Survey on Healthcare IT Systems: Standards, Regulations and Security

Christian Neuhaus, Andreas Polze,
Mohammad M. R. Chowdhuryy

Technische Berichte Nr. 45

des Hasso-Plattner-Instituts für
Softwaresystemtechnik
an der Universität Potsdam

Universität Potsdam

HPI Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Softwaresystemtechnik an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Softwaresystemtechnik an der Universität Potsdam | 45

Christian Neuhaus | Andreas Polze | Mohammad M. R. Chowdhuryy

Survey on Healthcare IT Systems

Standards, Regulations and Security

Universitätsverlag Potsdam

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind
im Internet über http://dnb.de/ abrufbar.

Universitätsverlag Potsdam 2011
http://info.ub.uni-potsdam.de/verlag.htm

Am Neuen Palais 10, 14469 Potsdam
Tel.: +49 (0)331 977 4623 / Fax: 3474
E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam** wird herausgegeben von den Professoren des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam.

ISSN (print) 1613-5652
ISSN (online) 2191-1665

Report
Christian Neuhaus, Andreas Polze: Hasso Plattner Institute at Potsdam University, Potsdam, Germany
Mohammad M. R. Chowdhury: Postdoctoral Fellow at UNIK-University Graduate Center, Kjeller, Norway

Online veröffentlicht auf dem Publikationsserver der Universität Potsdam
URL http://pub.ub.uni-potsdam.de/volltexte/2011/5146/
URN urn:nbn:de:kobv:517-opus-51463
http://nbn-resolving.org/urn:nbn:de:kobv:517-opus-51463

Zugleich gedruckt erschienen im Universitätsverlag Potsdam:
ISBN 978-3-86956-128-8

IT systems for healthcare are a complex and exciting field. One the one hand, there is a vast number of improvements and work alleviations that computers can bring to everyday healthcare. Some ways of treatment, diagnoses and organisational tasks were even made possible by computer usage in the first place. On the other hand, there are many factors that encumber computer usage and make development of IT systems for healthcare a challenging, sometimes even frustrating task. These factors are not solely technology-related, but just as well social or economical conditions. This report describes some of the idiosyncrasies of IT systems in the healthcare domain, with a special focus on legal regulations, standards and security.

Contents

1. Introduction

Computers are now widespread among almost every aspect of our lives, and in many cases their introduction brought tremendous benefits. Some tasks were made considerably easier, some were even made possible in the first place – such as extensive computational tasks and information search over very large amounts of data. Especially administrative processes and information exchange of large organizations could not function without computers anymore. Computers facilitate these tasks by providing information where it is needed.

A sector that depends very much on information but seems to lag behind these developments is the domain of healthcare[5]. In terms of computer usage, hospitals are even seem to be outdone by the public administration: collection of data is mostly done on paper and is seldomly fed into a computer system. The little data that does reach a computer system usually stays in isolated systems, such as a database for lab analysis values.

However, especially in the healthcare domain, a closer integration of systems and a use of computer-aided data processing could be very helpful (see section 2.2). Like almost no other domain, quality of healthcare depends on the availability of data. When a clinical decision has to be made, all the required information has to be available[4]. Integration of Information and Communication Technology (ICT) enables faster feedback, remote monitoring and analysis and above all ensure mobility of individuals across countries.

Neither these benefits come for free, nor can they be achieved without proper knowledge of the pitfalls and complexities specific to the domain of healthcare. This report tries to show the most notable characteristics of this domain, with a special focus on legal regulations, standards and security and privacy aspects.

The report is structured as follows:

Chapter 2 gives an introductory overview of the characteristics and adversities of the domain of software development for IT systems in healthcare.

Chapter 3 describes the most noteworthy sources of legal regulations concerning the development of IT systems and software in the healthcare domain.

Chapter 4 explains the importance of interoperability of medical devices and software in the healthcare domain and introduces the most important data and communication standards that enable the development of interoperable products.

Chapter 5 gives an introduction to the computer system security from a scientific perspective. It explains the very high importance of security and privacy considerations in the healthcare domain and shows by which technical means security goals can be achieved.

Chapter 6 summarizes the report. It lists the key points to keep in mind when dealing with software development for healthcare.

Appendix A presents a selection of industry solutions and describes their properties.

2. Healthcare and IT

This chapter examines the distinctive features of processing medical data in computer systems, how it is possible to benefit from that and identifies the obstacles, namely the security and privacy concerns. The descriptions of healthcare IT systems present the motivations of focusing on the security and privacy aspects in healthcare IT sector.

2.1. Characteristics of Healthcare IT

Computer systems for the healthcare domain differ greatly from other domains of IT in certain aspects. The reason for this are the high demands made on these computer systems – because of the special sensitivity of medical data.

2.1.1. Sensitivity of Medical Data

The term *medical data* applies to all data that is related to a persons health and medical history. Data of this kind is considered especially sensitive and in need of protection. This is understandable, since even fragments of medical data can reveal very much information. In this, medical data is very *side-channel*-prone[36]: For example, mere prescriptions of specific HIV-suppressive drugs clearly indicate that the patient is HIV-positive, although the prescription of the drug itself is not a diagnosis at all and may sound harmless and unimportant to someone unfamiliar with the name of the drug. In general, information about STDs opens up room for speculations on how these were acquired. And a patient may simply want to keep quiet about a condition he'd rather deal with himself.

The sensitivity of medical data and medical IT systems is explained in more detail in section 5.1.1.

2.1.2. Strong legal regulation

Due to the sensitivity of medical data, healthcare IT systems are subject to strong legal regulation: The processing, storage and dissemination of medical patient information is subject to many laws and regulations, which vary greatly between different countries and continents (see section 3).

2.1.3. Distributed Nature

As an additional challenge, medical IT systems tend to be highly distributed since medical treatment is a distributed process as well. Traditionally, distribution of computer systems would span over a single hospital. Today, however, cooperation between medical institutions crosses the borders of hospitals and even countries and include very large institutions as well as single doctors offices. The connection may even reach into the patients home, as telemedicine solutions become increasingly popular.

As a consequence, rights management and privacy policy definitions for processed information are not easy to determine: Many users from many domains with different functions may need access to stored medical data at different times. The roles that the users play may change at any time. An example for this are context-dependent privileges: The user rights for data access may depend on the context of the situation (i.e. emergency access).

2.1.4. Heterogeneity of Systems

A lot is to be gained by the introduction of modern IT systems in healthcare – this, however, does not mean that computer usage is totally new to this domain. In fact, computer have been used a lot in the healthcare domain, but these solutions are often legacy systems, independently developed insular solutions for single customers and incompatible to other systems [43].

Shortcomings of legacy systems The most important problem with many legacy IT solutions is the lack of interoperability. The desired level of integration is business process integration so that administrative and clinical processes can make use of IT capabilities with very little manual intervention. This, in turn, requires IT solutions to be interoperable on the functional level and on the data level. *Functional integration* requires the exposure of implemented functionality to the outside of the systems – so it can be used by other computer systems over a network. *Data integration* stands for the availability of interfaces for exchange of data with other systems – and a shared data model and a shared semantic understanding of exchanged data. These interfaces are often missing in legacy systems.

Furthermore, legacy systems often suffer from typical software engineering shortcomings such as poor maintainability and extendability. These problems often prevent further use when the environment of these systems changes and requires updates and adaptions.

Rip-and-Replace vs. Integration In spite of these problems, legacy systems are often kept in use as long as possible. Healthcare is a higly specialized domain – and many legacy solutions are custom developed for their application domain and serve their purpose well. Special application scenarios may even be beyond the capabilities of commercial off-the-shelf software and encapsulate domain knowledge and workflow

processes that cannot be easily extracted. Additionally, training personnel for a new software product may be very expensive.
Therefore, existing IT solutions are often re-engineered and adapted to be integrated into lager new IT systems instead of replacing them.

2.1.5. Usability requirements

Healthcare is a domain with high cost-pressure and its employees – nursing staff and physicians – are facing a high workload. Therefore, IT solutions in healthcare should integrate into the workflow of staff and slow it down as little as possible. If a new solutions does induce additional efforts, its rewards must clearly outweigh these efforts[6]. As a consequence, products and solutions should fulfill high usability requirements in interface design and operation.

This is especially important for the design of solutions for access control mechanisms: These may considerably slow down work by requiring the user to remember many different passwords and enter them frequently. As a consequence, these mechanisms are often circumvented and rendered useless[23]. More thoughtful approaches such as Single-Sign-On and RFID-tokens could remedy such problems.

2.2. Benefits and Barriers of Healthcare IT

Healthcare is a very complex domain that depends very much on the availability of information. The main responsibility of a physician it to make decisions on a treatment for patients. The indispensable foundation for these decisions is the availability of all relevant information from the patients medical history. This involves the treatment process, diagnoses and recorded vital parameters. The physicians task of decision-making therefore can be seen as gathering and acting on information[25]. Computer can facilitate this work tremendously, as gathering, management and presentation of information is their prime strength (see *Electronic Health Records*, 2.3.1).

Computer systems can also be very helpful with tasks related to resource planning, such as creating schedules for long-term treatments in accordance with the available resources at the hospital. It may be hard for a person to keep an overview over several timetables, which is fairly easy to manage by computers. The result could be a well tuned schedule for the patient, and offers the clinics the possibility to maximize the usage of their treatment facilities. This is a tremendous economical advantage, since medical equipment can be costly to maintain. A good overview over a patient's treatment can also be useful to avoid redundant treatment, which may occur if different treatment facilities do not have complete information about the patient's treatment history.
Even though the use of IT systems in could bring many benefits, simplifications and alleviations (see 2.2) the adoption process is slow and tedious. Various factors can be

identified that impede this adoption process[24]:

One problem encumbering the adoption of healthcare IT technology is the **unequal distribution of costs and benefits** of such systems[24]. Health funds pay for patient treatment, but do not directly reward investments into new technologies. The introduction of new technology such as electronic health record costs money and possibly takes a long time to amortize, this is often unaffordable to smaller doctor's offices. Additionally, the economical advantages of healthcare IT will likely start to take effect when they will have been adopted by the majority of healthcare institutions. This may pose an economical penalty to the ones adopting it first.

Moreover, medical IT systems are considerably harder to develop, since they are subject to strong legal regulation. Specifically, medical devices and software have to undergo a complicated certification process, which is not only expensive but also introduces various requirements, such as redundancy by dual-channel system design.

A very important requirement on medical IT system is the ability of different systems to interoperate. Currently, however, many competing standards exist on how medical systems can be interconnected and exchanges data. Since there is no one-fits-all solution to this problem, it contributes to the cost and complexity of the design and deployment of medical IT systems.

However, the most critical issue for the adoption of IT systems in healthcare are concerns about how **security** and **privacy** can be guaranteed in such systems which is the main focus of this report. This is described in more detail in section 5.

2.3. Applications

2.3.1. Electronic Healthcare Record

Recording and retrieval of medical information in electronic form is the core application for information technology in healthcare[25]. The most commonly known concept of this is the **Electronic Healthcare Record** (EHR):[1]

> ... we define the electronic healthcare record (EHR) as digitally stored health care information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times.[26]

The information typically recorded by an EHR are clinical observations, vital signs, diagnoses and examination results, treatment plans and drug prescriptions. As medicine become more complex, the amount and diversity of information that has to be managed and used in healthcare grows rapidly. Traditionally, this has been done on paper –

[1] Also referred to as *Electronic Health Record* or *Electronic Medical Record*

but paper-based solutions are hardly suited to meet today's needs[25]: It may be hard to read someone else's handwriting. Parts of medical records are likely to be missing, because over time, it becomes impossible to keep all records in one place due to space restrictions. Also, parts of a record might get lost. Most importantly, if paper documents should be used in more than one place simultaneously, they have to be tediously duplicated.

The use of an EHR offers a far more convenient way to handle medical data[26]: In its ideal form, an EHR keeps data quickly accessible and available to the clinician. Data can be used in more than one place at a time. Coping with the weight of large, heavy folders becomes obsolete. Instead, data can be flexibly viewed on mobile, handheld devices. By structuring the data, making it searchable and introducing user-specific view, data access becomes very flexible.

Apart from direct benefits for the patient, the use of electronic health record also provides the basis for data collection for clinical studies. However, for this purpose, patient data confidentiality and privacy considerations have to be the first priority.

A requirement for the successful introduction of EHR solutions is that the use of this solution should avoid additional workload for its users. They have to be designed in such a way that they are at least as convenient to use as the paper-based alternatives, otherwise they are likely to be rejected[25].

2.3.2. Clinical Decision Support

Computer support does not have to be limited to merely providing recorded information to the physician. It can can synthesize new information, such as suggestions for diagnoses, treatment options or expected development of a patients medical condition: This application is called **Clinical Decision Support**[20].These suggestions are made by connecting the available data in a patient's electronic health record and general medical knowledge. There are various ways the clinicians work can be assisted:

- Lab values can be analyzed for critical patient conditions. If such a condition is found, an alert is raised.[4]
- Reminders are sent to doctors for ordering preventive measures[25].
- Suggestions or warnings are issued to remind clinicians of compliance with standardized medical care guidelines[12].

2.3.3. Care Documentation

IT systems in healthcare can also record patient-related information beyond actual vital signs and examination results as in the classic health record (see section 2.3.1): The care carried out by the nursing staff has to be carefully documented. This is helpful for several reasons: For one thing, nursing processes have to be documented by hospitals in order to be able to prove that the necessary care and treatment steps have been performed. Furthermore, every single unit of work has to be documented to be able to bill the health insurance company of the patient accordingly. When implemented in a user-friendly fashion, electronic care documentation can be perceived as helpful by the staff[35].

2.3.4. Laboratory Data Systems

Computer systems for storing, processing and distribution of laboratory data is probably the oldest most widespread form of computer usage in healthcare. These systems were very effective since the beginning as typical lab results are the form of data that is most easily processed by computers: They are numerical values and the different kinds of measurements are limited to those provided by the lab, thus there is a limited data model that has to be supported.

The function of laboratory data systems (LDS) traditionally covers handling of lab results from the point of their creation to the moment they are being accessed and viewed. Therefore, LDS gather the measurements automatically from the capture devices and store them in a database. The data is then accessible over the network with viewer applications at the point of care.

Because of the long history of LDS, many custom-developed proprietary legacy solutions exist today, that are often closed-off information silos. However, LDS have been facing new challenges lately: Information silos have to be opened and data has to be accessible through interoperable interfaces, following open data standards (see chapter 4) – to be used in applications such as electronic health records (see section 2.3.1). Flexible import and export of data is also necessary for cases when special analyses have to be outsourced to more specialized labs and data has to be re-imported from those labs.

3. Legal regulations relevant to eHealth

The domain of healthcare - and consequently healthcare IT systems - is subject to a great variety of laws and regulations almost like none other. This chapter describes the most notable sources of regulation relevant to healthcare IT systems.

Complexity and multiplicity of regulations Laws and regulations are concerning healthcare IT systems are both numerous and and far-reaching. Both properties account for the complexity of developing healthcare IT systems and ensuring they are compliant with the corresponding regulations.

Several causes are responsible for the large amount of regulations. For one thing, many laws were put into effect when development of healthcare products was hardly internationally coordinated and normed, therefore numerous country-specific regulations. Furthermore, some regulations apply to healthcare IT systems that initially only targeted non-computerized medical products. These laws were partly and gradually adapted to also cover IT aspects or amended by new additional laws. Lastly, federalism like in the European Union delegates certain regulatory authority to its member countries, thus creating local regulations that may have to be taken into account.

For certain types of medical products and IT systems, the implications of the regulations and laws are quite profound and demanding, especially in respect to product certification and the complexity of this process. Even though this is a huge cost driver in product development, these regulations make sense as lives regularly depend on the concerned products.

It is notable that for products that to not fall into the highest categories of risk, self-control mechanisms apply. This means that the manufacturer itself is required to ensure that his product complies to the corresponding regulations.

3.1. ISO Standards

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) provides best practice recommendations on information security risks, management and controls through its ISO/IEC 27000-series standards. The standards cover the fundamental requirements of information management systems, provide

guidelines and principles for the implementation of such systems. Among the standards, ISO 27799:2008 and ISO/TR 27809:2007 meant for health informatics. The former provides guidelines for designing health sector specific information management systems following ISO/IEC 27002. The later provides control guidelines for patient safety within such systems.
ISO/IEC Joint Technical Committee 1 (JTC1) deals with all matters of Information Technology including develop, maintain, promote and facilitate IT standards by enterprises and users concerning the security of IT systems and information.

3.2. Health Insurance Portability and Accountability Act (HIPAA)

The US congress promulgated HIPAA in order to ensure security and privacy of individually identifiable health information. HIPAA deals with security and privacy through the HIPAA privacy rule (standards for privacy of individually identifiable health information) and the HIPAA security rule (security standards for the protection of electronic health information). The privacy rule ensures the flow of health information needed for quality care by addressing proper use and disclosure of health information. The security rule aims at protecting the privacy of individuals' health information by adopting new technologies with a goal of achieving improved quality and efficiency of patient care. It operationalizes the protection mechanisms contained in the privacy rule. This section provides the summary of the HIPAA privacy and security rules. The HIPAA privacy and security rules are applied to health care providers and non-health care providers supporting the health care providers holding or transmitting health information in electronic form.

3.2.1. HIPAA privacy rule

The privacy rule protects the following individually identifiable health information held or transmitted by the covered entities.

- Common identifiers (e.g. name, address, birth date, social security number);
- Past, present or future physical and mental health or condition;
- Provision of health care to individuals;
- Past, present or future payment provision for health care.

However, there are no restrictions to use or disclose health information that cannot identify an individual in any way.
The covered entities are permitted to use or disclose the health information for the specific purposes (e.g. treatment, payment etc.). The entities can disclose health information for research or public interest withholding certain specified direct identifiers.

The covered entity must obtain explicit authorization to use and disclose of personally identifiable health information for purposes other than treatment, payment and relevant health care operations. While using and disclosing, the covered entities should use and disclose the minimum amount of information needed to accomplish the intended purpose. In this regard, appropriate policies and procedures should be in place to restrict the use and disclosure of information. When other entities request for the information, a proper and explicit trust agreement should be established. The individuals and the actors must be notified about the privacy practices.

3.2.2. HIPAA security rule

The security rule protects all individually identifiable health information that the covered entities create, receive, maintain or transmit in electronic form. The security rules cover the following aspects.

- Ensuring authorized disclosure, integrity and availability of all personally identifiable health information;
- Identify and protect against anticipated threats to the confidentiality, integrity and availability;
- Protect against impermissible use and disclosure of information.

The security rule demands administrative safeguards thats include both the security management processes and personnel. Proper admission control to facilities and devices should be maintained. The rule advocates for technical safeguards by including access control, audit control, integrity control and transmission security.

3.2.3. HITECH

The Health Information Technology for Economic and Clinical Health Act (HITECH) extends the scope of security and privacy protections available in HIPAA and the act was signed into law in 2009. In the health care industry so far HIPAA has not been rigorously enforced, HITECH provides legal liability for non-compliance. Apart from enforcing the HIPAA rules, HITECH takes into care the notification of breach and access to electronic health records. HITECH Act requires that any unauthorized use and disclosure would generate a data breach notification for example patients be notified of any unsecured breach. The Act provides individuals with a right to obtain their electronic health records and they can also designate a third party to receive this information.

3.3. The European Union

The regulatory situation in Europe for the handling of medical data is complex, as there are different sources of regulation. Sources are the European Union as well as the legislation of the member states. Both issue regulations that apply to data protection in general as well as regulations targeted at medical data specifically. The *European Commission* is the executive body of the European Union and responsible for proposing legislation. For questions of data protection, the European Commission has set up the *Article 29 Data Protection Working Party*, an independent advisory board. It consists of the *European Data Protection Supervisor* and data protection officers from the EU member states. This board advises the European Commision in questions of data protection. For regulations on data protection, the European Union issues *directives*, which have to be implemented in national laws by the member states.

3.3.1. EU Directive 95/46/EC

The first directive issued by the European Union on data protection is the *Directive 95/46/EC*[16], which describes minimal standards that have to be guaranteed in the processing of personal data. The general principle states, that personal data should not be processed at all, unless the following conditions are met:

- Data processing is limited to certain purposes, such as given consent by the data subject or the necessity to fulfill a given contract with the data subject.
- To promote transparency, the data subject has the right to be informed about the processing of his personal data.
- Data processing has to be proportional to it's purpose: the more sensitive data is, the more effort hast to be made to ensure privacy and anonymity.

3.3.2. EU Directive 2002/58/EC

Since the first EU data protection directive in 1995, a lot of development took place in the field of telecommunication. Global public communication infrastructure makes wide range of electronic communications over the Internet possible. Not only it opens new possibilities for the citizens, governments and enterprises but also rises new risks of unauthorized use and disclosure of data. The transmission of personal data over the communication infrastructure for cross-border services may aggravate the situation. The uptake of the e-government services partly depends on the user that their privacy would not be compromised.

Directive 2002/58/EC complements the previous directive from 1995 with regard to new telecommunication technologies. It concerns the processing of personal data and the protection of privacy relevant to the electronic communication infrastructures and services. Only the overview of security and privacy related articles will be given here:

- The electronic communication service providers in conjunction with the network providers must take technical and organizational measures to safeguard the security of their services and networks. In case of breach of network security, the providers must inform the subscriber concerning such risks and any possible remedies including the indication of likely costs involved.

- The regulations of the member states must ensure the confidentiality of the communication and related traffic data prohibiting listening, tapping, storage, or any type of interception or surveillance other than the user, without user's consent and except the legally authorized entities to do so in accordance with law.
- The traffic data processed and stored by the providers must be erased or made unanimous when it is no longer needed for the purpose of the transmission of a communication. The provider can process the data (e.g. for marketing purpose) only with subscribers' or users' consent.

Health-related data specifically is subject to stricter regulations (Article 8). It's processing is generally forbidden, unless the data subject has given it's consent or data is handled by medical personnel for treatment or preventive purposes.

3.3.3. EU Directive 93/42/EEC

The EU directive 93/42/EEC[1] states criteria to define medical devices. For systems and devices that fall under these definition, the directive states requirements that have to be met.

Medical devices in the sense of the directive are devices that serve the following purposes:

- Diagnosis, prevention, monitoring, treatment or alleviation of disease,
- Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
- Investigation, replacement or modification of the anatomy or of a physiological process,
- control of conception

The important aspect for IT systems is that **software of medical devices is explicitly included** in this definition.

Every device classified a medical device under the above criteria has to bear a CE [2] mark that indicates conformity with the requirements on medical devices of this directive. These requirements are defined in *Annex I* of the directive and include:

- Device may not compromise the clinical condition or the safety of patients when used in the intended way

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0042:EN:HTML

[2] CE stands for *conformité européenne*

- Risks have to be minimized (elimination of risks through security by design, alerts have to warn about dangerous conditions, users have to be informed about residual risks)

Further detailed requirements concern sterility, used materials in manufacturing, influence or emittance of radiation etc.

Devices are classified into risk categories *I*, *IIa*, *IIb* and *III* depending on the typical duration of use, degree of invasiveness and inherent risk. Category *III* indicates the highest risk.

The requirements for the attainment of a CE mark depend of the risk category the device is classified into. Class *III*-devices must be approved by the corresponding authority in a EU country prior to market placement and may involve clinical trials.

3.4. National regulations

This section elaborates some of the national regulations supporting security and privacy medical data and relevant infrastructures.

Scope It would be out of reach for this report to elaborate the national regulations in all european countries. Instead, we focused on the regulations of the home countries of the authors of this report, Germany and Norway. We additionally included Austria, since with the austrian e-Card system it has a notable eHealth architecture in place.

3.4.1. Germany

Data protection in general and medical data protection in particular are regulated by several laws.

Bundesdatenschutzgesetz (BDSG) The most universal source of regulation in german federal law is the *Bundesdatenschutzgesetz* (BDSG, *Federal Data Protection Act*). The BSDG is the main implementation in national law of Directive 95/46/EC. The key points of the BDSG state:

- The law defines the term *personal data.* Data is personal data if it can be used to identify a person. It does not have to contain a name to qualify as personal data.
- All processing of personal data is forbidden unless either explicitly allowed by the BDSG or by consent of the data subject.
- The principle of *data parsimony* and *data avoidance* require that gathering of data should be kept to the necessary minimum or avoided completely where possible. Where data has to be collected, is should be anonymized as far as possible.

- Especially protected is data such as racial and ethnical provenance, political opinion and health-related information. This kind of data may only be processed in organizations pre-approved by the responsible data protection officer.

- Every organization with more than 10 members must appoint a data protection officer.

- Subjects of personal data have extensive rights to be informed about stored personal in organization, and can demand correction or deletion any time.

Patient-physician confidentiality Medical data is also protected by the *patient-physician confidentiality.* This regulation forbids medical personnel to divulge any information about their patients. German penal law §203 StGB allows up to a year of prison sentence for unlawful divulgement of such information.

Health-card regulations Germany's health care system is subject to a lot of regulation by law. Accordingly, the health insurance cards in Germany and the planned introduction of the health card are regulated in paragraphs §291 and §291a in SGB V (social law, book 5).

Medical products act In Germany, the EU Directive 93/42/EEC (see section 3.3.3) is implemented in national law by the Medical Products act (*Medizinproduktegesetz*).

3.4.2. Norway

The following acts and regulations support the relevant security and privacy situations in medical sector of Norway: Regulations on the use of Information and Communication Technology, Personal Data Act, Personal Data Regulations. The key points of these regulations are presented as follows:

- The organization must establish procedures to ensure protection of equipments, systems and information from damage, misuse, unauthorized access and modification. The procedures should include the guidelines for granting, changing, deleting and control authorization for access to ICT systems.

- Personal data refer to any information and assessment that may be linked to a natural person. The information security aspects of personal data consider the assurance of confidentiality, integrity and availability of data.

- Measures must be taken to protect unauthorized access to personal data where confidentiality is necessary. In this regard, techniques for identification, authentication and authorization must be used to protect the sensitive personal data. Proper access control mechanism must be in place.

- Personal data when transferred electronically beyond the physical control of data controller must be protected through encryption or other means to prevent unauthorized access, use and disclosure of data. Data should not remain in cleartext at Gateways.

- Measures should be taken to prevent unauthorized alteration of personal data.

- Security measures must prevent unauthorized use of information systems. The measure should include the detection of any attempt of misuse. In this regard, temper-proof logs are needed.

- Above all, all the measures should be documented.

3.4.3. Austria

The e-Card system in Austria is based on legal regulations in the Code of Social Law (*Allgemeines Sozialversicherungsgesetz*, ASVG), namely by the 56th amendment to the ASVG, §31. It provides the regulatory basis for the development of citizen e-Card system in Austria. The norm defines data that should be stored on those cards for fulfilling their purpose as authentication tokes to personal data and services. This data includes name, date of birth, gender and insurance number. Other personal information such as medical diagnoses and health-related data or financial information are forbidden to be stored on the e-Cards.

For privacy aspects, the norm refers to the Austrian data protection regulations as well as the EU directive 95/46/EG (see section 3.3.1).

4. Medical data standards

Standards play a tremendously important role in healthcare IT, as interoperability between systems depends directly on them[42]. The benefits described in section 2.2 can only be achieved when systems are open, interoperable and extensible as opposed to monolithic, closed-off information silos.

4.1. Interoperability

Interoperability between systems has to be established on three different levels (see [32], [42]):

- **Technical interoperability** describes interoperability on the physical level. This involves mechanically and electronically compatible hardware interfaces.
- **Syntactical interoperability** refers to structural aspects of communication, such as compatible data exchange protocols and data containers.
- **Semantic interoperability** means to share the same understanding of the meaning of data. When systems are interoperable on the semantic level, every relevant piece of data is connected to a concept of its meaning an can be processed accordingly and in a sensible way.

In order to build interoperable systems, their interfaces have to be designed according to standards that describe their properties on all three levels. As usual in IT systems design, this can be done with a layered approach: The interfaces does not have to be described by a single standard that describes all three levels, instead a combination of different standards can be used as it is commonplace with network protocols.

4.2. List of Standards

The list of standards presented in this section covers the most common standards used in medical informatics today, as could be identified from the reviewed literature (see [17],[42]).

4.2.1. openEHR

openEHR[17] started out in 1992 as an EU research project under the name *Good European Health Record* and is currently maintained by the *openEHR* non-profit organisation[1].

Archetypes The most distinctive feature of the *openEHR* standard is the introduction of the so-called *archetypes*[9]. In this approach, expressions of clinical information are modeled in a two-level concept – similar to meta-modeling[2]. On the first level, a relatively simple meta-model is defined, which contains only a few elements.

Using the elements of this meta-model, archetypes can be defined to represent domain-specific concepts such as clinical observations. This is done by assembling and naming elements from the meta-model, connecting them and putting constraints on them. In addition to naming, elements of an archetype can be linked to other semantic data standards. Archetypes can be defined using the *Archetype Definition Language* (ADL) introduced by openEHR.

For actual representations of data, these archetypes can then be instantiated to represent a dataset.

4.2.2. EN 13606

EN 13606 is a communication standards for medical information in electronic health records and focuses on interfaces for data exchange and structured data packaging for communication. Information exchange can take place between entities such as clinical applications, central data repositories and software components. Health records can be transmitted as a whole or in fragments.

For data representation, EN 13606 relies on the openEHR framework (see section 4.2.1).

4.2.3. ISO/IEEE 11073

The ISO 10073[40] family of standards describes protocols and data formats for communication between electronic medical devices. It focuses on bedside devices that are used in acute care settings, and is therefore designed with the following aims:

- Real-time interoperable plug-and-play of devices
- Simple implementation of protocol stacks
- Resource-efficient message processing

[1] Homepage of the openEHR Community: http://www.openehr.org/

[2] An example for meta-modeling is the UML, which is itself modeled by the Meta Objects Facility(MOF)

- Handling of frequent network configuration changes

The set of standards encompasses:

- An object-oriented data model (Domain Information Model (DIM), ISO 1173-10201), to define terms and services to be used in the communication protocol.
- A standardized nomenclature (ISO 11073-10101): A set of numeric codes to identify communicated items.
- Application profiles, which restrict the nomenclature and data model to specific communication needs.

4.2.4. LOINC

LOINC (see [3]) stands for *Logical Observation Identifiers Names and Codes* and is a naming and coding system for clinical observations. LOINC is published in a publicly accessible database and is maintained by Regenstrief Institute (Indianapolis, USA). Every observation is encoded in its own record and should contain the following information:

- Analyte: observation subject
- Observed property / measurement metric
- Time information
- System: kind of sample
- Scale: quantitative, ordinal, nominal or textual

LOINC is especially well suited to express the results of laboratory results. It does not explicitly cover acutal diagnoses, which are usually described and encoded by the ICD coding system (International Statistical Classification of Diseases and Related Health Problems.)

The LOINC coding system is used by other standards to encode data, such as Health Level 7 (see section 4.2.6) or CDA (see section 4.2.7).

4.2.5. Snomed CT

Snomed CT[4] stands for *Systematized Nomenclature of Medicine – Clinical Terms* and is a terminology standard consisting of medical concepts which aims at achieving semantic interoperability. Each concept is assigned a numeric, unique code consisting of six to eighteen digits.

Example: 22298006 stands for "myocardial infarction"

[3] LOINC User's Guide, June 2010, see http://loinc.org/downloads/files/LOINCManual.pdf

[4] Presentation by Kent Spackman, Chief Terminologist at IHTSDO: http://www.ihtsdo.org/fileadmin/user_upload/Docs_01/SNOMED_Clinical_Terms_Fundamentals.pdf

Concept Hierarchy Snomed CT is structured by a acyclic graph, which is formed by the concepts as nodes and connections between nodes. A connection indicates a specialisation/generalisation relationship between two concepts. For example, a *viral pneumonia* in generalized to a *infectious pneumonia*, which in turn is a specialisation of *pneumonia*, which is in turn a specialisation of a *lung disease*.

Snomed CT is used by other standards such as HL7 (see section 4.2.6) for providing semantic interoperability.

4.2.6. Health Level 7 (HL7)

Health Level 7 is a non-profit organisation founded in 1987 that develops a group of standards for communication of clinical information. These standards include:

- Message protocols (HL7 v2.x, v3)
- Conceptual standards (e.g. HL7 RIM)
- Document standards (e.g. HL7 CDA, see section 4.2.7)
- Application standards (e.g. HL7 Clinical Context Object Workgroup CCOW)

HL7 Message Protocols Message protocols in HL7[17] are designed to be triggered by events. A trigger event is an event in clinical work (such as a patient admission). A trigger event generates a request message that is sent to another system. There, data for the reply to the request is gathered and the reply message is assembled, e.g. in EDI[5] format.

The older message protocol HL7 version 2 is the most widely implemented standard and exists in different subversions ranging from 2.1 up to 2.6, which are backward compatible. The encoding uses textual delimiters but no XML. HL7 v2 defines a message exchange for many tasks in clinical work processes. However, these messages are not based a commonly agreed data model and therefore leave the definition and semantics of data fields vague. This allows for great flexibility on the one side, but adherence to HL7 v2 cannot guarantee interoperability without further bilateral agreements.

To improve this, HL7 v3 introduces the *Reference Information Model* (RIM)[6]. This model contains concepts and data entities that are communicated in message exchange and shows semantic connections connections between those entities. It is used along with medical data standards such as LOINC (see section 4.2.4) or SNOMED CT (see section 4.2.5) to encode data in messages in an unambiguous way.

[5] *Electronic data interchange*, set of standards

[6] The *Reference Information Model* has been criticized to be blurring the line between a data model and an ontology. However, this criticism[22] helps to may help to clarify the concept of the RIM

Clinical Context Object Workgroup The *Clinical Context Object Workgroup*[7] (CCOW) is a standard that supports the creation of a unified view on clinical data that is located in separate applications. CCOW is linked with single-sign-on solutions in such a way that a signing on to on local application automatically signs the user into other applications to have access to their data and functionality. Similarly, selection of a specific patient in one application triggers selection of the same patient in all other applications.

4.2.7. Clinical Document Architecture (CDA)

The *Clinical Document Architecture*[17] defines a XML-Markup-based document standard for the exchange of clinical information assembled into documents. It structural elements are based on data types of the *Reference Information Model* of HL7 v3 (see section 4.2.6).

CDA documents can fulfill three different levels of machine readability and processability. On the first level, CDA documents consist of a header (derived from the RIM) and a body, that may contain formatted text. This level only offers transmission for human-readable content without further interoperability. On the second level, the document body is structured into acts of observation that are compliant with the RIM. On level three, all data fields are semantically encoded to provide full machine processability.

[7] http://www.hl7.org.au/CCOW.htm

5. Security, Safety and Privacy in eHealth

The biggest challenges in broadening the use of IT systems in healthcare are probably the concerns about **security** and **safety** when computer systems are to be trusted with medical information[1].

Security describes the the property of a computer system of being immune to deliberate attacks and manipulation attempts from outside of the system. This explicitly includes the aspect of data privacy.

Safety denotes the property of a system to function according to its specification under all operating conditions. This may also require fault tolerance to mask internal failures of the system so they don't affect the observable behavior of the system.

5.1. Challenges

Making computer systems in healthcare safe and secure is the main challenge in system development and mainly arises from the following reasons:

5.1.1. Sensitivity of Medical Data & IT systems

The term *medical data* applies to all data that is related to a persons health and medical history. Data of this kind is considered especially sensitive in three different aspects: It needs to be protected from unauthorized access (privacy), has to be correct (safety) and available at all times (availability).

Security and Privacy requirements It is commonly agreed that medical data is among the most personal and sensitive information of people and in need of protection. This is understandable, since even fragments of medical data can reveal very much information. In this, medical data is very **side-channel**-prone: For example, prescriptions of specific HIV-suppressive drugs clearly indicate that the patient is HIV-positive. In general, information about STDs opens up room for speculations on how these were acquired. And a patient may simply want to keep quiet about a condition he'd rather deal with himself.

[1] Large parts of definitions in this chapter are taken from the lecture notes of the "System Security" lecture held by Jürgen Kleinöder in 2007/2008 at University Erlangen-Nürnberg

In general, the divulgement of medical data can have severe consequences. Some diseases still carry a social stigma and the spreading of such information can have serious implications for the social life of a person[31]. The consequences can be even more serious in the professional life, as medical issues may considerably worsen job chances. In most country laws prohibit the discrimination of job applicants because of their health status, however, in practice, enforcement of these laws is difficult. These laws do not apply to private health insurance companies, which may decline a customer because of his health status.

The following two incidents point out very clearly how seriously medical data can be abused when it falls in to the wrong hands:

> *A nurse had been working in Finland on fixed-term contract between 1989 and 1994. During the period she was infected with HIV and in 1995 she had been refused her contract renewal. Later it transpired that her colleagues at the hospital had had access to her patient records.*[2]
>
> *The Real IRA used records at the Royal Victoria Hospital to target policemen and their families for murder. An employee had been suspected.*[3]

Safety requirements When a patient's medical treatment depends on computer systems, malfunctions of these systems can have very severe consequences. Systems can be indirectly (i.e. supplying information to a physician) or directly (treatment devices) involved in the treatment process. Therefore, safety both refers to correctness of data and correctness of function.

A striking example of malfunction of a treatment device is the incident that occurred in the 1980s with the *Therac-25* radiation therapy machine[29]. This machine supported two different modes of operation, one of which used an unobstructed low-power beam – and another mode where a high power beam was turned into X-rays by moving a target, disperser and a shape limiter into the beam. Due to a race condition in the control software, these devices were not always moved in to the beam. In these cases, the machined applied a radiation dose up to 100 times higher than intended, causing at least three patients to die directly from radiation poisoning and injuring several more.

Availability requirements Another important requirement on medical IT systems is the availability of functionality and data. Availability is challenging, because measures taken to provide security and privacy may possibly slow down system performance and interfere with the design goal of availability.

[2] *ECHR (the European Court of Human Rights) finds Finland in breach of patient confidentiality*, Helsinki Times, 21 July 2008.

[3] *Dissident operation uncovered*, BBC News, 02 July 2003.

5.1.2. Public skepticism

In addition to difficulties with the various regulations, there is a lot of skepticism in the public perception of IT in healthcare, as can be observed in the current discussions in Germany about the introduction of a generic health card (”Gesundheitskarte”, see A.2). This may partly be due to lack of knowledge and understanding of computer systems, but is definitely fueled by data scandals that regularly occur. In a national survey conducted in US in 2005 stated that about 67% citizens showed medium to high level of concerns about the privacy of their medical records [34]. In another survey in response to a query about online health information, about 50-80% Americans responded that they were very concerned about identity theft or fraud and implications of unauthorized access to medical information [34]. This clearly identifies the need for protecting medical data and IT infrastructures.

5.2. Security & Safety Threats

When designing a system with security and safety properties, the most important possible sources of attacks and faults have to be evaluated.

In general, the **safety** of any computer system is threatened by hardware errors that may occur in its hardware components or maloperation. Medical devices are often used in rough environment, such as bedside devices or systems in an OR, which may require hardware components with higher physical tolerance against environmental stress compared to office computer systems. To tackle hardware faults that may for example result in wrong measurement values or wrong treatment parameters, medical devices often use a dual-channel design, where communication links exist double to detect and correct wrong transmission.
Deliberate tampering with medical equipment to cause malfunction is however a minor concern.

The **security** of IT systems – particularly *data privacy* – in healthcare is threatened on many levels because they are often highly distributed systems with many users and many communication links between system components. There is also a clear motivation for data theft: Insurance companies are very much interested in almost any statistical information about distribution of diseases to calculate their rates for private health insurance contracts. Also information about the health of an individual may be of interest: Employees may simply spy on their colleagues, and again, insurance companies may want to learn in advance if an applicant for health insurance suffers from a possibly costly condition. Consequently, security and integrity of healthcare information systems has to be protected against both outside and inside attacks. Insider security threats may be met by employing a fine-grained access control that limits access to the minimal amount information required for the task at hand. These fine-grained access control

solutions are in turn often rendered useless, as their complexity may get in the way of everyday work; as a consequence, passwords and authentication tokens are often shared, defeating their purpose (see *Usability requirements*, section 2.1.5).
Attacks from outside have to be tackled by employing respective security techniques for protecting networked systems in general.

5.3. Security Goals

Goals specify properties that a system needs to have in order to fulfill certain aspects of security and safety. These goals are:

Confidentiality ensures that data is only available to authorized parties and otherwise kept secret.

Data Integrity ensures that data cannot be modified without detection.

Accountability enables unambiguous identification of the creator of an event or data.

Availability of services promises that a service behaves according to its specification at all times. This includes timely response and correct function.

Access Control ensures that functionality and data is only available to authorized entities.

5.4. Practical Applications

This section presents concepts and technical mechanisms that are commonly used to realize the security goals listed in section 5.3.

5.4.1. Identity Management

Identity gives means of answering the question 'who are you' and thus identifying a subject to a relying authority. A set of characteristics can define the identity and these make it recognizable as a separate entity. Personal traits, surrounding environment and circumstances may determine diverse meaning of identity. For example, a role that refers to a specific duty or function one performs in a social system may identity a person [45], [33].
In an information system *identity management* encompasses all tasks of managing identity life cycle that includes representing, managing and deleting identities of users. Representing identity constitutes establishing identity and assigning attributes to it. Secure storage, disclosure and transmission of identity attributes have specific importance to identity management. In early days users and the systems they access might both belong to the same network or within the same domain of control. The centralized identity management approach based on a silo is enough for controlling access to services or

application within the same domain of control. Gradually the growth of Internet based services creates many identity management domains. This overloads users with many identities and creates a management nightmare. The increasing number of identities with their diverse forms has to be managed properly to make the system access secure and hassle-free. Federated identity management has become a potential solution to resolve these problems.

Federated identity management allows identities to be shared securely across desperate networks, autonomous security domains and applications. Identity federation can be accomplished using standards such as WS-Federation and OASIS Security Assertion Markup Language (SAML). A possible benefit and use of identity federation is achieving Single Sign-on (SSO) across multiple security domains. Apart from formal identity federation standards, there exist some open source solutions such as OpenID, OAuth and Higgins trust framework.

Relevance to medical domain The question is what constitutes the identity of a person in the medical domain. The Social security number(SSN) is commonly used to identify a person in the medical domain but while the patient is admitted into the hospital a temporary identity may need to be created. During the treatment the patient may be referred to different departments of the hospital or to another hospital. An identity management system creates new identities (if necessary), makes mapping between the identities, manages these identity instances and finally deletes the temporary ones from the database when they are no longer required. Suppose a patient is referred from hospital A to B. Doctors of hospital B may need to access relevant medical records and observations of the patient from the repository of hospital A. In such cases federated identity management [41] approach through SSO can be used to identify a person across boundaries.

Challenges Privacy concerns are the center of identity management challenges. In many cases more than necessary amount of information is revealed to the authorized users of the data. For example, it may not be necessary to disclose the mobile phone number of the patient to the nurses who are treating him. Therefore, it is required that the owner of identity should have full control of his data assets and only relevant information needed should be disclosed. In case of federated identity management approach, it is a concern that how much information of the access requester would be revealed during cross border interactions. If a SSO system is compromised, adversaries can get access to all services within the specific identity domain.

5.4.2. Access control

The access control mechanism limits the access to the resources of a system only to allowed people or processes [39]. Not only access to applications and databases needs to be secured but also the access to clients and intermediary machines. Access control can

be achieved applying **authentication** and **authorization** process. There exist two sets of identity attributes, the first set of attributes authenticates the user and the second set of information is applied to authorize the user [19]. In some systems complete access is granted when a user subjects to successful authentication only. This is very trivial and hence most systems require enhanced control involving both authentication and authorization process.
A user usually makes claims about him by presenting a part of his identity attributes for identification towards a system. This information can be a picture, certificates, a shared secret or any other credentials. The system needs to verify these claims against pre-stored information. Authentication process merely verifies these claims but says nothing about the access rights. Authorization process ensures the access right and makes sure one accesses only what he is allowed to access. A second set of identity attributes can be used to authorize a user. The claims made during authentication can be of three types: something a user knows (e.g. password), something a user has (e.g. a secure token), and something a user is (e.g. biometrics). Combination of these factors can secure authentication process further [1].
Access control often follows a standard access control model which in fact determines the access authorization in a system. Typically, access control models provide a framework to realize the access control functionalities in software and devices. The model deals with granting access permissions based on the characteristics of subject or objects. For a research perspective on access control models, see section 5.5.1.

Policies can be employed for controlling access. Security and privacy constraints can be encoded through policies. Typically a policy specifies (a) who is allowed to perform, (b) which actions, (c) on which objects, depending on requester's attributes (e.g. roles) and various contextual factors (e.g. location). Applying policy is nowadays a prominent approach to protect security and privacy of use and disclosure of information, contents and services in a distributed environment. For a comparison of policy languages, see section 5.5.2.

Relevance to medical domain Nowadays a medical domain involves many actors and is built on decentralized environment. The roles of the actors may change depending on the environmental contexts such as location and time. A person containing a set access rights may not hold them anymore when his context changes. The distributed but connected information systems, growing privacy concerns, and the new rules and regulations demand highly granular access control functionalities in the medical domain. This may apply access control down to individual data fields. Medical also requires proper delegation of access rights strategy.

Challenges Significant granularity of access restrictions is required because of complicated security and privacy requirements and the involvement of many actors in the medical domain. Granularity demands the flexibility of adding diverse access constraints.

For example, the presence of doctor in the operation theater might be necessary for the nurse to access certain information of the patient. However, the enhanced granularity of restrictions introduces complexity into the system and compromises the usability of it. It is true that multiple authentication factors increases the security of the access but it also overloads the system as well as the users of the system. Designing highly granular access constraints may result conflicting access policies. This may sometime compromise the availability of critical medical information which is unacceptable. With a growing number of actors scalability of access control mechanism may be a concern. Ease of maintenance and management are also an issue. It is not a trivial job to design an access control mechanism satisfying all these requirements.

5.4.3. Secure Information Transmission

Patient's personal information and EHRs are stored in decentralized databases distributed over different geographical locations. The distributed systems are connected with each other by various communications means. For example, distributed databases can be connected through fixed high capacity leased lines and retrieved medical data from the remote patient can even be transmitted through an existing mobile communication channel. Unlawful Interception, unauthorized disclosure and modification of data transmitted over various communication channels are the main concerns. In this regard there can be two types of adversaries:

Active adversaries can interfere with legal communications and start initiating malicious communications.

Passive adversaries only eavesdrop on ongoing communications and try to collect information.

Encryption of data is the most conventional means to prevent such disclosure. Even monitoring the encrypted data for a longer duration may result in useful information about the encryption key and algorithm used. It has been observed that the unauthorized access to data often occurs while the data or part of the data remains unencrypted in the intermediary devices such as gateways. In many case insiders are responsible for this sort of unauthorized access.

Relevance to medical domain The information exchange between the physicians and the patients during the course of treatment is regarded as confidential. The electronic health records and the relevant personal information are normally stored in tlocal medical databases. Access control mechanisms prevents unauthorized access to these data. However, data privacy becomes most vulnerable in the moment of transmission and therefore needs to be protected accordingly.

Challenges Though access to client machines or servers can be secured by various reliable means, preventing unauthorized access to data being transmitted is still a challenging issue. It is required to use an appropriate algorithm and sufficiently high key length to encrypt the data. Above all the information in medical domain has to be available whenever it is required. It is challenging to design a fault tolerant and **denial of service** (DOS) resistant system, to ensure availability of data across boundaries in a distributed system.

5.4.4. Security Audit

In information system, audit refers to the chronological record of activities occurring in the system. Typically a log file is maintained to keep the records. It enables investigations of the event sequences. Based on the examination of records, the complete system or an action can be reverted. In the medical information system, from security point of view event records may be used identify unlawful access, use or disclosure of information.

5.5. Research

This section reviews research on access control models in section 5.5.1 and policy languages in section 5.5.2.

5.5.1. Reviewing access control models

Several concepts exist to realize access control. This section describes and compares the most important ones.

Access Control List (ACL) Access Control List (ACL) is the most prominent but elementary access control model. It is an implementation mean of the access matrix model [38] which is mostly used in computer operating systems. An ACL is associated with an object. It specifies all the subjects that can access the object with a set of rights. The model is quite generic and straightforward to design. ACL is not expressive enough to specify complex constraints. Therefore, it cannot support varying levels of granularity. It is necessary to examine all the subjects in the system to review access privileges. To revoke all rights of a subject, all ACLs must be checked one by one. Hence, troubleshooting is a tedious job. Its scalability is questionable from maintenance point of view. ACL cannot support high level specification of access rights and constraints. Delegation of access right is not clearly supported. There is no provision to include context information in ACL which under certain circumstances might be useful, for example a subject can access an object only within a specific time period. Capability list is another type of access list which is the inverse of ACL. Here access to an object is allowed if the subject possesses a capability for the object. The capability list has the similar limitations as the ACL.

Role Based Access Control (RBAC) In Role Based Access Control (RBAC) [39] users are grouped to roles and permissions are assigned to roles rather than to individual users.

As seen in ACL, assigning permissions directly to users makes it difficult to control user-permission relationships. Roles categorize groups of users sharing common set of rights. There is a similarity between the role used here and traditional group. RBAC has two logical parts: assignment of roles, and assigning access rights for objects to roles.
Classical RBAC [39] is not a generic model and applied where the notion of role is involved. Classical RBAC model provides limited access granularity because it assigns access permissions to users through roles only. However considerable efforts [48],[14] have been made to extend RBAC to support wide range of access constraints. Scalability of various RBAC models is a concern in terms of maintainability and efficiency. Adding semantics to RBAC[2],[18] facilitates high level specification of access rights and constraints. However these efforts were only limited to specification of RBAC using semantic technologies. The ability to delegate roles has been investigated in [8]. These literatures presented frameworks supporting various forms of delegation extending the RBAC models. Classical RBAC supports revocation through revoking user-role assignment or permission-role assignment.

More fine-grained access control Fine-grained access control needs to extend beyond RBAC by including attribute or context based access control. Thus additional features, such as attributes or contexts of subjects/objects, can be used to design finer grained access policies. In Attribute Based Access Control (ABAC) [10] access is granted based on the attributes of the related entities involved. Context is defined as the circumstances or events that form the surrounding environment within which something exists or takes place. Context-aware access control (CWAC) [28]incorporates factors that constitute surrounding contexts of a subject or an object as constraints to provide access. Both ABAC and context-aware access control models are quite generic but expressive enough to support varying levels of granularity. Scalability is again a design concern in terms of maintainability and efficiency. Semantic extension of these models [44],[37] can support high level specification of access rights and constraints. Delegation and revocation of access right are not clearly supported in ABAC and CWAC. In combination with roles and relationships, attributes or contexts of subjects/objects can be regarded as way to enhance granularity of access restrictions.

5.5.2. Evaluating policy languages

As described in section 5.4.2, policies can be one of the ways to achieve access control functionalities. There exist formal policy specification languages to encode policies. This section evaluates the well-known policy specification languages, such as EPAL [7], KAoS [46], Protune [11], Rei [27], XACML [30], Ponder [15], WSPL [3]. Coi and Olmedilla [13] listed the following policy specification criteria in order to evaluate them.

Well-defined semantics: Unambiguous description of policies.

Monotonicity: A statement in a policy will continue to be true even after adding new information.

Expressiveness of condition: Flexibility of adding numerous attributes as constraints.

Execution of action: Ability to perform action during execution of policy.

Extensibility: Ability to update and extend with new features.

Table 5.1 shows the complete evaluation of the policy specification languages. In this table, '++', '+', and '-' indicate 'strongly support','support', and 'do not support' respectively.

Policy languages	**Well-defined semantics**	**Monotonicity of condition**	**Expressiveness**	**Execution of action**	**Extensibility**
EPAL	+	-	+	+	+
KAoS	++	+	++	-	+
Protune	+	+	+	+	+
Ponder	-	-	+	+	+
Rei	+	+	++	-	+
XACML	-	-	+	+	+
WSPL	-	-	+	+	-

Table 5.1.: Evaluating policy specification languages according to the policy specification criteria.

Policy languages based on logic programming or description logics have well-defined semantics. Among the policy language reviewed, EPAL, KAoS, Protune, Rei have unambiguous semantics. The semantics of XACML is not well-defined. Protune is based on logic programming. De- scription logics is the foundation of KAoS, and the features of description logics, logic pro- gramming and deontic logic together form the basis of Rei. It is based on OWL Lite which is less expressive than OWL DL. There are no underlying formalism in Ponder, WSPL, and XACML. Policies with EPAL, Ponder, WSPL, and XACML are non-monotonic. All other languages are monotonic.
Ponder and EPAL provide solutions which allow specification of prerequisites involving attributes of requesters, objects and environment. WSPL and XACML use a trivial set of criteria to determine the policy's applicability to requests. Among all these languages, Rei and KAoS extensively support constraints specification. Constraints can be set on the attributes of subjects, objects and environment. EPAL, Ponder, XACML, WSPL, Protune support execution of actions from within the policies. However, KAoS and Rei do not support execution of action. Access rights can be delegated through policies specified with Ponder, Rei, Protune. EPAL, WSPL, KAoS and XACML do not support delegation of rights. Extensibility is supported in EPAL, Ponder, and Protune. XACML supports extensibility by including provision for adding new data types. Basic ontologies of KAoS and Rei can be extended for a given application. However, WSPL lacks the extensibility feature.

6. Summary

Computer usage has the potential of bringing big benefits to healthcare, both in terms of cost efficiency as well as quality of care.

Costs can be reduced by alleviations brought by less paperwork in administration and care documentation. Time planning of treatments can lead to better capacity utilization of medical equipment and can save time for patient and doctors. By using electronic health records, less time has to be used to retrieve and transport information, and due to a searchable and complete patient medical history, redundant treatments and examinations can be avoided.

The quality of healthcare can be also be improved in other ways than mere time-saving: Computer usage in diagnostic systems made treatments and examinations possible that were not available years ago and wouldn't be today without computers, especially in the domain of body imaging. Furthermore, as computers can aggregate a wealth of information easily, they enable physicians to keep track of guidelines and medical knowledge which cannot be grasped by human beings alone anymore. Medication dosages and combinations can be checked against counter-indications, and treatment steps can be checked for compliance with medical guidelines. In return, computers can make information about treatments and outcomes available to medical studies that contribute to medical knowledge.

However, computer usage in the medical domain has seen its share of setbacks and failures, as the domain is comparatively complex, and every step of medical treatment bears the responsibility for human lives. There are a number of challenges to be met, when developing IT solutions for the healthcare domain:

Security and data privacy The security of medical IT systems, especially with regard to data privacy of stored information, it probably the biggest concern. There is a high amount of skepticism in the public, whether the proposed or used systems provide the require level of security. Regularly occurring data scandals – more often with non-medical than with medical data – do not help to resolve those doubts. On the contrary, they show that in terms of data protection, there is still a lot of work to be done: In developing technical means of protection, usage guidelines and legislative action.
Fine-grained permission control and easily usable authentication systems may be used to provide efficient access control to data on a need-to-know basis. However, the most sophisticated security system is useless if no one knows what information is to be protected in which way. In healthcare many datasets may exist about a patient exist, some

of which may be more freely distributed (such as name, adress, etc.) while others may be more sensitive and should only be available to concerned specialists. Others may even have to be made public in an emergency, such as allergy or medication intolerance. Therefore, data has to be classified into categories. Different roles can then be assigned different access rights for these data categories. Both data categories and roles have to be carefully adapted to the use case.

Safety and Availability Over the fuss about security, the fact is easily overlooked that the implications of unavailable or incorrect medical information can be even more serious than those of accidental data disclosure. While leaked information does not kill someone, wrong vital parameters supplied to a physician may very well result in an overlooked critical condition or wrong medication dosage. In case of treatment devices, wrong information or malfunction may even harm a patient directly.

There are effective technical means at hand to ensure the correctness of supplied information, such as checksums or dual channel transmission. However, the goal of availability of a system can sometimes interfere with the goal of data protection and security. A careful tradeoff must be made, so that enough information is available in case of an emergency, without compromising security to much in normal operation mode.

Complex laws and regulations The legal regulations that apply to healthcare IT systems are manifold, complex and often very far-reaching. The systems are not only affected by regulations for data privacy but may also be classified as medical product, where separate regulations and laws apply.

These regulations apply often very strict criteria for data privacy, and – in case of medical products – may require a complex and costly certification process before a product may be sold and used.

Understanding the corresponding regulations is not trivial and requires profound expert knowledge, both for extracting the requirements for the planned product as well as for ensuring, the own product complies with the requirements and regulations. This makes the development of products and computer systems for healthcare time-consuming and costly.

Interoperability and interworking issues Medical devices and computer systems do not always interoperate the way they should. Most medical devices still have proprietary connections and communication protocols at best, or none at all. Medical data and communication standards are emerging to provide a common basis for exchanging medical data, but their use is not very widespread yet. Instead, many manufacturers are trying to achieve a vendor lock-in to bind customers to their range of products. However, cost-pressure on the customer side and political influence by pilot projects and guidelines is helping to promote the use of commonly agreed standards, making it more attractive to device vendors, too.

Usability Usability is a key success factor of computer systems in the healthcare domain. Although the argument may be abused sometimes, medical staff is under a lot pressure to handle a growing workload due to massive cost pressure in healthcare. Therefore, if a computer system for medical staff is to be successful, it should integrate well into their work processes and slow down work as little as possible. If it does impose an additional workload, the benefit of the system should be clearly visible to the users. Currently, there is a lot of progress in this domain, since hand-held, wireless, touchscreen-operated devices gained considerable attention and have created a very convenient way to access and record information. The touch-screen operation especially has brought a lot of attention to thoughtful interface design.

A. Solutions & Products

This chapter introduces different government initiatives and industrial products to develop secure and privacy aware medical information systems. The main goals of the projects and research works involving ICT and health sector include improved services, digitization, efficient administration, integration of ICT, increased reliability and availability, provision of cross-border health care, etc. Though ICT contributes highly in the improvement of health care sector, it also introduces many security and privacy challenges. In this section we introduce only those projects and initiatives that also deal with security and privacy apart from specific healthcare related goals. The further overview of each initiative will be given in the following sections. This chapter also provides insight of research initiatives targeting the mentioned security features.

Government Initiatives In most of the countries especially all over Europe healthcare services are managed by the government. In this regard, governments initiated several initiatives to tackle security and privacy concerns in health IT systems. Some of the noticeable ones will be described in this section.

A.1. Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC)

Category Government Initiative

Purpose To use ICT to support the delivery of cross-border public sector services to citizens and enterprises in Europe

Scope Europe-wide

Technology Authentication policy, digital signature, Public-Key Infrastructure, certification authority

The goal of IDABC was to issue recommendations, develop solutions and provide services that enable national and European administration to communicate electronically and offer advanced services to citizens and enterprises with underlying support from interoperable telematic networks. The following projects, actions and measures of IDABC have a direct and indirect link with securing healthcare information systems, especially for providing cross border health services. These are Electronic Exchange of Social Security Information (EESSI), Health-EU, Common Identity Management Service (CIMS), eID Interoperability, and IDABC Certification Service. IDABC also developed a common secure communication infrastructure (STESTA) for trans-European secure information exchange. Besides deploying a secure channel, IDABC provided Certification Authority, Public Key Infrastructure and authentication policy to ensure secure data communication and authorized access to personal data.

A.2. Germany: Elektronische Gesundheitskarte

Category Government Initiative

Purpose Introduction of a telematic infrastructure in german healthcare to facilitate secure information exchange and administrative tasks

Scope Nationwide

Role-based aspects Special ID-Cards for medical personnel with extended permissions (*Elektronischer Heilberufsausweis*)

Technology Public-Key Infrastructure, Smartcards

Structure Decentralised structure with centralized key management

The use of electronic smartcards in healthcare in Germany isn't a new undertaking. Since 1995, electronic health insurance cards are in use (Krankenversicherungskarte). These electronic smartcards contain administrative data about the patient, identifiy the patient and certifiy that the patient has health insurance. The card also contains information to enable the physician to receive payment for treatment from the issuing health insurance company.

Development History In 2003, the german parliament passed a bill to modernize and extend the functionality of the health insurance cards. The main goal was the use of telematics to better connect healthcare facilities with an electronic health card as the technical foundation (*Elektronische Gesundheitskarte*)[47]. In the same year, the *bit4health*-consortium was founded to examine the conditions and requirements for the project. In 2005, a company named *Gematik mbH* was founded to develop, deploy and maintain an electronic health card system.

The schedule planned for field tests with 10.000 participants in 2005 and full deployment by 2006. However, the project was not yet deployed and operation in 2010. Initially, complicated proceedings about financial issued delayed development. In further test-runs in 2007/08, technical difficulties occurred, such as locked cards because of repeatedly mistyped PIN numbers. A test rollout took place in the region of North Rhine-Westphalia, but after government project reviews, health insurance companies declined further adoption because of the uncertain future of the project. In 2007, the german physician congregation *Deutscher Ärztetag* voted against adoption of the health card in its current form.

Objectives The project aims to extend the already existing electronic health insurance cards by means of storage and retrieval facilities for medical data. This extended functionality available to patients by choice, but is not mandatory. The central requirement on the project is to give patients full control over stored and shared data: They determine what data is stored or deleted, which data is stored and who else gets access to which data. Patients have to be able to access all stored data themselves free of charge. It also has to be impossible to create centralized data pools in which patient data is aggregated.
In addition to the functions provided by the predecessor insurance cards, the health cards offer functions for electronic prescriptions, electronic doctor's letters and a dataset of emergency information about the patient. The telematics infrastructure provided by the health card project can also be used by doctors without health card for secure communication between facilities.

A.3. Norwegian healthcare system

Category Government Initiative

Purpose Contrained access to information and exchange of information in the distributed healthcare systemss

Scope Nation-wide

Technology Digital signature, PKI, LDAP

In Norway, a patient in an healthcare institute identifies himself using his Social Security Number. The EHR in Norway is distributed and by law each healthcare institutes has to keep only one health record of the patient containing all episodes of care from birth to death. When it comes to accessing the health records the general rule is that a healthcare professional taking part in an event of care should be given only the required information needed in relation to that specific event. The traditional role-based access control is not sufficient for such provision and hence it has been supplemented with some dynamic variables that can modify access rights satisfying individual patient's needs. Overall the Norwegian EHR standards cover the following areas: access control; patient consent; editing, correcting and deleting EHR information including audit trails; archiving.

As Norwegian eHealth infrastructure is a distributed one, the transported messages between entities are protected from unauthorized access, use, disclosure and alteration. The infrastructure can provide non-repudiation service. Integrity, confidentiality and non-repudiation of messages are ensures using XML digital signature, XML encryption in conjunction with a proprietary PKI solutions. Verification of signatures and certificates is done with Lightweight Directory Access Protocol (LDAP).

A.4. Austria: e-Card

Category Government Initiative

Purpose To support administrative processes electronically between citizens and different entitities

Scope Nation-wide

Technology Smartcard, Multi-factor (physical card and PIN) authentication, digital signature, encryption

E-card is a smart card given to Austrian citizens and is voluntarily upgradeable to a *citizen card*. The aim of this is to support administrative processes electronically between citizens, employers, doctors, hospitals and the social security institutions. Bank card, student ID card or official ID cards can also be activated as E-card. Health care services is one the services where E-card can be used. It holds only the identification data acting as access key to authenticate users to applications. The E-card stored only minimum amount of data necessary for identification. PIN number protects the unauthorized access to the data. Certificate of the signature can be revoked in case the card is stolen from the revocation center. The E-card system provides a secure broadband connection between the closed user groups within the health sector. It has also the provision to create electronic signature. Besides social insurance signature (for application within the social insurance field), E-card contains secure electronic signature and advanced electronic signature according to e-government law. The card enables citizens to preserve confidentiality by sending and receiving data using citizen card encrypted (CCE). In addition to E-card administrative professions (e.g. physicians) hold o-card and only both keys together open the access to allowed services and data.

A decentralized electronic health record system is a goal of Austria's e-Health project. The project also includes electronic prescription, electronic referral and electronic medication history. The project envisioned that patient's data will remain with individual hospitals but it is accessible to patients and doctors can access them in private practice. E-card identification is required for citizens to access their individual patient data. Patients can use their E-card to grant pharmacists access to their individual medication data. Doctors can able to view medical history of a patient and access patient data from a national patient document registry.

"ELGA" initiative is a plan for implementing a nationwide **EHR** system in Austria. MAGDALENA-guidelines provide several technical and organizational recommendations to build a health data network which act as a foundation for data exchange within ELGA. ELGA contains identification index for patients and health care providers, a role based authorization concept, integration to e-Card system, ELGA portal containing medical knowledge and personal health data, and a document registry linking the original documents. E-card controls the access to ELGA data.

A.5. Imprivata

Category Industry Solution

Purpose Simple identification and authentication for healthcare IT systems

Scope Enterprise-wide

Technology Single-Sign-On, one time password (OTP), biometric authentication, RFID-badges, smart card

Imprivata provides identity and access management solutions for healthcare organizations. It addresses the password management problem by introducing single sign-on (SSO) solution through its *OneSign*® solution. It supports strong authentication through OTP (one time password) token, smart card or biometric based solution. These authentication techniques are used to provide portable desktop to users and automatic sign-off functionality when a user leaves a workstation.

A.6. Sentillion

Category Industry Solution

Purpose Application suite for single-sign-on and security audits in healthcare

Scope Enterprise-wide

Technology Singe-Sign-On (SSO), virtual desktop

Sentillion (a Microsoft subsidiary) is an identity and access management solution provider exclusively targeting healthcare industries. Sentillion provides set of solutions for single sign-on, strong authentication, identity management, clinical workstations and desktop virtualization.

A.7. CA Technologies Security Solutions

Category Industry Solution

Purpose Application suite for identity management, access control and monitoring of information exchange.

Scope Enterprise-wide

Technology Client-side watchguards, network traffic monitoring, fine grained access control

CA Technologies provides an application suite that covers identity management, access control and monitoring of information with auditing functionality integrated into all three. The secure identity solutions provide efficient identity management and access based on roles. The access solutions enable users to control access to systems and applications across physical, virtual and cloud environment. The information security solution of CA Technologies helps to find, classify and control how information is used based on content and identity of entities.

A.8. CAREfx

Category Industry Solution

Purpose SOA-based application suite for clinical workflow management, information exchange & integration

Scope Inter-Enterprise

Technology Single-Sign-On (SSO)

CAREfx provides solutions for clinical and business process management enabling rapid and accurate decision making by care providers. It also offers products for locating, accessing and interacting with distributed patient information by single sign-on, personalized access and distributed data synchronization.

A.9. IBM Tivoli Access Manager

Category Industry Solution

Purpose Application suite for security, access control, security audit and authentication hardware

Scope Enterprise-wide

Technology Single-Sign-On, biometric authentication, RFID-badges

IBM Tivoli has acquired Encentuate, a provider of single-sign-on solutions. With the Tivoli Access Manager IBM now provides a product suite covering identity and access management software focused on single sign-on and integration of strong authentication solutions.

A.9.1. HealthCast, Inc

Category Industry Solution

Purpose An application suite that targets the fields of **Identity Management**, **Access Control** and **Secure data transmission**

Role-based aspects None.

Technology Encrypted Terminal Sessions, Proximity Badges, Single-Sign-On (SSO)

HealthCast, Inc. offers a product suite that covers authentication management in combined with various hardware solutions such as RFID badges and biometric authentication. Single-Sign-On (SSO) is one of the main solutions HealthCast provides.

A.10. Sense

Category Industry Solution

Purpose Application suite to facilitate secure clinical document sharing

Scope Inter-Enterprise

Technology Cross Enterprise Document Sharing (XDS)

Sense, a eHealth solution provider has the provisions for making medical data available in the right place at right time and to authorized persons only. It offers integrated hospital networking solutions taking care of security, centralized or decentralized data storage, and interoperability between different information systems and international standards. The sense eHealth products adhere to and are tested for compliance with the IHE standards.

A.11. Siemens healthcare

Category Industry Solution

Purpose Main application are hospital information systems

Scope Enterprise-wide

Siemens healthcare among others provides communication and IT infrastructure services for healthcare organizations. Within this area, Siemens has products supporting identity management, secure communication, workflow management and archive solutions for clinical data. The most important product suites are *medico*, *i.s.h. med* and *Soarian®Clinicals*.

A.12. Nexus Medfolio

Category Industry Solution

Purpose Hospital information system, electronic health record

Scope Enterprise-wide

In addition to support digital patient information across hospitals, rehabilitation and social instituions Nexus supports integrated healthcare that enables data exchange between physicians, hospitals and rehabilitation clinics.

A.13. ICW Lifesensor

Category Industry Solution

Purpose Personal electronic health record

Scope Tested in a nationwide programme, available to individuals

Technology Centralized server architecture, web-based access, SSL, Certificates

The *Lifesensor*[1] by ICW electronic health record was started as a test program by the german *Barmer* health insurance. It implements the concept of a personal electronic healthrecord – it is thus administered and fed by the patient and it's use is optional. This concept brings several alleviations, since most of the regulations that apply to medical records kept by medical institutions do not apply. Data in kept databases is encrypted and access to the website is secured by VeriSign-issued SSL certificates. *Lifesensor* is certified as being compliant with the *HealthOnNet*[2] requirements. Data added to the personal health record is generally only availabe to the owner of the records, but access can be granted to other people or parties. Data can be imported and exported from and to other applications.

A.14. Google Health

Category Industry Solution

Purpose Personal electronic health record

Scope Available to individuals

Technology Centralized server architecture, web-based access, SSL, Certificates

Google Health[3] also implements the concept of a personal health record. The functionality is comparable to that of *Lifesensor* (see section solutions:lifesensor). Google explicitly states that because the service is a voluntary offering to individuals, it does not fall under the HIPAA regulations (see section 3.2).
The complexity of the IT system with its distributed nature and growing security and privacy threats require significant research efforts. Some of the existing solutions evolved through extensive research. Some solutions are in the test phase and require compre-

[1] https://www.lifesensor.com/de/de/

[2] http://www.hon.ch/HONcode/Conduct.html

[3] http://www.google.com/health/

hensive trials and investigations. This section explores some of the prominent research initiatives in the areas of security and privacy of healthcare IT systems.

A.15. Secure idenTity acrOss boRders linked (STORK)

Category Research project

Purpose To develop cross-border mechanisms for secure online delivery of documents

Scope European-wide

Technology Smart cards, multi-factor (passwords, PIN) authentication, cryptography, SAML, digital signature

European countries are introducing electronic identities through national e-ID cards for the use of e-government services including administrative services of health care institutions. The interoperability of e-ID is a critical issue in the availability of these services across borders. The use of national e-ID in foreign countries bears security implications from the aspect of acceptability, trust and data protection. The goal of STORK project is to establish the cross-border recognition and authentication of e-IDs issued by other member states. The authorized use of e-IDs, secure access to work stations, and confidentiality, integrity and availability of personal data are the major challenges in this area.

A.16. Netc@rds

Category Research project

Purpose To deploy electronic European Health Insurance Card

Scope European-wide

Technology Smart card, biometrics, security tokens, cryptography, SSL, web service

Netc@rds project is aiming to deploy electronic European Health Insurance Card (e-EHIC) in EFTA/EU countries in order to improve health care services for European citizens across member state boundaries. From security point of view, such initiative requires interoperability of electronic identification/authentication solutions being offered in national level. The cross border identification differs from its domestic counterpart from the following aspects: technical models (e.g. authentication protocols, wide range of smart cards and its datasets) and relevant laws. e-EHIC ensures interoperability in smart cards, personal data sets, technical infrastructure, and authentication protocols and procedures. It establishes secure infrastructure and provides acceptance and trust of personal data coming from another country. There are risks from confidentiality, integrity and availability point of view. But the major security issues identified in netc@rds are authenticity of e-EHIC, authenticating health care professionals and non-uniform laws on data protection [21].

A.17. epSOS

Category Research project

Purpose Service infrastructure for cross-border interoperability of EHR

Scope International

Technology Semantic technologies, privacy enhancing technology (PET), pseudonymisation, encryption, public-key cryptography (PKC), secure hashing, circle of trust

epSOS is a large scale European pilot project aiming to develop an eHealth framework including ICT infrastructure. The goal was to enable secure access to patient health information between different European healthcare systems. epSOS system is expected to create cross-border electronic health services consisting of common security service supporting for secure transport and authorization and secure use of patient consent, and common ID service for transformation between different ID mechanisms. epSOS identity management solution includes interoperable solutions encompassing patient identity, healthcare provider identification, and rights management.
Besides these healthcare focused projects, there exist some research projects whose objectives may satisfy some of the security and privacy aspects in healthcare IT systems. The FIDIS [4](Future of Identity in the Information Society) network of excellence project though did not target healthcare specific services but closely relevant to healthcare IT systems from the following aspects: identity and identity management, privacy of identity, interoperability of identity and identity management systems.

[4] The FIDIS (Future of Identity in the Information Society) project http://www.fidis.net/ [accessed on August 10, 2010]

Bibliography

[1] Authentication in an Electronic Banking Environment. *White paper*, August 2001.

[2] M. A. Al-Kahtani and R. Sandhu. Rule-based RBAC with Negative Authorization. *In proceedings of the 20th Annual Computer Security Applications Conference*, pages 405–415, 2004.

[3] A. H. Anderson. An Introduction to the Web Services Policy Language (WSPL). *In POLICY 2004*.

[4] J.G. Anderson. Clearing the way for physicians' use of clinical information systems. *Communications of the ACM*, 40(8):83–90, 1997.

[5] J.G. Anderson. Social, ethical and legal barriers to e-health. *international journal of medical informatics*, 76(5):480–483, 2007.

[6] J.G. Anderson and C.E. Aydin. Evaluating the impact of health care information systems. *International journal of technology assessment in health care*, 13(02):380–393, 2009.

[7] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter. Enterprise Privacy Authorization Language (EPAL 1.2). *Technical report*, 2003.

[8] Ezedin S. Barka. Framework for Role-Based Delegation Models. *Dissertation for Doctor of Philosophy*, 2002.

[9] T. Beale. Archetypes: Constraint-based domain models for future-proof information systems. In *OOPSLA 2002 workshop on behavioural semantics*. Citeseer, 2002.

[10] Hai bo Shen and Fan Hong. An Attribute-Based Access Control Model for Web Services. *In proceedings of Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pages 74–79, 2006.

[11] Piero A. Bonatti, D. Olmedilla, and J. Peer. Advanced Policy Explanations on the Web. *In ECAI 2006*, pages 200–204.

[12] B. Chaudhry, J. Wang, S. Wu, M. Maglione, W. Mojica, E. Roth, S.C. Morton, and P.G. Shekelle. Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. *Annals of internal medicine*, 144(10):742, 2006.

[13] J. L. D. Coi and D. Olmedilla. A review of trust management, security and privacy policy languages. *In Proceedings International Conference on Security and Cryptography (SECRYPT 2008)*, July 2008.

[14] Anour F. A. Dafa-Alla, Eun Hee Kim, Keun Ho Ryu, and Yong Jun Heo. PRBAC: An Extended Role Based Access Control for Privacy Preserving Data Mining. *In proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05)*, 2005.

[15] N. Damianou, N. Dulay, E. Lupu, and M. Sloman. The Ponder Policy Specification Language. *In POLICY 2001.*

[16] EU Directive. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities L*, 281, 1995.

[17] Marco Eichelberg, Thomas Aden, Jörg Riesmeier, Asuman Dogac, and Gokce B. Laleci. A survey and analysis of electronic healthcare record standards. *ACM Comput. Surv.*, 37(4):277–315, 2005.

[18] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. H. Winsborough, and B. Thuraisingham. Role based Access Control and OWL. *In proceedings of the Fourth OWL: Experiences and Directions Workshop*, 2008.

[19] F. A. Foll and J. Baragry. Next Generation of Digital Identity. *Telektronikk 3/4*, pages 52–56, 2007.

[20] A.X. Garg, N.K.J. Adhikari, H. McDonald, M.P. Rosas-Arellano, PJ Devereaux, J. Beyene, J. Sam, and R.B. Haynes. Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review. *Jama*, 293(10):1223, 2005.

[21] Sławomir Górniak, Ingo Naumann, Dirk Hartmann, and Stephan Körting. Security Issues in Cross-border Electronic Authentication. *the European Network and Information Security Agency (ENISA) study report*, February 2010.

[22] A. Gunther Schadow et al. The HL7 reference information model under scrutiny. In *Ubiquity: technologies for better health in aging societies: proceedings of MIE2006*, page 151. Ios Pr Inc, 2006.

[23] P. Gutmann and I. Grigg. Security usability. *Security & Privacy, IEEE*, 3(4):56–58, 2005.

[24] W. Hersh. Health care information technology: progress and barriers. *Jama*, 292(18):2273, 2004.

[25] W.R. Hersh. Medical informatics: improving health care through information. *Jama*, 288(16):1955, 2002.

[26] I. Iakovidis. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe. *International journal of medical informatics*, 52(1-3):105–115, 1998.

[27] L. Kagal, T. Finin, and A. Joshi. A Policy Language for a Pervasive Computing Environment. *In POLICY 2003.*

[28] Young-Gab Kim, Chang-Joo Mon, Dongwon Jeong, Jeong-Oog Lee, Chee-Yang Song, and Doo-Kwon Baik. Context-Aware Access Control Mechanism for Ubiquitous Applications. *In Advances in Web Intelligence, LNCS*, 3528:236–242, 2005.

[29] N.G. Leveson and C.S. Turner. An investigation of the Therac-25 accidents. *Computer*, 26(7):18–41, 2002.

[30] M. Lorch, S. Proctor, R. Lepro, D. Kafura, and S. Shah. First Experiences using XACML for Access Control in Distributed Systems. *In XMLSEC 2003.*

[31] A. Malcolm, P. Aggleton, M. Bronfman, J. Galvao, P. Mane, and J. Verrall. HIV-related stigmatization and discrimination: Its forms and contexts. *Critical Public Health*, 8(4):347–370, 1998.

[32] C. Mauro, A. Sunyaev, J.M. Leimeister, and H. Krcmar. Service-orientierte Integration medizinischer Geräte-eine State of the Art Analyse. *Wirtschaftsinformatik*, pages 119–128, 2009.

[33] G. J. McCall and R. Simmons. Identities and Interactions. 1966.

[34] Deven McGraw. Comprehensive Privacy and Security: Critical for Health Information Technology. *White paper*, May 2008.

[35] L.E. Moody, E. Slocumb, B. Berg, and D. Jackson. Electronic health records documentation in nursing: nurses' perceptions, attitudes, and preferences. *Computers Informatics Nursing*, 22(6):337, 2004.

[36] Milan Petković. Rights management technologies: A good choice for securing electronic health records? In *ISSE/SECURE 2007: securing electronic business processes: highlights of the Information Security Solutions Europe/SECURE 2007 Conference*, page 178. Springer, 2007.

[37] Torsten Priebe, Wolfgang Dobmeier, and Nora Kamprath. Supporting Attribute-based Access Control with Ontologies. *In proceedings of the First International Conference on Availability, Reliability and Security*, pages 465–472, 2006.

[38] Ravi S. Sandhu. The Typed Access Matrix Model. *In proceedings of the IEEE Symposium on Security and Privacy*, 1992.

[39] Ravi S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based Access Control Models. *In IEEE Computer*, 29(2):38–47, February 1996.

[40] L. Schmitt, T. Falck, F. Wartena, and D. Simons. Novel ISO/IEEE 11073 Standards for Personal Telehealth Systems Interoperability. In *High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability, 2007. HCMDSS-MDPnP. Joint Workshop on*, pages 146–148. IEEE, 2008.

[41] Simon S.Y. Shim, Geetanjali Bhalla, and Vishnu Pendyala. Federated identity management. *Computer*, 38:120–122, 2005.

[42] A. Sunyaev, S. Duennebeil, C. Mauro, J.M. Leimeister, and H. Krcmar. It-standards im gesundheitswesen: Überblick und entwicklungsperspektiven mit der einführung service-orientierter architekturen. *GI Lecture Notes in Informatics*, Band 1, Volume P-175:254–259, 2010.

[43] A. Sunyaev, J.M. Leimeister, A. Schweiger, H. Krcmar, et al. Integrationsarchitekturen fur das Krankenhaus-Status quo und Zukunftsperspektiven. *IM-MUNCHEN-*, 21(1):28, 2006.

[44] Alessandra Toninelli, Rebecca Montanari, Lalana Kagal, and Ora Lassila. A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments. *In proceedings of the 5th International Semantic Web Conference (ISWC)*, 2006.

[45] R. H. Turner. The Role and the person. *The American Journal of Sociology*, (84):1–23, 1978.

[46] A. Uszok, J. M. Bradshaw, R. Jeffers, N. Suri, P. J. Hayes, M. R. Breedy, L. Bunch, M. Johnson, S. Kulkarni, and J. Lott. KAoS Policy and Domain Services: Toward a Description-logic Approach to Policy Representation, Deconfliction, and Enforcement. *In POLICY 2003.*

[47] T. Weichert. Die elektronische Gesundheitskarte. *Datenschutz und Datensicherheit*, 28(7):391–403, 2004.

[48] Jianming Yong, Elisa Bertino, Mark Toleman, and Dave Roberts. Extended RBAC with Role Attributes. *In proceedings of the 10th Pacific Asia Conference on Information Systems (PACIS 2006)*, July 2006.

Aktuelle Technische Berichte des Hasso-Plattner-Instituts

Band	ISBN	Titel	Autoren / Redaktion
44	978-3-86956-113-4	**Virtualisierung und Cloud Computing: Konzepte, Technologiestudie, Marktübersicht**	Christoph Meinel, Christian Willems, Sebastian Roschke, Maxim Schnjakin
43	978-3-86956-110-3	**SOA-Security 2010 : Symposium für Sicherheit in Service-orientierten Architekturen ; 28. / 29. Oktober 2010 am Hasso-Plattner-Institut**	Christoph Meinel, Ivonne Thomas, Robert Warschofsky et al.
42	978-3-86956-114-1	**Proceedings of the Fall 2010 Future SOC Lab Day**	Hrsg. von Christoph Meinel, Andreas Polze, Alexander Zeier et al.
41	978-3-86956-108-0	**The effect of tangible media on individuals in business process modeling: A controlled experiment**	Alexander Lübbe
40	978-3-86956-106-6	**Selected Papers of the International Workshop on Smalltalk Technologies (IWST'10)**	Hrsg. von Michael Haupt, Robert Hirschfeld
39	978-3-86956-092-2	**Dritter Deutscher IPv6 Gipfel 2010**	Hrsg. von Christoph Meinel und Harald Sack
38	978-3-86956-081-6	**Extracting Structured Information from Wikipedia Articles to Populate Infoboxes**	Dustin Lange, Christoph Böhm, Felix Naumann
37	978-3-86956-078-6	**Toward Bridging the Gap Between Formal Semantics and Implementation of Triple Graph Grammars**	Holger Giese, Stephan Hildebrandt, Leen Lambers
36	978-3-86956-065-6	**Pattern Matching for an Object-oriented and Dynamically Typed Programming Language**	Felix Geller, Robert Hirschfeld, Gilad Bracha
35	978-3-86956-054-0	**Business Process Model Abstraction : Theory and Practice**	Sergey Smirnov, Hajo A. Reijers, Thijs Nugteren, Mathias Weske
34	978-3-86956-048-9	**Efficient and exact computation of inclusion dependencies for data integration**	Jana Bauckmann, Ulf Leser, Felix Naumann
33	978-3-86956-043-4	**Proceedings of the 9th Workshop on Aspects, Components, and Patterns for Infrastructure Software (ACP4IS '10)**	Hrsg. von Bram Adams, Michael Haupt, Daniel Lohmann
32	978-3-86956-037-3	**STG Decomposition: Internal Communication for SI Implementability**	Dominic Wist, Mark Schaefer, Walter Vogler, Ralf Wollowski
31	978-3-86956-036-6	**Proceedings of the 4th Ph.D. Retreat of the HPI Research School on Service-oriented Systems Engineering**	Hrsg. von den Professoren des HPI
30	978-3-86956-009-0	**Action Patterns in Business Process Models**	Sergey Smirnov, Matthias Weidlich, Jan Mendling, Mathias Weske
29	978-3-940793-91-1	**Correct Dynamic Service-Oriented Architectures: Modeling and Compositional Verification with Dynamic Collaborations**	Basil Becker, Holger Giese, Stefan Neumann

ISBN 978-3-86956-128-8
ISSN 1613-5652