Enabling Patients Online Access To Their Health Records

Consequences, Hindrances and Opportunities

Uppsala University, IT in Society

Rose-Hulman Inst. of Technology, Computing in a Global Society

2009-03-23

Table of Contents

Abstract

This paper is designed to provide a detailed assessment of the issues concerning the creation of a perceived online medical record system called the Online Health Account, giving the patient free and direct access to his or her medical record. The paper examines the economic and ethical implications of the introduction of such a system, as well as development and security challenges.

The research has been performed by an international academic group over a period of four months. The research provides an analysis of these topics and, where possible, it suggests solutions. It hopes to provide a clear roadmap to implementation. The authors have performed interviews, worked in collaboration with healthcare professionals and researched related projects in the area.

The report is presented as a scenario that describes the interaction with the Online Health Account as the patient is diagnosed and receives treatment. Issues such as security, accuracy of medical records and legal prerequisites are investigated at a national level in Sweden in particular and with an international perspective when it comes to legislation.

The authors have found that there is a potential for an improved relationship between the care provider and the patient. Patients will be able to get a better understanding of the health care process and learn more about issues related to their health which in turn will lead to a more efficient ward of higher quality.

The service under consideration will most certainly function as an accelerator in the demand for creating an infrastructure of systems which are able to communicate health record information with each other in a secure and accurate way.

There are good reasons to believe that deployment of an online Health Account will be an important test bed for new legislation and most probably an example that will be followed closely also at an international level.

1. Introduction

This paper is designed to provide a detailed assessment of the issues concerning the creation of an online patient medical record system. The research examines the economic implications, development challenges, ethical implications of the system, and security issues. The research provides an analysis of these topics and, where possible, it suggests solutions. The research hopes to provide a clear roadmap to implementation.

A trend in society throughout the western world is the increased mobility of the population with families living further away from each other and elderly people living alone. [KOCH-2008]. A traveling population will have higher expectations on receiving care from informed professionals regardless of their location. Also, the increased ability for patients to choose their health care provider based on personal preferences is having an effect on the needs of patients.

Medical records today are digitized to a large extent. For example, nearly all of the records in Sweden are stored in digital form. Recent changes in the law, including the passing of the Patient Data Law (Patientdatalagen) in Sweden in July of 2008 have made it legally possible for patients to access their medical records electronically. ???

The Swedish Strategy for eHealth 2008 Status Report is aimed at providing a better exchange of information. A common goal is attempting to tie information to individuals instead of to organizations where the information is created. [SWEHEALTH-2008]

The epSOS project (Smart Open Services for European Patients) is a European project with twenty seven members in twelve European countries. The countries' goal is to develop frameworks and infrastructure to enable access, across borders, to electronic medical records and medicinal prescriptions for European citizens. [epSOS-2008]

These trends, the change in demographics, the digitization of health records and efforts by the European Union to unify and improve information exchange across health care providers sets the scene for our proposal: the introduction of an Online Health Account on a national level.

Research has been performed by an academic group over a period of about four months. As such, the scope of the report has been limited to ensure quality. The report considers the viability of an Internet system in the United States of America, Sweden, Germany, and Great Britain. Within this grouping the report focuses primarily on Sweden, specifically the Uppsala area. This region has, during our research, been identified as a suitable candidate for a trial of personal patient data access system. While not completely comprehensive, the research contains a significant amount of information that represents a substantial effort in discussing the topic.

In order to more clearly explain the advantages of an Online Health Account, the report is presented in scenario form. The two scenarios presented are the first visit to the hospital and at home. The first visit to the hospital scenario follows a patient who notices a symptom and decides to visit the hospital. In the second scenario, the patient John awaits results of his visit at home and accesses the information using his computer. Each of these scenarios is based on research that is presented in the appendices of the paper.

The appendices of the paper contain the research regarding the system. The research is an in depth analysis into several areas including open source, development model, laws, ethics, related projects, information structure, standards, economy, security and impact on the medical staff. Each of the areas focuses on medical information that helps enable patients to access their own medical record.

The final conclusion of this paper weighs all of the research performed over a four month period. That research indicates that the medical field is ready for a pilot program introducing a personal patient data access system. The welfare of people that have the ability to access their health care could improve with the introduction of an expanded system that allows for patients to be able to

access their information from anywhere in the world. This pilot program, if successful, could be expanded to international use by countries and organizations in the European Union and the United States of America.

2. Scenario

In order for a reader to fully understand how an Online Health Account should be used and what role it will play for patients receiving healthcare, this chapter will describe a scenario of a patient interacting with an online health account while receiving healthcare. The scenario is set following a patient, John Anderson, during a process were he initially visits a doctor after noticing a symptom that arouses his suspicions.

John Anderson is 38 years old and works as a teacher at the local high school. As of last year, John lives in a studio apartment near the sea.

Two years ago, when John underwent his annual medical examination provided by his employer, he was diagnosed as having an increased risk of suffering from heart disease due to diet and hereditary factors. John was offered to sign up for the newly introduced Online Health Account that would allow him to submit his blood pressure readings to his doctor, using his computer and a blood pressure meter for home use. The Online Health Account also allowed John access to his medical record as well as his medicinal prescriptions from the comfort of his home. John continued to submit his heart pressure ratings for six months while he began to engage in more physical activities as well as changing his eating habits. As his readings began to improve, the doctor could determine that the risk for John to suffer from heart disease, had been cut in half, and John could stop submitting his readings.

One evening while brushing his teeth, John noticed that the birthmark on his right forearm was bigger than usual. Earlier that week John had read an article about skin cancer in relation to sun exposure; he had been spending a lot of time sunbathing recently and he got curious and concerned. The birthmark troubled him so he decided to check his father's medical record available on his father's online health account, which he had been granted access earlier this year, in order to see if such illnesses run in his family. He soon discovered that his father, when he was around Johns age, did have skin cancer and was forced to have it surgically removed. With this in mind, John immediately the next morning called his doctor and scheduled an appointment with a dermatologist.

During the appointment at the dermatologist the doctor examined John's birthmark and confirmed that John's suspicions may be valid. The doctor took some samples of the birthmark and sent it to the lab. He instructed John to go home while the lab processed the samples. The doctor reassured John that he was not in an immediate danger and he should not be all that worried.

The day after his visit to the hospital John was very anxious about his hospital visit. As soon as he had the opportunity, John checked his online health account and saw that a new entry had been made in his medical record. The entry said that lab result confirmed that the birthmark on Johns right forearm was Melanoma, that the tumor had to be surgically removed, and an appointment with a surgeon should be made as soon as possible. After researching Melanoma on the internet for a while, John contacted the hospital and scheduled an appointment. John decided to wait a couple of weeks until the end of the school year before having the surgery so he would have the whole summer break to recover.

3. First Visit to Hospital

After scheduling the appointment with the dermatologist, John visits the hospital. The most important aspect of the scheduled visit is how the doctor enters information. It will take a while after his visit until the result is entered into his medial record. If John has the opportunity to read his medical record online from home and the records are updated shortly after information is entered, the patients will

be able to read what the doctor or staff has written in the record. This will affect what information the doctor enters into the record and how accurate that information is.

3.1. Self-censoring

When implementing the Online Health Account, it is important that the information the patient views is not harmful to his or her well being. However, doctors need to be able to record information in the doctors' personal diaries. Without personal diaries, there is a risk that doctors would be overcautious when making diagnoses and not write down thoughts and suspicions that would arouse the patient. Certain illnesses need these diary entries because some require care by several physicians and these other doctors that read the record would not have information that they may otherwise have had. Any implementation of the Online Health Account should include an area for doctors to record notes that are visible to medical staff.

3.2. Doctors' Accuracy

In a pilot project, called the Sustains Project, that was run at a local family practice in Uppsala, Sweden [Appendix A, *Impact On Staff And Information*] — a system similar to the Online Health Account was introduced and made available to approximately 100 patients. The medical staff experienced an improved quality and accuracy of information written in the records. The staff knew that the information submitted would be accessible to the patients. The staff thought about what they were writing and they also developed a standard for writing in the record. The standard served as a means of communication among the staff, which was actually improved because of this. For example, the doctors and other staff developed standardized terms and expressions between different divisions within the clinic. The more correct information is available in records, the more that doctors can rely on the information. Having both patients and doctors monitoring and interacting with the records will increase the worth and quality of records.

3.3. Code of Ethics

The content of medical records are standardized and restricted by law to maintain a uniform standard of how a record should look. However, these laws do not always contain enough guidance. Therefore there are guidelines such as the Association of Computing Machinery (ACM) code of ethics [ACM-2008]. It provides a guideline of how to act when handling private data electronically, for example medical records. It states that we are able to handle personal information on a scale which has not been possible before and this increases the potential to violate the privacy of individuals and groups. The responsibility for the data is in the hands of the professionals and, by responsibility, we mean taking the measures to ensure accuracy of data, protecting it from unauthorized access, or accidental disclosure.

4. At Home

Arriving home after his appointment at the dermatologist John has the opportunity to view his medical record using his Online Health Account. He is faced with several tasks and options while getting accesses and interpreting information. This chapter addresses aspects regarding patients at home interacting with an Online Health Account.

4.1. Retrieving Information

4.1.1. Introduction

For John to retrieve his health related information from the Online Health Account, several information entities are needed. He would for example like to know when he last was at the hospital and what notes were made then. John is going to use a system which in turn typically will be connected

to several service providers and databases, working together according to standards specifying the structure and format of the information to be exchanged.

John is now waiting for the outcome of the analysis, and in the worst case, a possible skin cancer diagnosis.

The diagnosis is one of several main components of his medical record. Other information components are e.g. care planning and the drug list. First, the web portal system needs to authenticate John [Appendix C, *Security Issues*, Section 1, " Authentication "]. For this process, the national population register service and the Base Service for Information Exchange [BIF-2008] will be used.

The information entities made available to John are governed by an authorization process [Appendix C, *Security Issues*, Section 2, "Authorization"], which acts according to rules that ensure that only information relevant to John is passed on. The structure of the information is described by Regulations for Interoperability specifications (RIV) which are rule frameworks for health care interoperability, specifying the content of medical records and its data fields. Below is an example of such a specification, covering the diagnosis part of Johns medical record. This RIV specification describes the diagnosis code, diagnosis text attributes and format. The attributes of this particular RIV are the anamnes, diagnosis code and diagnosis free text part. The description field gives further explanation of the attribute. The data type field tells the format of the actual data, here represented by the text (TXT) and code (K) categories. Further on, the multiplicity field states the amount of possible occurences of an attribute within diagnosis module. The Code System indicates the origin of the specification, typically a standard like ICD-10 or the national KSH97. Finally the Rule of decision field link to an applicable law or regulation.

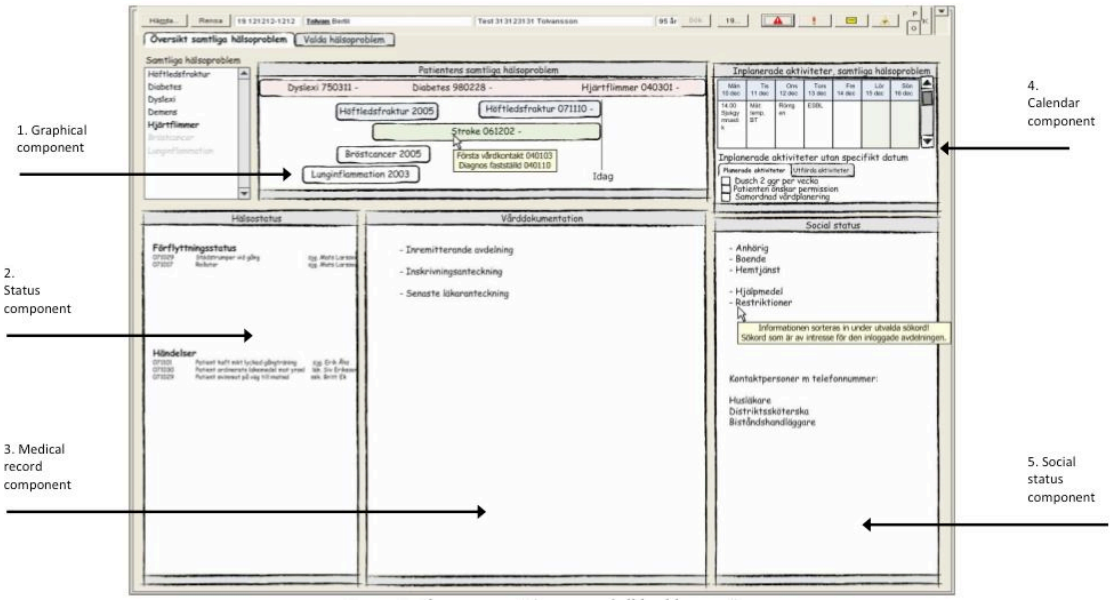
Attribute	Description	Data type	Mult	Code System	Rule of decision
Anamnes	Symptom descriptions, fee text	TXT	1		
Diagnosis code	Code of the disorder	K	0...*	KSH97	
Diagnosis	Description of disorder, free text	TXT	0...1		

Specification of John's Diagnosis Information

4.1.2. Information Representation on The Web

What medical information is most interesting for John to see when logging in to his health profile on the web and how can it be structured when represented? This question will not be answered here but interesting parallells to studies on the usage of a medical record IT system can provide some supplemental information.

Electronic Health Record (EHR) systems of today are typically complex and in many cases hard to overview. The filtering and scaling of information represent topics of research (e.g. at Uppsala University), the results of which are of interest when designing web-based systems like personal health accounts. What information is frequently changed? What information is frequently used? How is that information used and how could it be presented? The picture below shows a prototype developed by Sofia Persson presented in the paper "Design of a health issue focused patient overview". This prototype illustrates an enhanced and consolidated user interface of a typical medical record system, where commonly used categories of information are highlighted and grouped together to form a hands-on and rapid way to get a patient data overview. Furthermore, the prototype also presents a concept where the patient information and related events are graphically represented along a time line. [DESIGNP-2008]



Patient Health Overview Prototype

Above Left	Diagnosis overview
Above Center	Graphical tracking of medical events
Above Right	Health care calendar component
Left	Event list
Center	Health care documentation
Right	Social status

4.2. Accessing The Online Health Account

The acceptance, and ultimately the success of the Online Health Account will depend on the security of the system. Granting the patient access to his own medical data calls for new perspectives, and poses additional challenges on security related issues. The information will move out of controlled and protected internal systems and be made accessible in potentially insecure environments on the Internet. The security issues are:

- *Confidentiality:* Personal health records represent highly sensitive and confidential information. Information ending up in the wrong hands is a serious and unacceptable violation of the integrity of the patient.
- *Correctness (Integrity):* The information presented must be correct, in the sense that it correctly reproduces the information from the original systems. This implies that no non authorized entity must be able to access and modify the information.
- *Traceability:* There must be means to verify who has accessed what information at what time. This means that the system must provide audit trails for all relevant activities.
- *Availability:* As soon as a process supporting information system has gained wide acceptance, the processes tend to become dependent on the availability and proper operation of the system, to the extent that it becomes a security issue that the system service is available.

On the other hand, the *useability*, i.e. the ease, precision and efficiency with which the user interacts with the system is also an important acceptance factor. The objectives of security and useability might be in conflict with each other. High security levels may involve cumbersome security schemes, thus hampering the useability. Reduction of this inherent conflict calls for flexible approaches, such as adapting the security level to the needs of the particular use case. As an example, John should have

an easy way to log in to his health account (e.g. username/password) for basic, less sensitive services such as managing appointments and getting notifications. To get access to his medical record there needs to be a more secure way of logging in, since username/password schemes are often easily cracked and mismanaged by the users.

4.2.1. Authentication mechanisms

Having established the necessity for using strong authentication and other security mechanisms in order to meet the requirements in the sensitive context of the Online Health Account and prevent unauthorized access and other security breaches, such as "identity theft", we will in the following point out some mechanisms and choices for authentication.

It is important to point out that the authentication mechanisms need not, and ideally should not be part of the system itself. Rather, it should be a public service in itself which the Online Health Account in turn uses for its authentication needs. With the ever increaing set of eGovernment service, secure identification should be part of the public "electronic infrastructure", a tax financed service provided to the citizens just as any other public service, and as such obey to estalished standards, and be platform and vendor neutral. For a more extensive discussion of these topics, please cf. Appendix C, *Security Issues*.

4.2.2. Authorization in The Health Account Service

The record system's access control will have to take into account the "patient role". This role will allow access to all information (with a few, well defined exceptions) regarding the patient in question *and only that patient*. There will also be the related issue of rights delegation to relatives, trusted persons, etc. These features are ensured by means of the *authorization mechanisms* [Appendix C, *Security Issues*, Section 2, “Authorization”].

If our patient, John, wanted to get a copy of his record before the introduction of the Health Account, he would need to order it from the County Council. The request would be forwarded to CESÅ, the agency for scanning and reviewing medical records, and the routines for handling the request would be as described in: [Appendix D, *CESÅ*].

A service request in an online Health Record, would need a similar censoring step before making the information available. With a sophisticated authorization system, the process of filtering such potentially damaging information for the patient can be automated. If this is difficult to implement in the early versions, future implementations of a system for medical records should be able to flag sensitive entries that would automatically be filtered from the patient's view. For a more extensive discussion of authorization issues, please cf. [Appendix C, *Security Issues*, Section 2, “Authorization”].

5. Interpreting Information

United States law provides an exception for extreme cases. It allows the doctor to withhold a medical record if he or she believes that it will lead to harm of the patient. However, withholding results under this measure is only legal if the patient is considered to be suicidal. However in some countries it is legal for the hospital to merely refuse digital distribution. In this case you could instead require that a patient call the hospital to receive the information over the phone. Thus the patients are not refused access to their medical record, but the distribution method allows for more control. Please note that such a system is of questionable legality in the United States, where a patient can request the data in any readily producible form.

Although this method of data restriction can thus be considered legal in most countries, we must consider how this type of system would be managed. This issue is readily linked to the ethical evaluation of the entire method. The main moral objection to the restriction of records would be that it takes the power of decision out of the hands of the patient. Rather than being able to estimate their own well-being, they are instead evaluated by some third party. This practically that the patient is incapable to handle this information by him- or herself. It thus seems ill advised to allow the withholding of records in other cases.

If there is not personnel available to evaluate the effects of disclosure the patient may suffer from arbitrary desicions being made. However, one option is to recommend the patient to call the hospital in order to get the results from a professional, to control the way information is received without compromising the rights of the patients.

6. Automated Results

At some locations today, hospitals and primary care are using a computerized system to store records. Test results for a patient is often sent back to the care establishment via computer, and they go straight into the record. This is in most ways very practical as health care looks today, but there might be complications should The Online Health Account be active.

Today, the test results are color-coded when they are sent from the lab. There are different colors depending on what the patients value is compared to a normative value. If it is bad, over the limit, it is red. If it is ok and within the boundaries, it is black. The test values does not necessarily reflect the patients health condition, it is merely the result from a specific test. A red value may be all in order, for example if the patient is taking some medication that would give such a result. This is often obvious to an educated doctor who puts them into context, but may be misinterpreted by the average reader which can react in a negative way.

Today the test results go directly into the hospital computer, but they do not reach the patient until after, depending on the values, and it can take quite a long time. If the result is urgent, it is usually delivered right away because urgent care needs to be taken. But if the result is negative for medical problems, and the patient is deemed healthy, the result may delay for a long time and is sometimes not sent at all.

With The Online Health Account, patients would be able to read these test results at the moment they arrive from the lab, should this way of handling the results remain the same. Of course a lot of people will find it convenient to see these results right away but some might react differently, misinterpreting the information or overreact. One way of dealing with this would be to have very extensive descriptions of the test results, to avoid misunderstandings. Another possible solution would be to remove this feature, or censor the results in some way.

This can lead to an ethical discussion though. For example, some patients may prefer to get the test result right away via the web, regardless of if it will show that they are healthy or not while others would like to receive the results in the presence of a doctor. Today they would have to call their doctor or wait for a call, and therefor The Online Health Account could greatly decrease waiting times. On the other hand, some may argue that it is for the patients best that they find out in the company of a professional, that can comfort them and answer questions.

7. Error Detection

John has been assigned by his doctor to at regular intervals measure his blood pressure at home. When he was finished, John logged into his Online Health Account to enter his blood pressure for today, because now he can do this himself via his computer. John updated the information in the record, but when he read it through he noticed that his doctor actually had forgot to write about his tomato allergy. This made John a little upset, but at the same time he was glad and relieved that he noticed the error. He used the built in messaging feature of the Online Health Account and sent an alert to the medical staff at his care provider that the error needed to be corrected.

There are many positive aspects of an Online Health Account, one being the increased potential of discovering possibly incorrect information in a record. For example when patients can read the record themselves, they first hand be able to discover errors that might have gotten into their record. It does happen today that important information is lost when updating a record, or that incorrect information is entered by mistake. This can be data that has not been entered, or some information that is not entirely accurate, or completely faulty. With the Online Health Account, chances are increased that

errors like these are discovered. Furthermore, Dr. Ture Ålander said during an interview that happy as they were with the Sustains Project and how it had worked out, they had found one feature in particular that they would like to see in a future system, namely the opportunity for the patients to add some data into their record themselves. This data can be results from tests the patient can do at home. More than just being practical for the patient, this would also save valuable time at the clinic, and thus saving money as well as streamlining the work flow [Appendix A, *Impact On Staff And Information*].

8. Additional Considerations

The scenario covers one patient's use of the Online Health account. There are many other aspects to the system. Each aspect influences the design and operation of the system. These include how the system is organized and developed. Other aspects deal with ownership and misuse of information. It's also vital to consider how different patient groups interact with their accounts. What follows are only a few areas to consider when implementing the system.

8.1. Information Structure and Related ICT Projects

8.1.1. Sweden

As stated in the Swedish Strategy for eHealth 2008 Status Report, concrete and deepened cooperation on eHealth is a prerequisite for greater patient mobility within the EU as well as the creation of European specialist centres and skills centres. A major national goal in Sweden is that patient information should be utilized by different care providers.[SWEHEALTH-2008] This means that information needs to be digitally stored, accessible and have a uniform structure adopting a common vocabulary, codes and terms. A uniform structure requires well-specified information subject to a common regulatory framework and thus adjusted to a uniform information structure model. This will allow ICT (Information and Communication Technology) systems to handle and exchange information more efficiently. Patient safety and the ability to follow up care activities are contingent on a uniform information structure based on established terminologies and classifications. As discussed in this document, efforts in the field of information specifications will probably affect and simplify future extension towards solutions allowing people to interact with the health care systems themselves.

8.1.2. United States of America

In order to widen the perspective of the international trends, the authors of this paper have the opportunity to make comparisons to the general situation in the United States where there is also a push for electronic health records as well as in Europe. However, with different sets of laws and a plethora of private health care systems, a nationwide system for electronic access to health information will be difficult to implement. Health records and the storage of these records will have to be standardized nationwide. The US Department of Health and Human Services oversees policies in this area at the federal level. In addition, each state has its own government agency that oversees the health care industry. Finally, private hospitals and medical practices have their own policies and practices for medical records. In Sweden, several legislative efforts have been proposed to start the development of a standard patient assessment tool.[NBHW-2008]

8.2. Ownership

Who owns a medical record? A record is one of the primary tools available to a doctor, but at the same time it contains sensitive information about the patient. Many doctors view the record as the property of the health care in general and themselves in particular. With the introduction of an Online Health Account the ownership of records is shifted from the health care to the patient. The new Patient Data law enables transfer of power over the medical record to the patient. An Online Health Account is a good way to realize some of the aspects of this new law. The patient will now be able to see what doctors, nurses and secretaries are writing in the record. The law also states that the

patient has the right to see what staff and care institutions that have been accessing his or her medical record.[SWEHEALTH-2008]

8.3. Patient Groups

There will be some differentiation between user groups of the Online Health Account. Most will be ordinary users, logging in when they are expecting a result from their latest visit at the doctor. There will also be groups of people with special needs that cannot use the system to its full potential or cannot or do not want touse it at all. Some potential users will need assistance to log in to their Online Health Account. For example, a ten year old probably would not have that much use for the information in the system. Though with the new Swedish Patient Data Law, everybody owns their own medical record and has the power to delegate the authority to look at the medical record to somebody else.

8.4. Development Strategies

In the development phase of an electronic healthcare system such as Online Heath Account, the adoption of the correct development strategies is the key to the success. Some recommendations follows. Choice of a sustainable medical information standards as the carriers of the data used by the system and the schema of the data will be the building blocks of Online Health Account. Those standards are specifications of data and determine the interoperability inside and outside the system. The electronic healthcare system is recommended to be built as an open system because that will help stabilizing the setting of the system for future development. Furthermore, the modularization of Online Health Account allows the cooperation of different entities (such as the joint development between two software companies). Appendix F, *Development Model and Open Source*

8.5. Misuse of Information

What would happen if medical data was somehow released to the public?

Several studies conducted in the United States have found that around three-fourths of the public feel that "it is very important that their medical records be kept confidential". [IHF-WEB] Medical information is highly confidential and the release of such records could be disastrous. Several related studies have found that over half of all Americans fear the improper release of their medical records. [EPIC-WEB]

Many of these participants also believe that, if sensitive information were released to their employers, these would use that information against the employee. An example scenario would be where a worker may be denied certain benefits because of a particular disease or genetic trait that the employee has. The employers could possibly use this information to discriminate against a person.

Likewise, other citizens could use this information to blackmail people. Public figures, such as politicians and actors, could be victims of blackmail since the confidential information in the record may cause emotional or monetary harm. Other criminal acts such as identity theft and misuse of the released information could cause a great amount of stress and harm to the patients. The more information that the databank contains, the more vulnerable the data is. Considerations should be taken for the increased risk and the increased potential harm that come from centralization of data.

8.6. Saving Money

Research projects such as The Sustains Project (SP) running at Dr. Ture Ålander Family Practice in Uppsala, Sweden suggest that there is money to be saved by allowing patients to access their records online [SUSTAINS-final-report-2001]. Apart from the obvious reduction of paper records that are sent to patients by regular mail, surveys evaluating SP reported that the medical personnel spent less time answering phone calls from the patients. The patients also came to their doctors appointments better prepared which lead to less time needed to be spent with each patient, without lowering the quality of the care. With less time spent on each patient, more patients can be taken care of per

day, and that can lead to an economical benefit for the organization. Moreover, the patient as well can benefit economically from having less direct contact with health care. By being able to reduce visits to the doctor, money could be saved. For example, a patient would not need to schedule an appointment in order to get results from tests. The patient could save not only the fee he or she needs to pay every visit but also possible travelling costs to get to and from the doctor. The main benefit for the patient is the increase in quality The Online Health Account can hopefully provide.

9. International Perspective

When implementing the Online Health Account there are a large number of legal factors which we must consider. Patient records in particular are significantly regulated. By examining the patient record laws in Sweden, Great Britain, the United States, and Germany, we hope to gain a better understanding of how the Online Health Account would have to be structured to support international regulations.

9.1. Sweden

The law regulating online record system in Sweden is called the Patient Data Law and came into effect in June of 2008. It was designed with internet access in mind, and supersedes the older Swedish health care directory law and the Swedish patient record law. [PDL-WEB]

This law handles information management within the health care system and states that it should be organized to promote patient security and quality and cost efficiency. It is stated that the health care provider is accountable for the personal records according to the personal record law. Further the law concerns the obligation to keep a patient record and what needs to be put into it. One record should be kept per person. This is mainly to maintain a good and secure health care. It should also be a source of information for the patient, follow ups, laws of records and research.

The patient medical record should always contain:

- Information about the patient's identity.
- Relevant information regarding the reason for health care.
- Information about issued diagnoses and reasons for more significant measure.
- Relevant information about taken and planed measures.
- Information about the decisions that has been made and given to the patient.
- Information about who added information.

Note that only the health care giver that participates in the care of a patient is allowed to read that patient's record. The law also establishes rules for how information should be handled in a central digital system that gives health care personal direct access to record. A central digital system like this must be systematically and recurrently checked to determine if someone unauthorized has accessed the system. The system must also allow the patient to deny access by healthcare professionals to his or her record. A block by the patient may be overruled if it is decided that the patient is unable to make decisions. The rules also dictate how a digital system could be used to collect statistic information in order to assure quality in the health care system. It is stressed that personal records cannot be used for this purpose unless the patient allows it. The patient must be able to opt out of the quality assurance program at any time they wish. Finally, the new law establishes several security guidelines for patients accessing their records over the internet

9.2. United States of America

The primary document governing the management and disclosure of patient records in America is the Health Insurance Portability and Accountability Act (HIPAA). While it does mandate the release

of records to patients upon request, several facets of the law do restrict, and in some cases hinder a possible American implementation of the Online Healthcare Account. The main complications are with regards to two issues: the manner in which the record is disclosed, and the situations in which access may be denied. By examining all of these we can form a clearer picture of HIPAA. [HIPAA-WEB]

Under HIPAA, hospitals are required to either give to individuals, or allow individuals to view copies of their records. This includes all data, including tests as well as X-rays and records. Patients also have the right to request this information in any 'readily producible' form. As such, it would seem that a patient might reasonably receive the record in an electronic format if the hospital uses a digital system, since this record would be 'readily producible'. However, the system also restricts the fees a hospital can charge for the copy. Only the cost of copying, postage, or summary of the data may be asked. This is in fact a significant obstacle to the Online Healthcare Account or a similar system in the US. Here, the law essentially precludes any sort of fee or subscription service, as it is specifically worded to account for paper copies. This makes it a very hard sell, as you are asking hospitals to implement a new system that increases patient oversight while providing no financial incentive.

HIPAA also provides several cases in which access to records may be denied. Many of these cases are ones which our group had already identified as trouble areas. A healthcare facility may unconditionally deny access to psychotherapy notes, records which the patient intends to use in a civil or criminal proceeding, if the health information was gathered as part of a clinical trial, or if the patient is interned at a correctional facility. Furthermore, the hospital can deny the patients right to access under additional circumstances; however these are subject to review. These include, if the doctor believes that access would endanger the life of the patient or someone else, or if the record makes reference to another person.

9.3. United Kingdom

The law regarding how care providers and patients interact with patient data in Great Britain is called the Data Protection Act (1998). The DPA is broken down into six sections. Sections 2 and 4 are significant to us. Sections 2, "Rights of Data Subjects and Others" defines the basic relationship between the data holders and the data subjects. Section 4, "Exemptions", outlines some of the exemptions for the government and the data holders in certain circumstances. [DPA-WEB]

'Rights of Data Subjects and Others' concerns the powers of both the patients and the doctors. Under the law patients have the right to request to view their data as long as they are able to prove identification. The data holder may charge a fee as long it does not exceed a prescribed maximum. Section 2 also indicates that the data holder may withhold parts of the record that contain data about other patients. The patient also has the right to be notified whether or not any given data holder has information on them. On review the patient is legally entitled to request corrections to their file. Finally, the patient may stop the transfer of records in several cases. These include disclosure to third parties for marketing purposes or to another medical entity if such disclosure can be reasonably shown to cause distress or harm to the patient

Section 4 provides additional allowances under which a healthcare provider may deny a patient to his records, or grant special access to records. Firstly, information may be withheld for national security reasons, or to prevent or detect a crime. Mental health records are also covered. These are completely exempt, and need never be disclosed to a patient. Cases in which records may be disclosed beyond patient request include medical studies, research activities, or statistical collection. Several additional exceptions exist on top of this, however they are special situation which do not bear examination as they relate only tangentially to this system.

9.4. Germany

In terms of how the health care is handled electronically, Germany is in many ways similar to Sweden. They have recently had a law change that allows for an implementation of a central stage in a process similar to a project like the Online Health Account. This stage gives the patient more control

over their data as opposed to before, because with this law change patient have full access to their record and the patient even has the right to delete information in his or her record. This is something that goes far beyond what is legal in Sweden, U.S. and U.K. and positions Germany on the leading edge of technical medical health care. However, the doctor and the patient have to agree on access to the record and this access has to be done simultaneously, so no changes can be made without the doctor's consent. The development of the health care system in Germany is non-the-less interesting, and other countries and projects (such as the Online Health Account) might look to German implementations for advice and suggestions on how to proceed both legally and technically.

The law change discussed above is only the first phase of what is planned in Germany. What is to come is an implementation of a digital patient record. This is stated in the law text and is currently being tested in a few selected German counties.

10. Vision

Beyond its initial implementation, the Online Health Account holds significant promise for future improvements on an international level by facilitating record exchange. A unified digital system could allow for anywhere anytime access of records at every hospital in the world.

More revolutionary, patients themselves would be able to view and track this exchange. The end result of this overhaul is complete and total data transparency for patients and care providers.

The first implication of this is mobility. The clinic by your vacation home would be able to see the notes made by your hometown practice. Specialists would be able to seamlessly share and review your information. Location will no longer be a hindrance to care. Any patient with a complete record will be able to receive proper care at any facility.

Furthermore, the ubiquity of access will allow the patient to access the records themselves any time they see fit. Investigation on the part of the patient may become routine, as people become accustomed to taking steps themselves to monitor their own health. If everyone were as vigilant as John, we could prevent a huge number of illnesses.

Record sharing will also help care providers to avoid mistakes and omissions, improving the completeness of records. By increasing the opportunity and convenience of review the number of doctors able to examine the record will likewise increase.

Furthermore, giving the patient simple access to their own data will allow them to perform corrections (such as John noticing his unlisted tomato allergy). Although such errors might seem simple to correct, modern medical practice often suffers from these simple problems.

The communication between patient and care provider will also be more streamlined. The need for e-mails and phone calls between parts will decrease in number as the patients gather more knowledge by themselves at home. Moreover, it will also make them better educated, and visits to the doctor will be more effective and rewarding for both parts.

There will also be a lower latency in update frequency of the medical record, and the patient can view new data directly when it is added. It will thus allow the patient to not only check up on past entries but also to follow the current progress of treatment. This will improve the perceived quality of care.

Universal records also create entirely new opportunities for collaboration between facilities. With a system for distributing and sharing data, experts at different hospitals will be able simultaneously examine the same case. It may even be possible for diagnostic teams to work between hospitals, and perhaps even cross borders, instantly lending the best medical advice available to exceptional cases.

Ultimately, online health records are the first major step in such towards such a future. By empowering the patient to take an active role in their healthcare we pave the way for a healthier, better informed population.

11. Future Work

The research presented is just a step into the creation of the Online Health Account and further research in the area of providing patients with health information. Given more time or a budget, this team could produce more research into the area. Other teams could build upon the research, as well.

There is some research that the team would like to perform if given additional time. The research could be more in depth and broadened to more countries within the European Union. Also, it may be interesting to investigate opening the system up to the entire world. Researching a worldwide system would include researching representative developed countries of different regions such as Canada, China, Egypt, and Japan. In addition, research into standards, development models and continued integration with open source solutions could be performed. Each of these standards would improve the longevity and durability of the Online Health Account. Another challenge that could be further researched is the interoperability of the system.

Given a budget, the team would like to purchase some additional services to increase the quality of the research. While most information is free, some comes at a cost. Professional consulting and surveying would have been extremely useful for some of the research that the team performed. Legal consultants could provide more accurate and deeper analysis of each of the countries laws. Health care professionals could be hired to walk the team through some of the medical profession's procedures that may be affected by the system. Surveys could be performed that polls medical staff on their reactions to systems that have been introduced with the intention of improving the process of data entry. A budget would allow the team to formally research the specifics of this project.

Further work that could be performed as a result of this project could be projects that examine adding modules to the system that would enhance the functionality. For example, research could be conducted into the feasibility of a module that would allow for patients to communicate with their doctors using a messaging service built into the system. These modules could be a great way to solve unforeseen obstacles that occur in healthcare. Also, research that focuses specifically on the implementation of this kind of system at a larger level—the EU, for example—could use this research and the Online Health Account extensively in the research.

One very important aspect of the implementation of an Online Health Account is usability. We have made the deliberate choice of not researching this area during our project due to limited manpower. However, this is an important field that needs to be taken in consideration when dealing with the ordinary user in general and the user with disabilities in particular. Building a system that is accessible to the major part of the population is crucial for a widespread adoption

Whether it is researching the expansion of the Online Health Account into the European Union or adding modules to the Online Health Account, further research would be useful in this emerging area of health care. The team hopes that research will continue in the area of providing health care information to patients and that health care continues to improve for patients everywhere.

12. Conclusion

Web-based technology has enabled new services and ways of interaction between the health care providers and the patients. By well thought development and introduction, it can increase patient participation in the ward process, quality of service as well as productivity. Introduction of a service like the Online Health Account will by itself bring about changes to health care in several dimensions.

The relationship between the care provider and the patient will be affected by the increased interaction enabled by the service. Questions arising from unclear statements in the Health records will motivate increased clarity in the Medical Documentation Process. Findings from the Sustains project indicate that the initial scepticism shared by some ward personnel, to granting patient access to the health record is mostly unfounded. It turns out that the benefits outweigh the risks of misunderstandings or other damaging effects. Better informed patients make the appointments with the care provider more efficient and enables for more quality time with the doctor.

The underlying principle for the service is the patients' right to free access to their entire medical record, with few and well defined exceptions. When this right is also made a practical reality, the patients and their relatives will become more involved in questions related to their care. Patients will acquire a greater understanding of the health care process, possibly get a better "working relationship" with their physician and even learn more about issues related to their health, leading to a more more humane, responsive and efficient ward process.

There is a risk involved when exposing sensitive patient specific information on the Internet. The availability, confidentiality and integrity of the data are paramount not only for ethical and legal reasons, but also for general acceptance of the service. Introduction of the Online Health Account service therefore requires usage of state of the art methods for Authentication and Authorization. It should be emphasized, though, that there is also a potential for actual *increase* of the security level as compared to the actual situation. In todays situation, patient related information travel between ward units via open fax machines, telephone lines and by ordinary paper mail. The security involved in these processes leave a lot to be desired, and if something goes wrong, there is poor traceability, since no automatic logging is involved.

The potential threats resulting from increased exposure of sensitive personal data may well be outweighed by the benefits. Ethical and legal considerations will naturally transfer control of the information to the patient himself. The concept of *Patient Consent* will become central, and from there it is natural to expect that a more patient centric approach will drive the further development of health care systems.

When it comes to the Patients Electronic Health record, there is still a lack of standards for information interchange having gained overall acceptance. Most of these efforts have up to now been in the theoretical and negotiation stages in the standardization committees. Real life deployments are needed. The service under consideration will most certainly function as an accelerator in the demand for creating an infrastructure of systems which are able to communicate health record information with each other in a secure and accurate way.

Earlier attempts at making the health record available to the patient have also been hampered by legal obstacles. The recent change in Swedens "Patient Data Act" has been motivated by the need for modernization of the law due to the acute need for interoperability between ward systems across health care units. There are good reasons to believe that deployment of an online Health Account will be an important test bed for the new legislation, and most probably an example that will be followed closely also at an international level.

The cost of deploying an Online Health Account system service will be considerable. Uppsala is in a good position though, since the county council has standardized on one system. Consequently, there is not a plethora of systems to integrate with the service. Even in cases where there is a high number of different ward systems, the integration process is something which has to be undertaken eventually, since interoperability between ward systems is a crucial part of the Swedish Strategy for eHealth 2008 Status Report. The introduction of the service will possibly accelerate the integration process. In the long run, disregarding all other benefits, the pure economic benefits will probably outweigh the costs due to the improvements in the ward process and the resulting increased quality of the ward. [SWEHEALTH-2008]

Initiating development and deployment in a region which has a relatively uniform IT infrastructure reduces the problem of interoperability and makes it possible to focus more on the application itself. Nevertheless, the Online Health Account is an important step in the development of the Health Information Infrastructure. Special care should be taken in order to avoid the pitfalls, and to make the initial deployment a "future proof" step in the right direction:

- *Development in small and well defined steps.* "Big Bang" IT projects practically always fail. Their aims are both unclear and much too large at the same time, which leads to a flawed specification and lack of understanding of the problems ahead. The subsequent procurement process reflects these innate problems. To avoid this, the project must be subdivided into steps that are well understood and manageable. Each step should be validated in action before proceeding to the next step in the development.

- *Taking standards for medical information interchange seriously.* The great challenge of Health Care ICT of today is to tie together the many insulated information systems, constituting "islands of information" about the patient. In order for this to happen, the system must achieve *semantic interoperability*. That is, that the meaning of information is preserved as it is transferred between systems. For this to happen, the systems must be able not only to export and import data in a common format, but also the rich set of medical terms and concepts must be understood and agreed upon among the systems. The only way to achieve this is by adapting standards. Choosing the "right" standard is a success factor for the Online Health Account. This is important to take into account, although the problem might not arise initially, if the system is developed and introduced first in a region with a homogeneous IT-environment.

- *With respect for the legacy.* Many previous attempts to develop a Health Information Infrastructure have ignored or underestimated the enormous investments in the existing computerized systems. Introducing a new system, which tries to bridge the gap between the legacy must not disturb the ongoing production. This is best done by thinking about the legacy as a set of distributed systems which is to be tied together in a "virtual" electronic health record.

- *Ensure scaleability.* Right from the outset, it is important to consider scaleability issues, both from a pure technical point of view and that the system is designed so as to be "deployment scaleable". The former term refers to good practices when it comes to architectural aspects, such as choice of good server side components and a well devised modularization of the system, so that the system is adjustable to an increasing number of users. The second term refers to the way interoperability problems are adressed, so that adding of new ward units and system does not impose a prohibitive burden in the long run.

- *Avoid vendor lock in.* Platform independent solutions must be chosen, in order to avoid vendor lock in. This applies to both the server and the client side. The former, because the system will potentially be deployed in different and heterogeneous environments. The latter, because we are building a public service, and no assumptions must be made with respect to the choices of hardware and software of the citizen, as long as it obeys established standards and quality norms. This is e.g. particularly important for the Identity Management, and the Authentication subsystem.

- *Infrastructure and Open Source development—A perfect match.* The development of infrastructure puts high demands on openness and transparence. This makes it easier for a heterogeneous legacy to integrate with the new system. The Internet itself is a brilliant example of an infrastructure which was built according to the principle of openness. The immediate benefit of basing the development on open source is the ability to build Swedish and possibly international professional communities around the project.

Bibliography

[ACM-2008] ACM homepage 2008-12-13 http://www.acm.org/about/code-of-ethics

[BankID1-2008] BankID Homepage 1 BankID Homepage 1, 2008 2008-12-12 http://www.bankid.com/sv/Vad-ar-BankID/Test/

[BankID2-2008] BankID Homepage 2 2008-12-12 http://www.bankid.com/sv/Vad-ar-BankID/Lorem-Ipsum/

[BIF-2008] BIF, Bastjänster för informationsförsörjning 2008-11-12 http://www.logica.se/bif,+bastj%C3%A4nster+f%C3%B6r+informationsf%C3%B6rs%C3%B6rjning/400013091

[DESIGNP-2008] Design of a Health Issue Focused Patient Overview: A user-centred approach to increase situation awarness 2008-03 Teknisk- naturvetenskaplig fakultet, Uppsala University Sofia Persson

[EPJ-2008] EPJ-förvaltning CESÅ report 2008 Akademiska Sjukhuset

[epSOS-2008] epSOS Webpage 2008-12-14 http://www.epsos.eu/about.html

[PDL-WEB] Patient Data Law (Patientdatalagen) 2006-10-18 http://www.regeringen.se/sb/d/6150/a/71234

[INTERVIEW-TERNER-2008] Interview, Annika Terner, Uppsala County Council 2008-11-21

[KOCH-2008] Ubiquitous care in aging societies - a social challenge. Stud Health Technol. Inform. Vol 134 (s.89-95) 2008 Sabine Koch 0-201-83595-9

[IHF-WEB] Institute For Health Freedom Gallup Survey 2000-09 http://www.forhealthfreedom.org/Gallup-survey/IHF-Gallup.html

[EPIC-WEB] Electronic Privacy Information Center Webpage 2008 http://www.epic.org

[HIPAA-WEB] Health Insurance Portability and Accountability Act 1996 http://www.legalarchiver.org/hipaa.htm

[DPA-WEB] Data Protection Act (UK) 1998 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

[NBHW-2008] National Board of Health and Welfare 2008-11-14 http://www.socialstyrelsen.se/en/

[SOSFS-2008-14] SOSFS 2008:14 regulation 2009-02-07 http://www.sos.se/sosfs/2008_14/2008_14.htm

[NEDGE-2008] Nordic Edge homepage 2008-12-12 http://www.nordicedge.se/produktblad/OneTimePassword_eng.pdf

[NINFOSTRUKT-2008] Nationell Informationsstrukur 2008-11-14 http://www.socialstyrelsen.se/AZ/sakomraden/Nationell_Informationstruktur/

[NPÖ-2008] National Board of Health and Welfare 2008-11-12 http://www.carelink.se/utvecklingsarbete/vardinformation/undersida/

[OEHRARCH-2007] openEHR Architecture Overview 2007 openEHR organization http://www.openehr.org/releases/1.0.1/architecture/overview.pdf

[OEHRINTRO-2007] openEHR Introduction 2007 openEHR organization http://www.openehr.org/releases/1.0.1/openEHR/introducing_openEHR.pdf

[RIV-2009] RIV specifications 2009 Carelink http://www.carelink.se

[SWEHEALTH-2008] Swedish Strategy for eHealth 2008 Status Report 2008-11-04 http://www.regeringen.se/sb/d/10058/a/114873 978-91-633-3601-0

[SUSTAINS-final-report-2001] PROJECT SUSTAINS final report 2001-10-01 SUSTAINS Ingrid Joustra-Enquist Benny Eklund

Glossary

Audit trail	A chronological sequence of records, containing information resulting from the execution of a business process or system function.
ADL	Archetype Definition Language
BIF	Bastjänster för InformationsFörsörjning - Base Service for Information Exchange
CESÅ	CESÅ is a division for ordering paper copies of a record in Uppsala county
DICOM	Digital Imaging and Communications in Medicine
EHR	Electronic Health Record
HTML	HyperText Markup Language
ICD-10	International Statistical Classification of Diseases and Related Health Problems
ICF	The International Classification of Functioning, Disability and Health
ICT	Information and Communication Technology
NPÖ	den Nationella PatientÖversikten - The National Patient Summary
PKI	Public Key Infrastructure
RIV	Regelverk för Interoperabilitet inom Vård och omsorg - Regulations for Interoperability in Health Care
SAML	Security Assertion Markup Language
SNOMED CT	Systematized Nomenclature of Medicine
SP	The Sustains Project
SSL	Secure Sockets Layer
SSO	Single Sign-On
TIS	Tillämpad InformationsStruktur - Applied Information Structure
TLS	Transport Layer Security
V-TIM	Operational Applied Information Model
WHO	World Health Organization
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Appendix A. Impact On Staff And Information

Interview with Dr. Ture Ålander

On October the 15th of 2008 Dr. Ture Ålander was interviewed with the purpose of getting an inside view of what effects his clinic had experienced since the introduction of an IT-system similar to the Online Health Account, namely the Sustains Project (SP). SP has been in use at the clinic since 2001 and is still very much in active use.

SP is a service where patients are able to view their medical records via Internet, at home. It uses a basic security procedure where the user logs on to a computer, which then sends a text message to a mobile phone. This phone is registered when signing up for the service. The text message contains a pass code which is used to log in to the main system. An extended security measure is added by only allowing the user to read from a client computer, which fetches data from a central server. In SP there is also a built in secure messaging service for communication between doctor and patient. In practice it works like e-mail but the messages are always encrypted in order for the patient to feel safe and secure. Today there are about 450-500 active users of SP at Dr. Ålanders clinic.

These medical records does not always contain every single piece of information available, but rather what the doctor has evaluated should appear there, different from patient to patient. Most lab test results are made available at the moment they arrive, while some information requires the patient to contact, or be contacted by, the clinic. This may be serious cases of cancer for example, but it has been highly rare. The doctor decides what should be made available by signing different parts of information ok, or not ok. This is because sometimes the doctor wants to go through the result with the patient personally. This is for the simple reason that some information is, sometimes, best received when one has somebody to talk to, in this case a doctor who is able to answer questions and explain the concrete meaning of the result, who can calm the patient, or just be there for him or her. This way of working is being actively used at Dr. Ålanders clinic, though as previously mentioned very seldom needed.

A noticeable change following the introduction of SP was what was written into the medical records. Because the personnel became more careful about what they wrote, and thought it through even more carefully, the quality of the content was improved. However this was in no way experienced as a troublesome transition, but went rather smoothly.

Moreover, the personnel were unburdened in their work. The patients had access to more information at home, which led to a decrease in phone calls and doctor visits made that would have served the same purpose of updating the patient on current status. And at the same time the patients got the opportunity to check their medical record for errors or missing pieces of information, which could then be corrected by contacting the doctor. Furthermore, they can ask another doctor for a second opinion by easily logging in on a computer and view the medical record together.

The interview also touched upon the ethics of such a system as SP. What is written in a medical record differs depending on what care division has been in charge of treatment. For example people under treatment for psychological problems might not always be suited to read everything the doctor should write, because they are not always in a condition to view the information in an objective way and can misinterpret data. In cases like this there is a possibility that censoring what is entered into the medical record is in order, because of their special nature.

The results from surveys done about SP shows that patients are satisfied with practically everything. The one thing is that the secure messaging service is not widely used, but that is because the patients feel that they do not need more than regular e-mail. They feel secure when logging in and they feel confident that the medical record they read online is not excluding any information.

Dr. Ålander also mentioned a feature he would like to see in a future system, such as The Online Health Account. Today some patients measure their own blood pressure at home, and then call the

doctor to deliver the results. But with SP or The Online Health Account, the patient could be granted the authority to add this data themselves, for example in a special data added by patient section. This would reduce phone calls necessary for the patient and make everyday duties more smooth, as well as free up resources at the hospital or care giver in form of fewer phone calls and administrative work.

Appendix B. Information, Process and Standards Overview

1. A Future Common Medical Information Structure

An information structure is a description of a set of information, that is, how the information parts are to be interpreted and how they relate to each other in a specific context. A more formal description of two related terms frequently used in this section of the report:

Information Structure: An information unit structured with classes, attribute, relations, multiplicity rules, classifications, code systems and format

Information Specification: Documentation of the Information Structure (above)

The National Board of Health and Welfare (NBHW) is a government agency under the Ministry of Health and Social Affairs, with a wide range of activities including social, health and medical services. The government determines the policy guidelines for NBHW. By establishing the National Information Structure-project (NI-project), the National Board of Health and Welfare plans to take a total national and strategical responsibility to secure that patient information is transparent, accessible and possible to follow-up. [NBHW-2008]The Swedish Association of Local Authorities and Regions (SALAR) is an employer´s organisation for municipalities, county councils and regions. It ´s vision is to develop the welfare system and its services. SALAR has established a National Center for Coordination of e-Health including the Board of architecture. [NINFOSTRUKT-2008]

2. General Structure of Medical Records

By the provision SOSFS 2008:14 third chapter article 6, the Swedish National Board of Health and Welfare emphasizes several information to be included in medical records. [SOSFS-2008-14]

1.	Health status and medical judgement
2.	Information about prescriptions
3.	Reasons for prescription
4.	Results of health review
5.	Information on hypersensitivity
6.	Contagious disorder
7.	Epicrisis and other medical care loggs

3. NPÖ, the National Patient Summary - A Pioneer of Shared IT Solutions

The National Patient Summary is an essential partial delivery within the program of action for realization of the Swedish Strategy for eHealth 2008 Status Report. [NPÖ-2008]. The main goal is to increase the health care quality by providing transparent information exchange between different health care providers. A prerequisite to this is a future technical infrastructure and common security solutions. NPÖ states overarching specification of information units to be used by projects implementing the NI-project. The information units are defined as bounded information used in a specific context. Currently, the NPÖ- specifies ten information units. These are to be test implemented in the care organization and in ICT (Information and Communication Technology) system providers. The current information units of NPÖ- are:

- Care providers

- Important notifications
- Diagnosis
- Type of care service (for example primary or secondary level)
- Medicine
- Contact (for example planned and historic)
- Care documentation (for example epicrisis, anamnesis)
- Care planning
- Functional status
- Test results

NPÖ- specifies two main components, one information specification part (RIV/V-TIM, se below) and an information standard part according to SS-EN13606. The goal is to successively expand NPÖ- to cover the full range of related information.

4. TIS (Applied Information Structure)

The TIS group, one part of the Board of architecture, coordinates information structures on a national level. One of TIS responsibilities is to provide national development projects (for example the NPÖ project) with directives in order to provide a common structure and coordination

4.1. V-TIM (Operational Applied Information Model)

This project provides an information structure based on terms, classifications,nomenclature and information models needed to fulfill ongoing projects. The Swedish county councils have decided to develop a common applicable information structure for ICT in order to improve patient safety, enabling comparison and communicating across operational and organizational boundaries in Swedish care. Different information structures have been developed earlier in national and regional projects on the basis of everyday clinical experiences and needs as experienced by active clinical care personal. The V-TIM project merges and harmonizes a number of those national and regional projects information structures into one common clinical oriented applicable information structure.

4.2. Classifications, code systems (Standards)

The topical classifications comprise systems like terminologies, nomenclatures and conceptual systems. Today these classifications are based on both international and national standards. However, information structures according to V-TIM of today seem to need supplementary examination. [INTERVIEW-TERNER-2008]

Examples of classifications (Standards) used in Sweden today:

- Systematized Nomenclature of Medicine, Clinical Terms (SNOMED CT)
- Classification of health care actions (KV)
- Classification of disorder and health problems (ICD10/KSH97)
- Anatomic Therapeutic classification system (ATC)
- Foundational Model of Anatomy (FMA)
- Classification of questions related to health care requests Classification of functional status, functional limitation and health (ICF-SE)
- Classification of functional status, functional limitation and health, Children(ICF-CY/WHO)
- Classification of reason for contact (KKO)

- Classification of surgery actions (KK97)
- Medical Subjects Headings (MeSH)
- National Product Register for Medicine (NPL)
- Nomenclature of properties and units (NPU)

Explanations of a selection of the standards in the list above are found in Appendix.

4.2.1. Code Systems

Examples of code systems are "reason of enlistment", "relatives", "sex" and "e-mail address". A code system has codes like the example below:

Code System:	RELATIVES
Codes:	biological parents, adoptive parents, siblings, biological children...

4.2.2. RIV-information Specifications and Profiles

The RIV-specifications are rule frameworks for health care interoperability. [RIV-2009]. An example of a RIV-profile is the RIV HL7v3 that adopts parts of the international HL7v3 standard on functionality for information internet exchange. An example of RIV-specification is for the Diagnosis information unit. This information specification describes in detail the information specified by NP to be included in a medical diagnosis.

4.2.2.1. Classes and Attributes

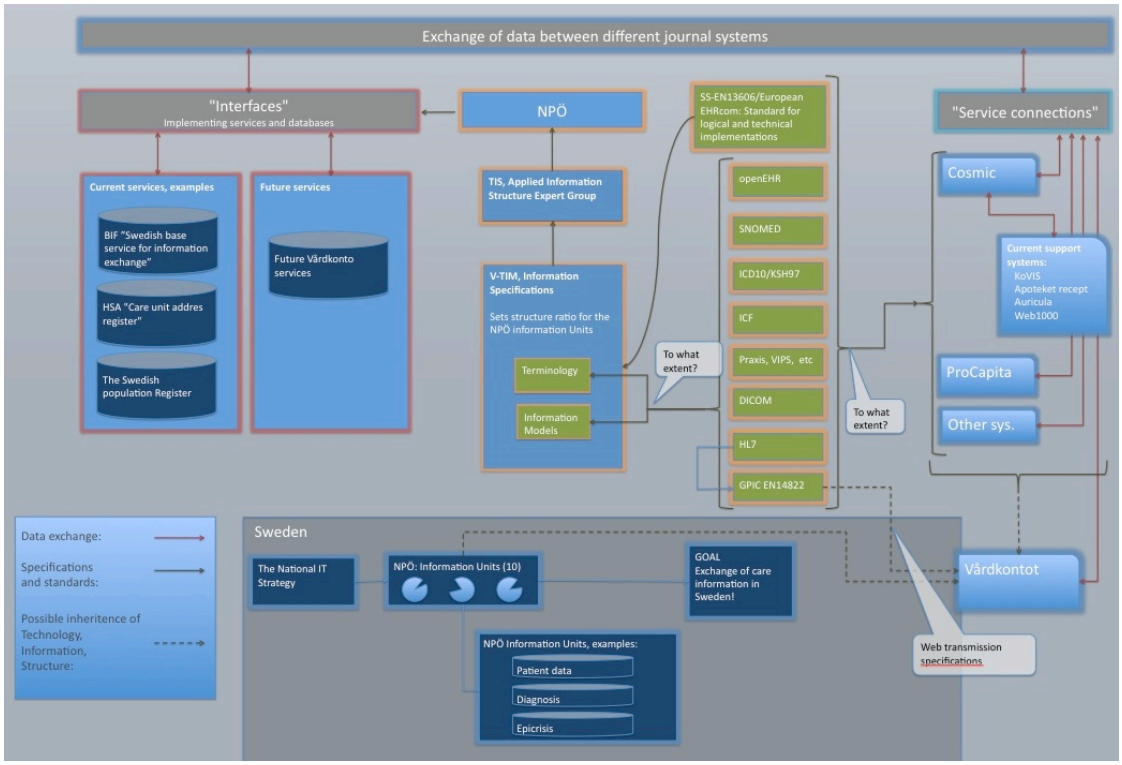
A class in the context of medical information specification defines a concrete thing (noun), as in the case of programming languages, such as "a patient", "a schedule" or a "document header". The attributes are the information content of the class. See example of RIV-specification of a class found in medical records:

Attribute	Description	Data type	Mult	Code System	Rule of decision
Person-ID	identity description of physical person	II	1	National personal ID-number	
First name	all of the individual names of the person	TXT	1..*	Current information from central register	The name rule 1982:670 http://www.skatteverket.se/folkbokforing/ovrigt/namn.4.18e1b10334ebe8bc80004083.html
Given name	the given name of the person	TXT	0..1	Current information from central register	

RIV-specification Example

5. Specification and Process Overview

In the picture below, the relations between various specifications and processes are shown. The Online Health Account should inherit functionality from both medical record systems and these specifications.



6. Selection of Classifications

6.1. HL7

Several current and upcoming standards in the field of health care are based on the HL7 Reference Information Model (HL7 RIM). The HL7 v3 standard also defines how health care information is to be transmitted by web services.

"Level Seven" refers to the highest level of the International Organization for Standardization (ISO) communications model for Open Systems Interconnection (OSI). This is the application level addressing the definition of data to be exchanged, the timing of the interchange, and the communication of certain errors to the application. This includes functions such as security checks, participant identification, availability checks, exchange mechanism negotiations, and data exchange structuring. HL7 provides health care standards. An example can be standard for tasks like message exchange where different capabilities are offered, e.g.: top-down message development emphasizing reuse across multiple contexts and semantic interoperability, representation of complex relationships, formalisms for vocabulary support and more.

6.2. DICOM

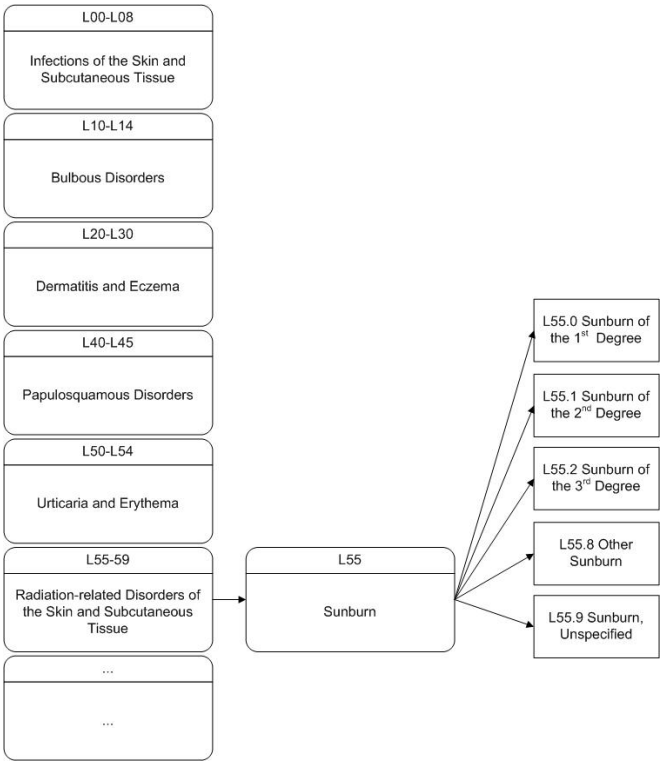
The Digital Imaging and Communications in Medicine (DICOM) is a standard for the communication of medical images and associated information. A data object in DICOM holds different attributes like patient identification, date and technical information about the equipment. This standard has been developed to meet the needs of manufacturers and users of medical imaging equipment for interconnection of devices on standard networks.

6.3. SNOMEDCT

Systematized Nomenclature of Medicine -- Clinical Terms (SNOMED CT) is a collection of medical terminology that is computer searchable covering almost every aspect of health care.

6.4. ICD-10

Describes diseases and related health problems. The Swedish adaptation of the standard is the KSH97. ICD-10 (International Statistical Classification of Diseases and Related Health Problems) provides codes to classify disease and a wide variety of signs, symptoms, social circumstances and external causes of injury or disease. Every health condition can be assigned to a unique category and given a code, up to six characters long. Such categories can include a set of similar diseases. Terms are structured in a hierarchical classification (see figure below) and give an easy way to navigate and seek for term to get an overview of terminologies.



Diseases of the skin and subcutaneous tissue.

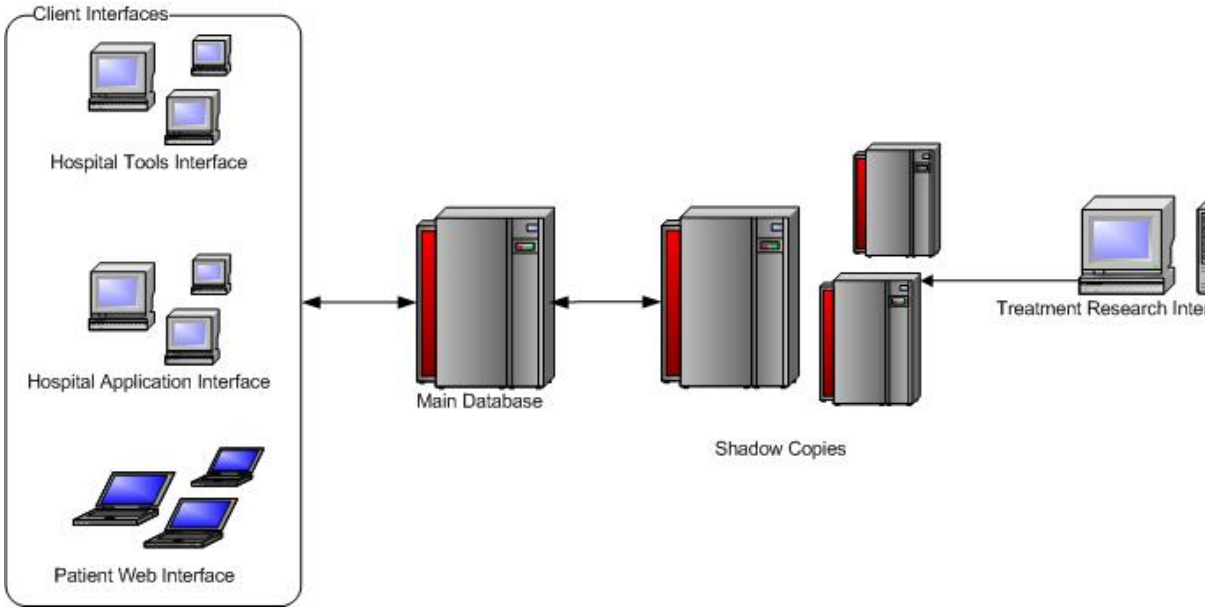
6.5. ICF

International Classification of Functioning, Disability and Health (ICF) is a classification of health and health-related domains. These domains are classified from body, individual and societal perspectives by means of two lists: a list of body functions and structure, and a list of domains of activity and participation. ICF complements WHOs ICD-10.

7. Epic Systems

7.1. Epic Systems Overview:

Epic Systems is a large healthcare software company in the USA. They have over 3,500 employees and develop healthcare software for over 20% of the nation's hospitals. This software helps care for 65 million patients. Epic offers its software as a solution complete with multiple components:



A graphical representation of the system and interfaces.

The solutions they offer are not cheap because they require certain hardware specifications and the price tag for the whole system is very rigid. Their clients are mainly hospitals with over 500 beds. The software is designed to deal with the patient during their entire stay at the hospital, from check-in to check-out. This includes all the monitoring a patient may receive while in the hospital as well as test results and doctors notes they might accumulate during their stay. Along with all this is the patient web interface so hospital patients can check records about appointments and test results from home.

7.2. Four Epic Interfaces

7.2.1. Hospital Application Interface

This is one of the bigger parts of the Epic software solution. This application is installed on all the workstations in the hospital. It provides doctors, nurses, secretaries and lab technicians with access to all the patient records. Each user profile sees different part of the application to prevent sensitive data from reaching the wrong people.

7.2.2. Hospital Tools Interface

There are many devices in the hospital like lab equipment, Intensive Care Unit equipment, and any other devices the hospital uses. This interface helps collect information on the patient directly from the machine so doctors are kept up to date.

7.2.3. Patient Web Interface

This interface is a way for the patient to keep in touch with their doctor and be able to stay current on test results, appointments and their own medical history. This is the system that and Online Health Account will function as.

7.2.4. Treatment Research Interface

Epic allows access to the shadow copies of the main server. This information ranges between days to hours old. However the information stored on the shadow copies is very useful to see how certain treatments helped patients in the long run. Because information from long term studies doesn’t have to be accurate to the second it can be run of the less busy copies and as a result doesn’t affect the main database which is being accessed constantly, by the other interfaces.

Appendix C. Security Issues

In the present discussion the focus is on the consequences of making the EHR accessible to the patient via the Internet. The discussion concentrates on the most essential security issues, namely *Authentication* and *Authorization* in order for such a system to be accepted among the patients and health care providers alike. The discussion does not deal with the important issue of authorization system *administration*. This is suggested as future work, see Section 11, “Future Work”. However, all security issues that relate to distributed systems on the Internet also apply to the discussion, and we have touched upon these in a subsequent section. The basics for a secure information infrastructure, i.e. secure connections with (SSL/TLS), the existence of a PKI-infrastructure etc. are taken for granted and will not be touched further upon in this document.

1. Authentication

1.1. Definition and Demands

Authentication is the process of determining whether someone or something is who or what it claims to be. For a project with high security demands, it is important that this process is secure, i.e. that it can not be manipulated, e.g. by a third party "stealing" the identity of a legitime user, thus gaining illegal access rights to the system.

The authentication system must be:

- Secure enough so that no one unauthorized can view or edit the patients medical records.
- Simple enough that a person with average computer skills can log in without trouble.

1.2. Authentication Strength

Authentication can be done in many different ways, depending on how secure you need the system to be. The most common method is called single-factor authentication. It requires a user to provide one way of justifying his id before being granted access, most commonly a name (user id) and a password. Each user either registers initially or is registered by someone else, using an assigned or self-declared password. To log in the user must know the declared password. The weakness in this kind of authentication is that the password can be stolen, revealed or forgotten. With the patients' privacy in mind, this may not the best authentication to use.

Two-factor authentication is a a more restrictive security process in which the user provides two means of identification, a physical token such as a card, and a memorized piece of data such as a security code. A common example of two-factor authentication is a bank card. The card itself is the physical item and the personal identification number (PIN) is the data paired with it. Two-factor authentication can drastically reduce the incidence of online identity theft, phishing attempts, and other online fraud, because the victim's password would no longer suffice to give a thief access to their information. The only way for an unauthorized person to get access to an account would be if he had access to both the computer (where he can scan the system for the password and enter the data manually) and the physical token (a card etc) of the victim. This is however very unlikely, and limits theft to people in the physical vicinity of the thief. However, existing two-factor authentication systems have shown to be expensive and inflexible for widespread implementations. These shortcomings are especially visible within organizations trying to protect their users from phishing attacks. In some cases organizations have even gone so far as to implement three-factor authentication systems. These involve possession of a physical token and a password, as well as biometric data, such as a finger or voice print.

The level of security will have a direct impact on usability and on the cost. For example, in three-factor authentication there are three things for the user to do and to remember before being authen-

ticated and this places a higher burden on the user. Simultaneously the cost increases for each item needed to authenticate a person.

1.3. PKI/Certificate based solutions

Electronic identification is being used more often when it comes to online services that require the user to identify him- or herself. One proprietary solution used is BankID. BankID is provided by many Swedish banks and is already widespread and used for many online services where the need for secure identification exists, for example, when submitting your tax return. Signing with BankID is a legally binding act equivalent to physically signing a contract [BankID1-2008]. Unfortunately, the BankID is a proprietary, non public and commercial service, and as such not well suited for the service under consideration.

1.4. One-time Passwords

In order to reduce this conflict without sacrificing security, it is desirable to adopt a flexible scheme, and An authentication service such as Electronic Identification (see below) or the use of one-time passwords sent to a predetermined mobile phone number is more secure and still easy to use.

The use of usernames and passwords are not sufficient enough in todays IT systems, a more secure login approach is one-time passwords. When you login to your application you need username, password and a one-time password (OTP) which is sent to your cell phone. Introducing OTP as a security solution is not a very complicated process and the need for educating the users is minimal. The solution uses existing infrastructure and resources, in other words, no further investments are needed. Here are some of the advantages of using one time passwords:

- No need for special devices, code cards or any other specific equipment for delivering the one time passwords.
- Users normally have their cell phone with them, making it convenient.
- Small investment, minimal support is needed.

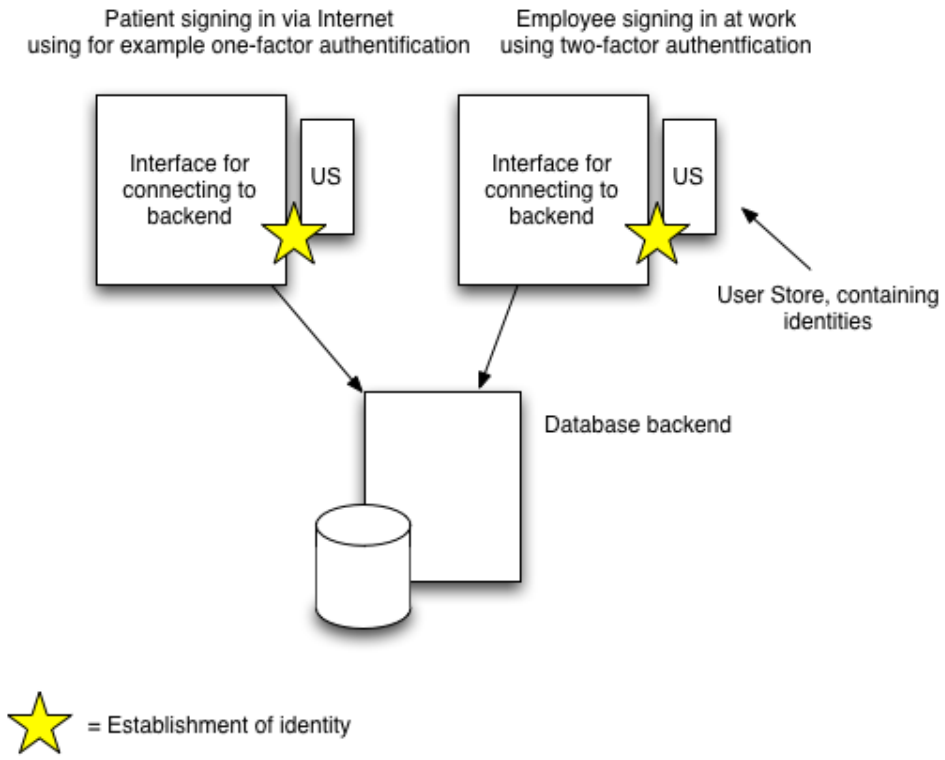
[NEDGE-2008]

1.5. Centralized versus Decentralized Authentication

The general case in health care is that there is one way to log in to the back end system that health care staff uses to access medical records (the system keeping all medical records and related information). When we consider an implementation of the Health Care Account it might be valuable to look into centralizing the authentication process. Centralizing the authentication process is closely related to Single Sign-On solutions used on the Internet. These are examined in a following section.

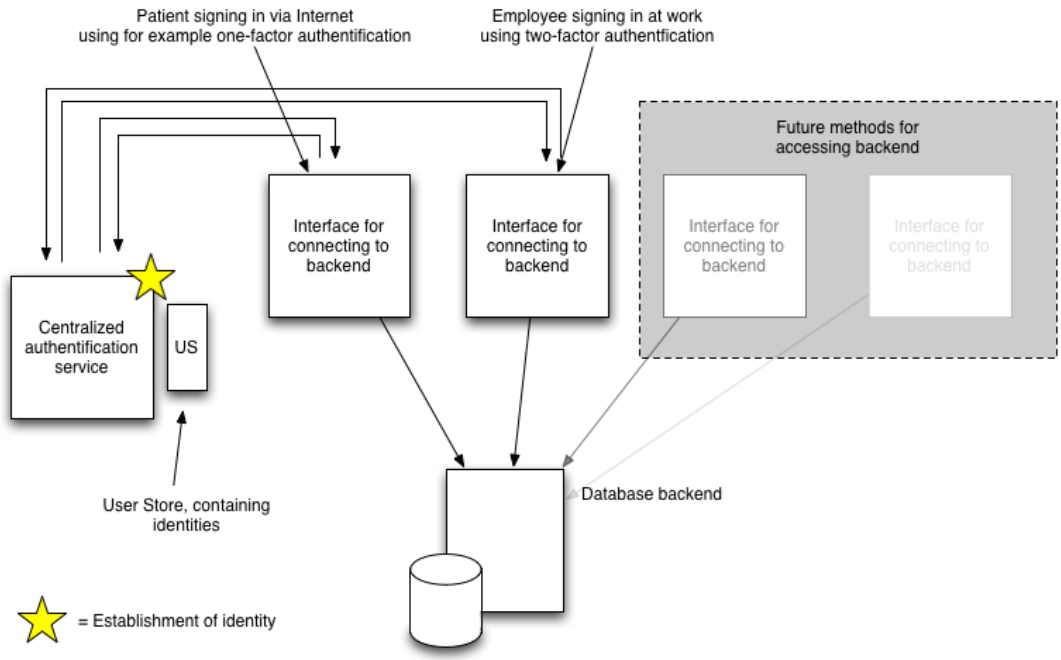
In decentralized authentication each way in to access the back end has it's own mechanism and identity database for authenticating users. This is generally the case in systems that where built to have only one way in. When adding the ability to connect through an internet portal we will need to add another interface (mechanism for authentication and authorization) for connecting to the back end. This interface will in the decentralized model have it's own mechanism for establishing the identity of the user and it will have it's own database storing the identities.

A third party connection to the back end, such as an interface for a mobile phone, would require another mechanism and user store for that purpose.



The decentralized solution

In the centralized model, we move the authentication process out of the interface for connecting to the back end. This allows the identity database to be kept in one place. As such, we are free to add more ways for connecting to the back end without having to re-implement an authentication checks.



The centralized solution

1.6. Single Sign On

1.6.1. Background

A possible situation in health care computer systems is the existence of a wide variety of support systems implemented at different times and by different vendors. When these systems contain information related to a patients medical record we have a need to make this information accessible to the patient. These systems could be:

- Servers for X-Ray images
- Systems for medical prescriptions
- Programs for booking of medical appointments

These systems differs in functionality and in physical location. Bear in mind that in an ideal situation, the patient should be able to access all primary care units in their area for making an appointment.

These systems will most likely already contain some kind of authorization feature. Some of the systems may even be available online. With the introduction of the Health Care Account, we will need to make all these systems available using a single entry and exit point. It is impossible to demand of the patient to remember log-in information for all these services. It will also place an enormous burden on the systems administrators when it comes to handling support errands related to patients having misplaced or forgotten their credentials.

1.6.2. Single Sign-On

The solution to this problem is to implement a unified portal for the patient to access all this information. When it comes to security we will require a Single Sign-On service to implement the authorization and authentication requirements.

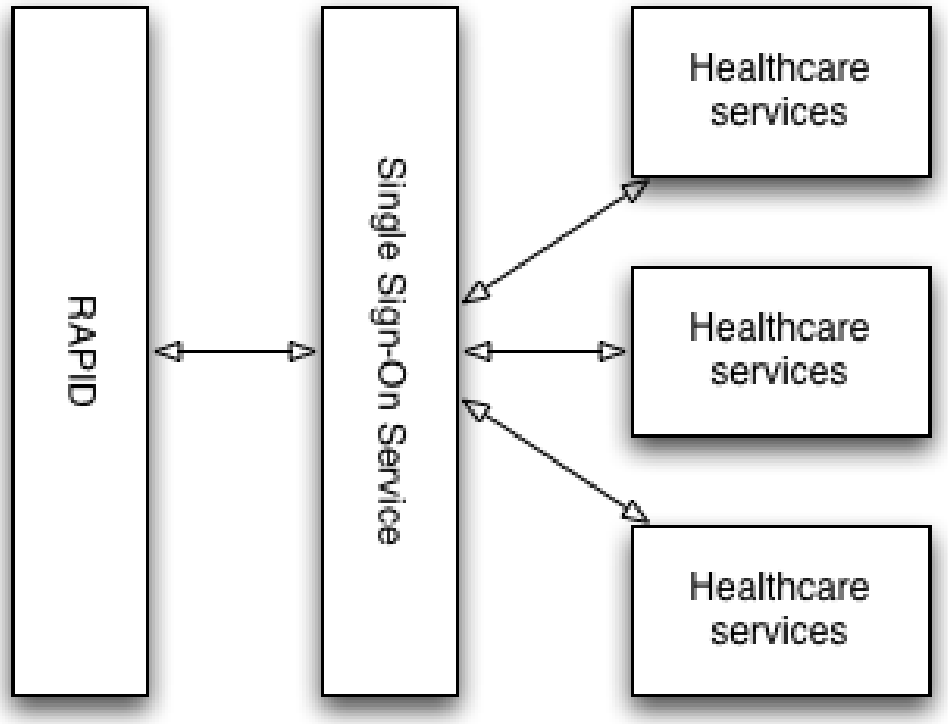


Diagram depicting the position of the SSO service in the information flow.

The Single Sign-On (SSO) allows the user to enter their credentials in one location (the Health Care Account portal) which will then allow him/her access to a set of security domains for a limited time.

This will require an addition or modification of the health care systems that contain the relevant information. In certain systems it may be possible to create a module for implementing the interface to the SSO server while other, typically older legacy systems, the system may need to be replaced. The cost for implementing the SSO interface will thus vary between systems. In modern modular systems it will probably only require the addition of a module but in older systems, where maybe the vendor have ceased development of the system, the cost will be greater.

1.6.3. SAML

SAML - Security Assertion Markup Language is an XML standard for exchanging authentication and authorization data between security domains. SAML is a standard set by the OASIS Security Committee. Many proprietary and open implementations of SAML are available and it is used as the standard underlying many web Single Sign-On implementations.

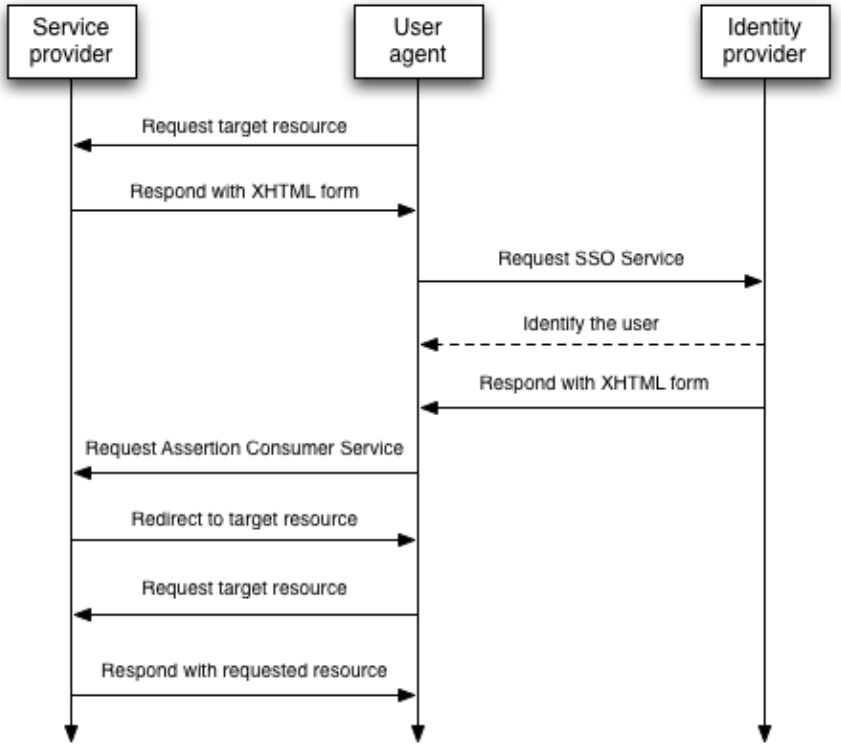


Diagram showing authentication process using a centralized authentication service implementing the SAML standard.

2. Authorization

2.1. Definition

Authorization is the process of deciding whether an *authenticated entity* may perform some action against some requested resource.

2.2. Authorization Mechanisms

ACL — Access Control Lists

An Access Control List is a data structure describing the access rights of the subjects to a *particular* resource. Thus, there is one ACL instance associated with each resource subject to protection. When a subject requests to perform an operation on an object, the system first checks the list for an applicable entry in order to decide whether to proceed with the operation.

Systems that use ACLs can be classified into two categories: DAC and MAC .

The original ACL based systems assigned permissions to individual users, which is unmanageable in an environment with a large and shifting population of users. This has led to more flexible approaches, such as RBAC and ABAC .

DAC — Discretionary Access Control

The Discretionary Access Control Policy restricts access rights to resources according to the identity of the subjects and/or groups to which they belong. The term 'discretionary' is used because third party access to a resource is at 'the discretion' of a user already having access to the resource.

MAC — Mandatory Access Control

In systems with mandatory access control, both subjects and resources each have a set of security attributes associated to them. Rules in global scope of the authorization system are enforced to govern the outcome of an attempted operation by a subject on a resource. As opposed to DAC, it is called 'mandatory' because the subject cannot in any way transfer access to a resource to another subject in the system

RBAC — Role Based Access Control

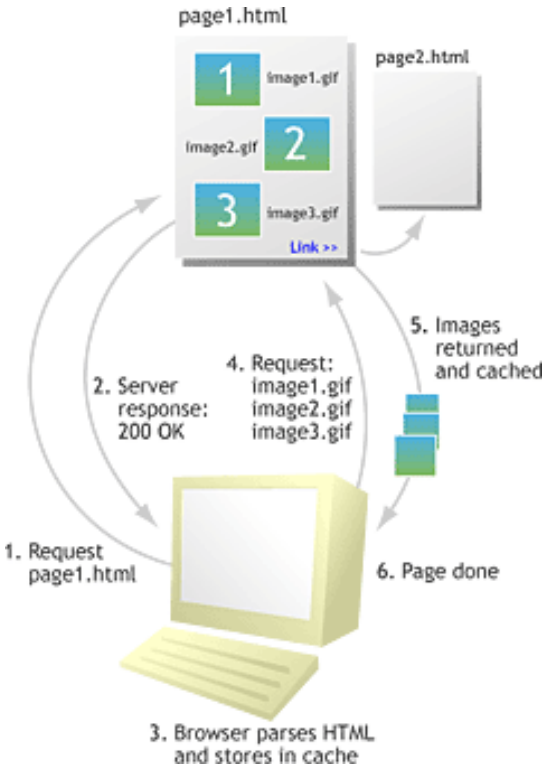
Role Based Access Control is an approach to authorization which grew out as a result with the difficulties to administer DAC and MAC based authorization systems. In RBAC, the subjects are decoupled from the operations they are authorized to perform on resources by introducing the concept of *role*. A subject can hold one or several roles, and each role encapsulates a certain set of operations which can be performed on the resources. At any given time, a subject can only take one role, the active role, but a role can inherit properties from a "parent role". It has turned out that RBAC is sufficiently flexible and general as to be able to simulate both DAC and MAC. Also, administration of the access rights becomes significantly less cumbersome, since a set of well thought roles tend to be rather stable. System administration is divided into the two distinct tasks of assigning roles to the subjects, and to assign authorized operations to the roles.

ABAC — Attribute based access control. Even an RBAC scheme lacks the requirements for authorization in a large-scale distributed environment. The problem is that in such a system, the subjects are so heterogeneous that the concept of role becomes less adequate. An access control system which can cope with this heterogeneity is needed. The Attribute based access control model evolved from this need. Instead of defining access permissions statically, the ABAC model restricts access based on a rule based comparison of subject and object descriptors, allowing for dynamically grouping objects and subjects. This dynamic scheme leads to the possibility of e.g. having different access rights at different times of the day.

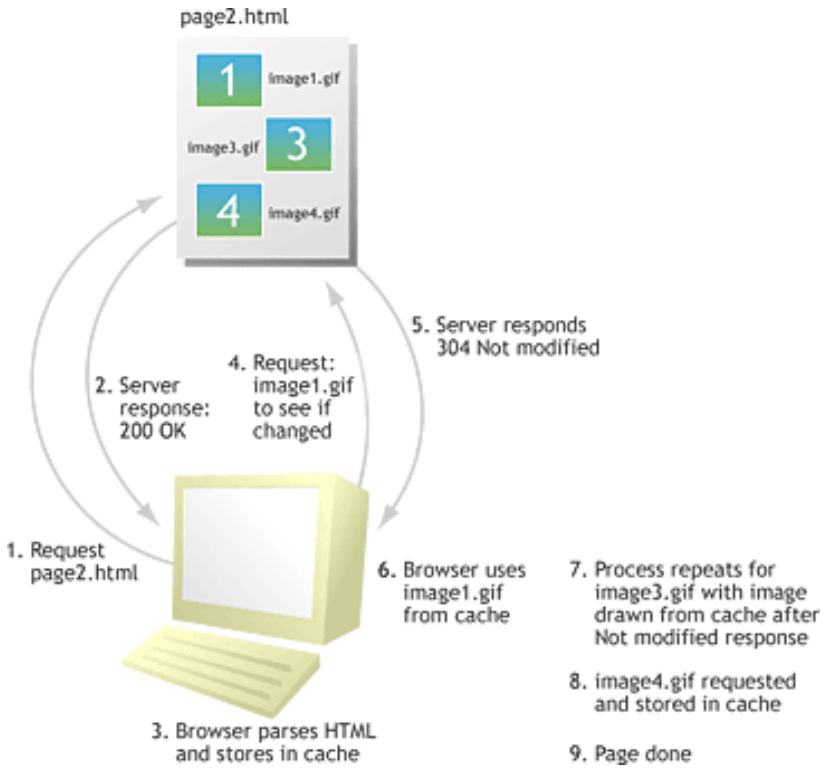
3. Other Security Mechanisms

3.1. Secure Cache Management

Web caching in short is the caching of web documents (e.g., HTML pages and images) in order to reduce bandwidth usage and server load. It stores copies of documents passing through it. So the nest time a user visits the same web page he will properly load most of the data from cache depending how often that web page is updated.



A Basic Example of Caching



For us to make the system as safe as possible for the user we need to make the cached data on the computer unreadable. For example, if a user goes to a public library to access his Health Care Account, the data in the cache would be readable by anyone using that computer (the worst case). The information in the medical record may be of sensitive nature and the release of said information could cause unfortunate consequences.

Web cache can easily be erased by the user to ensure that no one else can see the information in his medical record. This requires that the users are familiar with computers and have enough knowledge about web browsers and how to delete the content in the cache. Another way to solve this problem is to use a different approach of showing the information to the user. E.g., A Flash/Java interface could handle all the information shown on it and it would not be stored in the web cache like earlier. This would solve our problem.

The introduction of Internet Banking have driven the development of secure access to online services. The implementation of the Health Care Account share many of the challenges that the banks have been facing and thus many problems already have solutions. In our case with the Health Care Account the problem of securing the cache remains. The information stored in cache when accessing your internet bank consists of numbers and possibly names. This information is only sensitive to a certain degree and it will not allow a malicious user to transfer funds or make payments from your account.

The information stored in the cache after accessing the Health Care Account is of a different nature. The release of the data itself can be harmful to the patient to whom it belongs. This why we would like to trigger the deletion of, or preferably disabling, the cache when accessing the Health Care Account.

3.2. Intrusion Detection

For a complex distributed system exposed to the Internet it is impossible to be totally safeguarded against malicious attacks. New mechanisms and vulnerabilities are discovered all the time. Intrusion Detection Systems aim at detecting unauthorized access attempts to the system, not preventing it. However, such systems can be highly efficient in early discovery, thus contributing to damage control by serving as a second line of defence.

3.3. Audit -Log Analysis

An audit tool is a Web analysis software that parses a log file from a web server, and based on the values contained in the log file, derives indicators about who, when, and how a web server is visited. It is sometimes necessary to keep track of what changes were made to the database, and by whom. This is known as audit logging or audit trail.

The log-analysis is needed to see what is going in a system or a web page. By monitoring the activities we can detect people who are trying to do something malicious. The data needed to identify an attacker can be found in the logs of components that can be accessed from outside the network, such as a firewall, router, web proxy or mail server. Such logs will give the first indication of suspicious activity as an attacker needs to compromise one or more of these components before they can advance further into the internal network. Even once an external attacker has penetrated the internal network they effectively become internal and the same log sources that apply for a malicious internal user are used.

By using a Web analysis system we can detect these abnormal patterns and take action to prevent a breach or sabotage, and also to identify flaws in the system.

Log Analysis has its limitations . In general, it is an after the fact process, though some commercial products do offer real-time monitoring (making them similar in function to host-based Intrusion Detection systems). Logs alone can never provide the complete picture nor fully describe the intentions of the attacker. For example, a firewall may record an attempt to connect a port but it is unlikely to record what was in the IP packets. Therefore, it is only possible to surmise that an exploit was attempted but it is not possible to identify the specific exploit.

Appendix D. CESÅ

All requests about handing out records made in Uppsala County are handled by a censoring unit called CESÅ. According to statistics from 2007 and the first half of 2008 about 400-450 [EPJ-2008] of these requests are made every week and the records have to be reviewed for information that can be damaging for a third person that may have contributed with sensitive information concerning the person in question. How would an issue like this be solved if the records are to be handed out automatically via Internet? Letting the doctors flag this information as sensitive and have all information marked with this flag be invisible for the user is one way to deal with the input of new information. This feature can however be abused by the doctors to keep assumptions and other information hidden, so there need to exist some regulations to what information that the doctors are allowed to hide. Preferably the kind of information that now is censored by CESÅ. The issue with all sensitive information that a record may contain still remains. Even if only few contain this kind of information every record has to be reviewed to make sure it is ok to hand out and this would be a costly and time consuming process. This could be spread out over time by approving patients accounts when they sign up and in that process make sure his/her record is ok to hand out.

1. Telephone interview with Carola Hult, CESÅ, 17-nov-2008

How many medical records are handed out each week by CESÅ?

We hand out about 500 requisitions per week. A requisition may be ten different records, records from different units of a hospital that handles the same patient. A requisition is only one patient. A patient has the right to order his or her whole medical record but you can order only the last visit if that is desired

Who orders patient medical records? Only patients or can companies order them as well?

Medical Records are ordered by patient as well as insurance companies, lawyers and such. If it is not the patient it self that order the record a consent is needed

Are patient medical records censored before handed out?

It is extremely rare, but it happens. It can be done by for example hiding a comment.

What is censored?

Things that might hurt a third person can be censored. Say that a relative to a patient report information about the patient that would upset or hurt the patient if patient knew that the relative reported this information in question to the doctor. The information might have been reported without the knowledge of the patient. The censoring is done to protect a third part.

Appendix E. OpenEHR

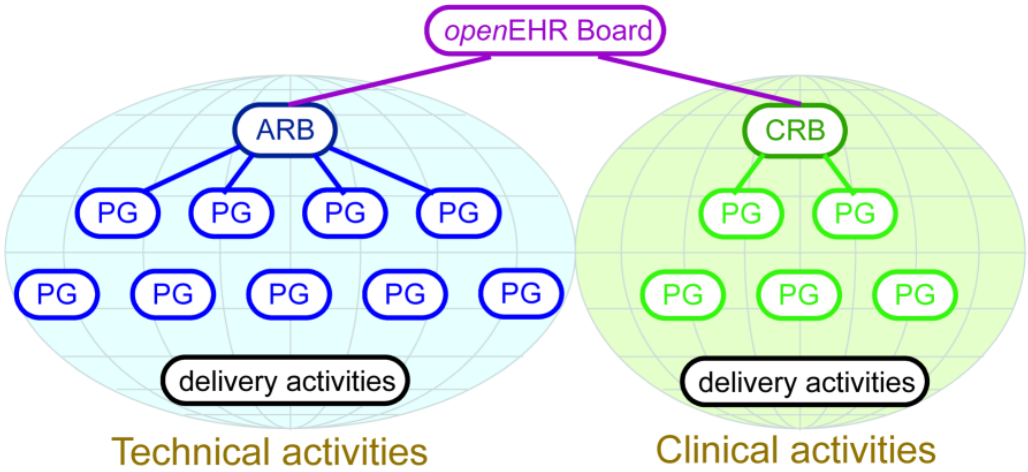
1. Introduction

OpenEHR is a new way of structuring, storing and managing patient data so that it can be shared and exchanged between different healthcare providers and other stakeholders in a safe and secure manner.

The OpenEHR foundation is a non-profit organization founded by the University College of London and Ocean Informatics Pty Ltd Australia. Their main aim is to develop an open, interoperable health computing platform with several requirements. (open EHR introduction, release 1.0.1, 2007)

1. Ability to record any clinical information
2. Archetype and template-enabling
3. Integration with terminology
4. Ability to integrate OpenEHR with messaging system
5. Ability to integrate with existing hospital information systems
6. Integration with applications
7. Distributed versioning
8. Componentized, adaptive and future-proof

Development of openEHR is carried out by different project groups (PG) and they are managed by two boards (one for the clinical side of the organization, and one for the technical side of the organization.)



OpenEHR board

The members of each board are specialists in their fields, and they help review the projects. An OpenEHR project must satisfy / be compliance to some rules defined by the foundation. For example a project is named OpenEHR if contributes to OpenEHR specifications or criteria, if it is being registered in the foundation and agrees to the intellectual property (IP) management. The use of version, Problems Reports (PR) and Change Requests (CR) is needed in order to make the project OpenEHR comply. Regarding licensing OpenEHR, as all open source projects, requests that all the OpenEHR projects must have a public license either the source code must have a open source license.

A product is said to be OpenEHR compliant if has been satisfying a testing procedure against test cases/data or material certified by the foundation. The OpenEHR intellectual property is concerned in different ways. The copyright is preserved through four kinds of deliverables: documents, software sources, executable software and knowledge products but all the OpenEHR are not requests to be copyrighted. Since the copyright law is unreliable for the software part of the project, the foundation rely on two kind of licenses (one for documents and one for software) to protect the developers. Alike the trademark and service-marks guarantee that a project is OpenEHR compliant when that is the fact. Further an end-use license preserve the rights of the users to not being altered their work even though the foundation does not consider the case when a business license is needed. [OEHRINTRO-2007]

2. Features

OpenEHR is an open standard which describes the management and exchange of electronic health data. It uses the two-level modeling architecture, which provides the interoperability between different standards and electronic health care data. First of all, the implementation of the reference model of the OpenEHR standard is available (which is provided by a Swedish software vendor). Based on the reference model, archetypes are built to describe the core structure and semantics of the health care standard. Templates are then derived from the archetypes to describe the actual standards and terminologies used in the real world. Archetypes and templates are implemented and maintained by domain specialists such as doctors and GPs and it is separated from the implementation and maintenance of the software system. Since the archetypes and templates are built using the ADL (Archetype Definition Language), they are guaranteed to be formalized and be able to communicate with each other. This allows the separation from the software implementation and the interoperability between different standards.

An important feature of the OpenEHR project is the high degree of personalization. If in the past the developer was to define the requirements of the system, have a collaboration with engineers to set up the environment and during the feedback stage discuss whether possible improvements could have been made, nowadays clinicians are getting directly involved in the development of the system. Therefore a solution with archetypes and templates could be one that allows a higher degree of personalization than traditional database systems by the involvement of the actual workers in the field. Such a solution is implemented in the OpenEHR project and further details can be found in the appendix section.

In conclusion, OpenEHR is a platform for other standards that separates the standards from the software implementation and meanwhile provides the ease interoperability between existing standards.

Two of the major challenges we identified of building an electronic health care system are interoperability and sustainability.

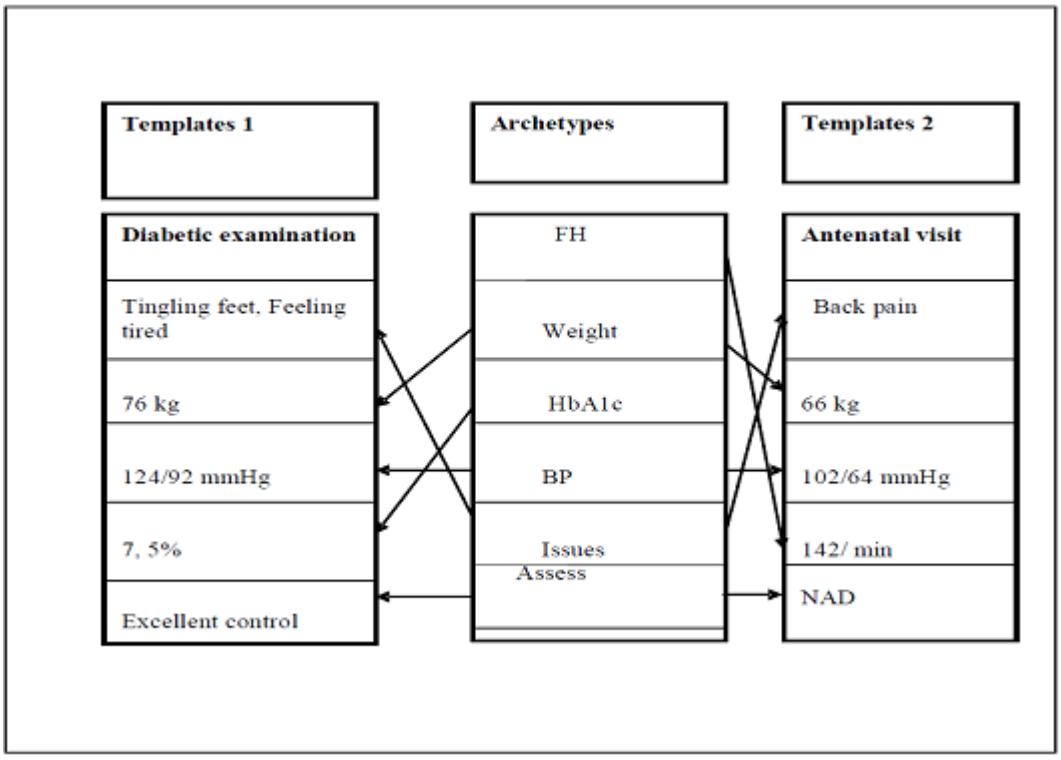
Interoperability can be interpreted from two aspects: electronic health care information and the software system. The first one is already addressed many times previously. The solution can be provided from different perspectives. From the information standard perspective, the emphasis is on the interoperability issue when the standards are designed. From the software perspective, a platform can be built, such as OpenEHR, which allows the co-existence of different information standards.

Another aspect is whether the healthcare system is built in one giant piece or in different interoperable parts. This will also affect the expense of the system. The interoperability of the software system relates to the communication issue between two different software systems. They could be: the kind of network protocol the two systems use to communicate each other; the language and format the two systems use to describe their own data, for example, XML (Extensible Markup Language) or ADL (Archetype definition language); furthermore, if a software system is developed and maintained by different organizations in a collaborative manner, it is also important to notice the interoperability among different modules inside the system.[OEHRARCH-2007]

2.1. Archetypes and Templates

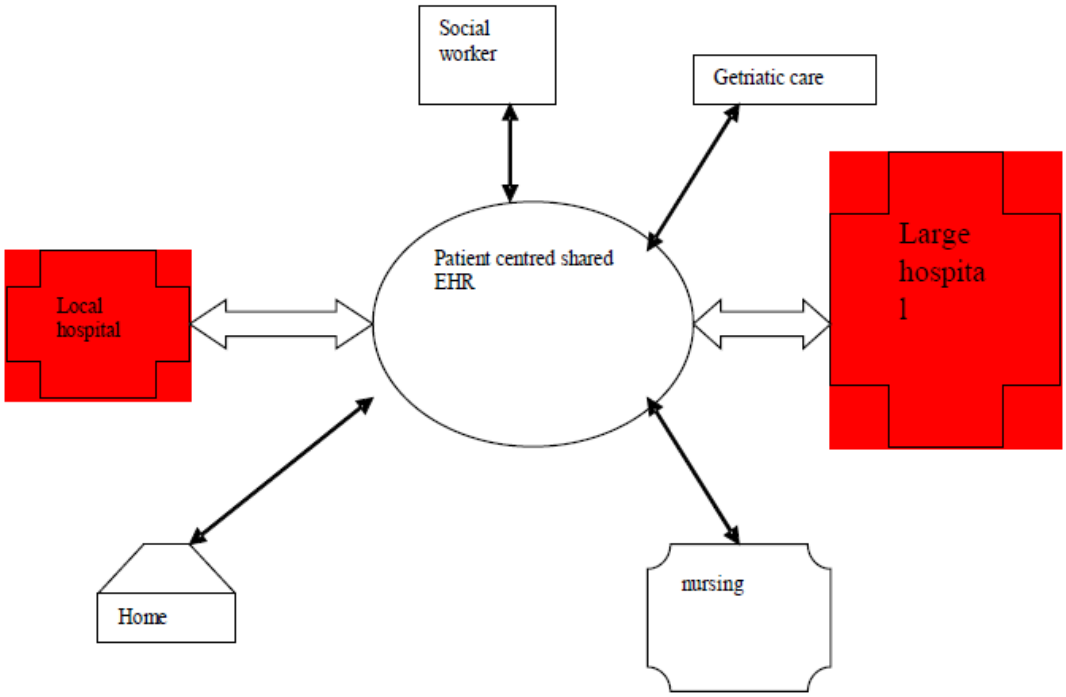
The OpenEHR architecture uses archetypes. Archetypes define how patient information will be structured. Archetype is a conventional model for a clinical information unit. The model contains

terms, classification and structure for patients record. Archetype defines how patient information should be structured in a patients medical record. They can be used for example to validate data input and enable searching of patient data.



Examples of An Archetype

Templates can be seen as a selection from archetypes and describe specific situations for example, setting-up for different measures for a diabetic patient.



Community Shared-care Context

3. Example of Usage

Among many organizations and companies, the Swedish ICT (Information and Communication Technology) provider Cambio has started to implement the OpenEHR model. For example, Cambio implemented the Reference Model, a core component, using Java programming language when enhancing their medical record ICT system, Cosmic.

The company sees a lot of opportunities in OpenEHR. The way of seeing OpenEHR as a standard is becoming more and more popular in countries such as Sweden, Norway, and Denmark. OpenEHR brings a paradigm shift in medical informatics system. By adopting the Archetypes paradigm of OpenEHR, the company will secure possibilities of information exchange.[OEHRARCH-2007]

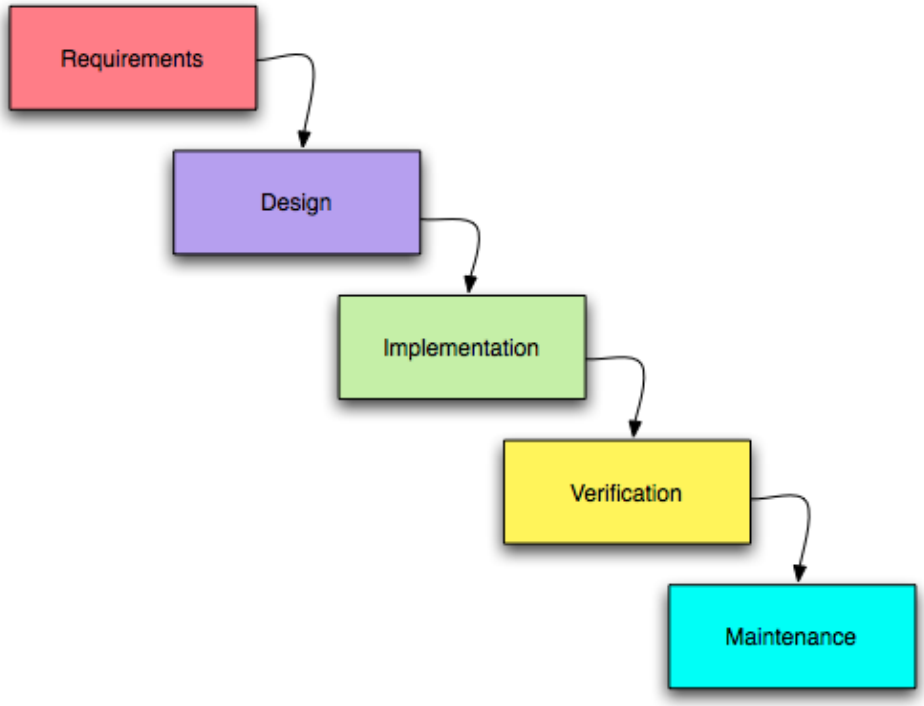
OpenEHR is an organisation based on research, reliable experienced and international standard in order to develop an open specification to software applications for the patient medical records.[OEHRARCH-2007]

OpenEHR organisation works in an open manner with experts, users within national and international bounds achieve to satisfy standards as ISO, CEN and HL7. The architecture of OpenEHR is designed to support the construction of a number of types of system. In this form, the OpenEHR services are added to the existing IT infrastructure to provide a shared, secure health record.

Appendix F. Development Model and Open Source

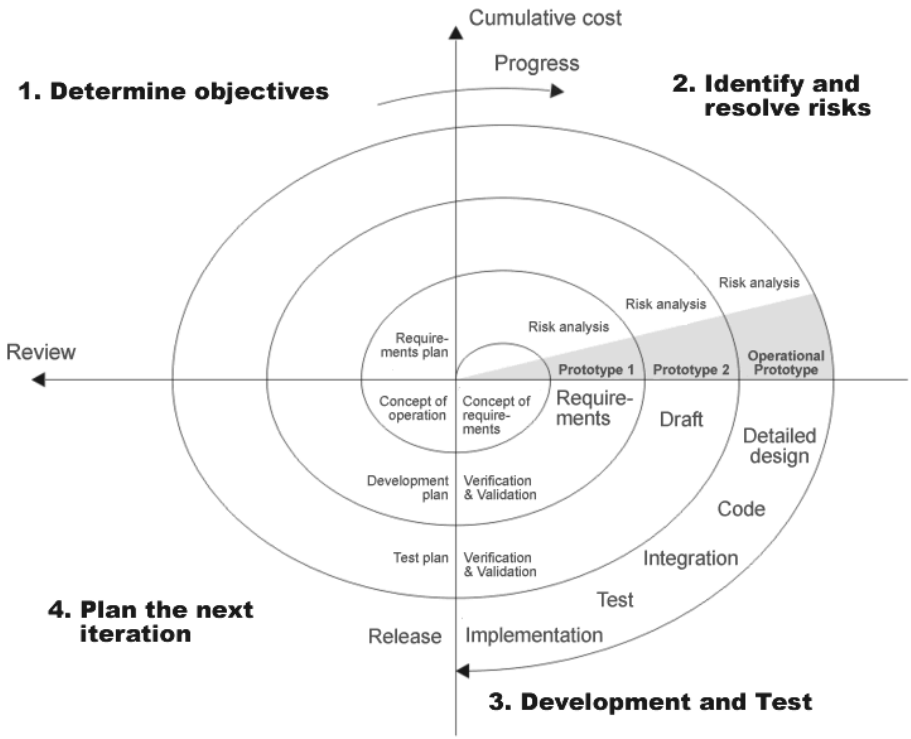
1. Development Model

The waterfall method, developed by Royce, strictly follows an ordered set of phases. These include requirements specification, design, implementation, integration, debugging, installation, and maintenance. This model is very similar to that of the manufacturing industry where minor changes to the beginning plan cannot occur. As a result, the initial planning must be correct. Unfortunately, this can lead to bugs because the model is unable to correct problems in previous phases. Reworking a phase is very expensive in terms of money and time. The forces the project to complete phases without full optimization.



The Waterfall Development Model

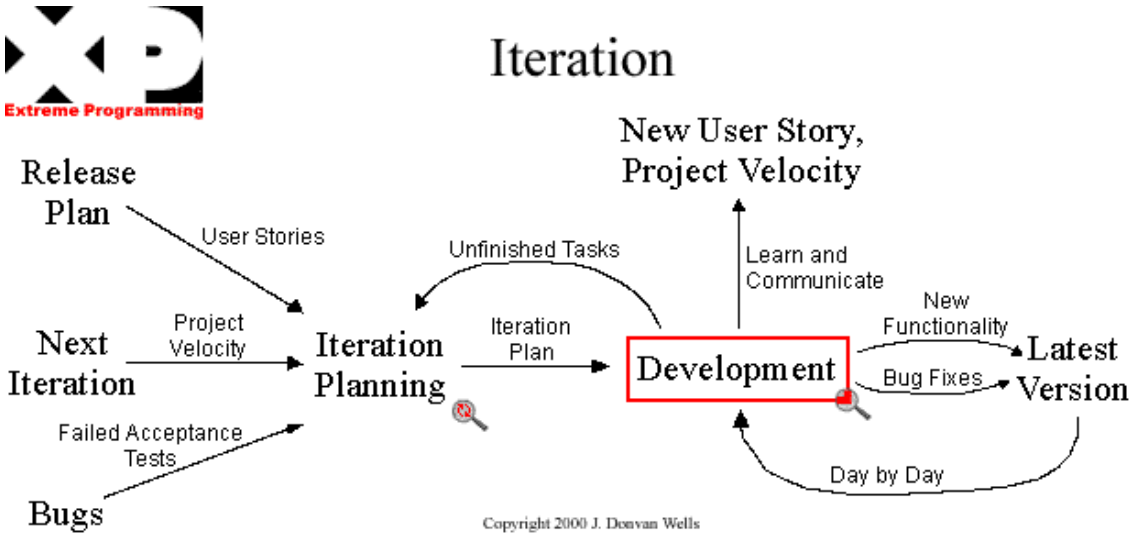
The spiral model is essentially an improved version of the waterfall model. Rather than moving linearly through all of the phases, the spiral model circles around to form multiple cycles. These cycles are referred to as iterations and follow the same order as the waterfall model. Typically, iterations last six months to two years. The iterative nature of this model allows for stable releases between iterations which enable the customer or client to use the software and give feedback.



The Spiral Development Model

Another category of models separate from those which are rather structured and ordered is agile. While it sounds rather counter-intuitive since it places less emphasis on structure, the agile method of development has been shown to be very effective. This method is composed of a few essential components that ensure that all members of a given team are productive and efficient. At the beginning, the visioning process is used to help focus the team on key business values. During project initiation, the project is better defined through brief documentation. The scope, objectives, constraints, clients, risks, and other essential things pertaining to the beginning of the project are stated.

Extreme Programming is a subset of the agile models category. It focuses on short iterations which are determined by user stories and client interaction. Before each iteration of development, a meeting is had with the client to review the previous iteration, discuss the next iteration with the client, and create user stories with the client. User stories are non-technical descriptions of the requirements of the next iteration, such as the user will be able to select text by highlighting it. These stories are simple enough that the end user or client can create and understand them, while still allowing the developers enough detail to understand the requirement. One key element of Extreme Programming is client interaction: if there are questions about the user stories, or if the user stories are ambiguous, then there must not be anything to stop the developers from getting this problem sorted out by the client, usually by asking them.



The Extreme programming paradigm

Epic Systems is a privately owned healthcare software development firm located in Madison, WI. They serve approximately 20% of all patients in the United States of America (about 58 million people). Several of the major challenges they have identified in software development for the healthcare industry are the fact that healthcare is real-time, all the time. Downtime has major consequences: emergencies dont wait for server maintenance, so the software must be stable enough to never go down, and be able to be updated real time. Scalability was another major concern for them, there are lots of people, and the amount of data each person has is substantial. The ability to deal with ever growing data and client base are major concerns for any healthcare software system that tries to help large firms. Another advantage is very good MANUAL quality assurance: having professionals in the healthcare field in on the usability testing is very important, as the end product will be used by them.

2. Open Source

Free as in speech, not as in beer. This is a common statement when referring to Open Source. Most preconceptions about open source meaning free software refer to the free beer concept, which is in reference to the cost of the software, not the availability of the code. The idea behind the freedom of access to the software rights helps to increase the reuse and redistribution of code. This is important because it reduces cost and time of software development by the use of modules which have been created before. Also, when a project or company of the closed source format fails, the software they created tends to disappear. The redistribution of code that Open Source allows, in the free as in speech way, multiple groups to attempt to succeed with the same project and not have to start over again. This allows multiple approaches to a single problem, and even enables merging of these projects later.

3. Development Strategies

The number of required fields during the data insertion phase greatly increases the complexity of the interface therefore reducing the usability. As the complexity increases the difficulty in filling in the required fields with the correct data becomes greater.

If all the items have to be inserted in the first page, this will create confusion. The time spent to complete the insertion stage will, in this case, be much higher compared to the case where different data is inserted in different pages.

Another key aspect is the importance of the fields being computed. Considering the amount of time the emergency area of a hospital has to input data, a detailed view may be less important when compared to an area curing cancer diseases. The simplification of the system will help hospital

assistants in different parts of the hospital to perform more efficient work in a simple manner because the interface is customized to their section.

Another key point to consider is which data should be inserted and in which way. From a computational point of view, the insertion of an identification number should not be a time consuming task. In a hospital located in a large city where the number of accepted patients in the emergency unit will be considerable, then a bar code reader for identity cards will expedite the processing of new patients. This is a simple example of how the number of fields could affect efficiency, time and quality of data insertion.

By utilizing open and closed standards or by having open or closed source, development of a health care system can be done in many different ways.

A distinction should be made between open and closed systems. Systems developed in the open source manner have source, specifications, and all other related documents available to the public domain. Closed systems are those that are developed with all of the above in the private domain. Not all systems utilize this black and white designation. Systems can be comprised of open and closed components. This classification is needed while different architectures imply different development strategies and therefore different costs.

An open source solution of the project will definitely lower the expense of maintenance.

The use of an openly developed system will probably avoid a possible vendor lock-in situation. Because the system is part of the public domain, the original developer is not required to continue development or maintenance of the project. A vendor could rely on a third party escrow agreement, so in the case of bankruptcy, another vendor can take over and continue the previous job where the first party left off.

A closed source development may result in the loss of the source if the company developing the system becomes bankrupt. All future modifications and changes that are desired by the client must be performed by the original company.

A different opportunity could be the one provided by an open source solution. The wide variety of developers that an open source development can attract allows for more international cooperation. This is a larger and more diverse developer base for debugging and feedback.

Open source software refers to software whose source code is available to the end user. This allows the users to use the software and improve or customize the software however they want. A large portion of open source software is developed by volunteer developers and thus cost almost nothing in the development phase. There are also companies who specialize in open source software, who have the same expertise and cost as a closed source company. There are plenty of successful open source software that serve as good examples. Ubuntu, a Linux-based operating system, is by far the most successful Linux distribution. One of the crucial reasons is that through open source the source code is available to developers as well as users who are willing to participate in the community to improve the software. Canonical, the company which supports Ubuntu, is making profits by providing consulting services based on their expertise in the operating system.

Another important aspect in the design of a health care system is the use of standards.

If the system is supposed to be interoperable, it must rely on some standards of international, national or local use that are used by the system it wishes to interact with. In this stage it is still important to consider which standard should be adopted while one could run into a lock-in situation. If for example the standard being adopted will not be an international one, the interoperability of the healthcare system will be limited to just the country who uses the same standard.

In terms of further development of the health care system, general and technical recommendations should be considered.

In the preliminary stage (development) of the system, particular attention has to be made to avoid vendor lock-in or the monolithic situation where the patient will be the last to get benefits to such a setting.

Open system might be considered in order to allow future interoperability between other systems/applications. Therefore the use of such solutions combine with a modularize architecture is highly recommended because will offer the possibility to get the best component with the best price. This might help vendors to invest in a worldwide scale and will certainly higher the quality of the products. Last, but not least, the possibility to exchange information between systems distributed on a local, national and international level has to be considered. It will be much appreciable to choose a project that includes an international view (since the design stage) than to choose a local one where the investments may vain in the future.

In order to achieve a good set up for a health care system some recommendations might be considered. Firstly the use of open system (instead of closed one) will help our commitment to get a stable settings for further system developments. By modularization (system created on different components) every component will be buy with the best price in the market. Modularization will get vendors to invest of R&D in a worldwide scale and will help the interchange between different components in different systems. A design of a new system, or the choose of an existing one must consider the possibility to interact with existing systems therefore the international ones will be preferably choose and the use of open source solutions might help a project to have a wider view.

There exists tons of health care and medical standards around in Europe. Different standards cater to the needs of specific user groups. They could be as small as a local health care clinic, a group of regional hospitals or a national organization. The challenges of information interchange between these different standards are obvious. From the medical staff's point of view, they use different terminologies and expressions to express themselves. Even though they use the same term, the semantics for that term could be different. From the software vendors point of view, a minor difference between the underlying implementation of the standards, such as the interfaces which connect different parts of the system, could lead to serious interoperability problems.

All of these standards have been adopted by different organizations and users to a certain extent and it is not feasible for these organizations and users to discard the existing one and shift to a new unified one.

Dipak Kalra, Architecture Review Board & Clinical Review Board Member of the OpenEHR Project states that "the amount of resources required to start a new design are considerable. There are many systems in existence who can be upgraded or modified to the requirements for less than starting a new design. Now its not the time for any project to look at electronic health care records and start again. I think that time is over. It was relevant in mid 90s and in 2008 I dont think that will be any good reasons to start again. There's too much already available now" (from interview with Dipak Kalra 08/12/24 CHIME)

Sustainability is a common issue faced by software vendors that are developing large scale information systems. And in the case of an electronic health care system, it is extremely large and complex. Most of the time, one software vendor does not have the resources to implement the entire solution. Therefore, collaborations take place during the development and maintenance phases. Local modifications of some system components, such as parsers and network communicators, can hinder the communication between systems or even greatly reduce the interoperability between them. Therefore, certain methodologies need to be discovered and employed to facilitate the collaborations during the development phase and an environment needs to be set up to allow the software survive for a long time and on a acceptable cost.

The economy issue is another interesting topic when talking about a system like RAPID. This issue can be addressed in two perspectives, the cost of developing a software system and the cost of maintaining one.

Usually, the cost of developing a software system is determined by the complexity of the software as well as the development model adopted. The more complex the software is, the more it costs. Also, if the development breaks the developing process into small pieces and allows several teams to work parallel, the overall time span of the developing process shrinks and the cost is reduced.

The cost of maintaining an information system is another important fact that needs to be taken into consideration, particularly with RAPID, as a life-long health care system. Different approaches can

be used to reduce the cost, such as setting up better information standardization, regional or cross country collaboration etc.

One of the things that can be compared is the adoption of close source and open source software. If a close source software company is chosen, then the rights to the software source are locked to the particular company and further services must be purchased from that company only. However, if the development company does not own the rights to the source, different software vendors can bid for a lower price for their service. Therefore, the cost spend on the system maintenance can be reduced.

Appendix G. Authors

This white paper is authored by the members of the RAPID project. The RAPID project which stands for “Remote Access to Patient Information Digitally” is a joint collaboration between Uppsala University and Rose-Hulman Institute of Technology. The twenty eight project members consists of twenty two students attending the course “IT in Society” at Uppsala University in Uppsala, Sweden and six student attending the course “Computing in a Global Society“ at Rose-Hulman Institute of Technology in Terre Haute, United States of America. On a mandate from Uppsala county council, the goal the of the project has been to produce a white paper addressing issues and possibilities of introducing an online health account where patients have access to their own medical record.

The project was initiated in September 2008 and the majority the project members have either software engineering, computer science or information technology background. Research and interviews has mostly been done in the Sweden and United States of America but other countries such as Germany and Great Britain has been taken into consideration. Although being an educational purposed university course commissioned project the involvement of trade professionals has been fairly high. The project has strived towards delivering an end product that is comparable with trade standards, but the academic background of the project should not be disregarded.

Zardasht Abdal	Zaid Al Abbasi
Patrik Backvall	Johan Bergman
Aaron Blankenbaker	Fredrik Brattlöf
Joel Edlund	Derek Hammer
Per Hamrin	Roland Hedayat
Magnus Johansson	Holger Karlsson
Jamie Kleeman	Daniel Knight
Isaac Lee	Jonas Lindén
Ida Lindgren	Jonas Lindholm
Samuel Oest	Martin Persson
Christian Ruhinda	Daniel Sabin Jr.
Poia Samoudi Asli	Paolo Santin
Bowen Sui	Mattias Wiklund
John-Oskar Ahlström	Henrik Åkerstrand

Appendix H. Acknowledgements

Special thanks to everyone who have contributed and taken their time to help us. Your contributions have been greatly appreciated and influential.

Benny Eklund (Uppsala County Council)

Rong Chen (Cambio Healthcare Systems, Chief Medical Informatics Officer)

Dipak Kalra (OpenEHR Project, Architecture Review Board & Clinical Review Board Member)

Rebecka Janols (Uppsala University, Research Assistant)

Torbjörn Schön (Uppsala University Hospital, Administrator Electronic Patient Record)

Mervi Friberg (Uppsala University Hospital, IT-support)

Ulrika Herman (Samariterhemmets vårdcentral, Medical Secretary)

Ture Ålander (Ture Ålander Family Practice, Medical Doctor)

Nils Daniels (TeliaSonera)

Björn Gustafsson (IT-Security Expert, Skandinaviska Enskilda Banken)

Mats Daniels (Uppsala University)

Åsa Cajander (Uppsala University)

Tony Clear (Auckland University of Technology)

Bengt Sandblad (Uppsala University, Head of Division Human-Computer Interaction,Professor in Human Computer Interaction)

Niklas Hardenborg (Uppsala University, Ph.D in Human Computer Interaction and Usability Designer)

Gunilla Bergman (Retired Pediatrician)