2009 Fourth International Conference on Systems

Technologies for the Pseudonymization of Medical Data: A Legal Evaluation

Thomas Neubauer
Vienna University of Technology
Vienna, Austria
Email: neubauer@ifs.tuwien.ac.at

Mathias Kolb
Secure Business Austria
Vienna, Austria
Email: kolb@securityresearch.ac.at

***Abstract*—Privacy is one of the fundamental issues in health care today. Although, it is a fundamental right of every individual to demand privacy and a variety of laws were enacted that demand the protection of patients' privacy, approaches for protecting privacy often do not comply with legal requirements or basic security requirements. This paper highlights research directions currently pursued for privacy protection in e-health and evaluates common pseudonymization approaches against legal and technical criteria. Thereby, it supports decision makers in deciding on privacy systems and researchers in identifying the gaps of current approaches for privacy protection as a basis for further research.**

I. Introduction

Privacy is one of the fundamental issues in health care today and a trade-off between the patient's demands for privacy as well as the society's need for improving efficiency and reducing costs of the health care system. Electronic health records (EHR) improve communication between health care providers and access to data and documentation, leading to better clinical and service quality [9]. The EHR promises massive savings by digitizing diagnostic tests and images (e.g., $81 billion in annual savings in the US, if 90% of the health care providers used it, cf. [2]). The pervasiveness of electronic devices has resulted in the almost constant surveillance of everyone and the permanent storage of personal data that is used and analyzed by corporations or intelligence services. With informative and interconnected systems (e.g., the Internet) comes highly sensitive and personal information that is often available over the Internet and – what is more concerning – hardly protected. It is a fundamental right of every individual to demand privacy because the disclosure of sensitive data (e.g., health data) may cause serious problems for the individual. Insurance companies or employers could use this information to deny health coverage or employment. Therefore, a variety of laws were enacted that demand the protection of privacy: Regarding the individual's privacy, historically the phrase "to be let alone", defined at the US Supreme Court in 1834, became famous. In 1948 the United Nations ratified a right to privacy in article 12 of the Universal Declaration of Human Rights. The UN declaration defines privacy as "'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation"'. UN member countries are morally, if not legally, bound by such declarations. Everyone has the right to the protection of the law against such interference or attacks. In 1966 a Computer Bill of Rights was suggested, followed by a Rights to Privacy Act in 1967 was proposed, which banned wiretapping and electronic eavesdropping. The current Privacy Act in the US dates back to 1974 that only has been applied to the Federal Government, and not the private sector. The individuals' rights are difficult and costly to pursue because they are limited in the absence of a dedicated authority to oversee and enforce compliance. In 1980/1981 the Organization for Economic Cooperation and Development (OECD) published the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Convention of the Council of Europe that defined the provisions for the protection of individuals with regard to the automatic processing of personal data. A citizen's right of privacy is also recognized in the Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Additionally, in the EU many domestic acts (e.g., the Austrian Data Protection Act) dictate strict regulations on the processing of personal data. In 2006 the United States Department of Health & Human Service Health issued the Health Insurance Portability and Accountability Act (HIPAA) which demands the protection of patients data that is shared from its original source of collection (cf. [21]). In the European Union the Directive 95/46/EC [3], and the Article 29 Working Party [4] demand the protection of health data.

However, only a few of the existing pseudonymization approaches comply with the current legal requirements. Researchers agree that more needs to be done to protect consumers' privacy against the onslaught of rapidly advancing technologies that track, store, and share sensitive data. This development has profound implications for our society and our freedoms; it influences the way we think and live. In this discussion privacy is often not the main concern, but surveillance, and the effects it has - both positive and negative - on human values, relationships, and daily practice. This paper presents an evaluation of current privacy enhancing technologies (PET) that specifically aim at protecting medical data and, thus, are used as a basis for EHR systems. In the scope of this paper we regard evaluation as the "systematic assessment of the operation and/or the outcomes of a program or policy, compared to a set of explicit or implicit standards, as a means of contributing to the improvement of the program or

978-0-7695-3551-7/09 $25.00 © 2009 IEEE
DOI 10.1109/ICONS.2009.48

policy" (cf. [25]). Based on the categorization of House ([8]) and Stufflebeam & Webster ([19]) we use a combination of the following objectivist approaches: Testing programs approach and Objectives-based approach. The objectives used for the evaluation are taken from the legal acts HIPAA and the EU Directive. This evaluation provides management decision makers such as chief privacy officers and chief security officers with a funded decision-making basis for the selection of privacy-enhancing technologies in the e-health area. As literature does not provide evaluations focusing on the comparison of PETs in e-health in literature so far, this paper provides a major contribution to the research area of privacy.

II. Description of selected Pseudonymization Approaches

This chapter describes major pseudonymization approaches in detail. Thereby, we differentiate between pseudonymization approaches that store patient's data (i) encrypted and (ii) unencrypted.

A. Peterson Approach

Peterson [11] claims to provide a system for making available personal medical information records to an individual without jeopardizing privacy. As the title of the patent states the main ideas behind the approach are (i) the encryption of patient's data, (ii) the universal access to medical records by any (also unauthorized) person while (iii) the patient is responsible for granting privacy. The user registers at the provider's website, receives a unique Global Key (GK) and server side key ($SSID$) generated by the provider and has to provide a unique Personal Encryption Key (PEK) as well as a password. GK, PEK and password are stored in the "Data Table". The user is demanded to enter a PEK until he provides a unique one. After registration the user may print the GK on an ID Card (on paper). This approach consists of three database tables: a "Security Table" that links the data in the "Data Table" (using attribute SSID) to the appropriate entries in the "User Table" (using attribute data table row number). Data is stored double encrypted in the database. If the user wants to retrieve data from the database, the user enters the GK or PEK which are sent to the server through a firewall and checked if they match any entry in the database. The user enters an arbitrarily key and gets immediate access to the records without authentication. The server looks up the $SSID$ and all corresponding data table row numbers needed for retrieving the (medical) data entries from the database. The records are decrypted using (i) the PEK and the PE method and (ii) the $SSEK$ and the SS method and delivered to the user. If a person knows the global key GK or PEK or both, but does not have a password, she is able to view medical data sets. To be able to add, modify or delete medical datasets, the person has to provide an additional password. Peterson arguments, that this access levels protect the privacy of a patient, because the data does not contain any identifying information. The approach of Peterson [11] provides a fall-back mechanism, if the patient has lost or used her GK. Therefore the patient has to login to the system with her PEK and password. Afterwards she requests a new GK, which could be printed on a new card. The new GK assures, that her medical data are protected against unauthorized access with the old one.

B. Pseudonymization of Information for Privacy in e-Health (PIPE)

PIPE (cf. [10], [13]–[15] introduces a new architecture that provides the following contributions compared to other methodologies: PIPE allows (i) the authorization of health care providers or relatives to access defined medical data on encryption level, (ii) provides a secure fall-back mechanism, in case the security token is lost or worn out, (iii) stores the data without the possibility of data profiling, and (iv) provides secondary use without establishing a link between the data and its owner. The client is a small service, which provides an interface to legacy applications, manages requests to local smart card readers and creates a secure connection to the server. The server, also called Logic (L), handles requests from clients to the storage. The data in the storage is divided into two parts, the personal data and the pseudonymized medical data. The link between personal data and pseudonymized medical data is protected through a hull-architecture. The hull-architecture contains a minimum of three security-layers: the authentication layer (outer hull), the user permission layer (inner hull) and the concealed data layer. To reach the next hull, there are one or more secrets, for example, symmetric or asymmetric keys or hidden relations, in every hull-layer. PIPE defines users with different roles comprising patient A, relative B, health care provider C or operator O. The patient is the owner of her data and has full control of her datasets. She is able to view her medical data, add and revoke health care providers and she may define relatives, who have the same rights as herself. Health care providers can be authorized to see and create subsets of anamnesis data by the patient. The operators are the administrators of the system.

- The authentication layer contains an asymmetric key pair, for example the patient outer public key K_A and outer private key K_A^{-1}. These keys are stored on a smart card and are protected with a pin code. The outer private key is used to decrypt the keys of the permission hull-layer.
- The permission layer contains an asymmetric key pair and a symmetric key, for example the patient inner public key $\widehat{K}_A$, inner private key $\widehat{K}_A^{-1}$ and symmetric key $\overline{K}_A$. The symmetric key is encrypted with the inner private key and is used to en-/decrypt pseudonyms in the concealed data layer. If a patient associate a relative, her inner private key $\widehat{K}_A^{-1}$ will be encrypted with the relative's inner public key $\widehat{K}_B$. So, the relative is able to decrypt the patient's symmetric key $\overline{K}_A$ with her inner private key $\widehat{K}_B^{-1}$, until the patient's inner private key $\widehat{K}_A^{-1}$ is changed.
- The concealed data layer contains hidden relations, which are called pseudonyms. Each medical data set is associated with one or more pseudonyms ψ_{i_j}. As the patient is the owner of her medical data and the person

with security clearance, she owns the so called root-pseudonym ψ_{i_0}. These pseudonyms are calculated with an algorithm, which is based on a secret key. In our case, this secret key is the symmetric key of the user. Only instances, who are able to decrypt one of these pseudonyms ψ_{i_j}, can rebuild the link between the patient and her medical data.

To find the pseudonyms to rebuild the link to the medical data, the authors introduced keywords. Keywords are selected on creation time of the medical data or when another user is authorized. They are encrypted with the symmetric key of the root user and the user, who is being authorized. After the keywords are stored in the database, the user can select any of this keywords to find the pseudonym. The hull-architecture assures a high level of security. As all data would be lost if a patient loses her smart card or the smart card is worn-out, PIPE implements a fall-back mechanism to replace the smart card. Therefore, operators O have been introduced, who share the inner private key $\widehat{K}_A^{-1}$ of a patient. To decrease the risk of abuse only several operators based on the four-eye-principle could re-build the key. Therefore the patient's inner private key $\widehat{K}_A^{-1}$ is divided into shared secrets by the use of Shamir's threshold scheme [16]. This scheme allows sharing keys between several operators. The inner private key is shared with N_A $(N_A \subset N)$ randomly assigned operators and to recover the key, N_k $(N_k \subseteq N_A)$ operators are needed. Additionally, operators have no knowledge which key shares they hold.

C. Electronic health card (eGK)

The electronic health card [1], [5] is an approach of the Fraunhofer Institute supported by the Federal Ministry of Health Germany. EGK is designed as a service-oriented architecture (SOA) with some restrictions. One of these restrictions is, that the health card can only be accessed locally on the client side. Another restriction is, that services should use remote procedure calls for communication due to performance and availability issues. Therefore, the system architecture is divided into five layers: (i) The *presentation* layer defines interfaces to communicate with the user, (ii) the *business logic* layer combines different services, which are processed automatically, (iii) the *service* layer provides special functional uncoupled services, (iv) the *application* layer primarily realizes the user right and data management, and (iv) the *infrastructure* layer contains all physical hardware and software management, for example, data storage, system management, virtual private networks, etc. With this layered architecture, the system provides several service applications such as emergency data, electronic prescription, electronic medical report or a electronic health record system. The system includes a ticketing concept to realize some uncoupled action in combination with security mechanisms, to comply with the privacy policy: All data, which will be stored in the virtual file system is encrypted with a one-time symmetric key, called session key. This session key is encrypted with the public key of the patient. To decrypt the data, the patient has to decrypt the session key with his private key and finally the data will be decrypted with this session key. A user is authenticated by using the Challenge-Response technique. Therefore the system generates a random number. This number will be encrypted with the public key of the user. Only the user is allowed to decrypt this random number with the private key, which is stored on her health card and can send it back to the eGK system. Furthermore, the ticketing concept manages the access rights to the system. A file or directory in this virtual file system has a default ticket-toolkit and any amount of private ticket-toolkits, called t-node. The user defines a private ticket-toolkit for every other user in the system. This private ticket-toolkit could have stronger or looser access policies as the default ticket-toolkit. The ticket-toolkit contains a ticket-building tool, a ticket-verifier, the access policy list and a encrypted link to the directory or file. Every user holds a root directory in the virtual file system, which does not have a parent node. Furthermore, any directory contains unencrypted links to the ticket-toolkits of their child nodes. This technique enables the system to perform a fast selection of sub nodes (select * from t-nodes where parentID = directoryID). To be able to find the root node of a specific user, the query service maps a unique identifier, for example the insurance number to the internal user and returns a ticket-toolkit containing a encrypted link to the root node. If there is no private ticket-toolkit available for the user, who performed the request, the system returns a default ticket-toolkit, which is based on a challenge. If the user is able to solve this challenge, she will get the access rights, which have been defined in the default access policy. Both, the hybrid encryption and the challenge response technique are based on the asymmetric key pair, which is stored on the patients' health card. Neither the operating company nor any public administration organization could recover the data, which has been stored in the system, if the patient lost the smart card or the card is worn out. To overcome this problem, the eGK architecture optionally provides the possibility to store a second private ticket-toolkit for every entry. This private ticket-toolkit uses an asymmetric key pair, which is stored on an emergency card. The architecture does not specify this emergency card, but recommends to use the card of a family member or a notary. In case the card has been lost, the patient requests a new health card. Therefore, the emergency card is used to decrypt the session keys of the second ticket-toolkit and finally the session keys are encrypted with the keys of the new health card. Additionally a new second private ticket-toolkit will be created for the new emergency card. After this process, the system does not accept the old health and emergency cards anymore.

D. Thielscher Approach

Thielscher [20] proposed a electronic health record system, which uses decentralized keys stored on smart cards. The medical data are split into identification data and the anamnesis data and stored into two different databases. The key stored on the smart card of a patient is used to link the patient identity

to her datasets. Therefore, this key generates a unique data identification code (DIC), which is also stored in the database. Such a DIC does not contain any information to identify an individual. Data identification codes are shared between the patient and health care providers to authorize them to access the medical data set. For more security the authorization is limited to a certain time period. After this period any access attempt is invalid. The keys to calculate the data identification code (DIC) are stored on smart cards. In case these smart cards are lost, a fall-back mechanism is provided by Thielscher. Every pseudonym hold by a patient is stored in a list, which is stored at an off-line computer. In case the smart card is lost or destroyed, this list could be used to re-link the data to the patient.

E. Approach of Slamanig and Stingl

The approach of Slamanig and Stingl [17], [18] stores the data in a centralized database and uses a smart card for authentication. The system keeps the pseudonyms of a user secret. Each pseudonym realizes a sub-identity of the user and is encrypted with a public key. In case the user wants to view the datasets of one of his sub-identities, she has to login into the system with her general pin code and she has to enter the pin code of the sub-identity to activate the private key on the smart card. Furthermore a public pseudonym of each user is available, which is used for authorization purposes. The system is divided into two repositories, the user repository and document repository. The link between these repositories is done by holding a 5-tuple dataset $(U_S, U_R, U_C, U_P, D_i)$, which contains the sender U_S, the receiver U_R, the creator U_C, the concerning user U_P, for example the patient, and the document D_i. To ensure, that on creation time no linkage between the concerned user is possible, all elements in the tuple, are encrypted with the public key of the receiver, except of the receiver element U_R. Until the receiver has not logged into the system, the receiver element U_R will be the public pseudonym. On the next login of the receiver, the system will replace the receiver element U_R with a secret pseudonym of the user and re-encrypts the other elements of the tuple. This tuple dataset can also be used for exchanging documents between users. There are six possible variations for exchanging or disclosure the message:

1) $(\_, \_, U_C, U_P, D_i)$: Creator and concerning user are known
2) $(\_, \_, U_C, U_P*, D_i)$: Creator is known and concerning user is pseudonymized
3) $(\_, \_, U_C, \_, D_i)$: Creator is known and concerning user is anonymized
4) $(\_, \_, \_, U_P, D_i)$: Concerning user is known
5) $(\_, \_, \_, U_P*, D_i)$: Concerning user is pseudonymized
6) $(\_, \_, \_, \_, D_i)$: fully anonymized

As fall-back mechanism, the authors mentioned, that a distributed key backup to N users using a (t, N)-threshold secret sharing scheme could be implemented, because the users private keys are essential for the system.

F. Pommerening Approaches

Pommerening [12] proposes different approaches for secondary use of medical data. The first approach is based on data from overlapping sources for one-time secondary use. In this case, overlapping sources can be data from different EHRs or a biomaterial bank. To connect the data a unique identifier (PID) has been introduced. A pseudonymization service encrypts the PID with an hash algorithm and the medical data has been encrypted with the public key of the secondary user. The secondary user can decrypt the medical data and merge the data of a person, but cannot identify it. The second approach is also based on one-time secondary use, but with the possibility to re-identify the patient. Therefore, Pommerening extends the first approach with an PID service, which stores a reference list containing the identity of the patient and the associated PIDs. In case the patient should be notified, the pseudonymization service decrypts the pseudonym and sends the request to the PID service, which allows to notify the data source owner. The third approach fits the need of a research network with many secondary users and it also supports long-term observation of patients (e.g., with chronic diseases). The research results can be send to the patient or her responsible health care provider. Therefore a physician export his local database to the central researcher database. The identification data will be replaced with a PID using the PID service. For each secondary use the data will be exported through the pseudonymization service. The PID is encrypted by the pseudonymization service with a project specific key to ensure that different projects get different pseudonyms.

III. Evaluation

Pseudonymization approaches (e.g., used for securing electronic health record systems) have to adhere certain requirements to accord with privacy laws in the European Union or United States. The following set of requirements have been extracted from actual legal acts (cf. [3], [6], [7], [22]–[24]).

- *User authentication*: The system has to provide adequate mechanism for user authentication. This could be done, for example with smart cards or finger print.
- *Data ownership*: The owner of the medical data has to be the patient. The patient should be able to define who is authorized to access and create her medical records.
- *Limited access*: The system must ensure that medical data is only provided to authenticated and authorized persons.
- *Protection against unauthorized and authorized access*: The medical records of an individual have to be protected against unauthorized access. This includes system administrators who should not be able to access these medical records, for example, through compromising the database.
- *Notice about uses of patients data*: The patient should be informed about any access to her medical records.
- *Access and copy own data*: The system has to provide mechanisms to access and copy the patients own data.

- *Unobservability*: means, that pseudonymized medical data could not be observed and linked to a specific individual in the system.
- *Secondary use*: The system should provide a mechanism to export pseudonymized data for secondary use and a possibility to notify the owner of the exported data, if new medicaments or treatment methods are available.

Table I applies the legal criteria defined above to the selected pseudonymization approaches. Characteristics that are accurate with the law or fully implemented are denoted with x, whereas characteristics that are not accurate with the law or not implemented are denoted with $-$ and o indicates properties that are partially implemented.

Most of the approaches implement the requirements of *user authentication*, *data ownership*, *limited access* and serve control mechanisms *against unauthorized and authorized access*. The implementation of the requirement *protection against unauthorized and authorized access* is inadequate. Additional requirements, which enhance the security of the system and the containing datasets, are widely implemented. The approaches of Pommerening and Peterson only pseudonymize data on export. The approaches of Pommerening have the drawback that the generated pseudonyms from the PID service are stored in a reference patient list, to be able to re-build the link to the patient. To enhance the security, this list will be stored at a third party institution, but this measure does not prevent an abuse of the list through an insider of the third party institution. An attacker could bribe an insider of the third party institution to get access to the patient list or the identifying data of some pseudonyms. The Peterson approach has some major security issues. Although the data is doubly encrypted an attacker getting access to the database gets access to all data stored on the server because the keys needed for decrypting the data are (i) also stored in the same database and (ii) what is even more important the relation between the tables (thus between the identification data and the medical data) are stored in clear text. An attacker getting access to the database can decrypt all information and what is even more important, as the password is stored in the database as well as the keys, the attacker may change data stored in the database. The PEK is selected by the user but must be unique in the system. This behavior does not only open a security leak because the user trying to chose a key is informed about the keys that already existing in the system. An attacker could use the keys reported as existing for immediate access to the medical data associated with this key. Moreover, this behavior is impractical and inefficient in practice as the user might have to select dozens of keys before he enters a valid one. Thielscher's approach comes with the shortcoming, that the pseudonyms are stored centrally in the patient mapping list for recovery purposes. To prevent attacks to this list, Thielscher keeps this list off-line, but this mechanism cannot prevent insider abuse or social engineering attacks. The usage of a patients-pseudonyms list as fall-back mechanism could lead to security issues. The work-around of Thielscher to keep the patients-pseudonyms list off-line promises a higher level of security, but does not prevent the system against social-engineering or insider attacks. Furthermore, it does not provide protection if the attacker gets physical access to the computer. Another drawback of the system is the emergency call center. This call center can abuse their access privileges to get access to medical data of any patient. The drawback of the approach of Slamanig and Stingl is that an attacker may authorize other users, send faked medical documents or disclose medical data. This attack is possible, because the authors use a week mechanism for authorization and disclosure. For example, the requirements to send a faked medical document are, (i) access to the database, (ii) the public pseudonym U_P of the user, which the attacker wants to harm, (iii) any public pseudonym to fake the sender U_S and creator U_C, (iv) the public pseudonym and the public key K_R of the receiver U_R, for example the employer, and (v) a harmful document D_i. After the attacker has all the required information, she inserts a new tuple into the authorization table (e.g., 1). After the next login of the receiver, the system replaces the public pseudonym of the user with a private pseudonym of the receiver.

$$(\{U_S\}_{K_R}, U_R, \{U_C\}_{K_R}, \{U_P\}_{K_R}, \{D_i\}_{K_R}) \qquad (1)$$

In contrast, PIPE, eGK and Slamanig/Stingl store the data pseudonymized in the database. Attackers who get access to the database or system administrators cannot link the data to individuals. Both approaches provide a high level of security. Even if the attacker breaks into the database, she would not be able to link and read the stored data. Maybe, the attacker could do a data profiling attack and get some informations from the unencrypted keywords, if these contain any identifiable words. The only way to link the data to an individual is by doing a social engineering attack and fake the identity of the person, the attacker wants to attack. Therefore, the attacker would have to fake a official photo identification in order to get a new smart card to access the system. Another method to link data to an individual is by doing a data mining or data profiling attack.

IV. Conclusions

Health care require the sharing of patient related data in order to provide efficient patients' treatment. As highly sensitive and personal information is stored and shared within highly interconnected systems (e.g., electronic health records), there is increasing political, legal and social pressure to guarantee patients' privacy. Although, legislation demands the protection of patients' privacy, most approaches that lay claim to protect patients' privacy fail in fulfilling legal and technical requirements. This paper gave an overview of research directions that are currently pursued for privacy protection in e-health and identified pseudonymization as the most promising approach from the group of candidates including role based access control, anonymization, depersonalization and encryption. By evaluating common pseudonymization approaches against legal and technical criteria taken from legal acts and literature,

Legal Requirements	*DPA*	*HIPAA*	*PIPE*	*eGK*	*Po*	*Pe*	*Th*	*St*
User authentication	x	x	x	x	-	o	x	x
Data ownership	x	x	x	x	-	-	x	x
Limited access	x	x	x	x	o	-	x	x
Protection against unauthorized and authorized access	x	x	x	x	o	-	o	x
Notice about uses of patients data	x	x	x	x	-	-	-	-
Access and copy own data	x	x	x	x	o	x	x	x
Unobservability	x	x	x	x	x	-	x	x
Secondary use	-	x	x	o	x	-	-	x

TABLE I
EVALUATION OF PSEUDONYMIZATION APPROACHES

this paper answered the question which approaches fulfill the current legal requirements regarding the protection of medical data. From the six candidates that were evaluated, only two can be seriously considered for use in practice. The result show that more contemporary approaches fulfill more of the legal requirements of the European Union and the United States. Whereas the eGK approach encrypts patients' data, PIPE leaves the decision of encrypting patients' data up to the user. Therefore, PIPE turns out to be the more appropriate option if secondary use is demanded. Apart from this difference both approaches - eGk and PIPE - provide a similar level of security and fulfill the majority of the applied criteria. The results of the evaluation can support decision makers (such as chief security officers) especially in health care in their decision process when it comes to the selection of a system for protecting patients' data according to legal requirements posed by HIPAA or the EU Directives. Furthermore, the results may assist researchers in identifying the gaps of current approaches for privacy protection as a basis for further research.

V. ACKNOWLEDGMENTS

This work was supported by grants of the Austrian Government's FIT-IT Research Initiative on Trust in IT Systems under the contract 816158 and was performed at Secure Business Austria, a competence center that is funded by the Austrian Federal Ministry of Economics and Labor (BMWA) as well as by the provincial government of Vienna.

REFERENCES

[1] Joerg Caumanns. Der Patient bleibt Herr seiner Daten. *Informatik-Spektrum*, pages 321–331, 2006.

[2] Frank R. Ernst and Amy J. Grizzle. Drug-related morbidity and mortality: Updating the cost-of-illness model. *Journal of the American Pharmacists Association*, 41(2):192–199, 2001.

[3] European Union. 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 281:31–50, 1995.

[4] European Union, Article 29 Working Party. Working document on the processing of personal data relating to health in electronic health records (ehr), February 2007.

[5] Fraunhofer Institut. Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte, 2005.

[6] Stephen Hinde. Privacy legislation: a comparison of the US and European approaches. *Computers and Security*, 22(5):378–387, 2003.

[7] Gerrit Hornung, Christoph F.-J. Goetz, and Andreas J. W. Goldschmidt. Die künftige Telematik-Rahmenarchitektur im Gesundheitswesen. *Wirtschaftsinformatik*, 47:171–179, 2005.

[8] E. R. House. Assumptions underlying evaluation models. *Educational Researcher*, 7(3):4–12, 1978.

[9] S. Maerkle, K. Koechy, R. Tschirley, and H. U. Lemke. The PREPaRe system – Patient Oriented Access to the "Personal Electronic Medical Record". In *Proceedings of Computer Assisted Radiology and Surgery, Netherlands*, pages 849–854, 2001.

[10] Thomas Neubauer and Bernhard Riedl. Improving patients privacy with pseudonymization. In *Proceedings of the International Congress of the European Federation for Medical Informatics*, 2008.

[11] Robert L. Peterson. Encryption system for allowing immediate universal access to medical records while maintaining complete patient control over privacy. *US Patent Application Publication, No.: US 2003/0074564 A1*, 2003.

[12] Klaus Pommerening and Michael Reng. *Medical And Care Compunetics 1*, chapter Secondary use of the Electronic Health Record via pseudonymisation, pages 441–446. IOS Press, 2004.

[13] Bernhard Riedl, Veronika Grascher, and Thomas Neubauer. A secure e-health architecture based on the appliance of pseudonymization. *Journal of Software*, 2008.

[14] Bernhard Riedl, Thomas Neubauer, and Oswald Boehm. Patent: Datenverarbeitungssystem zur Verarbeitung von Objektdaten. *Austrian Patent, Nr. 503291, September*, 2007.

[15] Bernhard Riedl, Thomas Neubauer, Gernot Goluch, Oswald Boehm, Gert Reinauer, and Alexander Krumboeck. A secure architecture for the pseudonymization of medical data. *Proceedings of the Second International Conference on Availability, Reliability and Security*, pages 318–324, 2007.

[16] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[17] Daniel Slamanig and Christian Stingl. Privacy aspects of e-health. In *Proceedings of the Third International Conference on Availability, Reliability and Security*, pages 1226–1233, 2008.

[18] Christian Stingl and Daniel Slamanig. Berechtigungskonzept für ein e-health-portal. In Günter Schreier, Dieter Hayn, and Elske Ammenwerth, editors, *eHealth 2007 - Medical Informatics meets eHealth*, number 227, pages 135–140. Oesterreichische Computer Gesellschaft, 2007.

[19] D. L. Stufflebeam and W. J. Webster. An analysis of alternative approaches to evaluation. *Educational Evaluation and Policy Analysis*, 2(3):5–19, 1980.

[20] Christian Thielscher, Martin Gottfried, Simon Umbreit, Frank Boegner, Jochen Haack, and Nikolai Schroeders. Patent: Data processing system for patient data. *Int. Patent, WO 03/034294 A2*, 2005.

[21] United States Department of Health & Human Service. HIPAA Administrative Simplification: Enforcement; Final Rule. *Federal Register / Rules and Regulations*, 71(32), 2006.

[22] U.S. Congress. Health Insurance Portability and Accountability Act of 1996. *104th Congress*, 1996.

[23] U.S. Department of Health & Human Services Office for Civil Rights. Your Health Information Privacy Rights. ONLINE.

[24] U.S. Department of Health & Human Services Office for Civil Rights. Summary of the HIPAA Privacy Rule, 2003.

[25] C. H. Weiss. *Evaluation: Methods for studying programs and policies*. Prentice Hall, 2nd edition, 1998.