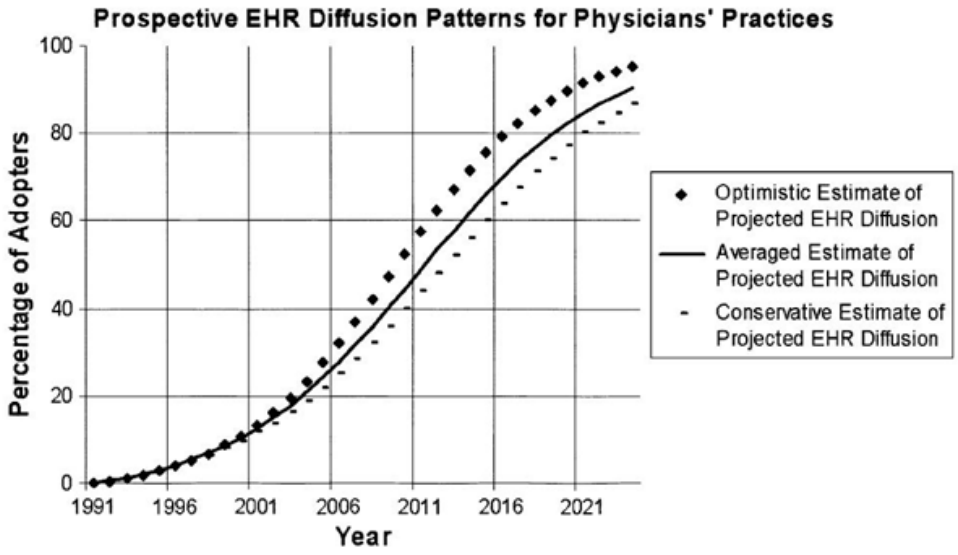

Figure 1: Three models of EHR diffusion based on prior empirical estimates (Ford, Menachemi, & Phillips, 2006, p. 108)

The technology needed for most health IT systems has existed for some time and would not be extremely risky to implement were it not for all the stakeholders with varying interests (Tulu, 2010). A good EHR system will take into account the different needs of the patients, doctors, and hospital administrators involved, as well as satisfying the policymakers' legal issues with privacy and security laws concerning sensitive electronic data. These needs often create large conflicts of interest, further complicating development, implementation, and use of EHR systems. A truly effective EHR system will be designed especially for a certain group so that their specific needs can be met, which means that technological solutions cannot simply be reused for everyone (Dobrev, Jones, & al., 2009). EHR systems that are not specifically designed for an institution risk not only failing to provide promised benefits, but also causing new problems that can lead to an overall negative effect (Gaffey, 2009).

2.1.1 Key Attributes of an Effective EHR System

In order for any EHR system to be worthwhile and effective, a number of important attributes must be present. The system must take into account the healthcare-related laws of the country it exists in. It must be as interoperable as possible with other EHR systems, including adhering to various technical standards. The last issue discussed here is the privacy of patients – systems must match both the patients' and government's expectations for privacy of sensitive health information.

Figure 2 illustrates some different metrics that can be used to evaluate how EHR systems make use of data. Accountability refers to the severity of punishment for illegal disclosures of patient data. Transparency refers to whether the patient is informed of the ways in which their data can be used. Patient Consent measures how often a patient is given opportunity to consent to or refuse uses of their data. Cost Re-identification measures how difficult it is for a patient to be re-identified in a different system. Oversight refers to how much a system can be supervised by an external source. Regulatory refers to the number of rules and regulations that the system abides by.

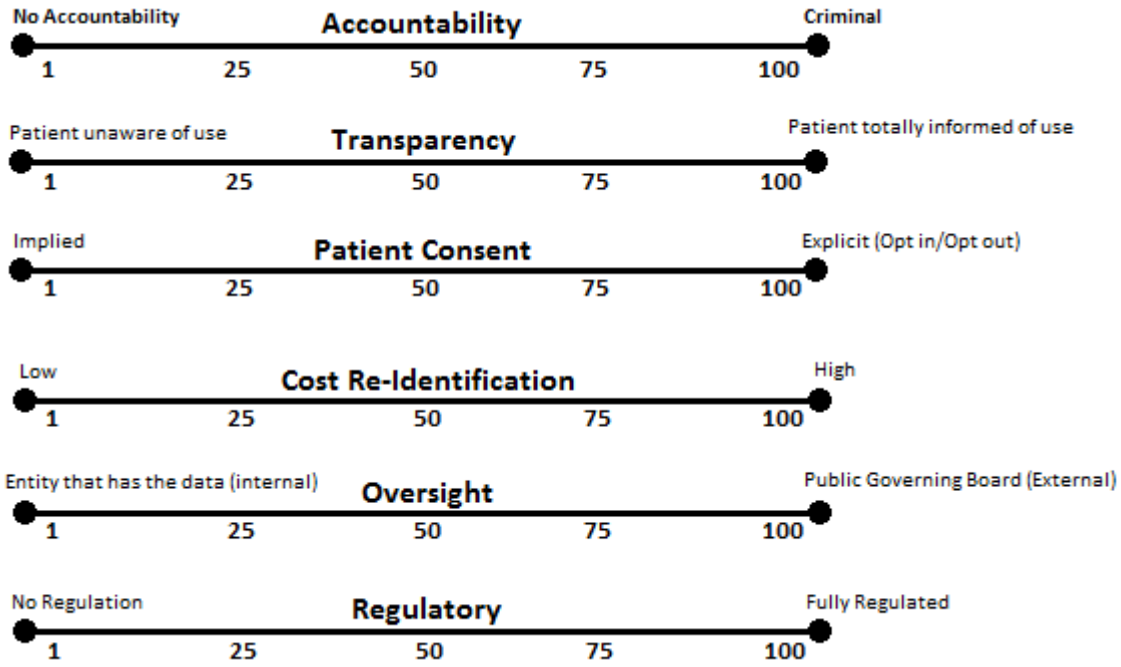

Figure 2: The Framework Line used to Assess Status of Health Data Uses. Adapted from: (Bloomrosen & Detmer, 2008, p. 720)

2.1.1.1 Privacy

The confidentiality of a patient's medical information is one of the cornerstones of medical practice. Doctors and nurses are always expected to keep all of the patient's conversations, test results, medication, diagnoses, and current health status in confidence. If a patient's sensitive medical information is leaked out, it can potentially damage them in a variety of ways (Barrows & Clayton, 1996). In addition, the nature of health IT is to allow information to be easily shared with other parties, so ensuring that only the right people can see the data is even more crucial. Therefore, patient privacy is a top concern when developing a strong health IT system.

Privacy can be lacking in many systems of health IT. For example, providers in Denmark often use e-mail as a form of communication between patients and doctors (Jensen, 2010). E-mail is efficient, already widely used, and provides records of communications. However, e-mail is insecure – e-mails can be intercepted and read, and intruders can potentially break into e-mail accounts and access the records of communication or impersonate the doctor. The need for security is plainly evident (Hodge, Gostin, & Jacobson, 1999).

Australia's HealthLink system is an attempt to provide adequate privacy for users of EHR systems. It breaks privacy down into seven key areas. First, patients must consent to use the system. Second, the system must be transparent by granting a patient access to the records and giving them knowledge of how the system works. Third, the patient can control which parts of their record are visible to healthcare providers. Fourth, the patient can restrict what data are actually collected by the system. Fifth, data transfers must be secure. Sixth, patients must be able to correct inaccurate information in the system. Finally, the system must be able to confirm a patient's identity with confidence. These different areas provide a good breakdown of exactly how complicated patient privacy is and what needs to be considered for a good system (Ray & Wimalasiri, 2006).

2.1.1.2 Interoperability

Interoperability is the ability for different EHR systems used in different hospitals and departments to seamlessly exchange data. One of the major benefits of implementing EHR and using strong health IT systems is the ease with which electronic data can be shared. It is now potentially possible for detailed personal patient data to be instantly accessible to all hospitals and all health care providers around the world at very little cost. If realized, this potentially would help to ensure that patients receive the best possible service by allowing any physician to know important personal health data about patients. Additionally, the issues of dealing with paperwork, waiting for information, using outdated information, and needing to report the same information multiple times for different providers could all disappear. EHR systems have the potential to create substantial savings after the initial investment period (Walker, Pan, & al., 2005).

All of these benefits, however, require strong health IT interoperability. Without interoperability, the benefits of EHR systems are severely undermined, and one of their greatest advantages cannot be utilized effectively. Currently, a substantial amount of EHR data are stored in isolated locations, which is only useful to the one system that has access to the data. In order for EHR and other health IT services to succeed, interoperability must be regarded as an essential element of systems (Kalra, 2006). Figure 3 shows some of the different health IT systems across which interoperability is desired.

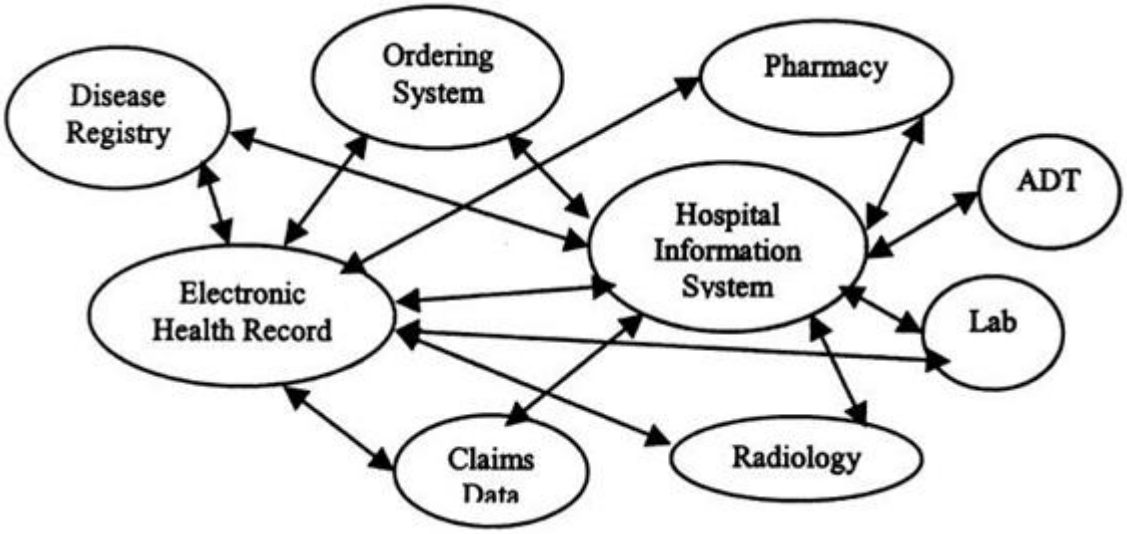

Figure 3: The flow of information across different healthcare information systems (Liu, Cooper, & al., 2001, p. 289).

Healthcare providers can be broken down into four different levels based on the amount of interoperability they provide. Level 1 providers use no electronic IT whatsoever. Level 2 providers have basic IT available, such as faxes and computer documents, but this information cannot be manipulated by specialized software. Level 3 providers have software specifically created for health IT and have message formats that can be passed between systems, but the message translation is imperfect and loss of data might occur due to multiple incompatible formats used. Level 4 providers have solved this problem and use standardized health IT message formats, rarely experience loss of data, and have near-perfect transmission of data between systems (Walker, Pan, & al., 2005).

Looking into the future, interoperability reaching across national barriers becomes much too complicated and difficult because differences exist between the needs of users in different countries. The laws for protecting and securing sensitive patient data differ from country to country, and EHR systems must be built differently to abide by these differing regulations. Different cultures also have different expectations for privacy (Tulu, 2010). These factors, among others, force each country to build a unique EHR system that fits these needs. These needs help define a blueprint for a country's EHR systems, but the fact that a new system must typically be built for each country and their various providers is also a significant barrier to EHR's adoption. In order to generate and organize the data needed by both patients and doctors, expensive, complicated database systems must be put in place (Gunter & Terry, 2005). Figure 4 shows some of the different ways patients can receive medical information through an EHR system, and how complicated that process can become.

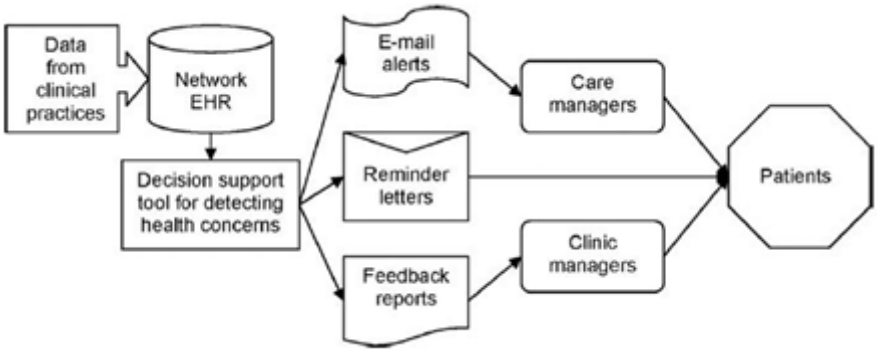

Figure 4: Schematic view of a community-based EHR system and data-driven interventions designed to impact healthcare (Lobach & Detmer, 2007, p. S108)

Standards

Defining and adopting technological standards for EHR and health IT in general is an excellent way to improve interoperability between systems. With the development of standards, hospitals can adhere to commonly accepted rules in order to be interoperable without having to make specific negotiations with other institutions. Health IT standards are the clearest and most effective solution to aid interoperability (Kalra, 2006).

The issue is that there are many different standards currently in use in different places. Providers in Denmark currently use MedCom standards, which were created using European Committee for Standardization (CEN) standards. Recently, Denmark has had some success in developing the Common Conceptual Domain Model for Danish EHR Systems, called GEPJ – a nationally used standard for documenting EHR data also created using EU standards (National Strategy for Digitalisation of the Danish Healthcare Service, 2007). However, different countries use their own standards, so it is worth considering which seem to be more effective.

Due to the complexity of systems, standards for EHR systems need to address a broad range of topics. However, each standard discusses a different set of areas to standardize – some standards will cover certain issues while others miss them. The full set of topics that standards must address has not yet been universally agreed upon. Examples of some of the different areas that are being standardized and which standards are addressing which ones can be found in Table 1(National Strategy for Digitalisation of the Danish Healthcare Service, 2007) (Kwak, 2005). These are only part of the issues these standards must address. These standards are complicated and require strong understanding of EHR systems and information technology in order to implement and design systems around them.

Table 1: Examples of Standards Required for Data-Sharing Interoperability. Adapted from: (Hammond, 2006, p. 1206)

Category of Standards Required for Data-Sharing Interoperability		
Class of Standard	**Example Standards**	**SDOs Creating the Standard**
General standards, broad use	XML, TCP/IP, 802.11, Web services, security, wireless, GPS	W3C, IETF, IEEE, OMG, HL7
Data components	Reference Information Model (RIM), data elements, data types, terminology, templates, clinical statements, clinical document architecture	HL7, CEN, ISO, openEHR, SNOMED, LOINC, RxNorm, UMLS, others
Data interchange	Structured and free-form documents, images	HL7, ASTM, DICOM, IEEE 1073, NCPDP, X12N, CEN, ISO
Knowledge representation	Guidelines and protocols, decision support algorithms, Arden Syntax, GLIF, GEM, Prodigy, Protigé, vMR, GELLO	HL7, ASTM, others
Electronic health record (EHR)	Functional requirements, EHR models, Continuity of Care Record (CCR), patient summary record, personal health record	HL7, ASTM, openEHR, CEN
Application level support	Identifiers, resource registries, disease registries, tool sets, conformance requirements, implementation manuals	HIPAA, HL7, ASTM, ISO, CEN

Detailed in Appendix C – Relevant Health IT Standards are some of the more important and widely used standards in use today. Many of these standards use a dual model approach, which divides standards into two groups – a reference model, and an archetype. The reference models define what the individual health record components are and what data are included in them. Table 2 shows how a reference model might break down a health record into basic parts. The archetypes organize these components into combinations useful for different health departments (Kalra, 2006).

Table 2: Main Building Blocks of EHR. Adapted from: (Kalra, 2006, p. 141)

Logical building blocks of the EHR	
EHR	The electronic health record for one person
Folders	High-level of organization of the EHR e.g. per episode, per specific clinical
Compositions	A clinical care session, encounter or document e.g. test result, letter
Sections	Clinical heading reflecting the workflow and consultation process
Entries	Clinical "statements" about observations, evaluations, and instructions
Clusters	Nested multi-part data structures (tables and interval time series) e.g. audiogram
Elements	Leaf nodes with single data values e.g. reason for encounter, body weight
Data values	Data types for instance values e.g. coded terms, measurements with units

2.1.1.3 Legal Considerations

Privacy and interoperability are two of the most important issues in health IT, but the legal issues raised by these systems must be taken into account. The many legal requirements on practicing medicine and protecting the privacy of patients must be followed while using systems. National policy is also a key factor in the widespread adoption and advancement of health IT systems. Because laws between countries differ, it is also important for a country to take others' laws into account when attempting to design interoperable systems.

Keeping a patient's data in confidence is one of the primary legal issues that a provider must worry about. In general, a system must ask for the patient's consent before sharing his/her data with another party. Exceptions and specific details to this rule differ between countries. Other providers and insurance groups might need to have access to data for various legal reasons (Hartlev, 2008). Laws such as the U.S.'s HIPAA compliance work to keep patient data private (Ray & Wimalasiri, 2006). In 2008, the Danish Health Act passed in Denmark allowed the Danish Medicines Agency to keep a database of patients' personal electronic medicine profiles (The Danish Health Act., 2010). The act specifically sets a number of guidelines for how electronic health data can be used, and is an example of how systems must adhere to their country's laws.

The legal system can also strongly aid the health IT field. Government bodies often help decide which standards a country should use through legislation. The use of national requirements for health IT systems vastly improves the interoperability standards between systems. Studies have found that this is actually the fastest way to improve a nation's interoperability and is a key element in developing health IT (Castro D. , 2009). Details on Denmark's government structure relevant to health IT can be found later on in Section 2.3.1 Denmark.

Interoperability between countries is also greatly affected by national policies. Because systems will differ in what they can and cannot do in each country based on its laws, each country must implement its own version of the system. This limits interoperability in health IT between countries, and extra effort must be expended to ensure that systems can be most effective. The need for legal health IT systems represents another key issue to consider during their design (Hansen, Pang, & Maeder, 2005).

2.1.2 Stakeholders and How EHR Benefits Them

The primary reason the implementation and effective use of health IT systems is so complicated is due to the large number of stakeholders involved in the process. All of these stakeholders have

different interests in the systems, and can all benefit from them in different ways. Because effective health IT systems must be specifically designed to meet a group of stakeholders' unique needs, it is very helpful to understand what some of the most common needs and potential benefits are.

It should be noted that the use of health IT systems is not solely positive and includes risks – these are detailed later in Section 2.2.4 Potential Risks to Stakeholders.

2.1.2.1 Patients

Through EHR, patients expect to gain more authority over their care, including safer, higher quality care, appropriate levels of privacy, specific abilities to access and correct their personal records, and the capability to give consent for the use of their health information for research. Unfortunately, what the patient needs is not always consistent with what doctors, hospitals, or insurance companies want. There are also issues with the level of technology available to fulfill patients' wishes. From the patients' point of view, the implementation of an EHR system is aimed to give them more say over their records as well as better healthcare, and obtaining both of these comes with benefits as well as risks (Gunter & Terry, 2005). One patient, Rhona MacDonald explains her predicament,

> *"Here is my dilemma. I want my notes to be strictly confidential but readily accessible to those who need them. Electronic notes, while potentially solving my second problem, sets alarm bells ringing with regard to the first. I am not a technophobe, but I am wary of giving out personal financial information over the internet, and the thought of my entire medical history floating somewhere in cyberspace doesn't fill me with confidence."*
> (MacDonald, 2001)

According to the Institute of Medicine (U.S.), there are six specific patient-minded endeavors that must serve as the core values of an EHR system. The first is safety for the patient, where special consideration is taken to avoid injury due to treatment. The second issue deals with effectiveness of the process. It is not necessary for every medical service to be offered to every patient in the system. Therefore, a health IT system that can organize and filter patients according to specifics would improve the current state of EHR. The third imperative core value of EHR systems is patient-centered programs. All care that is provided due to the use of EHR must provide responsible and respectful care to patients, in the timeliest way possible. Fourth, EHR must be efficient in all types of systems. Fifth, costs are expected to be lowered to allow efficiency levels to increase. The final core guide to improving healthcare for patients is to keep in mind patient equality. Even when just accessing one patient's information, it is imperative to remember that all patients are equal and that no one should receive special privilege over anyone else in any part of a health IT system.

One of the most important benefits of an EHR system to the patient is the improvement in actual offered care. Having a patient's complete medical history electronically available no matter where the patient is can potentially save that patient's life. Medical errors such as misdiagnosis, not knowing allergens, or unintentional negative drug reactions can be reduced because health records would be available when they are needed to answer questions about these issues. Not only would all health records be electronically accessible, but information on medications would also be available to patients and their providers.

Another benefit of EHR for the patient is the accessibility and ease of use of many important resources. Allowing patients the ability to view and correct his/her health records would not only benefit the patient with the most up-to-date and accurate records available, but the doctors who would treat them in the future would also be able to treat them more accurately. Online donor registration and helpful information pertaining to specific hospitals such as patient-to-patient communication, health laws and standards, information about specific medicines, hospital waiting lists, and patient feedback on satisfaction would all be easily accessible electronically for patients (Ministeriet for Sundhed og Forebyggelse, 2010).

2.1.2.2 Doctors and Nurses

Doctors and nurses are the primary end users of EHR and related health IT systems. They use health IT on a daily basis and should their facility decide to implement EHR, it will become integral to all their work. As such, they are a critical group to consider in any discussion on the field of health IT (Spil, 2007).

Physicians stand to gain an enormous amount from the use of health IT. If an effective, standardized EHR system were implemented, doctors could retrieve important patient information and share it with those who need it. Easier and quicker retrieval of important information would lead to higher quality of care. In addition, doctors would not have to run duplicate tests on patients, as all of a patient's test results would be conveniently available. A well-designed system could grant all these benefits and reduce errors in patient treatment and help avoid malpractice suits (Goldschmidt, 2005). A majority of U.S. doctors without health IT systems believe that implementing them would lead to all these benefits (Anderson, 2007). Overall, effective health IT systems would allow doctors and nurses to more easily manage the enormous amount of important data that is critical to their occupations.

Nurses also have much to gain. In a recent study, an EHR system was implemented at a rural U.S. hospital (Whittaker, Aufdenkamp, & Tinley, 2009). After using the system for 1-2 months, some of the nurses at the hospital were interviewed and asked for their opinions of its effects. At least half of the nurses reported that the system was easy to use and improved their ability to work as a team. This provides some evidence that EHR implementation can be used anywhere and is not limited to large urban hospitals. The study did also find a number of issues which will be discussed in Section 2.2.4 Potential Risks to Stakeholders.

2.1.2.3 Healthcare Officials and Hospital Administrators

While doctors and nurses are more concerned with how EHR will affect their work on a day-to-day scale, officials and administrators are worried about large issues of their entire hospital and its efficiency. Economics, feasibility and implementation problems are the big issues that administrators are concerned with (Tulu, 2010). Administrators are also the group most directly interested in interoperability, as they are the group most concerned with how the system functions as a whole and they most often deal with other hospitals.

Creating and implementing an EHR system requires a large initial investment, but will typically eventually pay off. The EHR Impact study found that it usually takes up to nine years for an EHR system to produce a net benefit (Dobrev, Jones, & al., 2009). Another U.S. study projected that implementing a minimal level of health IT would result in immediate savings, and implementing more advanced health IT would also result in savings after about ten years. Improved quality of care to patients is also a large potential benefit from the use of health IT systems (Walker, Pan, & al., 2005). In addition, decreased error rates through misinterpreted data can lead to fewer legal troubles and malpractice suits. All of these benefits lead to better business and a stronger healthcare system for those who are able to make the initial investment.

2.1.3 Examples of EHR Technology

EHR technology can be utilized in many creative and useful ways. Evolution of EHR systems can start small, with the implementations of PHR. A Personal Health Record (PHR) is a record of an individual patient's medical information that the patient can interact with directly. There are many types of PHRs – some simple being a PHR that is a stand-alone program stored on a patient's home computer for their own recordkeeping, or it can be a record inside a bigger EHR system that the patient can view. Details about the different types of PHRs can be found in Figure 5. PHRs allow patients to easily view their own health data and to take responsibility for their own healthcare

(Sprague L. , 2006). Google Health is an example of an existing PHR system – it is free to use and allows a patient to record their health data securely online, so that it can be easily accessed from anywhere (Tulu, 2010).

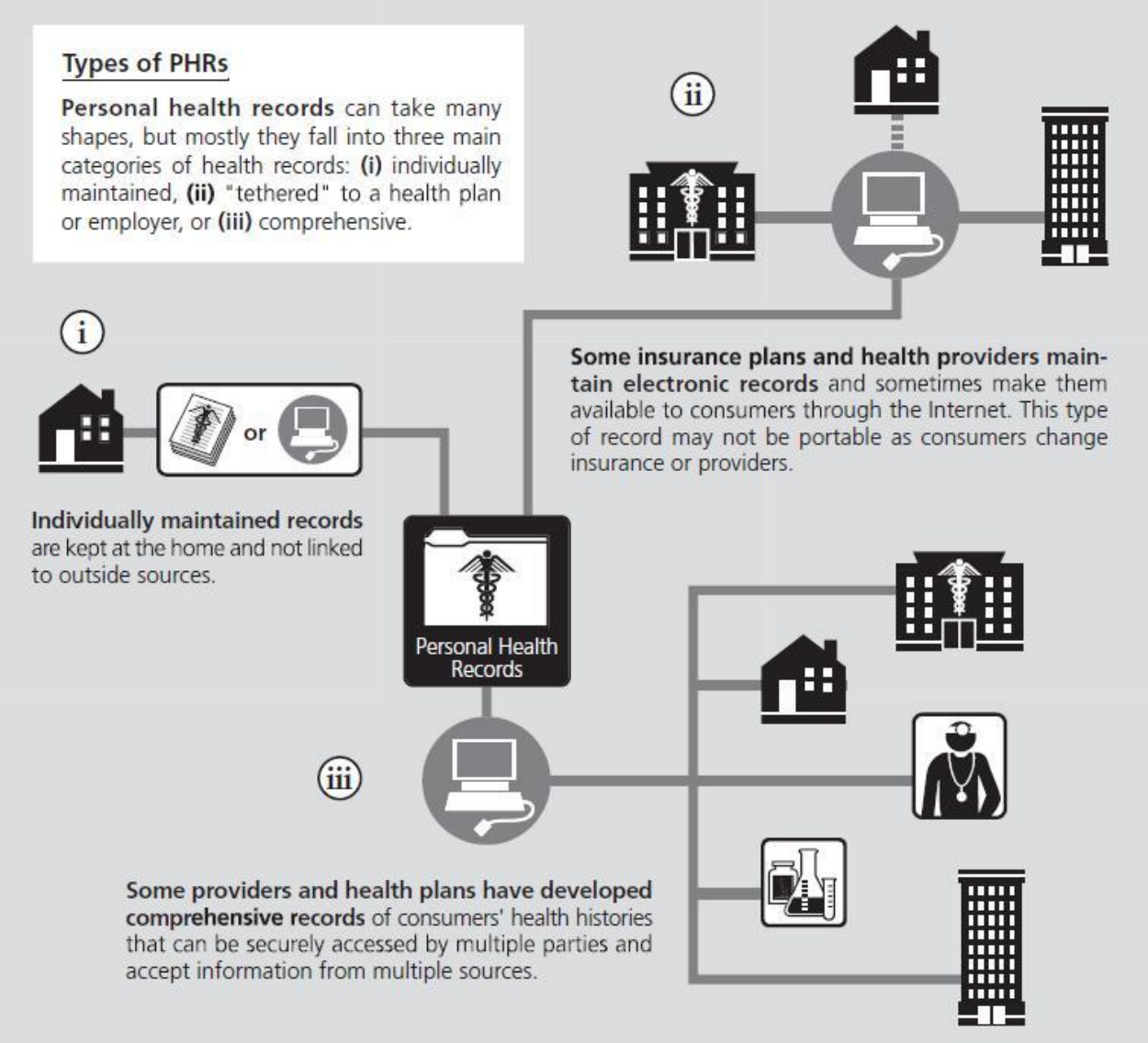

Figure 5: The three main types of PHRs (Sprague L. , 2006, p. 4).

The collection of PHRs can evolve into larger EHR systems. A simple implementation of EHR technology that can improve healthcare is through Computerized Physician Order Entry (CPOE). This system will allow a physician to prescribe medicine to his/her patients through an electronic system that will relay the information to the pharmacy and nurses who may have to administer the medicine. This system will prevent any misinterpretation by nurses or pharmacists about the

prescribed medicine due to the doctor's illegible handwriting. Figure 6 shows another interoperable system in a hospital where all the medical devices can communicate with each other.

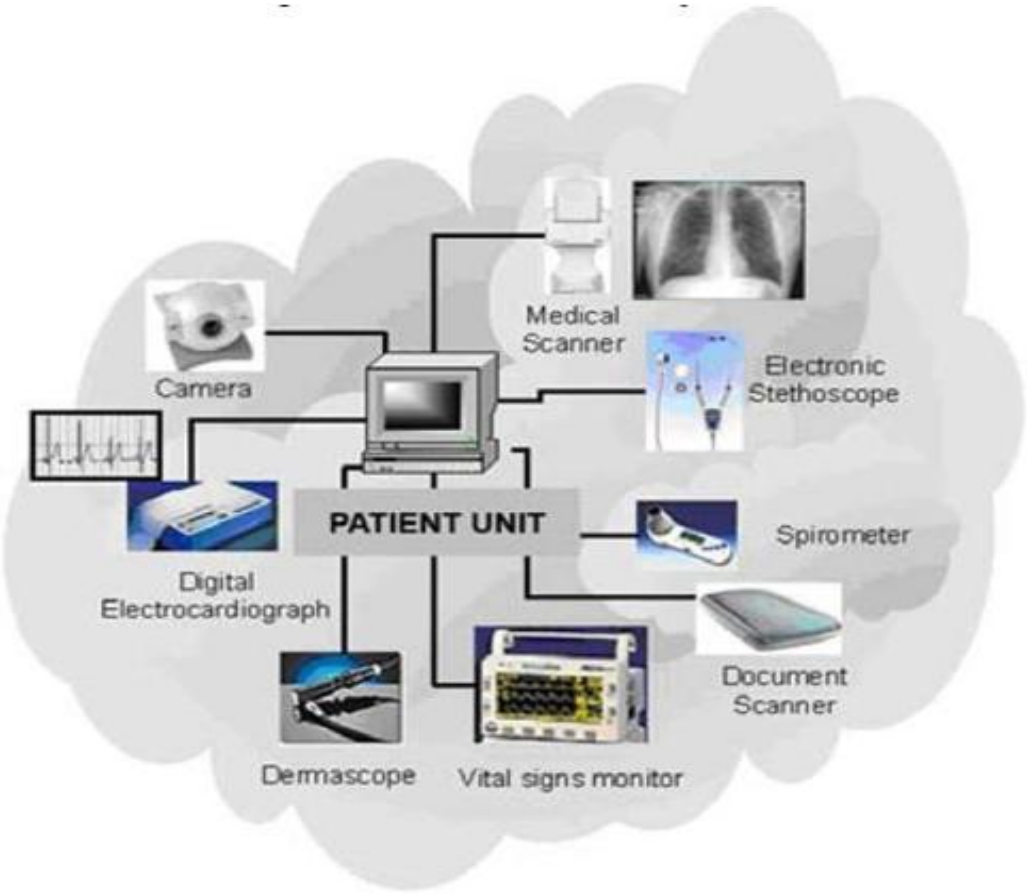

Figure 6: Examples of medical devices developed as modular components (Spanakis, Lelis, & al., p. 2)

Another step in the evolution of EHR technology would be a decision-making system that can suggest or discourage certain treatments and prescription drugs based on previous patients' experiences, drug interaction data, and health care protocols. Further advancements can be made so that the implemented EHR technology can track drug and patient movement in a hospital through RFID technology, and the EHR system can identify and troubleshoot medical problems that occur due to a technical or human error (Terry, 2004). Another technology that improves interoperability between EHRs is Health Data Integration (HDI). Rather than implementing one standard system where all the EHRs will have the same format, HDI just links all the different EHR systems together and allows a means for them to communicate with each other. Figure 7 shows the structure of the HDI system.

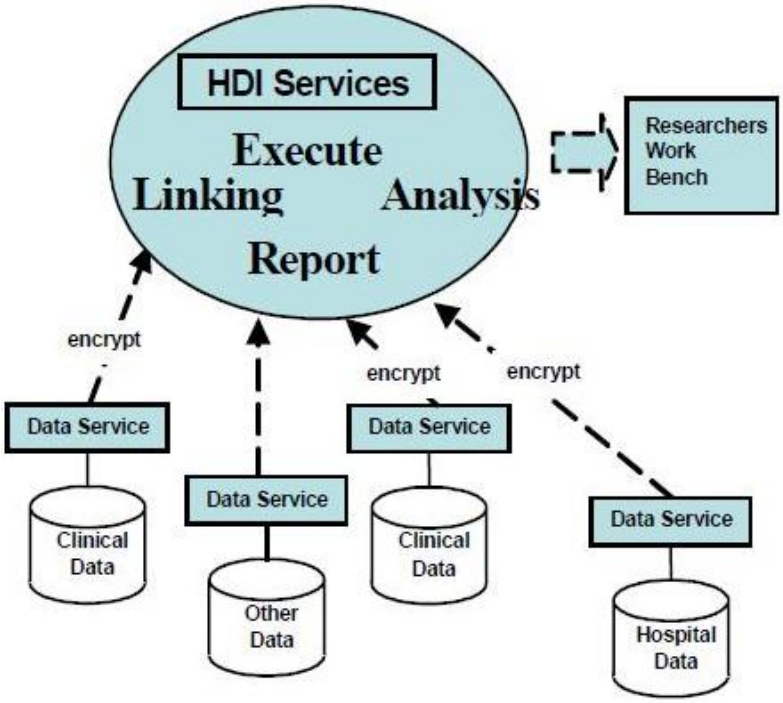

Figure 7: Overview of the HDI Architecture (Hansen, Pang, & Maeder, 2005, p. 5555)

Some proponents of HDI think that one standard EHR system is impossible to implement nationally across large countries, such as the U.S., and especially internationally given the costs, resources, and time that will be involved. HDI is an effective alternative that does not require major changes to the current EHR infrastructure (Hansen, Pang, & Maeder, 2005).

2.2 Issues with Health IT and Electronic Health Records

EHR technology has not immediately solved all the issues it promises to solve, and in some places it has not been as quickly and widely adopted as many had hoped. Two of the major reasons are first because many people are skeptical about the problems that could occur if EHR technology is implemented, and second because currently, there is no efficient model to implement EHR technology on either a national or an international scale. To these skeptics, the benefits are not always obvious and visible, and the risks outweigh the benefits. Legal and technical issues also prevent EHR technology from being more widespread and efficient. Thus, it is difficult to create an efficient technical model that is able to conform to all the proper legal laws and regulations, and it is difficult to pass legislation in any country that encompasses the varied types of EHR technology.

Another major obstacle is the cost of implementation. The return investment of EHR technology is seen only after a significant amount of time has passed after implementation. A short-term implementation plan might not have much effect on patient healthcare and may even be detrimental

(Sidorov, 2006). Social attitudes of the medical providers and administrators and economic constraints also play a role in the decision for EHR implementation. Figure 8[1] is a good example that shows the type of attitude the medical community needs to have when implementing an EHR system. The algorithm outlines different social criteria, such as the EHR being physician-centered, lack of political motive for EHR system implementation, and the hospital being strongly patient-centered. The algorithm also offers suggestions to improve and increase the use of the EHR system in a hospital, such as having different medical and technical language for different EHR users, increased sharing of data between physicians, and regular gathering of patient feedback regarding the EHR system in order to improve it. Another important idea in the figure is that even though the implementation of the EHR system would be the hospital administrators' decision and the EHR system would be used primarily by the healthcare providers, it is very important to include the patients in the process of improving the EHR system and making it more efficient.

[1] Figure 8 mentions EPR, which is a synonym for EHR

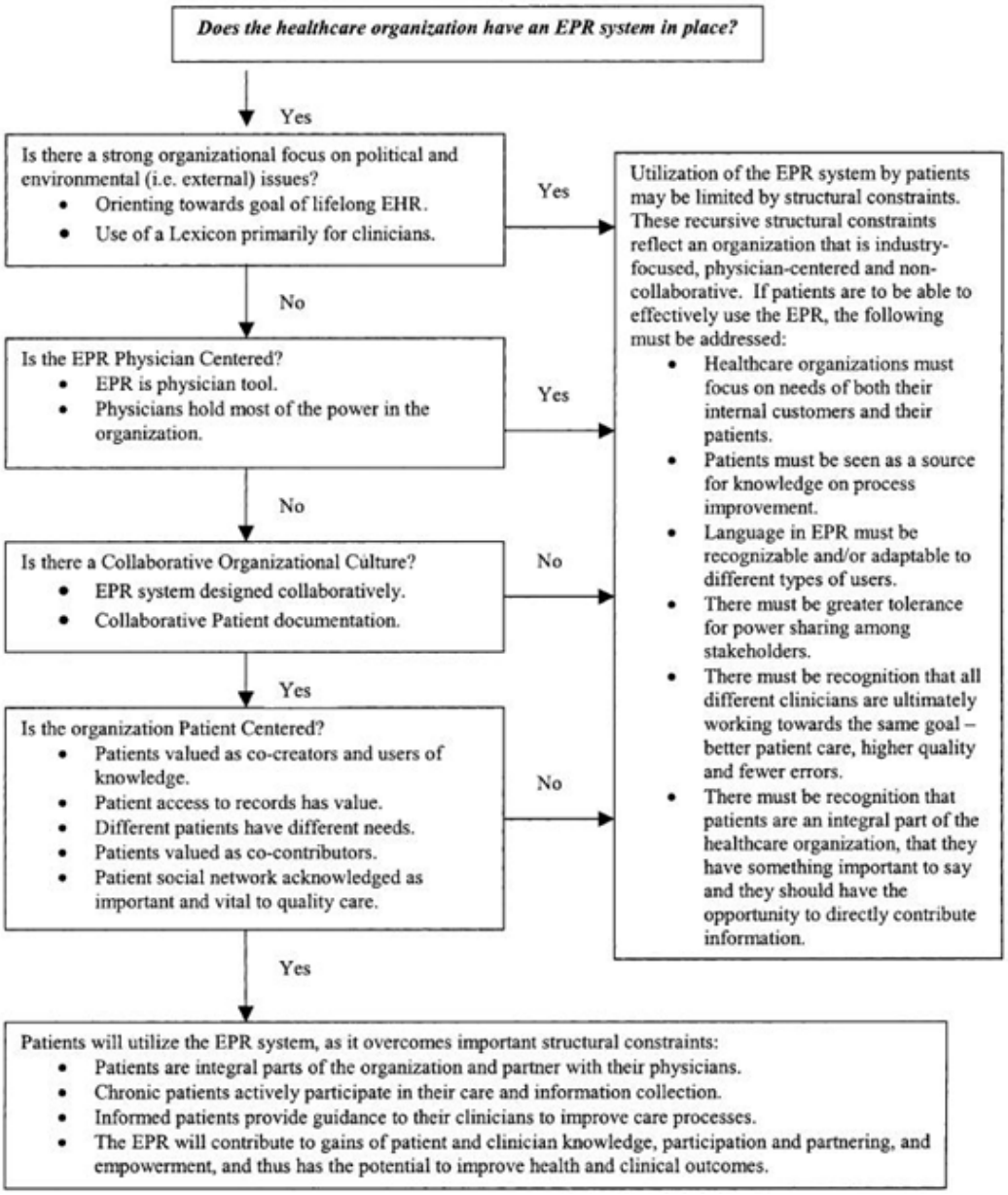

Figure 8: Evaluation framework for assessing the impact of medical record structure on patient utilization and accessible EPRs (Winkelman & Leonard, 2004, p. 156)

2.2.1 Legal Issues

Every country has its own rules and regulations, and this has a big impact on how EHR technology is received in a specific country. For example, in 2009, Denmark abolished a rule which required consent from the patient for doctors to release the patient's information to other medical parties (Jensen, 2010). The logic behind this was that with the increase in EHR technology, abolishing this rule will allow a smoother flow of information and will save more lives. In contrast, in 1996, the United States enacted HIPAA compliance which makes it mandatory for hospitals and doctors to get consent from the patient or his/her relatives in order to send or receive the patient's medical

records. In terms of interoperability, it becomes very difficult for an EHR system to respect the legal rules of each country and to send and receive patient EHR smoothly. Moreover, sometimes regional rules differ from federal rules concerning medical records and the same issue could occur when EHR technology is implemented (Barrows, R. C., & Clayton, P. D., 1996). Due to the various types of laws such as "fraud and abuse, antitrust, federal income tax, intellectual property, liability and malpractice and state licensing" that apply to healthcare providers, they are unsure how these laws affect the implementation and use of EHR technology (Anderson, 2007). More specifically, legal rules affecting privacy can be divided into three categories: quality and accuracy of the medical data, privacy of an individual patient's medical data, and "tort-based liability".

To increase the quality and accuracy of the medical data that are collected, three changes need to be made from the legal side. First, the physician-patient relationship should be strengthened by privacy assurance. This assurance makes the patient more comfortable with disclosing their medical condition and will be less prone to provide false data to protect their confidentiality. Second, by adding fair information practices, there is a legal incentive for patients to look up their medical records and add or amend information. This will allow physicians to have access to more complete and accurate records. Third, there should be federal regulations specifically relating to medical data protection. This will increase the sharing of medical data between hospitals and could potentially make healthcare more efficient for patients (Hodge, J. G., Jr, Gostin, L. O., et al, 1999).

Protecting individual privacy for EHR is even more important due to the Internet and other technology. It is now easy to form a detailed medical profile of anyone with just some basic information. Current federal laws in most countries such as the United States do not cover all the possible scenarios regarding EHR. Presently, there are rules and regulations that are used to patch together current laws as health IT and EHR technology is evolving at a fast rate. There is a need for a comprehensive, national legislation for electronic medical data protection. As EHR allows an easier venue than paper records to share patient medical information, informed consent becomes an issue. It is easy to make a copy of a patient's EHR and send it to another party without the patient's knowledge. Thus, regulations mandating a notification system need to be developed and enforced so that the patient can know who accessed his/her EHR and when the access happened.

Tort-based liability refers to liability of a person who commits an intentional illegal act. In the case of EHR technology, the most common case of tort-based liability is when a healthcare provider intentionally changes, deletes, leaks, or sells patient information. Sometimes it is difficult to figure

out the liable party as security trails for EHR have not been implemented in all EHR systems. Furthermore, clear rules need to exist for EHR when physicians commit errors of omission or errors of commission (Hodge, Gostin, & Jacobson, 1999).

2.2.2 Technical Issues

As with any technology, risks exist. Even though EHR technology can prevent certain risks such as dangerous drug interactions, it can add new ones. These new risks include issues with "computer crashes, data capture anomalies, programming errors, and other failures of automation [that] may replace lost charts, bad handwriting, missing information, and other problems experienced with manual systems" (Goldschmidt, 2005, p. 73).

There are numerous EHR systems on the market and each one of those systems is developed by a different company. As EHR is a booming market, more and more companies are trying to increase their share of the market; thus, making an EHR software inoperable with another company's EHR is actually beneficial to a company (Tulu, 2010). However, this has a negative effect for the patients of a country as some hospitals have EHR technology from one company while another hospital has EHR technology from another company. With such a wide variety of formats and standards, it becomes difficult for one EHR system to communicate with others.

A survey conducted in the United States found that two-thirds of physicians blame the lack of EHR technology on the lack of a technical implementation plan and lack of proper IT personnel to support the EHR system. Furthermore, over one-half of the physicians stated that a personal lack of technical knowledge is a major barrier to EHR technology (Anderson, 2007). Thus, even if the technology and budget exists to implement an EHR system, sometimes it is the end-users' issues with the technology that slows implementation.

Most of the current EHR software is web-based as it the fastest way to add interoperability. However, without secure and standardized channels to transfer sensitive medical information, many doctors are concerned about security breaches and hacking. Also, not all EHR software currently provides varying levels of data accessibility. This means that nurses could have the same level of access to patient data as doctors and hospital administrators. This could be dangerous as an EHR system could provide various unsecure outlets for a malicious hospital provider to extract patient information (Anderson, 2007).

As EHR systems will evolve in the future, a concern that could arise will be the judgment system in decision-making EHR systems. If the systems make decisions for patients using past history and aggregated data, the decision-making processes need to be highly controlled, as there is a large room for medical mistakes to occur.

Figure 9 is a powerful illustration that explains a common problem in EHR technology known as "the gap". The figure shows that as time increases, the number of patients and their medical data increases. Also, with the advances in the field of human genomics, there is a plethora of new information that is being collected. At some point in time, the large amount of data will be difficult for healthcare providers to handle and a need for a complex data management system would become imperative. To make such a system feasible, there is a need for increased computing power, internet bandwidth, wireless coverage, and interoperability between systems.

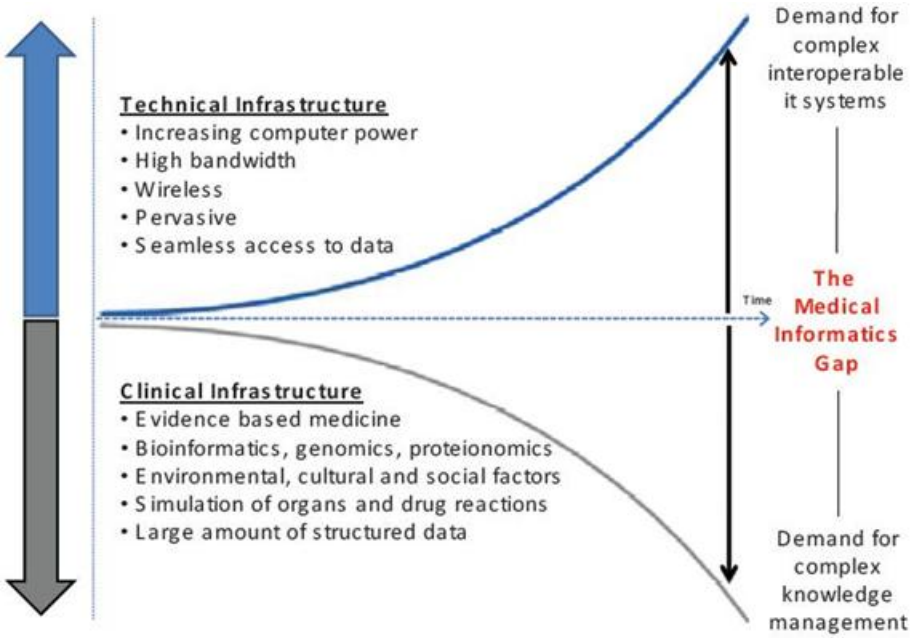

Figure 9: Illustration of the Medical Informatics Gap (Bruun-Rasmussen, Bernstein, & al., 2008, p. 2)

Figure 9's main point is that since the rate of data collecting continues to increase with time, hospital administrators need to keep up with the technical side by implementing the infrastructure that can handle the collected data, otherwise the "gap" will continue to increase.

2.2.3 Other Issues

The initial cost of installing an EHR system has been a major issue for healthcare providers and administrators. On average, it costs around $16,000 to $36,000 per doctor to install an ambulatory

EHR system. Ambulatory care refers to medical care that is provided only on an outpatient basis. Furthermore, due to the issues that exist while transitioning between paper records to electronic records, there has been a noted reduction in the revenue for the doctors and the hospitals (Anderson, 2007).

2.2.4 Potential Risks to Stakeholders

Even though health IT systems offer a large number of benefits to all their stakeholders, they can specifically create risks for all parties involved with the systems. The use of EHR has already had strong effects on all those involved beyond the technological and legal issues presented. Because EHR systems are used by various stakeholders, it is important to analyze what each group's problems typically are. Sometimes, the interests of certain stakeholders are in conflict with each other. Table 3 displays four important factors that need to be considered carefully during an EHR system implementation to make sure the system will be used at its maximum potential. The first factor is quality – a high quality EHR system needs to fulfill the needs of the healthcare providers and needs to be error-free. The second factor is usability, which refers to the different level of accessibility based on the role of the medical provider. Lab technicians, pharmacists, doctors, and nurses all need to look at different information about the patient in order to perform their duties. The EHR system also needs to be user-friendly by having an intuitive user interface and by displaying information in varying technical and medical language based on the end-user.

Table 3: The QUiPS model for successful deployment of EHRs. Adapted from: (Croll & Croll, 2006, p. 2)

Code	Attribute	At Risk
Q	Quality	i. Not developing the right product (i.e. not meeting requirements) ii. Not developing a robust product (i.e. not well engineered)
U	Usability	i. Degree of usage (i.e. full or partial use of functions) ii. Acceptance by users (e.g. clinicians, patients, administrators)
P	Privacy	i. System security (i.e. preventing clinicians, patients, administrators) ii. Patient confidentiality (e.g. not revealing personal health data)
S	Safety	i. Harm to the system (e.g. availability, data corruption) ii. Harm to people (e.g. medical errors, medical data integrity)

The third factor is privacy – improper implementation of an EHR system can lead to unauthorized access to patient data; patient confidentiality could also be compromised. The final factor is safety of the system. The EHR system designer needs to put in fail-safes that will prevent healthcare providers, either intentionally or unintentionally, from changing the EHR software, as this could

lead to unauthorized access. Furthermore, there needs to be a backup data storage system in case of data corruption.

2.2.4.1 Patients

Perhaps the biggest risk patients face in an EHR system is with security, privacy, and confidentiality of their personal health information. If records become accessible from home, the risk of records being hacked into or spied upon becomes a reality. Making the access of health records more user-friendly runs the risk of making them more easily reached by unauthorized users (Goldschmidt, 2005). Security of EHR is much more complex than that of singular Electronic Medical Record (EMR) systems or paper records. As more information becomes centralized into an EHR system, the security of the information diminishes. So for patients, it is a combination of trade-offs. More of the patient's medical record in the EHR system means more accurate and better healthcare can be provided to them. Yet this flood of information into the EHR system brings in a higher concern for security. If a patient's health records are accessed by an unauthorized user, this could bring forth negative consequences for that patient. For example, if a patient has an illness that requires a potentially expensive surgery, and the medical records of this patient are accessed by a potential future employer or health insurance company, it could create a bias against this patient and cost them the job because they are too much of a liability. Another risk to a patient's medical records being accessed by unauthorized users is the potential for public intolerance of a certain illness.

2.2.4.2 Doctors and Nurses

The risks for physicians in implementing health IT systems are not nearly as obvious as the gains. Doctors find a number of practical problems in EHR systems. First, doctors must spend large amounts of time and effort to get used to the systems, meaning their workflow is less efficient – sometimes for months. Poorly designed systems can also inhibit their work (Sprague L. , 2004). Because of the lack of interoperability between many health IT systems, smaller offices often have trouble implementing them since they have to work with many other institutions (Anderson, 2007).

Physicians, especially those unfamiliar to computers, also worry that the computer systems will diminish their relationship with their patients – a critical part of their profession. For example, if a physician is speaking with a patient, their communication may be interrupted if the physician is trying to use a computer at the same time to access an EHR system. This may lead to less perceived face time with a patient, and consequently a poorer relationship. In addition, if a provider is trying

to pay attention to a patient while using a computer, they are more prone to make errors in using the system (Gaffey, 2009).

The nurses from the study referenced in section 2.1.2.2 Doctors and Nurses of this report (Whittaker, Aufdenkamp, & Tinley, 2009) experienced many of these problems with their newly-implemented EHR system. Many of their complaints about the system were related to the computers being slow or inconvenient to use. They also cited the amount of training needed and their lack of proficiency with computers as major issues.

2.2.4.3 Healthcare Officials and Hospital Administrators

While many studies find that the overall economic impact of EHR systems is eventually positive, there are those who disagree and are skeptical about the long-term benefits. Because doctors and staff take time to get used to the new systems, productivity has a tendency to be reduced significantly for a few months after the systems' adoption. Also, while the physicians are busy learning the systems, they are more prone to becoming frustrated and either making mistakes or recording less patient data. More errors lead to more malpractice suits (Sidorov, 2006). This is in direct opposition with the supposed benefits of EHR systems. The overall risk is that the issues that come with implementation and adoption are simply too much trouble for officials and administrators to deal with, and there is not enough incentive to push hard for health IT, even with the potential long-term payoffs. Figure 10 is a simple diagram that shows the different factors hospital administrators have to deal with in a hospital system. The hospital administrators have to take all these factors in consideration before making any decisions such as the implementation of an EHR system.

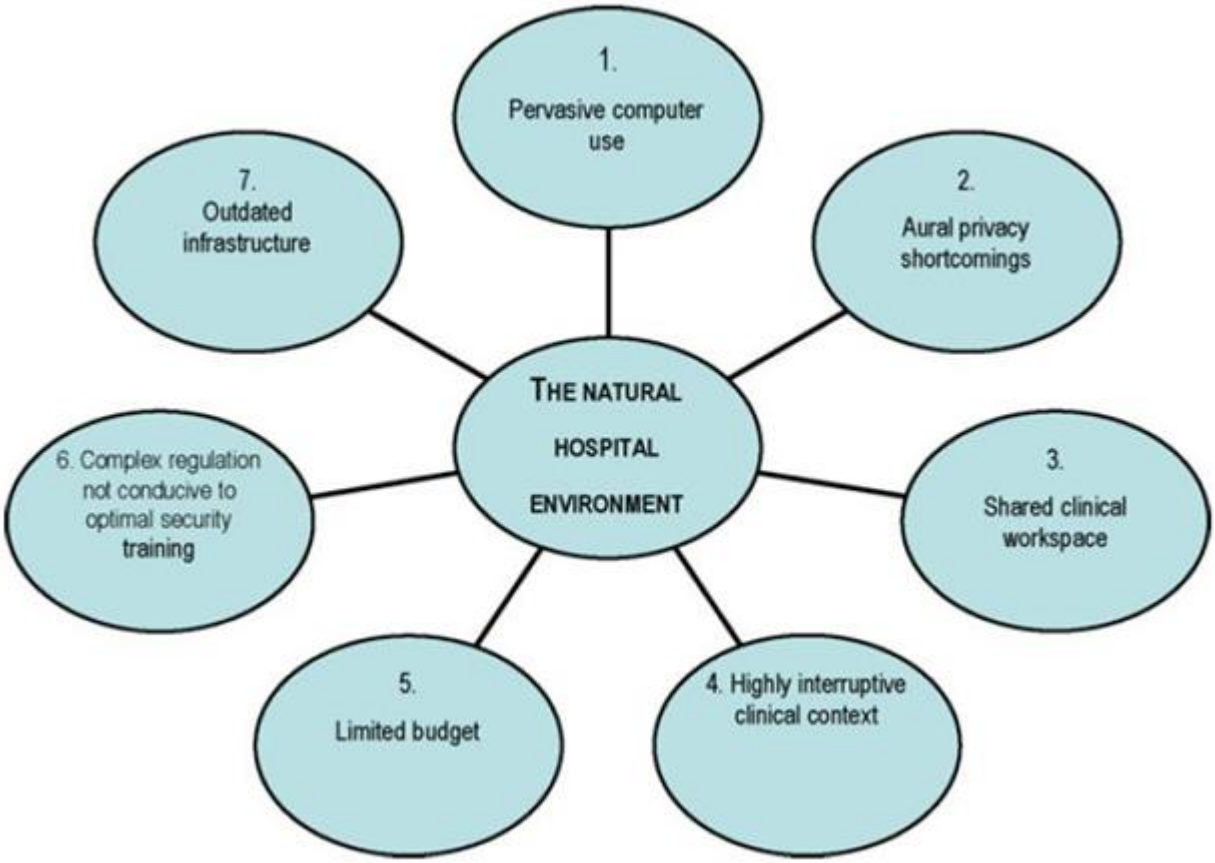

Figure 10: The characteristics of the natural hospital environment (Fernandoa & Dawson, 2009, p. 821)

A few important factors that affect EHR system implementation are hospital budget, outdated infrastructure, and the level of computer use in the hospital.

2.3 Health IT and EHR Case Studies

One important part of health IT is keeping a complete electronic medical history of patients. Even though the acronyms EHR and EMR are used interchangeably for this system, there is a difference between the terms. EMR usually refers to the electronic history of a patient at a certain institution or hospital. Thus, a patient can have multiple EMRs at many hospitals. However, his/her medical history is fragmented and no single hospital has a complete record. EHR, on the other hand, is the complete electronic medical history of a person or population from the time he/she was born to the time of death (Terry, N. P., 2004). Currently, most medical records are still in paper form and the first step towards a successful EHR system is to convert all paper records into electronic records. This will convert all medical records into EMR. The process of conversion from paper records to EMR is tedious, but does not begin to compare to the steps necessary to then convert EMR to EHR. If goals of implementing EHR are to be met in the next decade, the use of technical resources and

the collaborations between many government agencies and private institutions must receive significant aid. This section will review EHR implementation in multiple countries around the world, in comparison to Denmark's implementation.

2.3.1 Denmark

Since 1995, there have been 4 important IT strategies and initiatives implemented in order to digitize and improve Danish healthcare information in terms of accuracy, ease of access, information quality, and data security. The first strategy implemented was political when, in 1994, the Ministry of Research gave healthcare a high priority for information security while the Ministry of Health created an EHR action plan in 1996. The second IT strategy was implemented from 2000 to 2003 and acted upon the first strategy by implementing the ideas presented in the EHR action plan (Bruun-Rasmussen, Bernstein, & al., 2008).The main goal of the second IT strategy was to prepare health and medical institutions for EHR technology implementation in the future by using resources more effectively, offering high quality of care to patients, and providing clear and useful information to patients and any other authorized medical parties.

The third and fourth IT strategies span from 2003 to 2012 and they further build upon the past IT strategies. The third strategy, which was implemented from 2003 to 2007, dealt with "support the order of priority for the use of IT in health care services" (Bruun-Rasmussen, Bernstein, & al., 2008). Since the Danish government understood that more resources were required to have shared standards in all Danish hospitals, the Connecting Digital Health in Denmark organization (abbreviated SDSD) was created in April 2007. The fourth strategy was much more political as it involved large number of government officials. Also, this strategy emphasizes stakeholder involvement along with support from the business sector. Each IT strategy emphasized different areas of the whole infrastructure, which include business support, clinical infrastructure, governance, and stakeholder involvement. However, as each IT strategy moves into the next phase, more areas of IT infrastructure are being focused on (Bruun-Rasmussen, Bernstein, & al., 2008). Figure 11 illustrates the four strategies presented and compares them according to their levels involvement in business support, technical infrastructure, clinical infrastructure, governance, and stakeholder involvement. The first strategy dealt with finding and developing the necessary technical solutions to improve health IT in Denmark. The second strategy dealt with integrating the technical solutions into the clinical environment. The third strategy evaluated the integrated clinical IT systems and improved upon them. The final strategy is very different from the other three as it concentrates on improving how health IT is governed, expands support for it by including the

business sector in health IT's development, and involves the stakeholders in the process of improving and implementing the health IT systems..

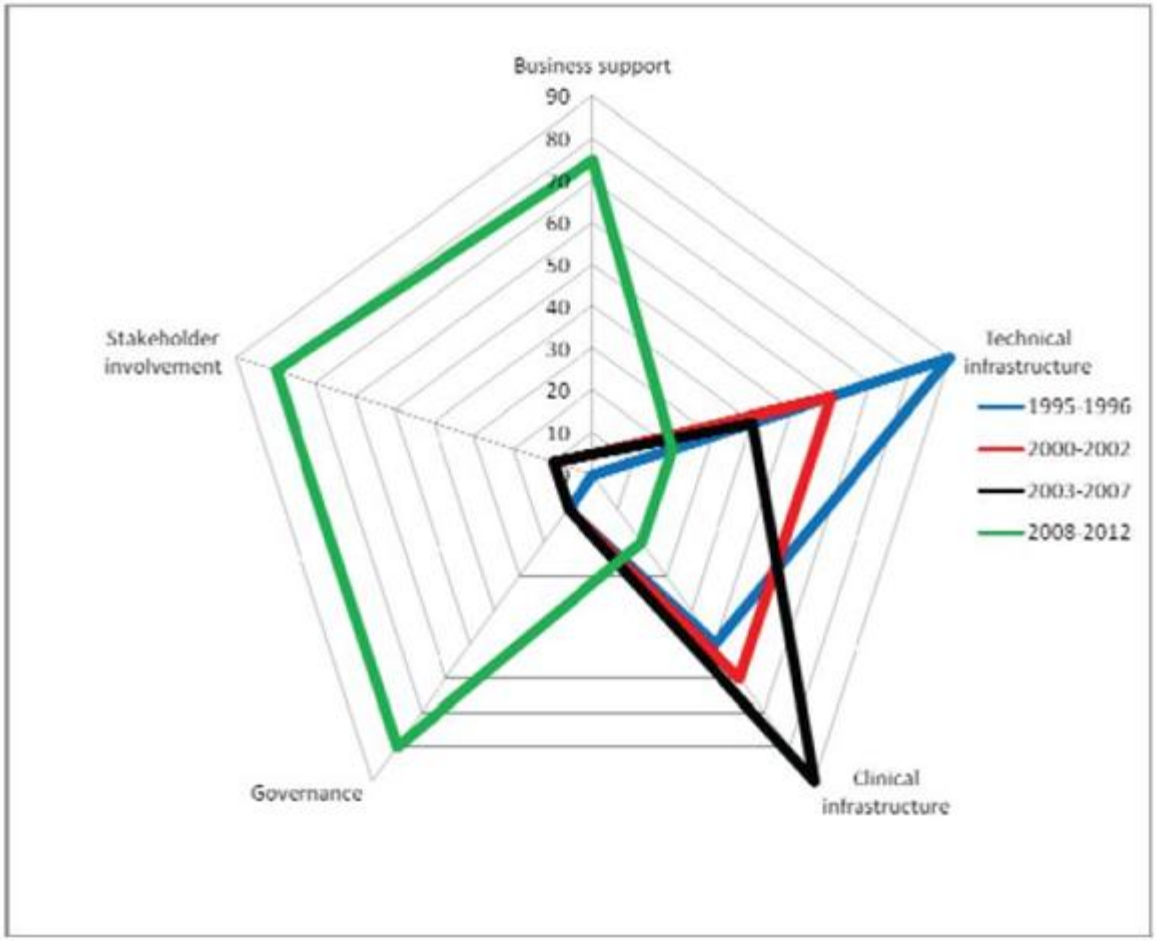

Figure 11: Radar diagram showing focus for the IT strategies (Bruun-Rasmussen, Bernstein, & al., 2008, p. 3)

As the health IT strategy began to focus more on stakeholder involvement and communication, the need for a structured communicating network became more apparent. Figure 12 illustrates the common Danish Health Data Network infrastructure presented in 2007 and how each area interacts with each other.

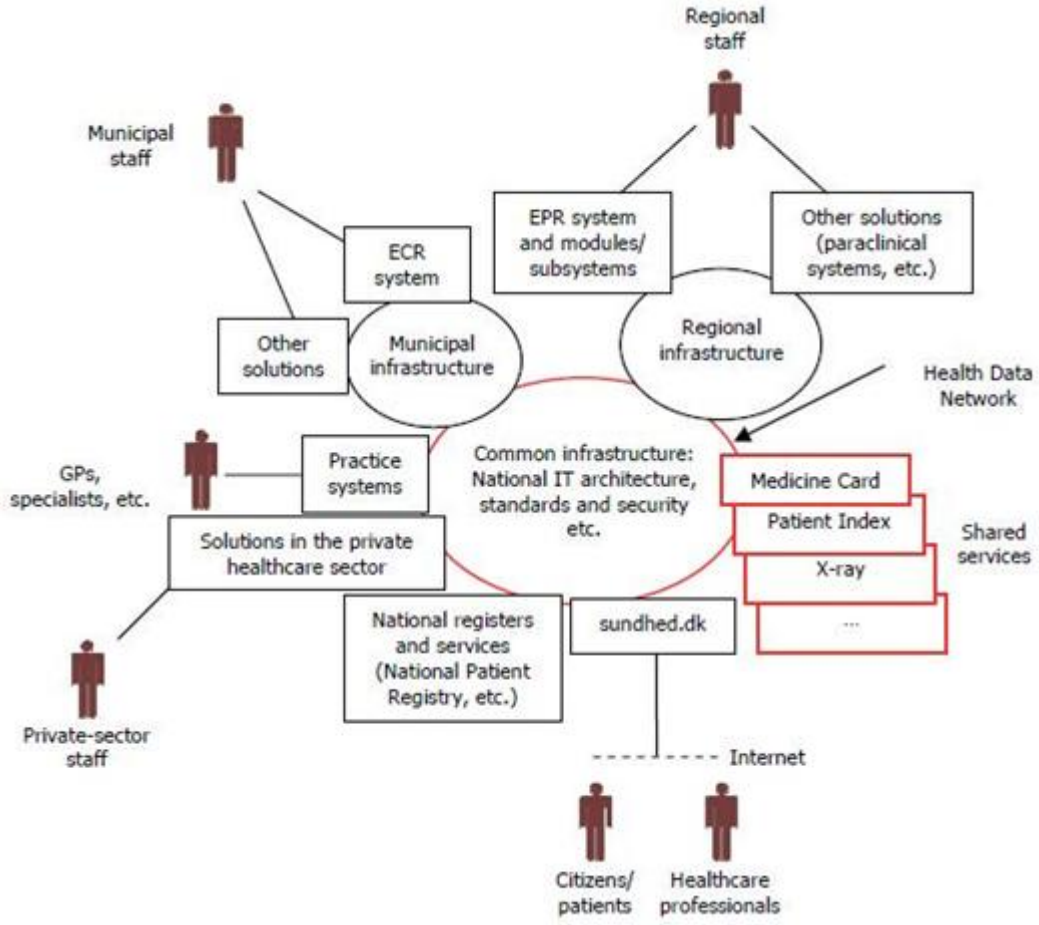

Figure 12: Model of the Danish Health Data Network (Digital Health, 2007, p. 31)

Areas outlined in red (medicine card, patient index, X-ray, etc.) are shared services that are in the system and can be shared by potentially all other areas depending on privacy. In 2007, this system allowed for users to reach outside databases, exchange all shared services, and use video conferencing. Yet the Digital Health organization has noted that future requirements in online access, capacity, and security will call for the network infrastructure to evolve (Digital Health, 2007).

As health IT evolves in Denmark, information shared between stakeholders in the system has become more and more complex. Denmark's Digital Health organization recognizes this, and has created a step-by-step plan of implementation for the best ease into higher levels. This step-by-step diagram can be seen in Figure 13.

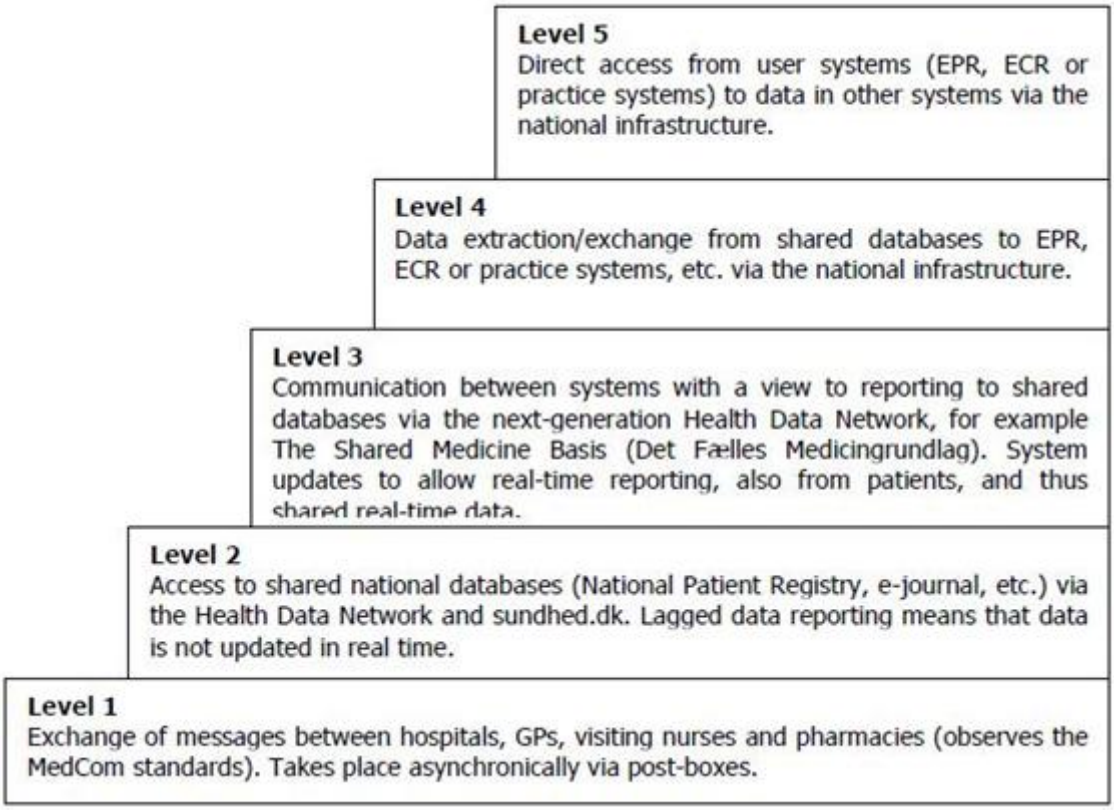

Figure 13: Levels of development of digital communication across the healthcare service (Digital Health, 2007, p. 22)

As of 2007, communication within health IT in Denmark had reached the second level – access to shared national databases – and within the few years since, application of the third level is underway. But because of how each level is structured with higher complexity on top of lower complexity, the implementation of each level can build and learn from the previous level. Denmark hopes that this strategy will allow for faster accomplishment each time a level is reached (Digital Health, 2007).

2.3.1.1 Political Structure of Denmark

The structure of Denmark's government is important to its health IT industry, as there are many different laws regarding patient privacy and healthcare that differ from area to area. Denmark's government is a constitutional monarchy where the monarch is considered the head of the state, but most of the political power lies within the Danish Parliament (Folketing) and the 9 Danish political parties. Before January 1, 2007, Denmark was split up into 270 municipalities and 15 larger counties in addition to the national level. After 2007's local government reform, the municipalities were consolidated from 270 to 98 and the 15 counties were replaced with 5 regions. The reform occurred because of a few reasons: first, Denmark is a very small country so having so many divisions in the form of municipalities seemed cumbersome and unnecessary. Second, consolidation

of resources allowed better exchange of information, goods, and services amongst Denmark. Finally, the reform created a simpler political hierarchy so it was easier for politicians and bureaucrats to identify problems in Denmark and to allocate resources. As municipalities were condensed, the hospitals also consolidated their resources and medical records. This increased interoperability in some sense, and with fewer medical record systems, health IT professionals will have to work with fewer systems. This makes it easier to link the various systems together. At the moment, there is discussion amongst the parliament to abolish the regional level so there will only be the state level and the municipality level. This decision would make a big difference in health IT implementation as currently, if hospitals need to request new equipment or services, there is a long bureaucratic chain the request has to go through. Removing the regional level will make the bureaucratic chain shorter and will as a result; increase the speed of implementation of new clinical IT systems.

2.3.2 How Denmark Compares

Denmark has been said to be one of the world's leaders in health IT, and it is therefore of value to compare Denmark's health IT initiatives with those of other counties.

2.3.2.1 Cost

Though every country's goal is to be able to provide the best health care available to their citizens, the cost of a system will play a substantial role in its implementation. Figure 14 displays the per capita cost of healthcare by country. Note that Denmark and Sweden have similar demographic and spent similar amounts in cost per citizen in 2005. Another country that is comparable to Denmark is Norway. Though Norway has a similar healthcare system to Denmark, the country spent a substantially larger amount of money per citizen on healthcare. And even though Denmark has universal healthcare, the cost per Danish citizen is less than half that of an American citizen. Healthcare costs over the past decade have continued to rise and increase in percentage of all countries' represented in the graph GDP. While cost is not the only criterion that determines the adequacy of countries' health IT infrastructures, finding comparative data on how specifically health IT in different countries affect quality of care and accessibility to care is difficult. This is mostly due to each country being in a different stage of health IT implementation.

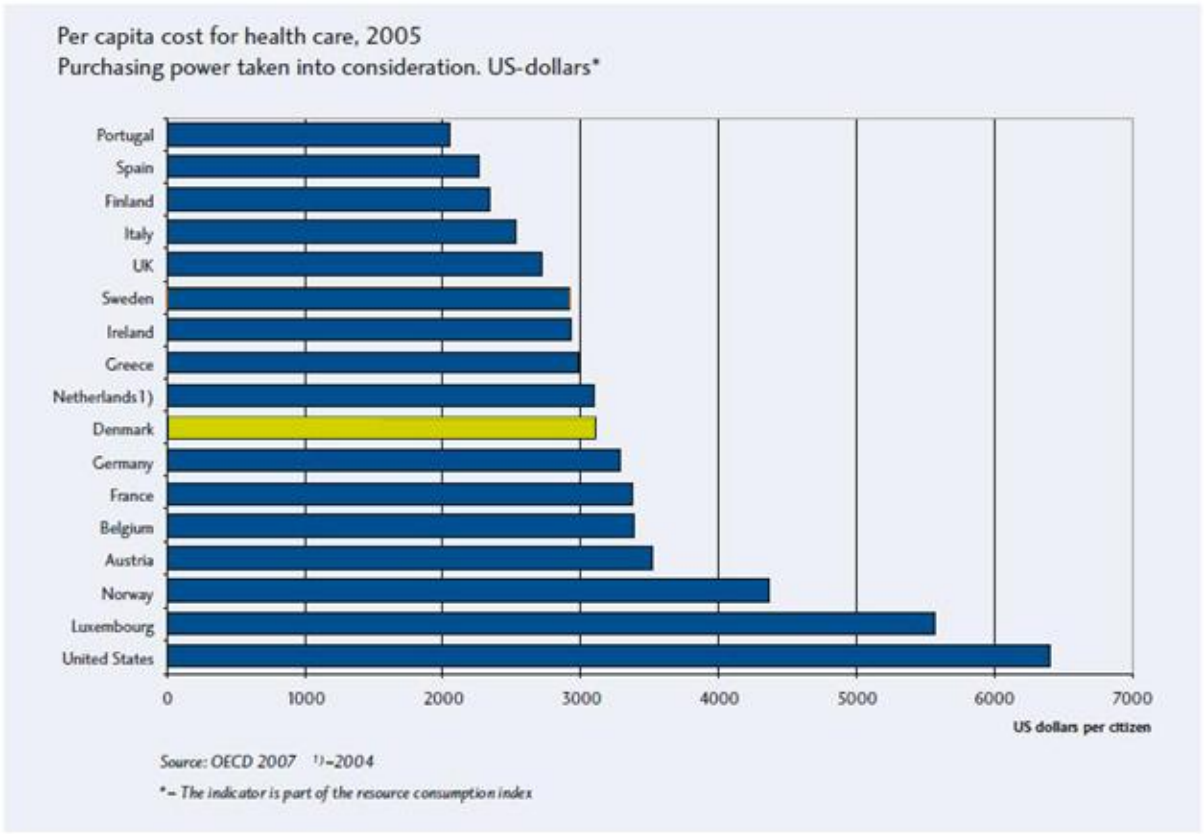

Figure 14: Per capita cost for healthcare, 2005 with purchasing power taken into consideration in US dollars. Adapted from (Swedish Association of Local Authorities and Regions, 2008, p. 31)

2.3.2.2 Acceptance and Implementation

Denmark has made a considerable effort to create a health IT system that will benefit the entire country. Table 4 illustrates how successful Denmark's implementation strategy has been in many different aspects of healthcare compared to other countries. It is important to note that Denmark's adoption figures will most likely increased due to recent laws passed pertaining to the use of EHR systems, and an active effort by the government to make EHR systems prevalent and useful.

Table 4: Use of EHR Systems in Primary Physicians and Hospitals. Adapted from: (Castro D. , 2009)

Country	% of Primary Care Physicians Using EHR Systems (2009)	% of Primary Care Physicians Using E-Prescribing	% of Hospitals Using EHR Systems (2009)
Sweden	100	100	88
Finland	99	100	100
The Netherlands	98	85	<5
Denmark	**95**	**100**	**35**
New Zealand	92	78	<1
United Kingdom	89	55	3
Australia	79	81	<10
Germany	42	59	<5
United States	28	20	8
Canada	23	11	<10

Column 1 in Table 4 shows the percentages of primary care physicians that have put into practice EHR systems as of 2009. Denmark is one of the world's leaders in this category with a 95% implementation rate. From country to country, it is uncertain what definition of primary care physician is used. Depending on the size of the practice, implementation percentages may vary. For example, the US's use of EHR varied from 16% of solo practitioners to 46% of practices having at least 10 physicians in the practice (Castro D. , 2009).

Column 2 in Table 4 shows the percentage of physicians per country using e-Prescriptions. Again, Denmark is a leader in this field (with 100% of physicians using e-Prescriptions) along with Sweden (100%), Finland (100%), and The Netherlands (85%).

Column 3 in Table 4 shows the percentages of hospitals using EHR systems, and Denmark, though only at 35%, are second-tier adopters after Finland (with 100%) and Sweden (at 88%). Following Denmark is Japan, with only 10%. Though hospitals can potentially benefit more from EHR systems than small physicians due to their size and complexity, the figures in column 3 illustrate that implementation in hospitals is substantially lower than with physicians. This could be due to the high costs of complex hospital systems as well as the initial time for set-up and conversion from paper to electronic records that can take more than 6 months (Corbett, MD. 2010).

2.4 Summary

Clearly, health IT and EHR systems have an impact on a large variety of people and bring with them a myriad of complicated issues to the table when they are used. The benefits of using these

systems are unquestionable – healthcare can improve a great deal through the effective use of these systems. However, great care must be taken when health IT systems are actually implemented, as it is easy for the negative effects to outweigh the benefits to all parties involved. In order for patients in particular to receive higher quality of care, only high quality health IT systems that specifically take the patient into account can be used. Due to the legal and technical challenges faced by each country trying to implement EHR in its hospitals, an international interoperable EHR system seems highly unlikely in the near future. Thus, the first step for a country should be to implement a standardized national EHR system for all its hospitals. Once many countries are able to successfully implement systems, an international system can be developed that can link the EHR systems from different countries together and thus allow global interoperability. This is an ideal solution and a very difficult one to implement. However, this should be the focus and vision of the international healthcare community.

Chapter 3: Methodology

This project was aimed to assist Forbrugerrådet in better understanding the issues of health IT systems that affect healthcare patients and providers. We accomplished our goal by conducting scholarly research, assessing EHR infrastructure in Denmark through interviews with experts in various fields relating to health IT, and analyzing the interaction between privacy and interoperability with EHR in different health IT systems. These methods helped us formulate suggestions for how to spread awareness on the effects of EHR implementation in Denmark.

It is also important for Forbrugerrådet to understand the stakeholders in Danish health IT by investigating their views, how they influence change in privacy and interoperability issues, and how changes affect them. Therefore, we conducted a stakeholder analysis that included interviews of stakeholders or their representatives. Because Forbrugerrådet is a lobbyist organization, our goal was to create a conclusion that best assists them with their advocacy efforts. Throughout the project, it was important for us to identify the most valuable way to present our findings as an advocacy tool. After consulting with our liaison Sine Jensen, we decided upon presenting a policy paper.

Our project objectives were as follows:

- Identify technical, legal, and social issues of health IT faced in Denmark.
- Identify the organizations involved in health IT in Denmark and understand how they interact with each other, patients, and healthcare providers.
- Understand the social implications of privacy and system interoperability issues within health IT on Danish patients and healthcare providers.
- Organize and analyze our findings in a manner that allows Forbrugerrådet to make an objective and knowledgeable argument about EHR privacy and interoperability in the best interest of the public.

In order to complete these objectives and reach our project goals, many key attributes were addressed. Figure 15 diagrams the approach we used in meeting our objectives.

Figure 15: Methodology Flowchart Illustrating the Goals as well as the Process of the Project

Because health IT is such a broad topic, it was important for our report to concentrate on the issues that most affect the consumers of health IT. Through research and interviews with our liaison, Sine Jensen (transcripts of these interviews found in, Appendix F- Interview Transcripts and Summaries of Attached Documents), we have concentrated our research and report on the issues surrounding privacy and interoperability of EHR systems in Denmark.

The project took place from March 14, 2010 through May 12, 2010. Table 5 is a Gantt chart outlining the timeline of our objectives. The following sections delineate how we achieved our objectives.

Table 5: Timeline Illustrating the Project Outline

WEEK							
Prep	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Assess the Danish Consumer Council's needs							
	Conduct Stakeholder Interviews						
	Assess Needs of each Stakeholder						
Analyze Organizations in other Countries and How they Deal with Health IT Issues							
					Present Our Findings		
				Complete Report and Fact Sheet			

3.1 Identify Technical, Legal, and Social Issues

This section refers to our first objective: *identify technical, legal, and social issues of health IT faced in Denmark.* Our preliminary research looking at credible sources identified many of the main issues for all three of these aspects of health IT and can be found in the background chapter of this report. We have organized the analysis of health IT implementation into three areas of research: technical issues, which includes interoperability, social implications, which includes privacy, and legal issues, which takes into account both of these. By first identifying the main issues, we were then able to use this to direct our research and interview questions, and therefore our report.

3.2 Identify the organizations involved in health IT in Denmark

The section refers to our second objective: *to identify the organizations involved in health IT in Denmark and understand how they interact with each other, patients, and healthcare providers*. Since the Danish healthcare system is very different from the one in the United States, it was important for us to identify the organizations relating to health IT to understand the Danish health IT infrastructure. The most accurate way for us to understand the different organizations involved in health IT was to interview health IT experts from the different organizations. Table 6 is a list of the experts interviewed in Denmark and what organization he/she works for.

Table 6: List of Health IT Experts Interviewed in Relation to Understanding the Health Organizations

Contact's Name	Job Title
Dr. William Corbett	VP of Community Practices for UMass Memorial Health Care
Prof Bengisu Tulu	Professor of Management Information Systems at WPI
Sine Jensen	Senior Health Advisor at Forbrugerrådet
Kenneth Ahrensberg	Special Advisor at Connected Digital Health in Denmark
Morten Godiksen	Communications and Network Manager at sundhed.dk
Anette Høyrup	Lawyer, Senior Advisor in the Privacy Department at Forbrugerrådet
Frederik Endsleff	Teamleader at Region Hovedstaden - the Capital region KIT
Marianne From	Head of Clinical IT Department at Rigshospitalets
Pia Jespersen	Technical Consultant at Connected Digital Health in Denmark
Stephen Engberg	CEO and founder of PriWay
Pernille Bjørn	Professor of Computer Science at IT University of Copenhagen
Mette Hartlev	Lawyer at Copenhagen University, works on healthcare law
Henning Mortensen	Chief Consultant at ITEK (IT & telecommunication company)
Jan Petersen	Chief Consultant of MedCom

After our first four interviews of experts working in the Danish organizations, we created a chart showing the organizations involved in Danish health IT and how they interact with each other. The preliminary chart is represented in Figure 16, and it was broken down into governmental and non-governmental. The governmental side included the ministries, regions, municipalities, hospitals, and organizations. The non-governmental side included advocacy groups, private companies, private doctors, and the European Union. As we continued interviewing more experts, we presented them our organization chart and asked their opinions on the accuracy of the organizations' functions and their interaction with each other. Near the end of our interviewing phase, we had an accurate organization chart illustrating how the organizations involved in health IT interacted with each other. Where Figure 16 shows the basic diagram used for preliminary organization, Figure 19 in the Results and Analysis section illustrates the final diagram after full analysis. The purpose of this diagram was to give us and Forbrugerrådet a clear idea about how and which organizations interact.

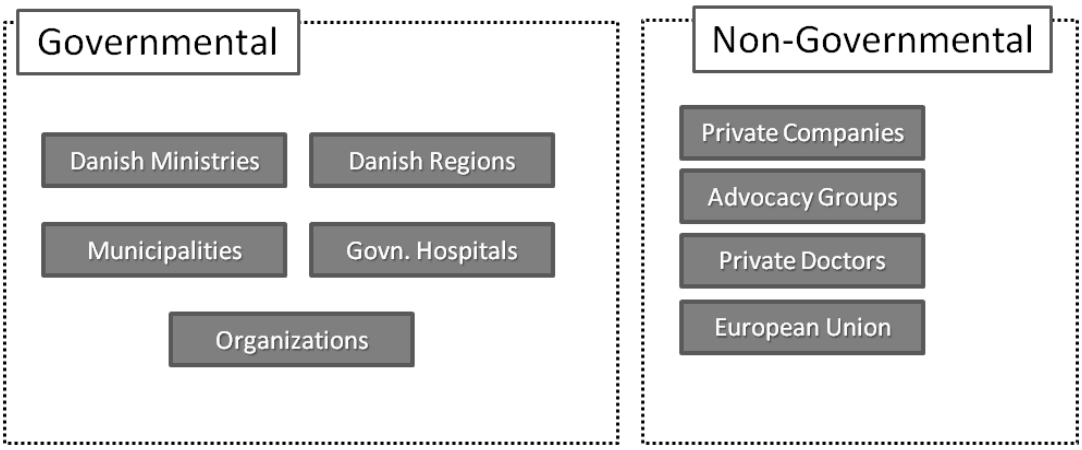

Figure 16: Danish Health IT Organization Chart

3.3 Understand the Social Implications of Health IT

The following section refers to our third objective, *to understand the social implications of health IT, specifically privacy and interoperability, on its Danish users*. We wanted to know about the variety of problems that affect the stakeholders (primarily with patients, doctors and nurses, and hospital administrators) that are involved with health IT systems, especially on privacy and interoperability issues.

Understanding the social implications affecting users specifically with privacy and interoperability was an imperative issue for the report to discuss. Different issues affect each stakeholder in a different way, and by comparing these implications, we gave Forbrugerrådet a better understanding of the issues and how and on what level to address them. Interoperability and privacy are a balancing act, and we assessed what approaches are most beneficial for each stakeholder. According to the stakeholder, different mixes between the levels of privacy and interoperability affected them in specific ways, either negatively or positively.

3.3.1 Research Questions

In order for our research to be of most use to Forbrugerrådet, we first established a set of questions for our project set out to answer. These questions were not necessarily the questions we asked the stakeholders, but they were the basis of the interview questions. The following are our research questions and they stem from the main problem with health-IT: the balance between privacy and interoperability. This list consists of the main objective questions, but a more detailed list can be found in Appendix D – Project Research Questions:

- What problems do consumers face that arise from Denmark's current health IT systems?

- What are the different organizations involved in Denmark's health IT infrastructure?
- Why should patients worry about privacy of their data?
- How does interoperability between health IT systems affect patients?
- How does the current legislation on healthcare and health IT affect the quality of the systems?
- Should users be provided with the right knowledge in order to use the health IT systems in Denmark most effectively?
- What actions can Denmark take in order to improve the current health IT systems?

In addition to establishing our primary research questions, we ensured that the stakeholders are those who most affect Danish legislation on the balance between EHR interoperability and privacy. These included, but were not limited to: researchers of Danish patients who act as patient representatives, healthcare administrators, electronic privacy experts and healthcare technical experts from the government and non-government side, representatives from doctors' and nurses' unions, and lobbyist groups such as Forbrugerrådet. Questions asked to these stakeholder representatives helped us answer our research questions.

After our interviewing was complete, we were able to use our research questions to formulate our results. There were some holes in our research, and therefore there were some questioned that remained unanswered. Seeing this allowed us to make decisions as to who else needed to be interviewed to help fill in the gaps. One gap was with questions pertaining to standardization, and we therefore interviewed Jan Petersen, a manager at MedCom that deal with international standards. The other gap was with law, and although this was not one of our main concentrations for the report, we had a short interview with Mette Hartlev, a lawyer who works at Copenhagen University and specializes in privacy.

3.3.2 Interviewing

Interviewing was the most effective way to analyze our stakeholders. It was important to understand each stakeholder group and how they are affected by privacy and interoperability issues with EHR implementation. A technique we used to create new stakeholder contacts was the snowball sampling method. Using the snowball method, we asked the interviewee if he/she has any other contacts that may be beneficial for us to talk to. From there, we interviewed those contacts given, and asked them the same questions. This helped us create a complete list of necessary contacts to assess each stakeholder group. As we continued our research, using the names of experts from relevant reports

and studies as potential interviewees was a good addition to the snowball effect. Appendix E - Interview Tree and Interviewees' Job Titles shows the list of interviewees we consulted.

In order to assess and analyze each stakeholder/interviewee on the same level, we developed an interview template that can be viewed below in Table 7. These questions changed depending on the type of stakeholder we were interviewing. For example, a researcher that specializes in the needs of disabled patients may not be able to answer our question about advice for how Forbrugerrådet should lobby for a change in legislation.

Table 7: Template for Stakeholder Interviews

Stakeholder (interviewee):	
Questions:	**Answers:**
What is your role within the implementation and use of EHRs in Denmark?	
Have you dealt with patient privacy in the past?	
Have you dealt with interoperability in the past?	
In terms of interoperability and privacy within the implementation of EHR in Denmark, what does your company/organization advocate for?	
In your opinion, where is the state of the discussion and the state of current legislation of EHR systems in Danish health care? Do you feel that legislation on the issue should be changed?	
What is your view on where the levels of privacy ought to be?	
What do you recommend to Forbrugerrådet for the most effective lobbying on changing and improving legislation on the balance of privacy and interoperability?	
Do you have any examples of issues you have had when dealing with the EHR systems?	

Not only was it important for us to ask interviewees the same set of questions, we also needed to analyze each interviewee, the information and views they portrayed to us, and what type of information they gave us insight into, either social, legal, technical, or a mixture of these subjects. Figure 17 is a Venn diagram that illustrates what type of expertise each interviewee had, and we put each interviewee's name in one of the seven categories of the diagram.

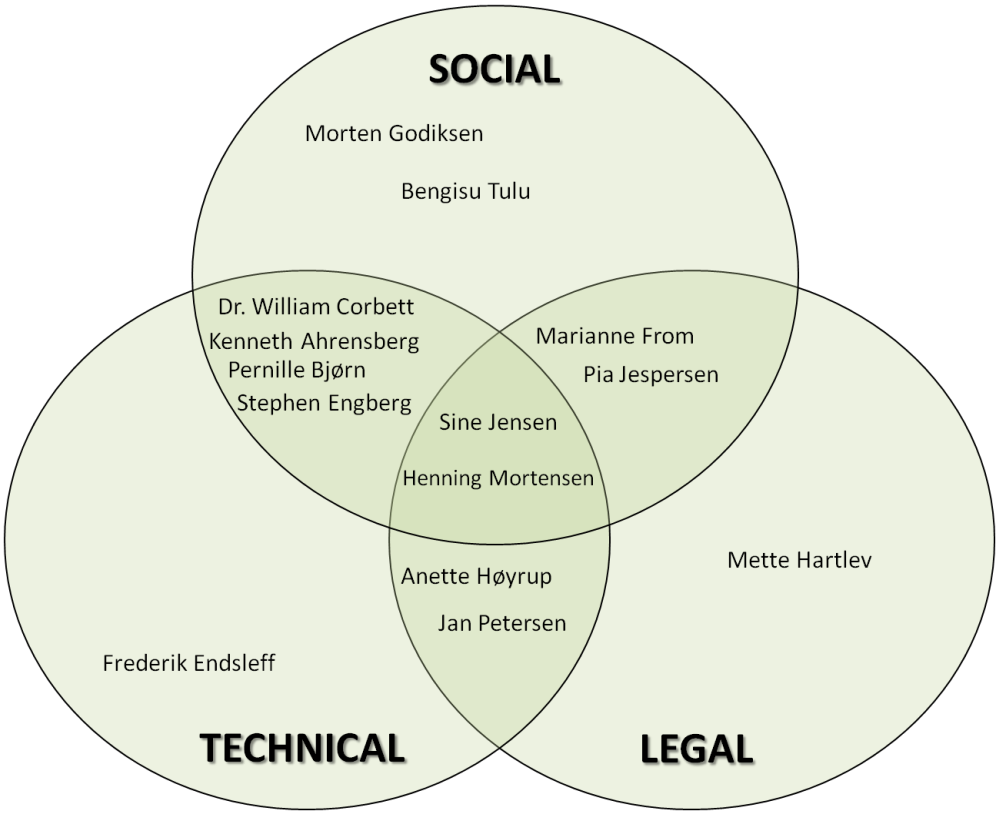

Figure 17: Venn Diagram Illustrating Interviewee Expertise

An interviewee usually fell into one of the three main circles. However, they also have expertise or interest in another subject. Thus, their name went in the overlap between the two subjects. For example, Prof. Pernille Bjørn from IT University is a computer science professor who looks at how doctors and nurses interact with IT systems in the hospital. She was placed in the overlapping area between technical and social. This diagram was a method that helped us understand if we talked with enough experts in the three main areas outlined in our first objective. The diagram also illustrated how many interviewees are involved in more than one of the three areas. Though it was not important for us to present this diagram in our analysis, it did help us organize our time and it helped us to see what areas we were lacking knowledge in.

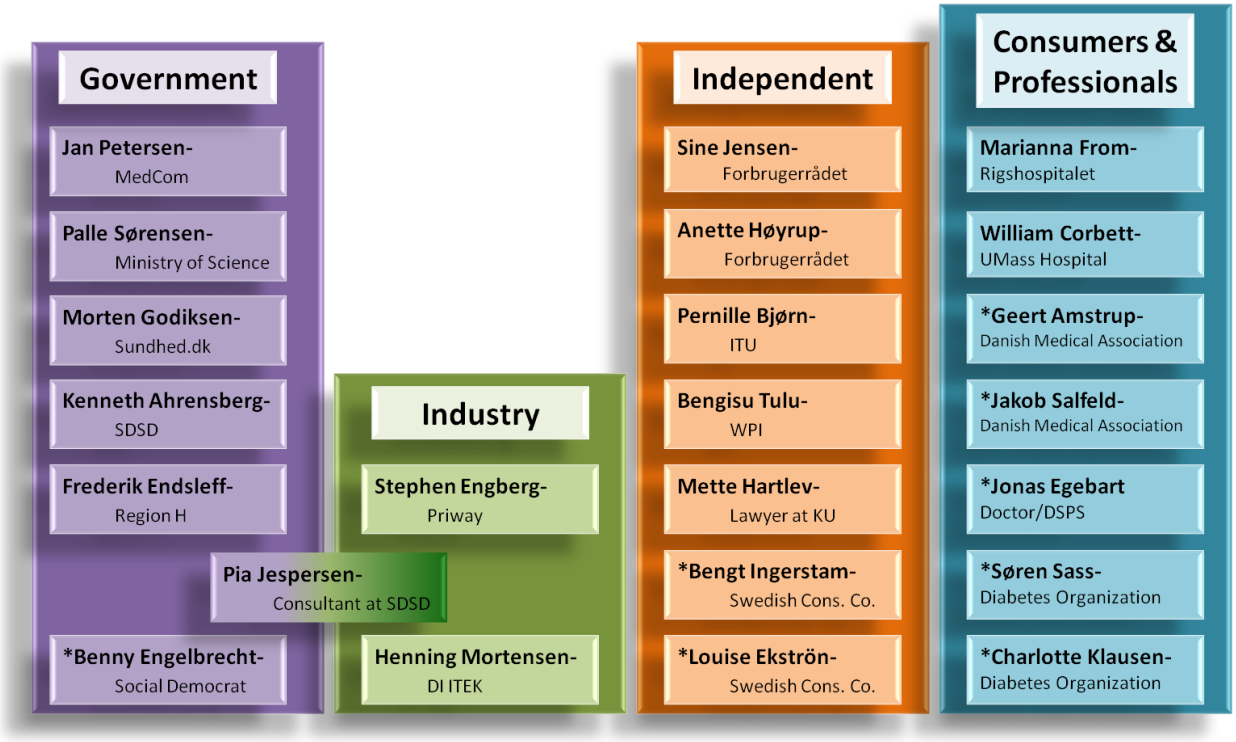

Figure 18: Bar Graph Illustrating "Independency" Factor

Because Forbrugerrådet is an independent organization, Sine made it clear that we needed to present an unbiased report. Therefore, a very useful diagram for her was Figure 18 that shows whether each interviewee belonged to the government, industry, independent, or consumer sectors. The graphic also helped to illustrate how many interviewees we contacted from each of the four sectors. The graph included all the experts we contacted, though the names with "*" are those who we could not interview. The reason this diagram was useful was because Forbrugerrådet highly considers the "independency" factor of each decision they advocate for. Forbrugerrådet needed to know where each interviewee's interest lies. For example, if an interviewee works for a government organization, we would assume they have a bias towards government interests.

3.4 Organize and Analyze Our Findings.

This section is in reference to our fourth objective, to *organize and analyze our findings in a manner that allows Forbrugerrådet to make an objective and knowledgeable argument about EHR privacy and interoperability in the best interest of the public*. Since our project is a study that was used by Forbrugerrådet, it was important that we helped them understand what is best for the consumers of health IT by answering our research questions. Using these answers, we were able to better understand the various aspects of privacy and interoperability issues from different

perspectives. Forbrugerrådet is a lobbyist group with an influential voice in legislation. Any insight we gave them will help them to advocate what is best for the consumers. Because of this, it was of use for them to present our findings in the form of a policy paper presented to Danish legislators.

When writing our policy paper, there are important steps we followed in order to get the message across. First, identified who we were writing for – in our project, this included Forbrugerrådet and the legislators to whom Forbrugerrådet will present the policy paper. We next determined what to write for the Council. By answering our research questions, we were able to identify the issues that the Council was most concerned with. We reviewed our interview summaries and compiled the various answers to these questions that our interviewees provide. Forbrugerrådet wanted us to create a policy paper that helped advocate changes in legislation to benefit Danish patients and consumers of health IT systems. The next step to writing a policy paper for Forbrugerrådet was to construct an effective message. This step pertained to us organizing our findings and completely understanding how each stakeholder was affected by privacy and interoperability. By analyzing the answers to our research questions and discussing them with Forbrugerrådet, we were able to create a message that was useful for their purposes.

Our analysis of expert information was an important aspect as we look at our report as an advocacy report. Since Forbrugerrådet wanted to represent consumers of health IT systems – in particular, patients, doctors, and health IT administrators – our analysis has allowed Forbrugerrådet to assess the needs of each stakeholder.

In addition to the project report, we have written our conclusion in the form of a policy paper. When working with legislation, especially with the European Union, Forbrugerrådet uses policy papers to relay important information. These policy papers are only one to two pages, though they can in any form of media. Our policy paper addressed ten issues. It answered the question, "what needs to be done?" Through looking at examples of policy papers previously used by Forbrugerrådet, we have gained better understanding of how to write an effective policy paper.

3.5 Conclusion

The main goal of the project was to provide Forbrugerrådet with a lobbying tool that would influence policy and legislation that will benefit consumers of health IT and EHR systems. Through research and interviewing of stakeholders, we have gained an understanding of the effects on consumers and we have been able to relay this information to Sine Jensen and Forbrugerrådet.

Chapter 4: Results and Analysis

In order to get the most out of each interview, we identified a list of questions (Appendix D – Project Research Questions) that would provide the information to understand the interaction between privacy and interoperability issues in the Danish Health IT infrastructure. These questions were not necessarily the exact questions we asked the interviewee but they were the basis of all the interview questions. The following section is a compilation of the information we collected from our interviews and arranged loosely in the format of our research questions. This information helped us assess the benefits, obstacles, and strategies to implementation of EHR systems in Denmark's health IT infrastructure.

4.1 Organizations Involved with Danish Health IT

Denmark has an overwhelming number of both government and private organizations involved in different areas of health IT. As there are so many organizations, there is some redundancy in the medical data that are collected from patients and there are many organizations that do not communicate much with each other but are trying to achieve the same objectives. From our background research and numerous interviews, we have a general understanding of the many organizations that work with health IT and how they interact with each other. Figure 19 at the end of this section provides an overview of some of the major organizations' responsibilities and how they interact.

4.1.1 Political Entities

Since Denmark is a welfare state, the Danish government is very involved in almost all aspects of the country's infrastructure. Thus, the government has a large say in the country's healthcare sector. There are three Danish ministries that affect healthcare IT in Denmark: Ministry of Finance, Ministry of Science and Technology, and the Ministry of Health. Out of these three, the most important one is the Ministry of Finance as it decides on the healthcare budget every year. The next most important ministry concerning health IT is the Ministry of Science. They govern, through other organizations, all aspects of clinical IT systems: development, implementation, and evaluation. The Ministry of Health deals with administrative functions related to healthcare, approval of drugs, allocation of resources to different sections of healthcare, and promoting preventive measures to the Danish public.

Each of the five regions receives funding from the national government, through the ministries, and it is the region's duty to allocate it properly. Concerning health IT, Marianne From, the Clinical IT

Head at Rigshospitalet, said that each of the five regions in Denmark chooses an EHR system. Thus, since all the state hospitals are under the control of their region, the hospitals will have the same EHR system and can exchange data with each other. There is strict regional governance about the clinical systems used in a hospital and all the healthcare providers have to abide by it. However, the problem is that all the five regions do not necessarily choose the same EHR system and thus, an interoperability issue occurs. The Danske Regioner is a non-governmental interest organization that supports the regions and is an outlet for the regions to communicate with each other and the national government. In healthcare, Danske Regioner will be an important player when Denmark comes closer to having a uniform EHR system throughout the country as many decisions and compromises have to be made so that all five regions can agree on utilizing the same standards and clinical IT systems.

Each of the five regions is further broken down into municipalities. The municipalities process all the billing information and pay the general practitioners, private hospitals and clinics for services provided to the patients. Compared to the 60 state hospitals in Denmark, there are fewer than 10 private hospitals. Yet, primary care is mostly handled by general practitioners and state hospitals are responsible for secondary care. Thus, even though the private sector of the medical community is not as large as the government one, it represents an important stakeholder concerning health IT (IT brings the Danish health sector together, 2008). The general practitioners are doctors with their own private practices. They can choose their own clinical IT systems but the municipalities and National Board of Health tries to recommend certain clinical IT systems so that the general practitioners' medical databases could be interoperable with those of the state hospitals.

4.1.2 Government-based Organizations

The government-based organizations have been established by the Danish government and are mostly made up of clinical and technical personnel who are trying to improve privacy and interoperability of the clinical IT systems in Denmark. There are four such organizations that are critical in improving the state of Denmark's health IT infrastructure: Sundhed.dk, Digital Health, MedCom, and each region's IT department.

Sundhed.dk is a government organization responsible for developing and maintaining the eHealth Portal in Denmark. Sundhed.dk operates under the Ministry of Health & Interior. Morten Godiksen, Communications and Network Manager at Sundhed.dk, stated that the eHealth portal is a resource intended primarily for patients that allows them to securely view, using the digital signature, their

health data through an online website. Doctors can also use the website to access the data of their patients, if needed. Sundhed.dk employs 600-800 web editors in various hospitals, pharmacies, and clinical labs who are responsible for making patient data from the hospital databases accessible on the portal. Jan Petersen, Chief Consultant of MedCom, said that Sundhed.dk's main purpose is to display data to the user, but it does not own the data as they are the property of the hospitals' databases that they are compiled from.

Another government organization is Digital Health (also known as SDSD - Sammenhængende DigitalSundhed i Danmark), which was established in 2007. It is a national organization for the digitalization of Danish healthcare working with the Ministry of Health, Ministry of Science, Ministry of Finance, and the five regional governments. The goal of Digital Health is to facilitate information exchange between private and public hospitals, as well as the municipalities and the regions. The Digital Health's role in Danish Health IT is to promote interoperability between the regions concerning medical data by evaluating new technical solutions and the current infrastructure, assessing current ethical standards, and documenting current health IT practices and possible improvements. Digital Health's only relation with Sundhed.dk is that Digital Health lobbies the government for funds in order to run Sundhed.dk.

The third government organization in Denmark is MedCom. Jan Petersen, Chief Consultant of MedCom, mentioned that for the past 15 years, MedCom's main goal, similar to Digital Health's has been to facilitate electronic communication within Danish healthcare. However, Petersen explained that MedCom and Digital Health have two different roles within the healthcare sector. MedCom is mainly an implementation organization that aims to implement practical solutions, and creates standards that are meant to solve problems with existing systems. In contrast, Digital Health takes care of the policies and the strategies within e-health. MedCom is a joint public organization that is financed by the Ministry of Finance, the Ministry of Health, the regions, and the municipalities. Petersen mentioned that one of the stakeholders of health IT that they communicate heavily with is the vendors of the clinical IT systems. This is because if the vendors are not implementing the standards then the systems will not be interoperable. Therefore, MedCom works very closely with the vendors that are developing applications for the general practitioner, home care, X-ray systems, full hospital systems, as well as EHR applications.

There are more than twenty different medical information registries in Denmark. There are registries for all types of medical information: past hospitalizations, vaccines, birth information,

medication, common diseases, etc. The data that populate these databases usually comes from state hospitals but some of it can also come from general practitioners and private hospitals. Furthermore, each registry is under the control of a specific government organization and thus, there is immense duplication of medical data. Sundhed.dk, Digital Health, and MedCom are trying to consolidate all these registries as this will improve service, interoperability, and privacy.

The final government organization is each region's IT department. Since we worked in the Capital Region, we were able to interview personnel from RegionH's Koncern-IT group (KIT) that is responsible for health IT operations within the Capital Region of Denmark. The other four regions have their own version of KIT. Frederik Endsleff, Teamleader at RegionH – KIT, stated that KIT's duties include providing health IT to different departments within the region's hospitals, providing service and support for the systems, aiding with local implementation of systems, and providing general counseling to hospitals on health IT. They are responsible for creating a system that integrates a large number of different health IT systems in the Capital Region of Denmark. They are trying to reduce the total number of different systems to aid interoperability, and have reduced the total number of systems in the region from some 800 to about 400 through multiple system integration. Endsleff said that KIT collaborates closely with Digital Health to try to ensure interoperability outside of the region, but is primarily concerned with interoperability within Region H.

A good example of a state hospital in Denmark is Rigshospitalet. It is the largest hospital in the Capital Region and in all of Denmark. Marianne From, the Clinical IT Head of the hospital said that in 2007, Rigshospitalet formed the Clinical IT division. Currently, there are nine clinical IT systems running at the hospital, all of which serve different purposes. Each system caters to a specific department. For example, since the data from the imaging department is very different from the data acquired by the Intensive Care Unit (ICU), different systems are needed to store the unique types of data. Examples of clinical data stored at Rigshospitalet are: patient's medical history, doctor's notes, medication information, imaging data such as MRI or X-rays, and laboratory test results. From also mentioned that the clinical IT systems used by Rigshospitalet are selected and bought, with the assistance and expertise of KIT, by the Capital Region from various clinical IT vendors. KIT's Endsleff works to make sure that these various clinical IT systems work with the current infrastructure of each of the hospitals in the Capital Region. His department is also responsible for

the security and standardization of the clinical IT systems used by Rigshospitalet and other Capital Region hospitals.

Concerning patient interaction with the Danish organizations, it seems that Sundhed.dk and the hospitals are the only organizations that interact directly with patients while the political entities, MedCom, and Region H just try to improve privacy and interoperability of the clinical IT systems in Denmark without any direct contact with the patients.

Similar to the patients, healthcare providers also use sundhed.dk and thus, their input is important in order to improve the eHealth portal. Healthcare providers' interaction with organizations related to health IT occurs primarily with the advocacy groups and the academic research organization. The academic research groups usually have focus groups for healthcare providers in order to design technical solutions that conform to the healthcare providers' needs.

4.1.3 Non-Governmental Organizations

Even though the Danish private healthcare sector is small compared to its government counterpart, the private sector has numerous subsets that work on improving privacy and interoperability in health IT systems. Henning Mortensen, Chief Consultant at DI ITEK, explained how the Danish private sector is organized. The Confederation of Danish Industry (DI) organizes the entire industry in Denmark which is comprised of around 11,000 companies. There are different trade associations for different sectors. For example, DI ITEK is the trade association for Information and Communication Technologies (ICT). Normally for different problems or topics, a committee is formed that is made up of members from DI and members from the trade associations. This allows the committee to have a user (DI) and a vendor (trade association) perspective on the problem or topic. The purpose of these committees is to facilitate conversation between the different stakeholders involved in the development of a specific product or service.

Mortensen talked in more detail about the initiatives the private sector is taking to improve privacy in IT solutions. In 2001, the DI's committee for information security was created. This committee had two objectives: 1) to improve security for Danish industry companies by implementing technical solutions that protected company data from viruses, spam, etc, and 2) to lobby for necessary legislation that will improve IT security for the private sector. Privacy was a topic that was addressed starting from 2005. Since then, the committee has written numerous reports and

guidelines. Unfortunately, in healthcare IT, the private sector in Denmark does not have a lot of influence over implementation decisions of clinical IT systems.

Another non-governmental venue for developing technical solutions for privacy and interoperability in healthcare IT is academia. Academic researchers who are developing novel privacy and interoperability solutions talk with healthcare providers in order to understand the problems healthcare providers face when using the current clinical IT systems. For example, Pernille Bjørn, a Computer Science professor at IT University of Copenhagen, actually observes healthcare providers in their natural environment in order to understand the improvements that need to be made to clinical IT systems. Academic research organizations usually get funding from the government but they operate independently and often collaborate with private companies such as Priway to develop their products.

Advocacy groups are independent groups that look at certain issues from the view point of a specific stakeholder. Some examples of advocacy groups are Forbrugerrådet (Danish Consumer Council), the Danish Medical Association, and the Danish Diabetes Association. These groups try to increase awareness about the problems that exist for their stakeholders and lobby for legislative or political changes that would help their cause. Advocacy groups, in some way, act as a policing body as they monitor what other organizations are doing to help their stakeholders. If some product or service is negatively affecting their stakeholder, the advocacy groups will try to increase awareness about it and rectify the issue.

As health IT systems such as EHR become more popular, the advocacy groups are also becoming more concerned about the issues it creates for patients and healthcare providers. Some of these issues are discussed in the following sections.

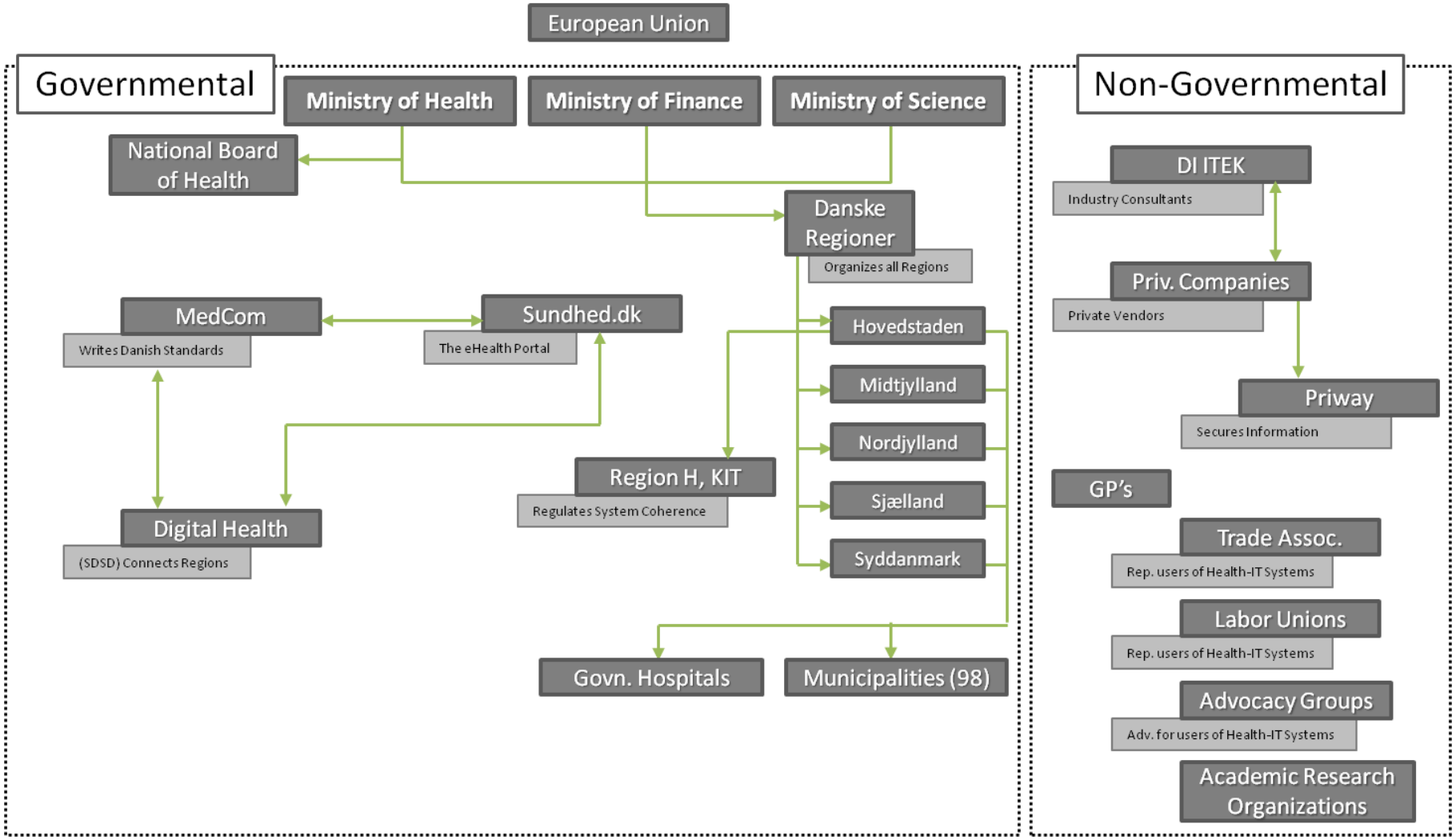

Figure 19 Chart showing the Organizations related to Danish Health IT

4.2 Patient Privacy

Though the transition from paper records to electronic records has allowed users to access information at a much faster rate, it has also brought forth many risks to patient privacy that did not exist with paper records. This section will discuss the patient data that is currently collected, parties that have access to the patient data, and the risk the data collection creates for patients.

One of the main issues, stated by Ahrensberg, From, and Mortensen is that the Danish people are very trusting of the government, assume that the government has their best interest by implementing health IT solutions that will protect their medical data, and do not inquire about privacy of their medical records. In the six years From had been working at Rigshospitalet, there have been only three official inquiries made about privacy of medical records and all three inquiries were made by people working for Rigshospitalet at that time. As medical information becomes more and more digitalized, this trusting mindset could cause problems in the future such as unintentional or malicious disclosure of sensitive medical information, and identity theft.

If the public was made more aware about privacy and the options they have, they would most likely support the IT option that makes their information more secure and as a consequence would pressure organizations that develop IT solutions to implement those security measures. When asked about why privacy seems to be of more importance for the private industry than the government, Mortensen said that it is because the government organizations concerning health IT are concentrating more on making EHR systems throughout Denmark interoperable rather than improving privacy. Another reason he mentioned is that the government cares more about their budgets than privacy and security of patients' data. The government organizations would opt for cheaper security systems rather than the more expensive, safer technology. Further evidence for this is that while both Mortensen and Stephan Engberg, CEO of a company that develops privacy-by-design technical solutions, have thoughts on how to advance systems in the area of privacy, the government-affiliated parties we interviewed did not seem to think that privacy was a pressing concern, and were typically unconcerned with privacy upgrades.

4.2.1 Patient Information that is Currently Collected

Marianne From gave us insight about medical information collection from the healthcare providers' point-of-view. She said that all the hospitals in Denmark are expected to send all

their medical data to the Danish eHealth portal so the Danish patients will be able to view their complete medical file. However, if a patient does not want his/her information available on the eHealth portal, he/she can ask for the information to be private.

In fact, it is only about 1% of all patients in Denmark that say they do not want to give their general practitioners access to their medical data, and of this 1% the majority is teenagers who don't want the family doctor to see, if they have been in emergency care due to alcohol, or other "embarrassing" situations. From also mentioned that the medical records of patients in sensitive hospital sectors, such as sexually abused children, raped women, and psychiatric patients, are exempted from sending information to the eHealth portal.

Engberg and Mortensen said that currently, too much unnecessary patient information is being collected. They believe that identifying data, such as a patient's name and address, do not need to be stored and in an emergency, a patient can be treated without these pieces of information. One specific concern they have is with the current Digital Signature and its next version, NemID. Digital Health is trying to make NemID popular. It will be used by patients and healthcare providers to access medical data on Sundhed.dk. Every Dane will have a NemID but he/she needs to activate it to use it. The problem is that the NemID is consolidating information from many sectors, it is difficult to use and, the public does not have much incentive to use it.

4.2.2 Hospital Parties with Access to Patient Data

In order to secure compliance for existing and future systems, it is important to implement methods that provide the knowledge about who to give access to and what information to give them. Data can be stored in many places, and that is why it is important to have a national infrastructure that supports technology that records who gains access to what information. For example, the National Board of Health has a patient registry and wanted to let doctors view information on patients. However, there was no way of checking if the doctor has the patient in his care and if he had the right to access that patient's medical information. Jespersen sees a need for a system that ensures the doctor accessing information has the right to do so, possibly though using registries that hold information on patient's general practitioners (GPs). If a doctor accesses a patient's data and they have not been authorized to do so, their access privileges to the system can be fully revoked and the doctor can be punished. Authorization to the system is overseen by the National Board of Health, a board made up of different doctors and general practitioners.

At Rigshospitalet, Marianne From said that each healthcare provider gets his/her own login information for any of the nine clinical IT systems. Given the position of the healthcare provider, he/she will only have access to the relevant clinical IT systems. Also, the level of access is different depending on the position of the person. The nurses only have "read and write" access to the medical records of patients in their ward. Doctors have access to view medical records of all the patients in the hospital but they can only write information for the patients in their care. Patients have a right to look at their records. However, a patient's family member can look at the patient's medical record only if the family member files a request with the hospital.

In the case of an emergency, there is a level of trust that goes into the doctor accessing the patient's data without consent or referral. However, the system needs to be able to recognize when the doctors misuse this upfront access of the data. Pia Jespersen, a consultant working with Digital Health suggests a few solutions. For example, if a doctor accesses a patient's medical data of a patient not in his/her care, the system will alert the user to his/her questionable access. In some cases, a GP will give hospital doctors a written referral that will allow those doctors to access the necessary information. However, in the case of an emergency this is not possible.

Concerning doctors' access to patient data on sundhed.dk, Ahrensberg mentioned that it was easy to give the patients access to their own information as one patient's digital signature provides access to only one medical profile. However, the problem occurs when giving the doctors access to their patients' profiles. Sundhed.dk administrators have to keep track of which doctor is in charge of which patients so that the doctor can only access relevant medical profiles. One clarification Ahrensberg made was that the doctors do not use Sundhed.dk to access patient information, only to access their hospital administrative information such as payroll, hospital calendar, etc. The doctors use the EHR system implemented in their hospitals to look up information on patients. Ahrensberg and Godiksen contradicted each other when explaining the access privileges a doctor has for Sundhed.dk. Ahrensberg said that doctors can only access administrative information on Sundhed.dk while Godiksen said that the doctors can access any patients' record on the portal. After conducting more interviews, we found out that Godiksen was correct.

4.2.3 Risks for Patients

According to Anette Høyrup, privacy advisor at Forbrugerrådet, the biggest risk that users who put their personal information onto electronic systems face is unauthorized users hacking into the system and gaining access. The more information consolidated together (which is becoming more and more the case with electronic health systems), the easier it is for all of it to be misused. Stephan Engberg, CEO of a private company that develops privacy-by-design technical solutions, says that if an attacker manages to break into one system which stores a universal identifier like a social security number, the attacker will know how to find that user in other systems using the same identifier. Because of this, if an attacker breaks in, there is no way to know the extent of the data that has been compromised. Engberg refers to this as "uncontrollable risk".

Another risk that Pia Jespersen mentioned is that only 1-10% of doctors' access logs are checked so the chance of a doctor performing malicious activity is very low. This method is greatly lacking in ensuring patient data protection. The system of punishment only acts as a deterrent and does not actually protect patient data from being misused. Only 1-10% of the access logs are actually audited to ensure that no illegal activity has taken place, meaning illegal access could be occurring much more often than is currently known.

Høyrup urges that systems execute tracking users of the system and what information they access as a major security measure. For example, Denmark's public transit travel cards do not track which users see what information. This seems dangerous when each travel card member's travel information is stored and accessible to 2-3 thousand employees. Another safety measure, for any electronic data accessing system, is to delete the stored data after a certain amount of time.

4.3 Interoperability between Health IT Systems

The consumer group most affected by interoperability is the healthcare practitioners, as they actually use the systems and are most directly affected by whether or not they are interoperable. Denmark currently makes extensive use of many different health IT systems and has made large efforts to make them interoperable with each other. Currently, there are systems that provide interoperability within each individual region. Sundhed.dk also makes some patient data available across the entire country. Denmark's use of standards for data exchange, however, appears to need more work. While much effort is being made to make systems interoperable, there is not as much focus on maintaining patient privacy while doing

so. This section provides insight into the current state of interoperability within Denmark, and covers some future plans currently in place to improve interoperability.

4.3.1 Methods for Patient Data Transfer

Danish EHR systems can be divided into two main categories: those that make data interoperable within each region, and those that make data interoperable between all the regions. Each of the five regions of Denmark is responsible for implementing their own EHR system. However, due to these different EHR systems, hospitals from different regions typically do not have the capability to directly access each others' data. Healthcare practitioners must usually use other methods to receive data from other regions, such as Sundhed.dk, the Danish eHealth Portal. Data transfer inside each region and data transfer between all the regions therefore use different systems, which will be discussed separately briefly.

Digital Health's original goal was to make all the hospital EHR systems in the five regions of Denmark completely interoperable. However, this goal became infeasible, as each region is its own authority for its own health IT and makes its own decisions, and no "off the shelf" products exist that meet the needs and expectations for all the regions. Digital Health also did not want to create a monopoly in the EHR market by forcing providers to use the system Digital Health has chosen. Digital Health revised their goal to create a system that allows certain data to be interoperable between the five regions of Denmark. This is called a level-based system. This level-based system will allow sharing of certain data, such as medication information and imaging files like x-rays. Currently, the level-based system is not completely implemented except in some areas such as Jutland.

4.3.1.1 Data Transfer Inside the Capital Region

Our study was able to look at the data transfer methods used inside one region – the Capital Region. According to Kenneth Ahrensberg, the Capital Region was the first to implement an EHR system, but their system is becoming obsolete. Since the smaller regions implemented an EHR system much later, their systems are state-of-the-art. Marianne From also believes that the Capital Region lags behind since it has the most clinical users and healthcare providers, making it more difficult to implement new systems.

The Capital Region uses a system developed by KIT called the Distributed Healthcare Environment (DHE) to centralize all the data in the Capital Region. The DHE is a shared database that currently services 15,000 to 18,000 health care providers, and manages many

different health IT systems, including a master patient database and an electronic medication system that manages virtually all medications in the capital region. The DHE is a system that all hospitals in the capital region can potentially use, and typically doctors themselves interact with the system. Vendors are responsible for making their systems interface with the DHE, and typically the contract between a vendor and KIT gives the data rights to the DHE. However, Endsleff believes that standards are needed to simplify this process, since a significant amount of work is put into ensuring that vendors' systems and the DHE are interoperable. Better use of data standards, discussed below in Section 4.3.2 Use of Standards for Interoperability, will simplify interoperability implementation in the Capital Region.

4.3.1.2 Data Transfer Between the Regions

The eHealth portal, sundhed.dk provides a way for both patients and doctors to view patient data across the different regions by aggregating data from each region into its own format. According to Morten Godiksen, the Public Relations Manager at Sundhed.dk, the portal has 600-800 different web editors responsible for gathering information from the different EHR systems used in hospitals and making it available to the portal. Hospitals typically differ in their systems and how their standards are implemented, so the portal editors do the work in making the data interoperable with the portal's system. Anyone can view data through the portal through an internet connection using their digital signature.

Godiksen stated that patients were the primary users of the health portal, and he believed that doctors typically do not use the portal. Marianne From confirmed that the portal is a very useful website for patients to use in order to see their various types of medical information all in one location. However, From pointed out that doctors also view patients' records using the eHealth portal. Doctors usually use their respective hospital's EHR system to access information about their own patients and other patients from the same region. However, in case of an emergency, a doctor might have to treat a patient from another region and can use the eHealth portal to access the patient's information. Hence, all doctors have access to any patient's medical file on the eHealth portal. If the patient is from another country, there are currently no technical solutions to receive the patient's medical information at Rigshospitalet.

4.3.1.3 Planned Upgrades to Current Data Transfer Methods

There are multiple efforts being made to improve the quality of cross-regional systems. According to Endsleff, the Capital Region's DHE system receives data from many systems from different vendors with different data formats, and currently stores data of patients from

the capital region. Endsleff said that patient data from around the entire country will soon be stored in this system, as well. This will make receiving patient data in the capital region easier.

Denmark currently has a nationwide database of patient information known as the National Patient Index (NPI) which has existed since the 1970s, but is not yet interoperable with region-wide services such as sundhed.dk. The NPI is planned to become a database system accessible to patients and healthcare providers through the internet that will fill in the lack in certain features Sundhed.dk does not currently have. The NPI is being upgraded by both Digital Health and Sundhed.dk. The first phase of the NPI's implementation was started in early March 2010.

4.3.1.4 Issues with Current Methods

While the eHealth portal does currently exist as an interoperability solution between regions, other parties are making efforts to create new nation-wide solutions. KIT is trying to make its own system interoperable with the entire country, and Digital Health is pushing its NPI system. Pia Jespersen of Digital Health also believes that there needs to be a national infrastructure to help systems communicate between regions. This national infrastructure could also offer the advantage of usability inside the individual regions as well, to simplify communication between systems inside regions. It appears as though the eHealth portal is not an adequate system for healthcare practitioners when treating patients from other regions, since it contains limited information and multiple efforts are being made to create better systems.

From the private sector, Henning Mortensen stated that very little of the industry's opinion is taken into account when implementing IT systems and solutions. He thinks this is because the regions system is not very mature and the regions do not have enough personnel to perform technology evaluations. Thus, the regions just use popular IT products that have been on the market for a long time. The regions also do not communicate very much with each other and thus have many different implementation strategies for the same problem. Mortensen thinks that since the regions only prefer well-tested and popular IT products, IT start-up companies have difficulty selling their products due to a lack of demand and hence cannot develop their business. Another problem for the small companies is that it is very difficult for them to convince a region to buy their IT systems as it would cost the region a lot to install a

completely new system. However, Mortensen still thinks that the regional government should consider new health IT solutions in order to improve the patients' experience in the hospitals.

4.3.2 Use of Standards for Interoperability

The use of standards for the exchange of health IT data is an important part of making different systems interoperable with each other. Each of the five regions is responsible for its own set of standards, but there are also efforts being made to implement standards between the regions as well. Digital Health would like Denmark to have one set of standards, but trying to implement only one would be time consuming and expensive.

The government-sponsored MedCom organization is responsible for creating standards for interoperability between the regions. The organization deals with standards such as ISO, CEN13606, and HL7, as well as international standardization organizations such as IT Integrated Health Enterprises. Jan Petersen of the International Division at MedCom mentions that MedCom uses and adapts these standards into Danish standards in regards to messaging interoperability. In the Capital Region, KIT works with all of these standards. There are also efforts to review and improve the adaptations of international standards used in Denmark.

4.3.2.1 Implementation Issues with Standards

Petersen believes that many interoperability issues in Denmark come from municipalities not implementing international standards such as ISO, CEN13606, and HL7 (all hospitals have already implemented MedCom standards). Henning Mortensen of DI ITEK agrees that the Danish industry does not follow the European Union's standards as much as other countries, especially in healthcare.

MedCom standards are based on the EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) standards, which were originally developed by the United Nations and adopted by ISO. The main problem within healthcare systems is that the standards used are only *frame standards* – developers must still make significant design choices when implementing them. Therefore, even though two systems comply with the same standard, more work is often required to give the systems the ability to communicate. In order to get practical interoperability, organizations such as Integrating Healthcare Enterprise (IHE) are analyzing current standards in order to make the standards more specific.

Another major difficulty is that the demand for standards does not come from vendors, which is where the burden of implementing the standards falls. Frederik Endsleff thinks that vendors of different health IT systems do not usually rely on standards. He thinks many existing standards are hard to understand, and that many vendors simply do not think about them or why they would be useful. He also believes that not enough standards exist to cover all the different data types used by the healthcare industry. Larger companies tend to not use standards as much because they are more likely to develop more systems and can interconnect their own systems themselves. In contrast, smaller companies tend to like standards more, as they are more willing to work with other companies due to their small size. Endsleff believes that when larger companies create their own proprietary systems that do not adhere to different standards, hospitals using these systems are locked into that vendor and cannot try using other products. This undermines the point of using standards and weakens interoperability. Smaller vendors also have more trouble selling their systems, as they are often not interoperable with the more commonly used large vendors' systems.

The main issue with standards in Denmark appears to be that although the international standards Denmark uses are adequate and used successfully by other countries, the Danish adaptation of these standards is not strict enough and does not promote interoperability well enough. If the standards in place do not actually work well enough to make systems interoperable, then they are not useful and vendors will not be motivated to use them. Thus, large companies will dominate the market and hospitals will lose choice when buying systems. Interoperability and the use of standards are therefore important in encouraging a competitive health IT market.

4.4 Legislation on Healthcare and Health IT and Consequential Issues

Experts we interviewed have had different opinions on the current legislation surrounding Danish health IT. Though some experts advocate for new legislation that must be adapted to fit the needs of evolving EHR systems, others believe it is not the laws that need to be adapted, but how the laws are interpreted and implemented. This section illustrates and analyzes experts' viewpoints from the government, industry, and independent sectors of Danish health care, as well as the effects of current legislation on the different consumers and aspects of health IT such as privacy and accessibility.

4.4.1 Legislation in Regards to Patient Privacy

There are two options when dealing with privacy. The first is through technical solutions, also known as privacy enhancing technology (PET). PET builds the privacy and preventative measures into the system. The other privacy option is setting legal guidelines, such as terms and conditions of use, like a legal contract for users to follow. Here, the privacy measures are not built into the system, but instead become legal guidelines the user must follow.

As mentioned, the majority of security is set in place through "terms of use" and legislation about accessibility. Therefore, the data can technically be distributed, but it is not necessarily legal to do so. As an example of "terms of use" security, when a doctor views a patient's medical file that he/she is not treating, the doctor's name and time of access gets logged. The patient is also potentially notified if his/her file is accessed by any practitioner. Various security checks are done in the hospital to ensure that the system is not being modified or abused by the hospital staff (From). The main issue with this is that the damage is done; the data have been accessed and the patient only finds out after the fact. In the short term, hospitals must concentrate on having strict tort-based liability regulations. As mentioned in Section 2.2.1 Legal Issues, of the background, tort-based liability pertains to when a healthcare provider intentionally and illegally changes, deletes, leaks, or sells patient information. (Hodge, Gostin, & Jacobson, 1999).

4.4.2 Legislation in Regards to Data Accessibility

As with privacy, in many instances it is not the law that is the problem, but the interpretation of the law, system to system. In addition, different laws may cause contradictions in accessibility which makes it technically difficult to implement barriers when it is unclear as to who has access.

Jespersen mentioned the new 2007 Danish law on health that dealt with access to all kinds of electronic data. This law specified who has access to what data, and how they could obtain that data. Unfortunately, this law is difficult to implement technically, system to system. Currently, government groups in Denmark are working on a security roadmap because as it is now, the common national systems in use are not compliant with the law and cannot prevent all hazards. The security roadmap outlines the tasks that are supposed to end up as a National Security Infrastructure.

4.4.2.1 Patient Consent

On one hand the law says there must be a way to register if a patient does not give his or her consent. On the other, Jespersen recognizes that the solution to this law needs to be economically practical. This is just one of the components that Jespersen thinks Digital Health and other relevant health IT groups need to consider when making the national infrastructure. Hartlev explained that all patients are assumed to have given implied consent to the doctor so that the doctor can access important patient information and provide optimal care. However, the patient should be informed that the doctors do have this implied consent and the patient, if he/she wishes, can object to the doctors' access to his/her information. If the patient does not give consent and if his/her information is still accessed, the patient can file a complaint with the Danish Patient Complaint Board or contact the National Board of Health. It would be beneficial for the government to require by law that healthcare providers explain patients' options in terms of their rights to giving consent of access to their medical data.

4.4.2.2 Confusions with Data Access for Doctors, Nurses, and Other Healthcare Providers

Due to the different interpretations of laws and regulations, contradictions between laws, and even potentially out of date laws, issues arise with laws that impede the work of doctors, nurses, and other hospital staff.

With such broad access to large amounts of data, EHR systems can create new liabilities for parties involved. If a doctor does not use the information that was made available to him/her through the system, he/she could be liable for malpractice. However, because of the sheer volume of data, it might not be practical to look at it all. Laws to clarify these issues would be useful to avoid such situations.

More clarification is needed with the multiple additions, terms of use laws, amendments, etc. established every time the law leaves some sort of gap, and accessibility can become even more confusing and potentially cause more harm than good. For example, Jespersen mentioned the existing law that the Ministry of Health helped to pass where all medication history is viewable to doctors and a patient cannot prevent this access. Though doctors may not have access to the patients' surgery or sickness history, they can always see the patients' prescriptions, which will allow him/her to know what sicknesses or surgeries the patient has had according to what medication the patient was prescribed. Because of this, legislation made another special terms-of-use amendment to try and fix this problem.

There is a clause in the Law Concerning the Access to Personal Data that refers to what a specific user of a system is able to access. The clause specifies some differences between what a doctor has access to and what any other healthcare providers can access. Doctors technically can view all of a patient's medical data, while for nurses and technicians cannot gain access to information that is not required for the current treatment. Though this may make data more secure, it makes providing treatment more difficult for nurses and gives other hospital workers difficulties in their jobs. In most cases, nurses are the first health care providers to treat a patient, yet they are not given access to any of that patient's existing medical information that may be of relevance. Therefore they must go through the doctor to get access to important data, which is time consuming and impractical. With this law, they are not legally able to do what they are obliged to do under other laws that regulate patient care. The need for information and the access to that information differs from job to job, and the hospitals should be able to define what is necessary for each hospital worker to be able to view under all circumstances.

These discrepancies are one of the things Jespersen and Digital Health are working on because it is necessary that the law is feasible and practical to implement. When it is not, people are more likely to become negligent in privacy and information security. Digital Health has talked to the Ministry of Science about changing this part of the law pertaining to nurse accessibility, and Digital Health has also stated the importance of building a national infrastructure on security to technically support the law. From here, it is important to raise the awareness on what healthcare professionals are and are not allowed to do because this is not currently supported by the technology.

4.4.3 Current Conflicts in Regards to Legislation on Healthcare

There has been a debate as to the relevance of the current legislation pertaining to EHR systems and electronic data protection. The question is whether to adapt the current laws according to each situation within the system, or to keep the laws as is and concentrate more on standardizing the interpretations of the laws. It is difficult to say what will benefit the systems more, but many experts have given their opinions on the matter.

A big issue is whether laws concerning patient privacy need to be updated to deal with electronic medical data rather than paper-based medical data. Mette Hartlev, a lawyer at Copenhagen University with research interest in patient privacy in healthcare, said that the legislation for medical data three to five years ago was primarily framed to deal with paper-

based records. In a scenario where a hospital requested information about a patient from another hospital, the doctor in the second hospital in charge of the patient will retrieve the paper-based medical record, review the file to see if the whole file or only parts of it need to be sent, and then finally contact the patient to obtain permission to disclose the necessary information. For electronic medical data, the procedure is not the same. A doctor from one hospital can access data for a patient whose medical records are stored in another hospital. The doctor's access is logged but he/she might have access to more of the patient's electronic medical data than is necessary to treat the patient. Because disclosure of patient's data that was unnecessary to properly treat a patient was illegal when the legislation for paper-based medical data was created, the same rules and regulation still apply for electronic medical data. Thus, Hartlev does not think that the current legislation needs to be changed. However, she thinks that if one asked the healthcare providers the same question, they think that the rules are very strict and do not allow them enough access to patient information that is necessary to treat a patient. Hartlev thinks that the Danish law has found a good balance between protecting the patient's right to privacy and allowing healthcare providers access to important patient information for proper treatment.

Two experts that also advocate for this opinion are Pia Jespersen, a consultant currently working with Digital Health, and Henning Mortensen, a Chief Consultant at DI ITEK (Danish Industry). They state that although the laws are broad, they do not need to be adapted. Instead of changing laws, some stakeholders' opinion says that how the law is interpreted and implemented needs to be more standardized.

Jespersen and Mortensen both explained that the 1980 EU directive on personal data has been adapted into Danish law since 2000. Though the EU directive itself has been able to encompass all new technological developments, the problem is that the directive is interpreted very loosely in Denmark. As a comparison, Norway has also implemented this directive, and the country's interpretation is much stricter, which allows its data protection agency to be much more powerful and influential. More specifically, one part of the directive states that privacy enhancing technologies have to be current to the time. Unfortunately, this section was marked as a footnote in the directive and was overlooked in the translation into Danish legislation. Hence, currently, there are many organizations still using old IT security systems.

One particular Danish law is *Lov om Behandling af Personoplysninger,* which translates to the Law Concerning the Processing of Personal Data. This law touched upon access to personal data and stated that medical professionals are allowed to access personal data if it is necessary for their work. The access to patient data is also regulated through the law on health, specifically to the electronic access to data. These laws are very broad but in Jespersen's and Mortensen's opinions this is a good thing. If the law is too specific, it is difficult to implement strictly. If legislation was adapted and changed for every situation, it would become much too complicated and some laws would contradict each other. In fact, there are instances where this already is the case, as noted above.

However, there are many problems with this, as electronic data can be manipulated in ways that data on paper cannot. Some stakeholders' opinion has been that the law is outdated, works better for paper records, and does not adequately respond to the vast changes in security and interoperability of EHR technologies. Two experts that share this viewpoint are Morten Godiksen, a PR Manager at Denmark's e-portal Sundhed.dk, and Kenneth Ahrensberg, a Special Advisor at Digital Health. Ahrensberg stated that the legislation and security technology change almost on a day-to-day basis and thus it is very difficult to develop a technical solution that conforms to all the laws and regulations and is up-to-date. This has also prevented the e-health portal from being developed further. Laws specifically designed with EHR systems in mind are needed for further success of these systems.

What is interesting to note in relation to the difference in opinion is the sector of government in which the experts work. Both Godiksen and Ahrensberg work for government organizations funded by the ministries, and run by boards comprised of ministry, region, state, and municipality members. Because they are directed by those who would be making the changes they call for in the laws, it is most likely these changes will only further benefit Sundhed.dk and Digital Health's access to data and interoperability. On the contrary, Mortensen works for the industry and is a consultant that represents private vendors in Denmark. Because Jespersen is a consultant, she does not officially work for Digital Health and is not bound under its title. Hartlev works with Copenhagen University, and therefore is an independent source. Because Mortensen represents private vendors that already have more difficult barriers to get their systems implemented than government funded companies, it is possible his opinion stems from representing what is best for the private vendors. It is difficult to say which opinion and which direction is the "better" one. If laws are kept broad,

it is more likely they will stay relevant with the fast pace that EHR system technology evolves.

4.4.4 A Need for Change

Jespersen mentioned that the municipalities are also a part of the healthcare system because they are in charge of the care of elderly, among others, in addition to general practitioners. In some of the municipalities' activities, there is discrepancy as to whether certain treatment pertains to the law on healthcare or the law on services. The law on health says consent is not necessary if one is to access data electronically, but the law on service says it is necessary for consent. For example, when a physical therapist is working with a patient who was referred to her after a hospital stay, this is considered health-related so therefore consent is not needed. However, when the same therapist works with a patient who has not been referred, it is considered service-related so consent is required. Workers must know which law applies under which circumstances.

In general it's not the law that is the problem; rather, the interpretation that is more important. There needs to be guidelines directing people how to interpret the law. The same is important for implementing technical solutions; many IT solutions, especially international solutions, do not follow the privacy laws. Jespersen believes the laws will become stricter because of the way the IT systems have been implemented. Because of integration, too many people can be given access to information. Jespersen does not believe the average citizen has any idea who has access to his/her information.

Another major issue with the laws pertaining to security and health IT is the confusion of the system users. To address this confusion, Mortensen suggests a public authority to be able to give advice to the health IT vendors on how to technically implement the privacy law. Currently, this is not possible – the public authorities can only police vendors to ensure that the legal regulations are being followed. If authorities worked with the industry, or furthermore, worked also with consumers and published a pamphlet that explained all the laws and their potential interpretations, more systems and users would stay within the laws.

4.5 Other Issues in Health IT Systems

A big social problem that hinders implementation is the reluctance of healthcare providers to adapt to a new system. Thus, each region has IT people whose job is to persuade doctors of a hospital system to implement new technical solutions. Marianne From, head of clinical IT at Rigshospitalet, mentioned that when Rigshospitalet started transitioning from paper records

to electronic records, doctors, nurses, and other healthcare providers had a hard time adjusting to the new system. Now, there are nine separate clinical IT systems. Some healthcare providers easily embrace the digitalization of medical data while others oppose it because they perceive that there is a big learning curve or time sink when it comes to learning the new clinical systems. From noted similar issues occur on the patients' side as even if the public in general believes the health portal is convenient some patients who are less skilled with computers have trouble accessing the system. Thus, Rigshospitalet gives the doctors a choice between typing their medical notes into the EHR system or dictating their notes which are transcribed and added to the EHR system by other hospital personnel. From said that the medical staff needs to be trained on using new systems. However, training the medical staff will become less of an issue every year as newer generation of healthcare providers are much more tech-savvy.

4.6 Potential Solutions for Current Health IT Issues

While the health IT systems in Denmark are fairly effective, there are clearly many improvements that can be made, both in the sectors of privacy and interoperability. Every individual interviewed is concerned with improving the state of health IT, and many groups have thought up possible solutions for the different sectors. These solutions include both technical changes and changes in how the groups interact with each other. This section details some of the solutions presented by different interviewees and discusses the reasoning and feasibility behind them.

4.6.1 Pseudonyms for Identification

Engberg, the founder of Priway, believes that when using the highly centralized systems of today, users lack control over their data. Because all their data are stored in an outside system and linked directly to them through a universal identifier, the people running a central system have the real control over virtually all of a user's data. The user must trust the system to keep their data safeguarded. The Danish CPR number is used often as a universal identifier and any Danish citizen has to give the number to various people in order to receive most of the government services. With the proper tools, anyone can find a specific person's CPR information and be able to access their data. Figure 20 illustrates the current CPR system in place which is an example of a large, centralized system. Currently, a user uses his/her CPR number to log into many important systems. This creates a very large "secure area". If an attacker breaks into this secure area, he/she can use the user's CPR number to access all of the other systems in the area as well, resulting in potential identity theft.

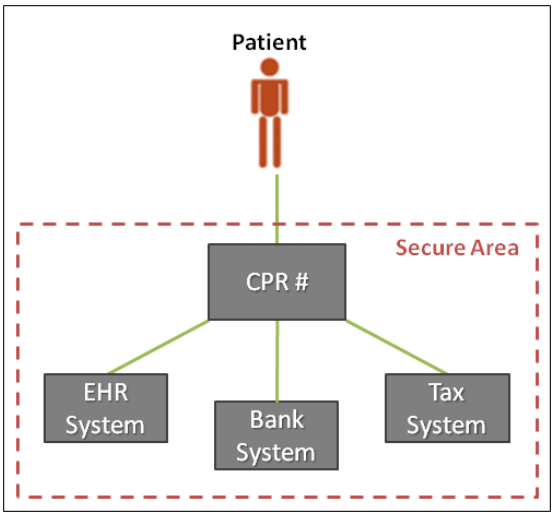

Figure 20: Centralized Security System – Breach of one system allows access to other systems

Engberg has a novel solution intended to greatly improve user privacy by avoiding a universal identifier and using pseudonyms instead. Pseudonyms involve using a different identifier for every different purpose – for example, an identifier for health IT systems, a different one for financial systems, etc. Engberg believes that systems do not need to know personal information in order to properly service their users – as long as a system can identify a user by a pseudonym, it will be of the same service as if it knew who a user was as a person. The system that stores the data will also only store the user's data in an encrypted format that can only be decrypted by a key that the user has. This way, even though the system stores the data, only the user can actually unlock it and view it, giving control of the data to the user. In the event of an emergency or a situation where a user's data are needed and they are unable to relinquish control, the system can be designed such that a doctor can use a user's key in order to temporarily gain access to emergency-critical information.

Priway is working on developing a Citizen ID, which can manage the separation of IDs for a user to allow them to easily use pseudonyms in systems. The Citizen ID would automatically connect to outside systems using the right identification key. This allows pseudonyms to easily be used without forcing the user to individually manage many different pseudonyms. Figure 21 illustrates how a pseudonym system would protect a user's data from attacks. The user has a number of pseudonyms, which are managed by his/her Citizen ID device. The Citizen ID knows which pseudonym and encryption key to use when logging into different systems. If an attacker breaks into one system, the secure area that he/she can gain access to is highly limited, and he/she cannot break into any other systems. Because the system also

does not store any identifying information beyond the pseudonym, the attacker could not identify whose data they had obtained, making the attack unsuccessful.

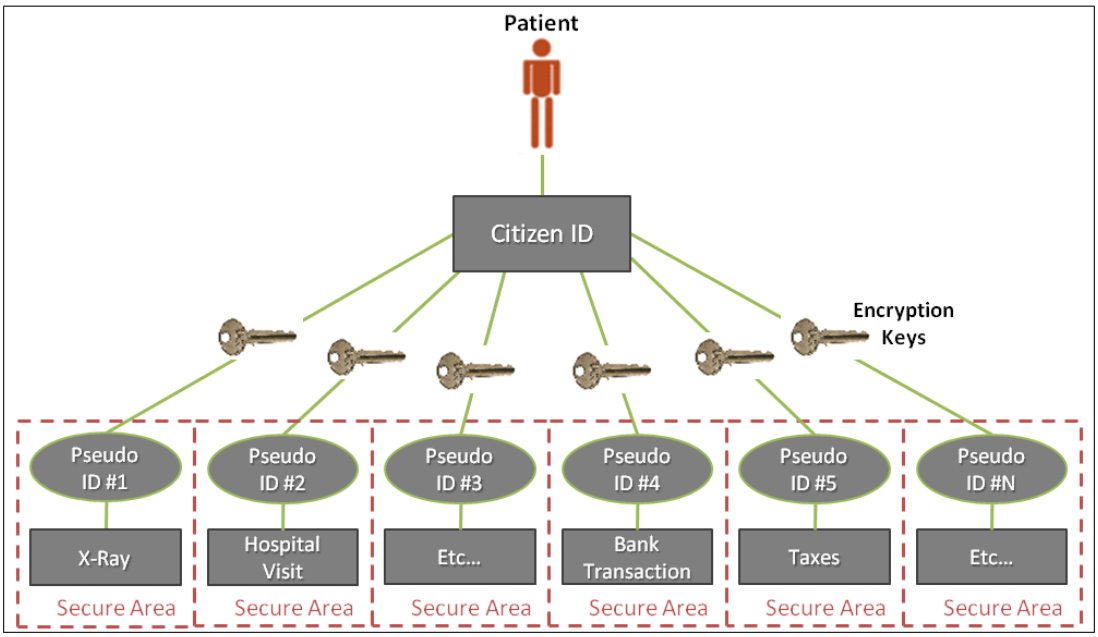

Figure 21: Use of a Pseudonym System – No storage of identifying information and division of secure areas

The Digital Signature's contract is renegotiated every 3 or 5 years. Mortensen of DI ITEK hopes that the next version will use pseudonyms and would like a system that will create multiple signatures for one person to use for different functions. Ideally, Mortensen would like to completely replace the CPR numbers for all citizens with pseudonyms.

4.6.2 Role-Based Access Control

Current EHR systems in hospitals log the patients that a provider accesses and punish providers when they illegally access data. However, any doctor can access any patient's data if he/she chooses to. Figure 22 illustrates the current amount of access doctors have to patients' medical information.

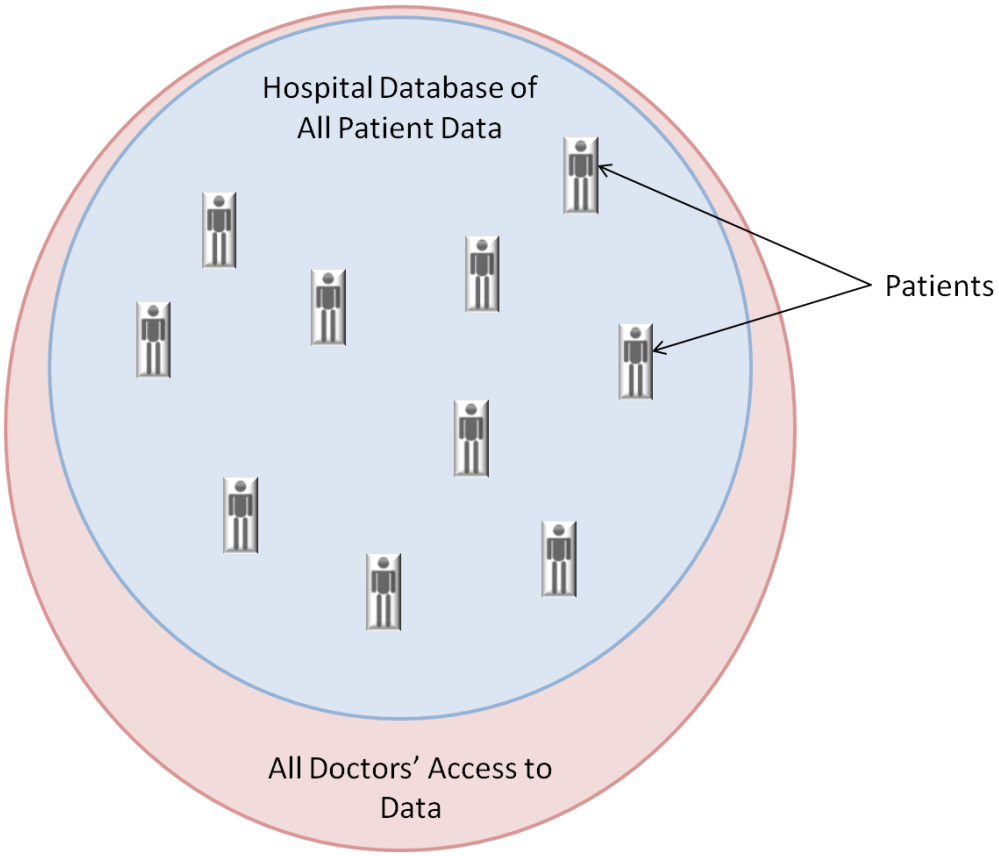

Figure 22: Current Patient Data Access given to Doctors

Henning Mortensen believes that the use of role-based access control in Danish health IT systems will allow systems to restrict access of patient data to relevant providers. In a role-based access control system, practitioners would be limited by the system in whose data they can access based on who they are treating. Mortensen would like to limit the current level of data exposure as he finds it unnecessary and unsafe. Figure 23 illustrate an example of role-based access control in a hospital. Doctor A, Doctor B, and Doctor C have access only to the medical data of the patients they are in charge of. Sometimes more than one doctor can be in charge of one patient as is the case with one of the patients in the diagram who is under the care of both Doctor A and Doctor C. All doctors lose access to a patient's data once the patient is discharged from the hospital. If in case of an emergency, a doctor needs to treat a patient that is not under his/her care, he/she can perform an emergency access of the patient's data. When a doctor performs an emergency override to access patient data, the override is logged so that proper authorities can question the doctor later in order to deem whether his/her actions were legitimate.

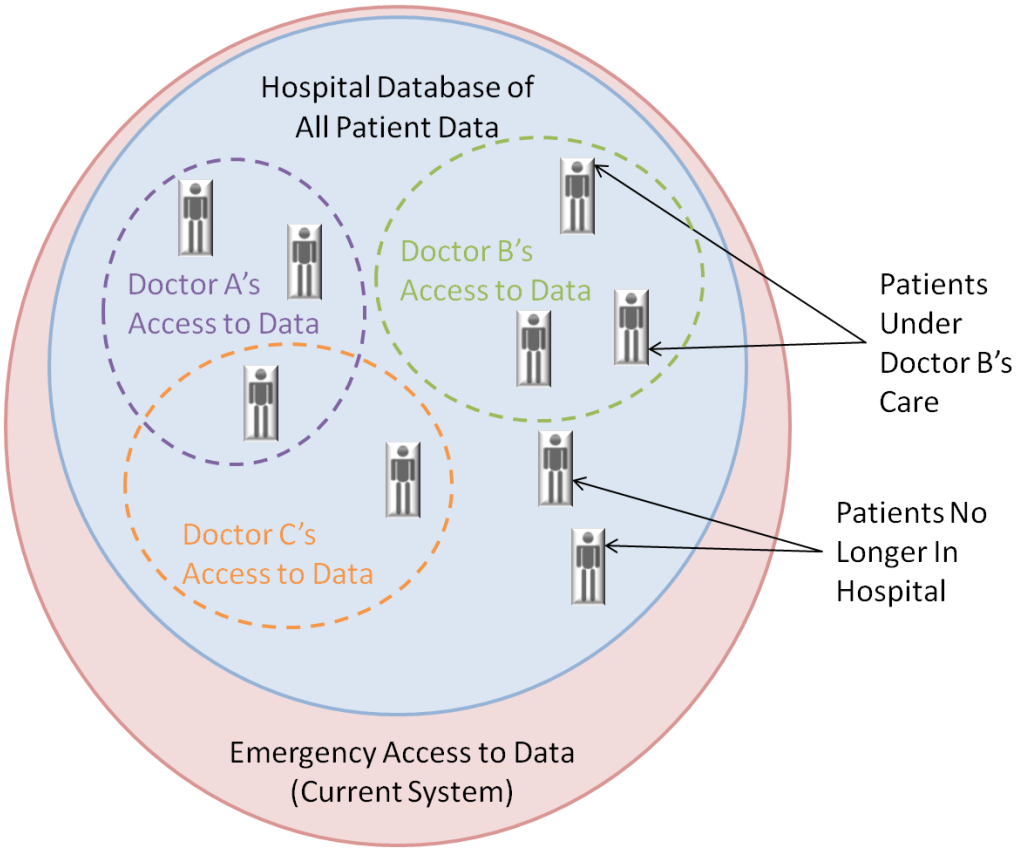

Figure 23: An example of a Role-based Access System in a Hospital

The role-based access system illustrated in Figure 23 follows the QUiPS model for a successful EHR system illustrated in the background of this report, Section 2.2.4 Potential Risks to Stakeholders, Table 3. This model is a four-step guideline for successful deployment of EHR systems, and the second factory refers to usability, which advocated for the different level of accessibility based on the role of the medical provider. Lab technicians, pharmacists, doctors, and nurses all need to look at different information about the patient in order to perform their duties, just as the role-based system proposed.

4.6.3 Use of Smaller, Modular Systems

The large, centralized systems currently used tend to be "one size fits all" solutions that attempt to address all of its users' issues. However, because these systems are so large, it takes a long time to change them and it is difficult to make small changes that can adapt to problems as they arise. Security systems need to change and evolve rapidly in order to stay effective, and a system must be able to support that. In addition, the use of fewer, large systems means that, as consumers, users have less choice over which systems they can use. Figure 24 shows that in a centralized, singular system, all subsystems needed in an EHR system are created by the same vendor. While this is relatively convenient to implement,

upgrades to the system can only come through this vendor, and other vendors' systems cannot be used in conjunction with this system.

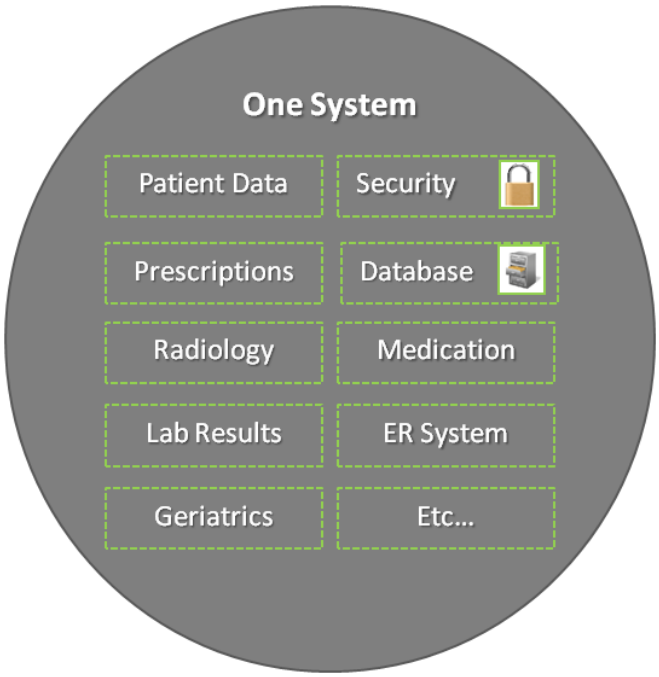

Figure 24: Current Large Singular EHR System

Frederik Endsleff is in support of large systems. He believes that increased use of standards will allow vendors to more easily make their systems interoperable with the region-wide EHR system, the DHE, which the Capital Region uses. This will allow vendors to make their systems more useful by being easier to implement, and also give hospitals a wider variety of choice in vendors when choosing a system. However, the DHE itself is a large, centralized system, which means that hospitals are locked into using it anyway.

Engberg, on the other hand, believes that systems in use today lack adaptability to healthcare practitioners' different needs. Practitioners, such as doctors and nurses, work best with systems that are designed specifically for use in their work environment and field. Doctors often complain when first using new systems, as they must adapt to the system itself. Smaller systems can generally be more easily configured to suit their needs, which would lower how much a doctor must change his/her workflow. Smaller, modular systems can also scale up to larger overall sizes better, as new systems can be added more easily when upgrades are needed. This contrasts with a large system, which must be entirely changed in order to be upgraded.

Pernille Bjørn, a professor at the IT University of Copenhagen, has been involved in a research project that is focusing on understanding the needs of the doctors and nurses using the electronic artifacts. Her research supports Engberg's claims that modular, customizable systems will be advantageous. Most clinical IT systems use a one-size-fits-all solution and it is not ideal for the different wards in a hospital. Bjørn and her group work on customizing these generic systems in order to make sure that each clinical system works with the respective ward. She found that when designing IT systems, sometimes the system is not organized for the work environment. Thus, people have to adapt to the way the system functions and not the other way around. For example, in both pediatric and adult ERs, doctors and nurses must check for unblocked airways, breathing, and circulation. However, the order in which these are checked is critical and differs between adults and children. It is important the IT systems in both ERs are specialized for the order in which they treat the patient. Therefore, in any new health IT solution, Bjørn believes that developers should observe the work environment before designing the system and ensure that the system can be changed to handle future scenarios.

Figure 25 shows that in a modular system, a number of small, interoperable systems are used together. Systems can be added or removed as needed, and can come from different vendors. Each system must only be interoperable with the security system and database, which can both also be changed as needed. Though this is just a potential solution, there is a technology in support of this that is already being used, Health Data Integration (HDI) technologies. An example of this can be found in the background chapter of this report, Section 2.1.3 Examples of EHR Technology, Figure 7.

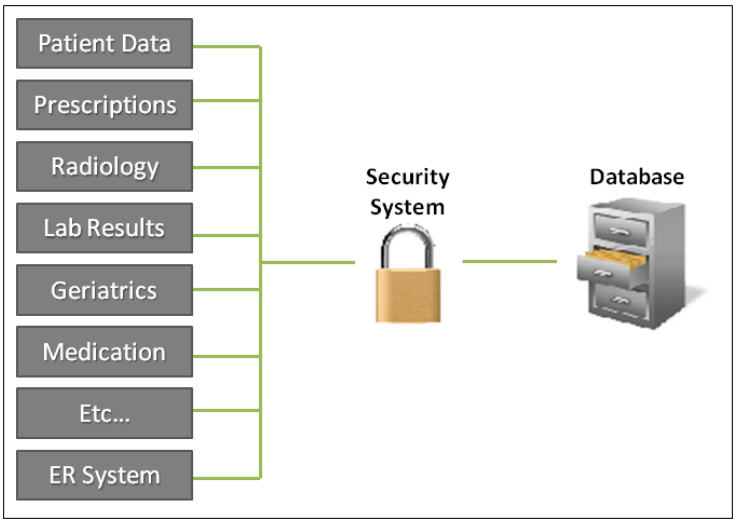

Figure 25: Small Modular Systems

4.6.4 Wider Use of Privacy Impact Assessment (PIA)

Høyrup and Mortensen would like to see all EHR developers to conduct more Privacy Impact Assessment (PIA) when developing EHR systems. The reasons why project or service developers would perform a PIA are that 1) it is required by law, 2) there is a large public concern, and 3) the developers want to make their product and service as small of a privacy risk as possible. A PIA is conducted for a project or an initiative of a company. PIA involves identifying all the privacy risks that could occur during each stage of the project or initiative and creating countermeasures to reduce risk as much as possible. This ensures that the product or service will not have any avoidable privacy risks. While conducting a PIA, the project or service developers need to think not only about the privacy of the end-users, but also about partner organizations. An organization should change the product or service to mitigate any risks that are identified by the PIA. A PIA also creates the need for communication between developers and the management personnel which creates a product or service that includes input and ideas from people of various backgrounds.

4.6.5 Feasibility for Implementing New Solutions

The biggest barrier to new solutions being implemented is the cost. Mortensen does not think it is a practical idea to tear down the current health IT infrastructure and completely rebuild it around the standards as it will be too expensive. Therefore, work must first be done to convince the public, as well as politicians and healthcare organizations that the change is needed. In the long run, the systems and the security in place will not adapt with new technologies, and always having to update entire systems will also become very costly and ineffective. There are solutions in place now that can improve the future of health IT.

Though implementing systems that are based on privacy by design will be very difficult for the healthcare sector, implementing pseudonyms on a small scale is the first logical step. The problem occurs when a patient gets hospitalized and there are many doctors and nurses who want to know the patient's medical information before administrating any treatment. To test a pseudonym system, a pilot program should be done on a small section in the healthcare sector.

Using smaller, modular systems will also require a large shift in how health IT systems are developed, and will probably take a longer time before they are widely used, since a switch away from current large systems will be difficult. The first step in implementing modular systems would be to improve healthcare data standards in order to improve interoperability. Modular systems naturally require a large amount of interoperability, since they will not work unless systems can share data. The more effective the standards are, the easier it will be for vendors to build smaller systems that can interconnect.

Role-based access control systems would not be as difficult to implement, since these systems can be built on top of existing systems rather than having to replace current ones. Implementing these systems is largely a matter of motivating the industry to take privacy into account and acknowledge current privacy issues. Using Privacy Impact Assessments is also a matter of motivation – if emphasis is placed on privacy issues, it would not be difficult to begin applying PIAs when creating new systems. Applying PIAs to current systems, however, could mean that major changes must be made and would be more difficult.

Many different parties are proposing and implementing possible solutions and improvements for health IT. Engberg clearly has the most revolutionary ideas and has excellent thoughts on how to improve patient privacy, but because most of the government groups believe that patient privacy is currently adequate, it will be difficult to convince them that an entirely new type of system is needed. Mortensen also agrees with many of Engberg's ideas, but has a more realistic view of how to implement them. It is interesting to note that Endsleff of KIT actually thinks that trust-based systems would be more useful, as this change would aid interoperability, but at the cost of lowering patient privacy. The idea of using smaller systems also seems to go against the wishes of government groups such as Digital Health and KIT, who have long held the belief that a larger, off-the-shelf solution will be best.

Chapter 5: Conclusions

The findings have indicated that EHR systems in Denmark cause different issues for different consumers. The risks and frustrations faced by the patient differ from those faced by healthcare providers. Organizations within Denmark differ in that some focus on patient issues and others focus on provider issues. The conclusions are broken up accordingly into issues faced by patients and issues faced by healthcare providers.

5.1 Issues Faced by Patients

Privacy of medical data is a bigger issue affecting patients than interoperability between medical systems. Important issues affecting patients are their lack of concern for privacy of their medical data, use of the vulnerable CPR number, widespread use of centralized systems, difficulties in accessing health IT systems, and lack of restrictions on healthcare providers when accessing patient data.

Danish "Trusting" Mindset Risks Compromising Medical Data

Due to the national culture and mindset, the Danish patients are not very concerned with privacy and are very trusting of the Danish government decisions about the storage and security of their medical information. Most Danes do not know the privacy options they have concerning their data and are uninformed about where their medical data are stored in many of the medical registries in Denmark. This creates more access points for persons with malicious intent to obtain information.

Danish CPR Poses a Large Security Threat

The Danish's Personal Identification Number (CPR) is an integral part of any Dane's life. However, any person's CPR number is easy to obtain and sensitive information, such as certain medical information, can be accessed using it.

Threats of Centralized Systems

The use of large, centralized health IT systems raises privacy concerns for patients and creates general security risks. Furthermore, larger systems amplify the threats caused by the CPR, as an attacker can gain more information by breaking into fewer systems.

Technology is Difficult for Certain Patient Groups to Use

The transition to using technology associated with EHR is difficult for patients of certain demographical groups. Patients who are not tech-savvy have a difficult time understanding how to use a computer or other devices properly to access their medical information. Some patients can also have difficulty remembering the authentication information.

Lack of Restriction on Patient Data: Illegal to Access but Technically Available

The findings indicate that a doctor may not legally be able to view a patient's medical data on past sicknesses or surgeries, but he/she can access a patient's medication history without consent, which gives him/her insight into what sicknesses and surgeries caused the patient to take a certain medication. In addition, technologies that can restrict access to medical information are not legally required of systems and therefore not utilized. The punishment system also places unnecessary burden on providers to know exactly when access of data is legal or illegal.

5.2 Issues Faced by Healthcare Providers

Interoperability of medical data is a bigger concern for providers than patient privacy. However, privacy is still a concern for providers, as they have a responsibility to patients to keep their data secure. There are also some legal issues that providers face. The important health IT issues affecting healthcare providers are a lack of strict standards, large and inflexible systems, data accessibility laws contradicting treatment requirement laws, and confusion from constantly changing laws on providers' rights and responsibilities.

Lack of Strict and Effective Data Standards

The implementation of data transfer standards in many health IT systems in Denmark is inadequate and restricts hospitals' choice when buying systems. Various implementations of the same set of standards can differ enough to cause systems that use the same standards to not be interoperable. In addition, large system vendors can overlook standards and create proprietary systems that are not easily interoperable with other vendors' systems.

Large Systems are Inflexible for Providers' Use

The large, universal systems that are commonly used as health IT solutions are difficult to customize when addressing healthcare providers' specific needs. Large systems also take longer to upgrade, since the entire system must be upgraded all at once by the vendor.

Data Accessibility Laws Contradict Treatment Requirement Laws

Healthcare providers other than doctors, such as nurses, cannot access patient records even though they may be the first to treat a patient. This causes issues for the nurses because in some instances they cannot properly treat a patient without data that only a doctor can access.

Additions and Stipulations to Laws Cause Confusion for Providers

As Danish laws on electronic data accessibility have become more complicated, confusion on the part of healthcare providers has occurred. In some instances, this causes providers to care

less about privacy and security issues and in other instances, to be wary and not access data because the provider is unsure of the repercussion.

Chapter 6: Recommendations

The following recommended solutions address the issues raised. Many of the proposed solutions are relevant to more than one issue. In particular, the use of pseudonyms and role-based access systems would significantly improve patient privacy. Greater focus on effective data standards would help solve interoperability issues. The use of smaller, modular systems in place of large systems will make systems more user-friendly.

Spread Awareness about Patient Privacy Issues

Patients should be made more aware of the significant risks to their privacy so that they can take the proper precautions. Public awareness of privacy issues will also motivate both the industry and legislators to focus more on keeping patient data private.

Implement Smaller Modular Systems

Using smaller, more modular health IT systems instead of larger, universal systems will be more flexible to fit both healthcare practitioners' and hospital administrators' needs. Upgrades to specific parts of systems can happen more rapidly as well. This is very important for security technology, which must be as modern as possible in order to be effective.

Design Systems with Users in Mind

If vendors work directly with users when creating systems intended for both patients and providers, it will ensure that new systems are of the highest quality and that their systems are actually usable and effective for their users. Using modular systems will also give providers wider choice in selecting the most effective system for their needs.

Use Pseudonym Systems for Patient Identification

The use of pseudonyms for identifying patients in all IT systems will vastly reduce the significant privacy risks to citizens caused by the Danish CPR number. Pseudonyms will allow patients to keep control of their data instead of relinquishing control to the owner of the system. Pseudonyms also naturally support the use of small modular systems and discourage the use of large, centralized systems.

Use Role-Based Access Control to Prevent Illegal Access of Data

Using role-based access control in systems can allow healthcare providers to only access the data of the patients they are currently involved in treating. This will help prevent providers from illegally accessing data. Providers will also no longer have the burden of interpreting potentially confusing laws and deciding whether or not they can legally access a patient's data and can instead rely on the system.

Create Stricter Data Standards with Less Room for Differing Interpretations

Using stricter interpretation of standards would promote interoperability between systems and empower smaller vendors of health IT systems, creating more competition in the market. Stricter standards would also make small modular systems more feasible.

Aid Vendors in Adhering to Data Standards

An organization that helps vendors properly adhere to data standards would reduce differing implementations and encourage vendors to ensure that their systems are interoperable with other systems. This would be much more useful than current organizations, which only check to see if vendors are properly following standards and do not offer any help.

Clarify Contradicting Laws Relevant to Health IT

A revision of the laws related to health IT issues to remove contradictions would reduce complicated situations in which a healthcare provider must decide which law to follow at what times. If possible, a compilation of law and regulations of privacy and interoperability pertaining to health IT into one document will help healthcare providers to quickly look over relevant legal information if necessary.

These solutions vary in how difficult and time-consuming they will be to implement. The use of pseudonyms in security systems, although effective, will likely take a long time to gain support, as it requires a major change in how security issues are approached not only in health IT, but in all sectors of IT as well. Spreading awareness of privacy issues in the public is also likely to be difficult, since it will require a shift in the trusting mindset of Danish society. Government-based organizations will need to put more focus on better privacy solutions. Other solutions, such as improving standards and implementing role-based access control, are much shorter-term and could be implemented within a few years. These recommendations provide a set of general guidelines on how to improve the quality of health IT systems for consumers in Denmark, and should be considered by both the government and the industry as health IT moves forward.

References

Anderson, James G. (Department of Sociology and Anthropology, Purdue University, 700 West State Street, West Lafayette, IN 47907-2059,United States).Social, ethical and legal barriers to E-health. *International Journal of Medical Informatics, 76*(5-6), 480-483.

Ash, J. S., & Bates, D. W. (2005). Factors and forces affecting EHR system adoption: Report of a 2004 ACMI discussion. *Journal of the American Medical Informatics Association, 12*(1), 8-12. doi:10.1197/jamia.M1684

Atienza, A. A., Hesse, B. W., Gustafson, D. H., & Croyle, R. T. (2010). E-health research and patient-centered care examining theory, methods, and application. *American Journal of Preventive Medicine, 38*(1), 85-88. doi:10.1016/j.amepre.2009.10.027

Barrows, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association, 3*(2), 139-148. doi:10.1136/jamia.1996.96236282

Bernstein, Knut (MEDIQ, Copenhagen, Denmark), Bruun-Rasmussen, M., Vingtoft, S., Andersen, S. K., & Nhr, C. (2005). Modelling and implementing electronic health records in denmark. *International Journal of Medical Informatics, , MIE 2003, 74*(2-4)

Blobel, B. (2004). Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics, 73*(3), 251-257. doi:DOI: 10.1016/j.ijmedinf.2003.11.018

Blobel, B., & Pharow, P. (2008). Analysis and evaluation of EHR approaches. Studies in Health Technology and Informatics , 359-364.

Bloomrosen, M., & Detmer, D. (2008). Advancing the framework: Use of health data--a report of a working conference of the american medical informatics association. *Journal of the American Medical Informatics Association : JAMIA, 15*(6), 715-722. doi:10.1197/jamia.M2905

Bos, J. J. (. H.Digital signatures and the electronic health records: Providing legal and security guarantees. *International Journal of Bio-Medical Computing, 42*(1-2), 157-163,.

Brailer, D. J. (2005). Interoperability: The key to the future health care system. *Health Affairs (Project Hope), Suppl Web Exclusives*, W5-19-W5-21. doi:10.1377/hlthaff.w5.19

Castro, D. (2009). Explaining international IT application leadership: Health IT (ITIF Publication). Washington, DC, United States of America: The Information Technology and Innovation Foundation.

Croll, P. R., & Croll, J. (2007). Investigating risk exposure in e-health systems. *International Journal of Medical Informatics, 76*(5-6), 460-465. doi:DOI: 10.1016/j.ijmedinf.2006.09.013

De Toledo, P. (., Lalinde, W., & , D. P.Interoperability of a mobile health care solution with electronic healthcare record systems. *Annual International Conference of the IEEE*

Engineering in Medicine and Biology - Proceedings, p 5214-5217, 2006, 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS'06,

Dobrev, A., Jones, T., Stroetmann, K., Vatter, Y., & Peng, K. (2009). *The socio-economic impact of interoperable electronic health record (EHR) and ePrescribing systems in Europe and beyond.* Bonn, Germany: European Commission, DG INFSO & Media.

Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: An informatics theory. *International Journal of Medical Informatics, 78*(12), 815-826. doi:DOI: 10.1016/j.ijmedinf.2009.08.006

Ferrara, F. M. (1998). The CEN healthcare information systems architecture standard and the DHE middleware.: A practical support to the integration and evolution of healthcare systems. *International Journal of Medical Informatics, 48*(1-3), 173-182. doi:DOI: 10.1016/S1386-5056(97)00123-8

Ford, E. W., Menachemi, N., & Phillips, M. T. (2006). Predicting the adoption of electronic health records by physicians: When will health care be paperless? *Journal of the American Medical Informatics Association, 13*(1), 106-112. doi:10.1197/jamia.M1913

Ford, E. W., Menachemi, N., Peterson, L. T., & Huerta, T. R. (2009). Resistance is futile: But it is slowing the pace of EHR adoption nonetheless. *Journal of the American Medical Informatics Association, 16*(3), 274-281. doi:10.1197/jamia.M3042

Gaffey, A. D. (2009). Communication and documentation considerations for electronic health records. *Journal of Healthcare Risk Management* , 16-20.

Gasch, B., & Gasch, A. (2010). Finding the right EHR : Your guide to electronic health records success /. *Chichester, West Sussex : Wiley-Blackwell,*

Goldschmidt, P. G. (2005). HIT and MIS implications of health information technology and medical information systems. *Communications of the ACM* , 68.

Gunter, T. D., & Terry, P. N. (2005, March 14). *The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions.* Retrieved from Journal of Medical Internet Research: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550638/

Hammond, W. E. (2005). The making and adoption of health data standards. *Health Affairs (Project Hope), 24*(5), 1205-1213. doi:10.1377/hlthaff.24.5.1205

Hansen, D. P., Pang, C., & Maeder, A. (2005). HDI: Integrated services for health data. Paper presented at the *Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on, , 9* 5554-5559 Vol. 9.

Hartlev, M. (2008). *Study of Legal Framework of Interoperable eHealth in Europe – Nation Profile Denmark.* Copenhaen, Denmark: European Commission Directorate General Information Society.

Häyrinen, Kristiina (University of Kuopio, Department of Health Policy,and Management.Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics, 77*(5), 291-304,.

Hill, J. W., & Powell, P. (2009). The National Healthcare Crisis: Is eHealth a key solution? *Elsevier Ireland* .

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? potential health benefits, savings, and costs. *Health Affairs (Project Hope), 24*(5), 1103-1117. doi:10.1377/hlthaff.24.5.1103

Hodge, J. G.,Jr, Gostin, L. O., & Jacobson, P. D. (1999). Legal issues concerning electronic health information: Privacy, quality, and liability. *JAMA: The Journal of the American Medical Association, 282*(15), 1466-1471. doi:10.1001/jama.282.15.1466

Huang, L., Chu, H., Lien, C., Hsiao, C., & Kao, T. (2009). Privacy preservation and information security protection for patients' portable electronic health records. *Computers in Biology and Medicine, 39*(9), 743-750. doi:DOI: 10.1016/j.compbiomed.2009.06.004

IT brings the Danish health sector together (2008)

Retrieved from Digital Health: http://www.sdsd.dk/~/media/Files/WoHIT/2009/WoHit%2005%2001%2009_2.ashx

Jensen, S. (2010, 1 28). Project Sponsor Interview. (S. Bhagat, D. Fontaine, & K. Gibson, Interviewers)

Jha, A. K., Bates, D. W., Jenter, C., Orav, E. J., Zheng, J., Cleary, P., & Simon, S. R. (2009). Electronic health records: Use, barriers and satisfaction among physicians who care for black and hispanic patients. *Journal of Evaluation in Clinical Practice, 15*(1), 158-163. doi:10.1111/j.1365-2753.2008.00975.x

Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., et al. (2009, March 25). Use of Electronic Health Records in U.S. Hospitals. *The New England Journal of Medicine* , 1-11.

Jha, A. K., Ferris, T. G., Donelan, K., DesRoches, C., Shields, A., Rosenbaum, S., et al. (2006, October 11). How Common are Electronic Health Records in the United States? A Summary of the Evidence. *Health Affairs- Web Exclusive* .

Kalra, D. (2006). Electronic health record standards. *Yearbook of medical informatics* , 136-144.

Kluge, E. H. (2004). Informed consent to the secondary use of EHRs: Informatic rights and their limitations. *Studies in Health Technology and Informatics, 107*(Pt 1), 635-638.

Kluge, Eike-Henner W. (Department of Philosophy, University of Victoria, Victoria,B.C.V.8W.3P.4, Canada).Secure e-health: Managing risks to patient health data. *International Journal of Medical Informatics, 76*(5-6), 402-406,.

Kwak, Y. S. (2005). *International Standards for building Electronic Health Record (EHR).* Kyungpook National University: Republic of Korea.

Lobach, D. F., & Detmer, D. E. (2007). Research challenges for electronic health records. *American Journal of Preventive Medicine, 32*(5, Supplement 1), S104-S111. doi:DOI: 10.1016/j.amepre.2007.01.018

MacDonald, R. (2001). Commentary: A patient's viewpoint. *BMJ* (322:283-287).

Maldonado, J. A., Robles, M., & Cano, C. (2001). Integration of distributed healthcare information systems: Application of CEN/TC251 ENV13606. Paper presented at the *Engineering in Medicine and Biology Society, 2001. Proceedings of the 23rd Annual International Conference of the IEEE, , 4* 3731-3734 vol.4.

Maloney, F. L., & Wright, A. (2010). USB-based personal health records: An analysis of features and functionality. *International Journal of Medical Informatics, 79*(2), 97-111. Retrieved from http://dx.doi.org/10.1016/j.ijmedinf.2009.11.005

Meeting the need for inter-operability and information security in health IT. (2008). *Washington : U.S.G.P.O.: For Sale by the Supt.of Docs., U.S.G.P.O.,*

Menachemi, N., Powers, T., Au, D. W., & Brooks, R. G. (2010). Predictors of physician satisfaction among electronic health record system users. *Journal for Healthcare Quality : Official Publication of the National Association for Healthcare Quality, 32*(1), 35-41.

Middleton, B., Hammond, W. E., Brennan, P. F., & Cooper, G. F. (2005). Accelerating U.S. EHR adoption: How to get there from here. recommendations based on the 2004 ACMI retreat. *Journal of the American Medical Informatics Association : JAMIA, 12*(1), 13-19. doi:10.1197/jamia.M1669

Miller, Amalia R. (Department of Economics, University of Virginia, Charlottesville, VA 22904,United States), & Tucker, C.Privacy protection and technology diffusion: The case of electronic medical records. *Management Science, 55*(7), 1077-1093,.

Milosevic, Z. (2006). Addressing interoperability in e-health: An australian approach. Paper presented at the *Enterprise Distributed Object Computing Conference Workshops, 2006. EDOCW '06. 10th IEEE International,* 39-39.

National Strategy for Digitalisation of the Danish Healthcare Service. (2007, December). Retrieved from Digital Health: http://www.sdsd.dk/~/media/Files/Strategi/Strategy_english.ashx

O'Connell, R. T., Cho, C., Shah, N., Brown, K., & Shiffman, R. N. (2004). Take note(s): Differential EHR satisfaction with two implementations under one roof. *Journal of the American Medical Informatics Association, 11*(1), 43-49. doi:10.1197/jamia.M1409

Porter, S., & American Academy of Family Physicians. (2004). Pilot project studies EHR implementation issues. *Annals of Family Medicine, 2*(4), 377-378.

Protti, Denis (Health Informatics, University of Victoria, BC, Canada), Johansen, I., & Perez-Torres, F.Comparing the application of health information technology in primary care in denmark and andalucía, spain. *International Journal of Medical Informatics, 78*(4), 270-283,.

Pruitt,Gina (Deloitte & Touche L.L.P.).Legal implications of electronic medical records. *Annual Quest for Quality and Productivity in Health Services Conference, ,* 17-24,.

Pyper, C., Amery, J., Watson, M., & & Crook, C. (2004). *Access to Electronic health records in primary care- a survey of patients' views.* Oxford: Med Sci Monit.

Ravizza, P., & Pasini, E. (2001). Electronic medical records: Medical and legal aspects, privacy, safety, and legal validity. [Informatizzazione della cartella clinica: aspetti medico-legali, privacy, sicurezza e validita legale] *Italian Heart Journal.Supplement : Official Journal of the Italian Federation of Cardiology, 2*(3), 268-286.

Ray, P., & Wimalasiri, J. (2006). The need for technical solutions for maintaining the privacy of EHR. Paper presented at the *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE,* 4686-4689.

Shields, A. E., Shin, P., Leu, M. G., Levy, D. E., Betancourt, R. M., Hawkins, D., & Proser, M. (2007). Adoption of health information technology in community health centers: Results of a national survey. *Health Affairs (Project Hope), 26*(5), 1373-1383. doi:10.1377/hlthaff.26.5.1373

Sidorov, J. (2006). It ain't necessarily so: The electronic health record and the unlikely prospect of reducing health care costs. *Health Affairs, 25*(4), 1079-1085. doi:10.1377/hlthaff.25.4.1079

Spil, T. A. (2007). Balancing supply and demand of an electronic health record in the netherlands; not too open systems for not too open users. *Proceedings of the 40th Hawaii International Conference on System Sciences.* Hawaii.

Sprague, L. (2004). Electronic health records: How close? how far to go? *NHPF Issue Brief / National Health Policy Forum, George Washington University* , 1-17.

Sprague, L. (2006). Personal health records: The people's choice? *NHPF Issue Brief / National Health Policy Forum, George Washington University, (820)*(820), 1-13.

Stanberry, Benedict A. (Avienda Limited, 63 Colchester Avenue, Cardiff, CF23 9YW, Wales,United Kingdom).Legal and ethical challenges of telemedicine and e-health. *Proceedings of SPIE - the International Society for Optical Engineering, 4912*, 47-66,.

Steven R. Simon MD MPH, M. L. (2008). *Electronic health records - which practices have them, and how are clinicians using them.* Boston, MA: Blackwell Publishing Ltd.

sunhed.dk. (2010). The Danish National e-Health Portal. *Open information as a strategic tool for healthcare imrovement* . Copenhagen, Denmark.

Terry, N. P. (2004). Electronic health records: International, structural and legal perspectives. *Journal of Law and Medicine, 12*(1), 26-39.

The Danish Health Act. (2010). Retrieved 2 3, 2010, from Danish Medicines Agency: http://www.dkma.dk/1024/visUKLSArtikel.asp?artikelID=11547
Walker, J., Pan, E., Jognston, D., Adler-Milstein, J., Bates, D., & Middleton, B. (2005). The value of health care information exchange and interoperability. *Health Affairs* , 10-18.

Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., & Middleton, B. (2005). The value of health care information exchange and interoperability. *Health Affairs,* doi:10.1377/hlthaff.w5.10

Whittaker, A. A., Aufdenkamp, M., & & Tinley, S. (2009). Barriers and Facilitators to Electronic Documentation in a Rural Hospital. *Journal of Nursing Scholarship* , 293-300.

Winkelman, W. J., & Leonard, K. J. (2004). Overcoming structural constraints to patient utilization of electronic medical records:: A critical review and proposal for an evaluation framework. *Journal of the American Medical Informatics Association, 11*(2), 151-161. doi:DOI: 10.1197/jamia.M1274

Yackel, T. R., & Embi, P. J. (2010). Unintended errors with EHR-based result management: A case series. *Journal of the American Medical Informatics Association, 17*(1), 104-107. doi:10.1197/jamia.M3294

Yu, W. D., & Chekhanovskiy, M. A. (2007). An electronic health record content protection system using SmartCard and PMR. Paper presented at the *E-Health Networking, Application and Services, 2007 9th International Conference on,* 11-18.

Zandieh, S. O., Yoon-Flannery, K., Kuperman, G. J., Langsam, D. J., Hyman, D., & Kaushal, R. (2008). Challenges to EHR implementation in electronic- versus paper-based office practices. *Journal of General Internal Medicine, 23*(6), 755-761. doi:10.1007/s11606-008-0573-5

Zsenits, B., Polashenski, W. A., Sterns, R. H., Brown, D. R.,4th, & Moheet, A. (2009). Systematically improving physician assignment during in-hospital transitions of care by enhancing a preexisting hospital electronic health record. *Journal of Hospital Medicine (Online), 4*(5), 308-312. doi:10.1002/jhm.401

Appendix A- Glossary

Anonymity – The state of being unidentifiable, which empowers data subjects to refuse to supply data or to restrict identifiers.

CEN – European Committee for Standardization

Clinical IT – Synonymous with health IT

Confidentiality – The control of data disclosure.

CPOE – Computerized Physician Order Entry

Decision-support tools – Tools that analyze machine-organized data in order to provide clinicians and patients with alerts, reminders, and other real-time decision aids.

eHealth – Term for healthcare practice which is supported by electronic processes and communication.

EHR – Electronic Health Record

EMR – Electronic Medical Record [Refer to EHR]

EPR – Electronic Patient Record [Refer to EHR]

ETP – Electronic Transmission of Prescriptions

GP – General Practitioners

HDI – Health Data Integration

Healthcare Providers – includes doctors, nurses, technicians, and hospital administrators.

HL7 – Health Level 7

HPCs – Healthcare Providers

Integrity – The validation and protection against unauthorized modification of data to ensure its security.

Interoperability – Communication between independent health IT systems.

ISO – International Standards Organization

NHIN – Nationwide Health Information Network

PHR – Personal Health Record

Privacy – The control of collection of information.

SDSD – Connected Digital Health in Denmark

Security – The restriction of data to authorized parties.

Telemedicine – The remote practice of medicine through the exchange of clinical information; patient and providers are separated geographically.

Appendix B – The Role of Forbrugerrådet

Forbrugerrådet (Danish Consumer Council) is a non-profit, independent organization that actively fights for the rights of the everyday consumer in Denmark. It is unaffiliated with any private organization or political body, and as such acts solely in the interests of consumers. Formed in 1947, the Council has grown into a politically strong organization containing members of 25 smaller Danish organizations that cover a very broad range of consumer issues. Trade unions, educational groups, and environmental groups are only a handful of the people involved in the Council. The DCC has representatives on over 200 different Danish committees and has a staff of about 60 (www.forbrugerraadet.dk).

The Council is a very influential organization in Denmark that affects Danish policy every day. Because it acts solely in the interests of the consumer, they are seen as protectors of the average person against larger corporations and political bodies (Jensen, 2010). It helps finance and advise consumers in legal cases when they have complaints about products and services. The Council publishes the trusted consumer magazine *Tænk* ("Think") 10 times a year, which reviews and provides test reports all types of new consumer products. The Council is also active on the international level in various ways. It has representatives in the European Consumer Organization (BEUC) and Consumers International. The BEUC gives the Council a voice in the European Union, and Consumers International allows the organization to deal with the United Nations, World Health Organization, and World Trade Organization (www.forbrugerraadet.dk).

Involvement in Health IT

Forbrugerrådet's senior health advisor, Sine Jensen, is concerned with the state of Denmark's health IT. It is commonly stated that Denmark is a leader in health IT, but Sine is unsure of what areas Denmark actually excels in and even has doubts to whether or not Denmark is a leader at all (Jensen, 2010). Denmark has a very large number of hospitals, so it is difficult to assess the state of IT across the entire country.

The Council's primary interest in this domain is in gathering more knowledge about the overall state of health IT in Denmark, and to identify areas for improvement in order to discuss the issue politically. This information could potentially lead to legislation that improves the quality of healthcare for consumers. The Council, presently, is most interested in the privacy of health IT systems and the interoperability between each of the systems used, as it feels these affect consumers using EHR systems the most (Jensen, 2010).

Interest in Privacy

Privacy of health information for patients is one of Forbrugerrådet's priorities for health IT systems. The primary issue is that sensitive personal health data can sometimes be accessed too easily and without the patient's consent using EHR systems. In 2008, the Danish Health Act allowed the Danish Medicines Agency to keep a database of patients' personal electronic medicine profiles (The Danish Health Act., 2010). These profiles include a patient's prescriptions, medicinal purchases, and other relevant health information. While it is useful to have such information in a centralized database, the DCC believes that the regulations for who can access a patient's information are somewhat lax. Patient information can be distributed at times without the patient's consent (Jensen, 2010).

Interest in Interoperability

Interoperability between hospitals is another of the Council's priorities. If a patient has to switch healthcare providers or use a new hospital, lack of interoperability might cause critical health information to be unavailable, affecting patient treatment. Enabling systems to communicate with each other can also reduce inconvenience and confusion for end users by reducing cases such as duplicate prescriptions being filled out. Interoperability has been shown to be an essential component in an effective and beneficial EHR system (Kalra, Electronic health record standards, 2006) (Dobrev, Jones, Stroetmann, Vatter, & Peng, 2009).

Appendix C – Relevant Health IT Standards

CEN Communications Standard EN 13606

The European Committee for Standardization (CEN) created a preliminary standard for EHR systems in 1999 called ENV 13606. It has been revised into the much more definitive EN 13606, which covers five specific areas: a reference model for electronic messages, a model for message syntax, a list of terms and archetypes, security measures, and message exchange models. The reference model has been adopted under the International Standards Organization, (ISO) and the first two parts are interoperable with HL7 standards, which will be discussed in the next section (Blobel & Pharow, 2008). Due in part to these reasons, EN 13606 has received worldwide attention and is a strong choice for a useful standard (Kalra, 2006).

Health Level 7 (HL7)

Health Level 7, formed by the United States in March 1987, is both an organization that creates standards for electronic information exchange and the name of the set of standards itself. It was created initially for use by the U.S.'s health insurance companies. It has since grown into international use in other sectors and has gone through two major revisions up to the most modern Version 3. HL7 Version 2 is still the most common and sees widespread international use, but is not scaling to meet health IT's needs. Version 3's features include a Reference Information Model, a document that strictly defines EHR message content, and a Clinical Document Architecture that defines message structure. Version 3 is very similar to the CEN 13606 standard, and a method for allowing systems using the two standards to communicate has been developed. HL7 also has an EHR System Functional Model, which specifies what functionality EHR systems should implement in order to be standardized (Kalra, 2006) (Kwak, 2005). HL7's standards have been integrated under the ISO TC215 standard (Blobel & Pharow, 2008).

OpenEHR

In 2000, the University College London and Ocean Informatics formed the openEHR Foundation, which has created an open-source set of EHR standards. An open-source project allows anyone, under license, to contribute and assist in development and creation. The main advantage of open-source is that a larger number of contributors assist with the project. openEHR uses the dual model approach described on Page 11, works with HL7 and EN 13606 to ensure maximum interoperability, and is moving towards becoming the most complete internationally available set of standards (Kalra, 2006).

Appendix D – Project Research Questions

In order to get the most out of each interview, we must establish what questions our project has set out to answer. These questions are not necessarily the exact questions we ask the interviewee but they should be the basis of the interview questions. The following are our research questions and they stem from the main problem with health-IT: the balance between privacy and interoperability.

What problems do the consumers of health IT – both patients and healthcare practitioners – face that arise from Denmark's current health IT systems?

- What are the different organizations involved in Denmark's health IT infrastructure?
    - How do the organizations interact with each other?
    - How are doctors, nurses, and other practitioners involved with the organizations?
    - How do the organizations interact with patients?
- Why should patients worry about privacy of their data?
    - What patient information is currently gathered by the EHR systems used in Denmark?
        - How much of the accessible data is not needed to treat a patient?
        - How do privacy laws dealing with the gathering of patient information affect the gathered data?
    - What are the various security measures and systems (i.e. digital signature, NemID) used in Danish health IT?
        - How do the systems keep patient data private?
            - Who is given access to patient data, and how does the system ensure that only these parties have access?
            - If the systems are breached, what information can be accessed?
        - What risks are introduced to the consumer?
- How does interoperability between health IT systems affect patients?
    - How easily transferrable is patient data between systems?
    - What standards are in place for interoperability between systems?
        - How are these standards enforced?
    - How easy is it to transfer patient data between different regions?
        - Looking into the future, if the 5 regions of Denmark are to be phased out, how will this affect the interoperability across the state?
    - As systems are made more and more interoperable, how can Denmark's health IT organizations continue to ensure patient privacy?
- How does the current legislation on healthcare and health IT affect the quality of the systems?
    - How does it affect patient privacy?
    - How does it affect interoperability between systems?

    - If there are any laws that create problems in health IT, how can they be changed to solve the problems?
- What knowledge should be provided to both practitioners and patients in order to use Denmark's health IT systems most effectively?
    - What do patients need to know when using the systems?
        - How should patients be informed?
    - What do practitioners need to know when using the systems?
        - How should practitioners be informed?
- What actions can the different health IT organizations in Denmark take in order to improve the current health IT systems for both healthcare practitioners and patients?
    - How can the current systems be improved for the different consumers?
        - What potential risks do the consumers face in the future if the current systems are not upgraded?
    - Is it necessary and feasible to propose an entirely new system?
        - What changes would this new system make for the different consumers?
        - Why would it be an improvement?

Appendix E - Interview Tree and Interviewees' Job Titles

Figure 26 is the list of interviewees we have contacted. They have been organized according to who gave us their contact information, using the snowball method. A detailed list of each interviewee and their job titles can be found in Table 8.

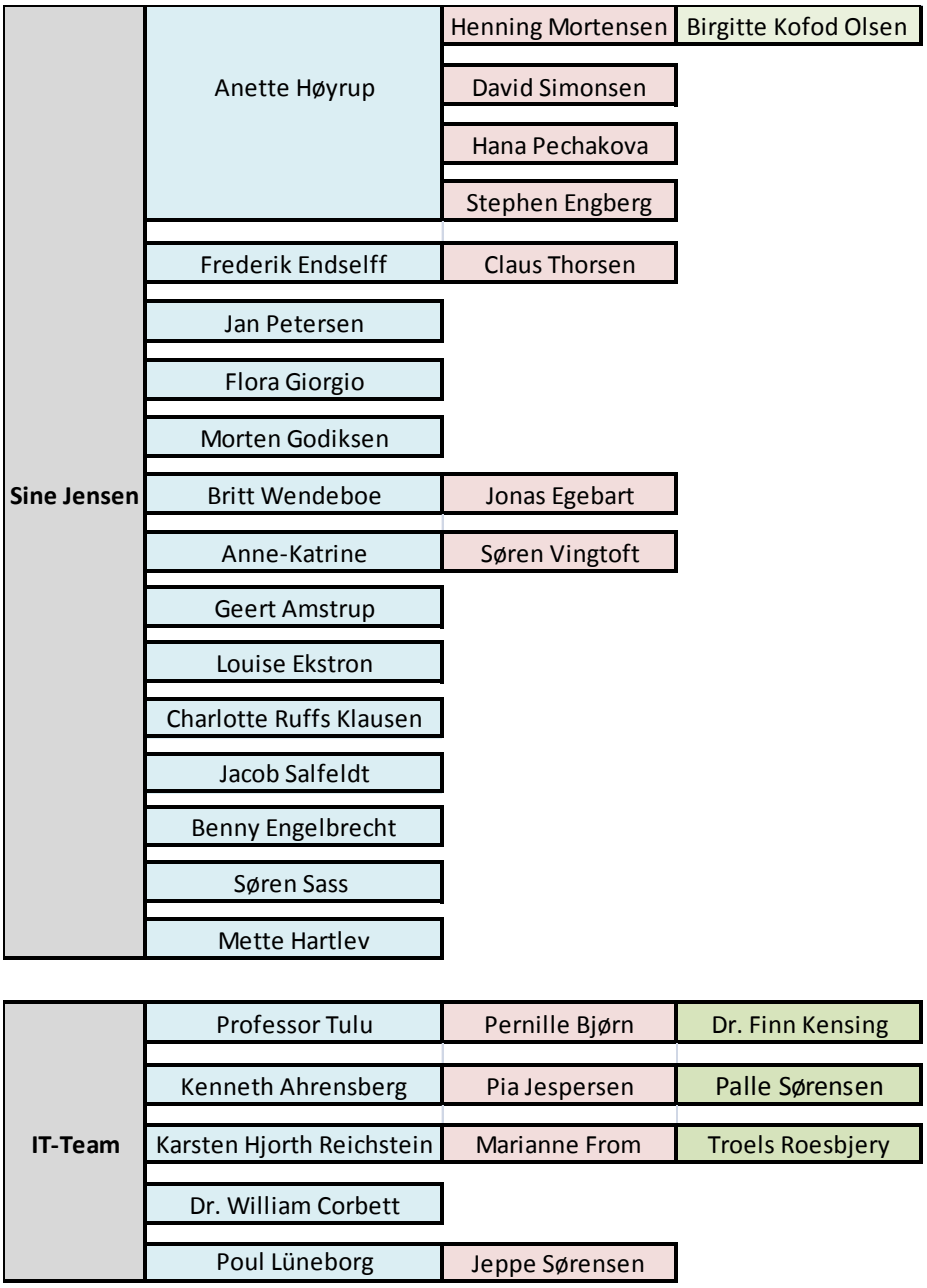

Figure 26: Interviewees and Contact Sources Illustrating the Snowball Technique

Table 8: List of Contacts and His/her Job Titles

Contact's Name	Job Title
Dr. William Corbett	VP of Community Practices for UMass Memorial Health Care
Prof Bengisu Tulu	Professor of Management Information Systems at WPI
Sine Jensen	Senior Health Advisor at Forbrugerrådet
Kenneth Ahrensberg	Special Advisor at Connected Digital Health in Denmark
Morten Godiksen	Communications and Network Manager at sundhed.dk
Anette Høyrup	Lawyer, Senior Advisor in the Privacy Department at Forbrugerrådet
Frederik Endsleff	Teamleader at Region Hovedstaden - the Capital region KIT
Marianne From	Head of Clinical IT Department at Rigshospitalets
Pia Jespersen	Technical Consultant at Connected Digital Health in Denmark
Stephen Engberg	CEO and founder of PriWay
Pernille Bjørn	Professor of Computer Science at IT University of Copenhagen
Brit Wendeboe	Staff member at Dansk Selskab for Patientsikkerhed (DSPS)
Henning Mortensen	Chief Consultant at ITEK (IT & telecommunication company)
Jan Petersen	Chief Consultant of MedCom
Geert Amstrump	Advisor at the Danish Medical Association
Flora Giorgio	Works for the EU Commission and works on health IT issues
Troels Roesbjery	IT staff member in the psyciatric ward in Rigshospitalets
Palle Sørensen	Works for the Danish Ministry of Science
Finn Kensing	Professor of Computer Science at IT University of Copenhagen
Søren Vingtoft	Consultant at Unit of Clinical Quality, Capital Region
Hanna Pechakova	Works for the EU Commission on PET solutions in Europe
David Simonsen	Project Manager for WAYF (database for students)
Claus Thorsen	Works for Koncern IT of the Capital Region concerning Privacy
Anders Bortne	Communications Consumer Policy at Norwegian Consumer Council
Bengt Ingerstam	Chairman of the Swedish Consumer Coalition
Louise Ekström	Health Expert at the Swedish Consumer Coalition
Mette Hartlev	Lawyer at Copenhagen University, works on healthcare law
Jonas Egebart	Doctor with expertise in patient safety and health IT
Charlotte Ruffs Klausen	Head of the Political Department of the Danish Diabetes Association
Jacob Salfeldt	Advisor at the Danish Medical Association
Benny Engelbrecht	Member of the Parliament for the Social Democrat Party
Søren Sass	Chief Consultant at Danish Nurses Organisation
Birgitte Kofod Olsen	Coporate Social Responsibility (CSR) Consultant at Tryg Vesta
Poul Lüneborg	Lawyer, Specialization in Law Related to the Blind
Jeppe Sørensen	Legal Health Policy Advisor at the Disabled Peoples Organisations Denmark