Assuring Integrity and Confidentiality for Pseudonymized Health Data

Bernhard Riedl
Asian University
Chonburi, Thailand
Email: briedl@asianust.ac.th

Veronika Grascher
University of Klagenfurt
Klagenfurt, Austria
Email: veronika.grascher@edu.uni-klu.ac.at

***Abstract*— Nowadays, the development in demographics results in increased costs for providing services in health care systems. Recent studies show that the installation of an EHR (Electronic Health Record) could help in lowering expense while improving the treatment quality at the same time. Apart from this, such systems could also pose the threat of a privacy invasion, because patients' sensitive medical datasets are stored within an EHR. Several architectures have been published which can be used to implement an EHR system, but most of them do not provide an appropriate level of security. With our approach PIPE (Pseudonymization of Information for Privacy in e-Health) we focus on addressing the occurring security issues and provide a safe system for medical information.**

I. Introduction

As an enormous quantity of datasets is produced in the health care sector, managing people's medical information tends to be cost-intensive. One approach to decrease these costs is the implementation of an electronic health record (EHR) system [1]–[3], which allows health care providers to communicate and collaborate by sharing medical data. Moreover, the digitizing of, for example, medical images not only helps to keep this part of the occurring costs in the health system under control [4], but additionally has an environmental benefit. The availability of life-long medical datasets would also help to reduce the alarming number of more than 98,000 annual cases of death in the US which are caused by medical errors [5].

As sensitive medical information is stored within an EHR system, it is understandable that people are concerned about privacy [6], because an attacker could exploit a vulnerability in order to gain unauthorized access to their sensitive information. A leaked medical history about substance abuse or depression could have a severe impact on a patient's life, because employers could terminate employment or insurance companies could deny coverage. Alan Westin concluded that privacy concerns are triggered by "distrust in institutions and fear of technology abuse" [7]. Thus, the success of the EHR is also based on the users' trust in such a system [8].

In 2005, the California Health Care Foundation (CHCF) involved 11,000 people in their "National Consumer Health Privacy Survey" and published the following results [9]:

- More than two-thirds of the subjects were "somewhat" or "very concerned" about their privacy.
- If a better coordinated medical treatment would be the result of the implementation of the EHR, nearly 60% would agree with the handeling of their medical data by such a system.
- On the contrary, every eighth person would opt out of the current plans towards an EHR, even with the knowledge of exposing their health to some risk.
- More than half of the subjects consented to provide their anonymized medical data for the secondary usage in medical studies, if their privacy was guaranteed.

To assure an appropriate level of privacy, medical information needs to be kept confidential. Avizienis et al. define confidentiality as "the absence of unauthorized disclosure of information" [10]. Besides the possibility to ensure confidentiality by the usage of encryption, a form of pseudonymization is often applied in medical environments. Pseudonymization is a technique which separates the identifying attributes of a dataset from the payload [11]–[13]. Given that, medical information can be stored while still assuring the patients' privacy.

In a safe system, not only the confidentiality, but also the integrity of data needs to be guaranteed. Otherwise an attacker could modify the stored data and as a consequence, patients would for example receive the wrong medication. In the worst case this could be lethal. Integrity can be defined as the "absence of improper system alterations." [10]. While pseudonymization can be used to provide confidentiality [11]–[13], the integrity of medical data needs to be safeguarded by the application of digital signatures, because pseudonymization is based on the storage of data in plaintext.

In this work, we present our approach PIPE (Pseudonymization of Information for Privacy in e-Health) which can be used for the secure handling of medical data.

II. Related Work

Several approaches have been contributed to provide a secure architecture for establishing an EHR. The system published by Thielscher et al. [14] is based on decentralized keys stored on smart cards. The storage is realized by the usage of two databases, of which the first one holds the patient's identification and the second one the patient's medical data. The crypto-chip on a patient's smart card can be utilized to calculate a unique data identification code (DIC) which is

associated with a medical dataset. Afterwards, the personal-related information is removed from the medical dataset. As the DIC cannot be associated with the patient, the medical dataset is kept confidential. Thielscher et al. also proposed a backup solution for the users' keys in case a patient does not have access to her smart card anymore because of loss or theft. They operate a centralized computer without network access which holds a patient-DIC list [14]. Nevertheless, an adversary may still conduct a social-engineering-attack on a system's insider to gain unauthorized access to a patient's medical data (cf. [15] for a description of social-engineering-attacks).

From a security point of view, Thielscher's approach is similar to two different architectures which Pommerening et al. developed [16]. Their system, which can be utilized for the secondary usage of medical data, relies on the combination of a hash and an encryption technique.

Pommerening's basic workflow consists of the following steps: Firstly, the identification data (IDAT) are separated from the medical data (MDAT). Afterwards, a hash algorithm, which they call the PID Generator, is applied to form a unique identifier (PID). Then this identifier is encrypted by a pseudonymization service to calculate the patient's pseudonym (PSN). Finally, the medical data together with the pseudonyms are made available to research centers for secondary usage. [16] In case the pseudonymization needs to be reversed, Pommerening et al. use a patients-pseudonyms list [16]. This list is comparable to the patient-DIC list of Thielscher's system, but in contrast to Thielscher, Pommerening uses a centralized secret key instead of smart cards. This opens up another vulnerability, because an attacker could find out this single key and consequently unveil the relation between the patients' PIDs and their MDAT.

Another attacking scenario exploits the fact that every user's PID and the resulting PSN is only unique for every single patient and not for every patient's medical dataset. Hence, it is possible to conclude the medical history by combining all database entries marked with the pseudonym of a particular patient. As a consequence, the identity of a certain patient may be guessed, based on her medical history. From a security point of view, it would at least be necessary to change a patient's PSN for each medical study in order to avoid these types of attacks.

In the next section we discuss our approach PIPE which is based on a hull architecture instead of storing the relations between patients and their datasets in a centralized form. PIPE can be used to establish a secure EHR environment for the primary and secondary usage of medical data.

III. Secure Pseudonymization

In our system PIPE, all datasets are held persistently in the storage St, which consists of two separate databases. One holds the plaintext pseudonyms and the related medical datasets, which are stored in plaintext due to performance reasons. The other database is used to save the users' personal information and their encrypted pseudonyms. The logic L is a centralized system that provides access to the storage St. As the logic handles the key management, we define it as a trusted instance. [12]

TABLE I
Definition of PIPE's System Attributes

	Patient	*Health Care Provider*
abbreviation	A	C
unique identifier	A_{id}	C_{id}
(outer public key, private key)	(K_A, K_A^{-1})	(K_C, K_C^{-1})
(inner public key, private key)	$(\widehat{K}_A, \widehat{K}_A^{-1})$	$(\widehat{K}_C, \widehat{K}_C^{-1})$
inner symmetric key	$\overline{K}_A$	$\overline{K}_C$
medical data	φ_i	φ_i
pseudonym	ψ_{i_0}, ψ_{i_j}	ψ_{i_j}
tags	τ_w	τ_v

In Table I, we provide an overview of the keys K and abbreviations, which we use to describe our system. In order to distinguish private keys from the corresponding public keys, we mark them with a superscript $^{-1}$; for example, the health care provider's (HCP) outer private key is denoted as K_C^{-1}. To point out that a message has been encrypted with a particular key, we apply curly brackets and the key as a subscript character. Moreover, every attribute within the brackets has been encrypted individually. This measurement is necessary for querying encrypted identifiers in the database.

A. Hull Architecture

Our system is based on a layered model [11]–[13], in which each layer comprises one or more secrets, like encrypted keys or hidden relations. To gain access to the secrets of one layer, any user U has to possess the unveiled secrets of the next outer layer to "peel the hulls". PIPE's hull architecture consists of three layers which we describe in this section.

The most inner layer holds the patients' diagnosis, treatment and anamnesis datasets, which are denoted as φ_i. Each of these entries is related to distinct pseudonyms ψ_{i_j}. These pseudonyms are shared with health care providers to authorize them to certain medical datasets. To assure that the patient is in full control of her data, we additionally introduce a so-called root pseudonym ψ_{i_0} for each φ_i. This pseudonym is only known by the patient herself and ensures that nobody except her is able to delete all pseudonyms of a certain anamnesis dataset and therefore the access to her medical data. For example, if two health care providers are authorized to see a specific medical dataset, three distinct pseudonyms exist. Thus, both pseudonyms which are shared between a patient and a health care provider may be deleted and the patient would still have access to her medical data.

To guarantee that nobody except an authorized person is able to access φ_i, we encrypt the pseudonyms in the next outer layer. The corresponding encryption key is called inner symmetric key and denoted as $\overline{K}_A$, if it belongs to a patient. As $\overline{K}_A$ is stored within the system, we encrypt it with the patient's inner public key $\widehat{K}_A$. Furthermore we encrypt the patient's inner private key $\widehat{K}_A^{-1}$ with the outer public key K_A. We choose the combination of a symmetric key and an asymmetric key pair in the inner layer because the encryption

with symmetric keys is more efficient whereas public-key algorithms allow us to avoid the key distribution problem.

The patient's outer key pair (K_A, K_A^{-1}) is only available on the particular user's smart card. The smart card, which is equipped with a logic chip to conduct encryption and decryption operations, represents the most outer layer. Nowadays, the usage of smart cards is a common practice to ensure confidentiality and integrity of sensitive information for conducting cryptographic operations. Thus, in combination with a certified card reader, this authentication technique can be considered as secure [17].

In the next sections, we show how data can be added to and retrieved from our system PIPE.

B. Adding Medical Data to the System

If a health care provider wants to add medical data on behalf of the patient to the system, both actors first of all authenticate against their particular smart card by entering a PIN. Afterwards, they use their outer private key K_U^{-1} to decrypt the inner private key $\widehat{K}_U^{-1}$ and subsequently the inner symmetric key $\overline{K}_U$. At the end of this mutual authentification process, which is depicted in Equation 1, both users are equipped with their inner symmetric key $\overline{K}_U$ and their inner private key $\widehat{K}_U^{-1}$.

$$f_{auth}(U_{id}) := \begin{cases} \left\{ \left\{ \widehat{K}_U^{-1} \right\}_{K_U}, \left\{ \overline{K}_U \right\}_{\widehat{K}_U} \right\} & U_{id} \in St \\ \text{error code} & U_{id} \notin St \end{cases} \quad (1)$$

In Equations 2-18, we describe the formal workflow. Please note that for exchanging information between two or more actors we use the notation of $Sender \rightarrow Receiver : Message$.

$$A \rightarrow L: \quad f_{auth}(A_{id}) =? \quad (2)$$
$$C \rightarrow L: \quad f_{auth}(C_{id}) =? \quad (3)$$

The patient and the health care provider authenticate against the system and establish each a secured channel between them and the logic.

$$A \rightarrow L: \quad A_{id} \quad (4)$$
$$C \rightarrow L: \quad C_{id} \quad (5)$$

Afterwards, the patient initiates the workflow by sending her identifier to the logic. The health care provider also sends her identifier to the logic.

$$L \rightarrow A: \quad C_{id} \quad (6)$$
$$L \rightarrow C: \quad A_{id} \quad (7)$$

The logic returns the health care provider's identifier to the patient and the patient's identifier to the health care provider.

$$A \rightarrow L \rightarrow St: \quad \{A_{id}, C_{id}\}_{\overline{K}_A} \quad (8)$$
$$C \rightarrow L \rightarrow St: \quad \{C_{id}, A_{id}\}_{\overline{K}_C} \quad (9)$$

Both participants transmit their own and their counterpart's identifier, encrypted with their particular inner symmetric keys, to the logic. This enables the logic to lookup an existing relationship between these actors. We included this measurement to deny unauthorized adding of data for a certain patient by another user. We enforce this security enhancement by checking for the existence of a quadruplet in the identification database, which consists of these four received encrypted attributes. In case no relation between the two actors exist, the logic — if authorized by the patient — automatically adds a corresponding authorization dataset for A and C.

$$St \rightarrow L: \quad \widehat{K}_A, \widehat{K}_C \quad (10)$$

Subsequently, the storage replies with the particular inner public keys of the communication partners.

$$L \rightarrow A: \quad \left\{ C_{id}, \psi_{i_0}, \psi_{i_j} \right\}_{\widehat{K}_A} \quad (11)$$
$$L \rightarrow C: \quad \left\{ A_{id}, \psi_{i_j} \right\}_{\widehat{K}_C} \quad (12)$$

The logic generates the root pseudonym ψ_{i_0} and the pseudonym ψ_{i_j}, which will be shared between the two actors in order to authorize the health care provider for the patient's medical dataset. Afterwards, the logic encrypts the health care provider's identifier and both pseudonyms with the patient's inner public key and transmits these ciphertexts to the patient. Likewise, the patient's identifier and the shared pseudonym are encrypted with the health care provider's inner public key and sent to the health care provider.

$$C \rightarrow L: \quad \left\{ A_{id}, \psi_{i_j}, C_{id}, \tau_v \right\}_{\overline{K}_C}, \varphi_i \quad (13)$$

After the health care provider has decrypted the received information with her inner private key, she adds her own identifier as well as chosen tags τ_v to the message. These tags or meta data (cf. [18] for a detailed description of a tags' taxonomy) are attributes to describe the medical data. Subsequently, she encrypts this information with her inner symmetric key and forwards it, together with the medical data in plaintext, to the logic. As tags are descriptive attributes of medical datasets, they may be used for conducting profiling attacks to guess a patient's identity. To prevent this fraud, tags and other identifiers need to be stored encrypted with the particular user's inner symmetric key.

$$C \rightarrow L: \begin{cases} \left\{ f_{sign}(f_{hash}(\varphi_i))_{\widehat{K}_C^{-1}} \right\}_{\overline{K}_C} \\ f_{sign}(f_{hash}(\varphi_i))_{\widehat{K}_C^{-1}} \end{cases} \quad (14)$$

For integrity purposes, the health care provider as the data enterer, has to ensure the medical data's integrity. Therefore, she signs a hash of the anamnesis, diagnosis or treatment data with her inner private key and encrypts this signature with her inner symmetric key. Finally, she transmits the encrypted signed hash value as well as the signed hash value in plaintext to the logic.

Please note that further integrity issues may arise as an attacker could inject encrypted identifiers or tags into the database. To circumvent this vulnerability, all authorized users could sign a hash of a medical dataset's related meta-data and verify this hash-value on every access. Nevertheless, this attacking vector does not pose a security threat because only authorized users are able to decrypt the pseudonyms that are necessary to retrieve the matching medical data.

$$L \rightarrow A: \quad \left\{ f_{sign}(f_{hash}(\varphi_i))_{\widehat{K}_C^{-1}} \right\}_{\widehat{K}_A} \tag{15}$$

The logic encrypts the plaintext version of the health care provider's signature with the patient's inner public key and forwards this ciphertext to the patient.

$$A \rightarrow L: \begin{cases} \left\{ \psi_{i_0}, \psi_{i_j}, A_{id}, C_{id}, \tau_w \right\}_{\overline{K}_A} \\ \left\{ f_{sign}(f_{hash}(\varphi_i))_{\widehat{K}_C^{-1}} \right\}_{\overline{K}_A} \end{cases} \tag{16}$$

Upon receipt, firstly, the patient decrypts her opposite's identifier, both pseudonyms ψ_{i_j}, ψ_{i_0} (cf. Equation 11) and the health care provider's signature with her inner private key. Secondly, she also chooses related tags and appends them to the pseudonyms, her own as well as the health care provider's identifier and the signed data hash. Afterwards, she encrypts this message and the health care provider's signature with her inner symmetric key and sends it back to the logic. As every participant of a medical dataset chooses her related tags independently, these keywords may differ from each other.

$$A \rightarrow L: \quad \left\{ f_{sign}(f_{hash}(\psi_{i_0}, \psi_{i_j}))_{\widehat{K}_A^{-1}} \right\}_{\overline{K}_A} \tag{17}$$

Furthermore, the patient, as the data owner, calculates a hash value over all pseudonyms and signs this hash with $\widehat{K}_A^{-1}$. This measurement assures the integrity of the plaintext pseudonyms in the medical database. Then she transfers this signature encrypted with her inner symmetric key to the logic. As other users are not able to commit authorizing operations, the patient is the only user who holds an encrypted version of this integrity attribute.

$$L \rightarrow St: \quad \varphi_i, \psi_{i_0}, \psi_{i_j} \tag{18}$$

The logic transfers the anamnesis, diagnosis or treatment data φ_i as well as the pseudonyms in plaintext to the medical database in the storage.

$$L \rightarrow St: \begin{cases} \left\{ A_{id}, C_{id}, \psi_{i_0}, \psi_{i_j}, \tau_w \right\}_{\overline{K}_A} \\ \left\{ A_{id}, C_{id}, \psi_{i_j}, \tau_v \right\}_{\overline{K}_C} \end{cases} \tag{19}$$

Then the logic saves the identifiers of both actors, the pseudonyms and the tags, all encrypted with the patient's inner symmetric key, in the identification database of the storage. Likewise, the logic transfers the identifiers of both actors, the pseudonym ψ_{i_j} and tags, all encrypted with the health care provider's inner symmetric key to the same database.

$$L \rightarrow St: \begin{cases} \left\{ f_{sign}(f_{hash}(\varphi_i))_{\widehat{K}_C^{-1}} \right\}_{\overline{K}_C} \\ \left\{ f_{sign}(f_{hash}(\varphi_i))_{\widehat{K}_C^{-1}} \right\}_{\overline{K}_A} \\ \left\{ f_{sign}(f_{hash}(\psi_{i_0}, \psi_{i_j}))_{\widehat{K}_A^{-1}} \right\}_{\overline{K}_A} \end{cases} \tag{20}$$

Moreover, the logic also sends the signed data hash, encrypted with each participant's inner symmetric key to the storage. Finally, the signed hash value of the associated pseudonyms, which is encrypted with the patient's inner symmetric key, will be saved in the identification database.

Given that, actors in PIPE can conduct SQL select statements, for example with encrypted identifiers, on the identification database to gain access to the associated pseudonyms and subsequently to the pseudonymized medical data. Please note that querying with ciphertexts optimizes the efficiency of the system, as encryption operations are minimized. Another runtime related measurement is to include not only a user's identifier but also related tags in the "where" clause of the SQL statement. This measurement also reduces the amount of returned datasets and thus the subsequent decryption operations. We recommend to choose meta data, like the timestamp of an anamnesis, diagnosis or treatment dataset, atomically. For example, March 19, 2009, would be split into the tags $March$, 19 and 2009. This was a $Thursday$, which is another tag. If we also add the week number, in our example $week\_12$, we are also able to query weekly follow-up appointments.

C. Retrieving Medical Data from the System

If the patient wants to retrieve a specific medical dataset, she firstly uses the authentication workflow to log on to the system. Then she encrypts chosen tags: for example, a keyword or a time stamp with her inner symmetric key in order to prepare the "where" clause in the SQL statement. This query is transfered to the storage via the logic. If there are matching results in the database, the storage replies with a minimum of one or a set of encrypted root pseudonyms which the logic forwards to the patient. Additionally, the logic provides the patient with all related tags of a certain pseudonym and the health care provider's identifier, even if they have not been within the query.

Consequently, the patient is able to decrypt the received pseudonym(s) with her inner symmetric key and subsequently to query the logic with the plaintext pseudonym(s). The logic forwards the patient's request to the storage, where the matching anamnesis, diagnosis or treatment data and their related encrypted signatures are returned.

As the medical information has been sent in plaintext due to performance reasons, it is necessary to check the integrity of the data. Thus, the patient decrypts the previously received health care provider's identifier and forwards it to the storage via the logic. The storage returns the particular health care provider's inner public key, which the patient uses to verify the signature after decrypting it with her inner symmetric key. Afterwards, the patient calculates the hash value of the

plaintext anamnesis, diagnosis or treatment data and compares it with the received signed hash. This procedure ensures that the medical dataset has not been modified in an unauthorized way.

D. Summary

Besides the confidentiality, which we assure by the usage of pseudonymization based on PIPE's hull architecture, an actor is able to prove a particular dataset's integrity by re-calculating the hash-value and checking the validity of the health care provider's signature on the hash value. The signature can be verified, after decryption, by the usage of the health care provider's public key. In case of positive verification of the medical dataset the information in the dataset can be trusted. Furthermore we store a hash value of the associated pseudonyms which has been signed by the patient with every medical dataset. This integrity attribute can be used to assure that no user can be authorized without the patient's explicit consent.

IV. Conclusions and Further Work

The EHR not only promises massive savings [3], [4], but also a better service quality [19] for patients. Moreover, as modern health care systems still lack standard processes, such a system could also support the definition and execution of e-Health workflows [20].

As a life-long medical dataset of a certain patient might also comprise, for example, an HIV-infection or an abortion, there is the requirement for assuring the patients' privacy to avoid misuse [11]–[13]. Patients have different perceptions of privacy and their participation in such a system [9]. As a matter of fact, it is a vital success factor for any privacy-related system to communicate all actions undertaken on a patient's sensitive medical data [21].

In this paper, we discussed the topics of security and privacy in EHR systems. Several approaches have been proposed to solve the challenge for implementing the EHR, but these architectures have vulnerabilities regarding their security [12], [13]. With our approach PIPE we focus on assuring the necessary level of privacy for the patients. PIPE can be used for the primary and secondary usage of medical information. We assure that the patient is always in full control of her data. The backup keystore in our system is based on a variant of Shamir's threshold scheme (cf. [12], [13] for a description of our backup keystore) instead of a relying on a vulnerable centralized patient-pseudonyms-relations list.

Apart from the confidentiality that we gain by the usage of pseudonymization with a multi-level hierarchical key store, we ensure the medical information's integrity with digital signatures. The gained signed messages are based on hashes to assure that every authorized user is able to verify if a medical dataset has been altered. In our approach, this integrity measurement does not reveal the identity of other users.

As further work, we plan to continue our tests in different medical environments and thus broaden our insights into the security and usability of this approach.

V. Acknowledgment

We want to thank Colin G. Black for his review.

References

[1] The Center for Information Technology Leadership, "The value of healthcare information exchange and interoperability," *Healthcare Information and Management Systems Society*, 2005.

[2] J. Pope, "Implementing EHRs requires a shift in thinking. PHRs–the building blocks of EHRs–may be the quickest path to the fulfillment of disease management." *Health Management Technology*, vol. 27, pp. 24,26,120, 2006.

[3] S. Wang, B. Middleton, L. Prosser, C. Bardon, C. Spurr, P. Carchidi, A. Kittler, R. Goldszer, D. Fairchild, A. Sussman, G. Kuperman, and D. Bates, "A cost-benefit analysis of electronic medical records in primary care," *The American Journal of Medicine*, vol. 114, pp. 397–403, 2003.

[4] A. Nitrosi, G. Borasi, F. Nicoli, G. Modigliani, A. Botti, M. Bertolini, and P. Notari, "A Filmless Radiology Department in a Full Digital Regional Hospital: Quantitative Evaluation of the Increased Quality and Efficiency," *Journal of Digital Imaging*, vol. 20, pp. 140–148, 2007.

[5] L. L. Leape and D. M. Berwick, "Five Years After To Err Is Human - What Have We Learned?" *Journal of the American Medical Association*, vol. 293, pp. 2384–2390, 2005.

[6] T. C. Rindfleisch, "Privacy, information technology, and health care," *Communications of ACM*, vol. 40, no. 8, pp. 92–100, 1997.

[7] B. Givens, "Medical records privacy: fears and expectations of patients," in *Toward an Electronic Patient Record Conference*, May 1996. [Online]. Available: http://www.privacyrights.org/ar/speech2.htm

[8] European Union, Article 29 Working Party, "Working document on the processing of personal data relating to health in electronic health records (EHR)," February 2007. [Online]. Available: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf

[9] L. Bishop, B. J. Holmes, and C. M. Kelley, "National Consumer Health Privacy Survey 2005," 2005. [Online]. Available: http://www.chcf.org/topics/view.cfm?itemID=115694

[10] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *Transactions on Dependable and Secure Computing*, vol. 1, pp. 11–33, 2004.

[11] B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, and A. Krumboeck, "A secure architecture for the pseudonymization of medical data," in *Proceedings of the Second International Conference on Availability, Reliability and Security*, 2007, pp. 318–324.

[12] B. Riedl, V. Grascher, and T. Neubauer, "A Secure e-Health Architecture based on the Appliance of Pseudonymization," *Journal of Software*, vol. 3, pp. 23–32, 2008.

[13] B. Riedl, V. Grascher, M. Kolb, and T. Neubauer, "Economic and Security Aspects of the Appliance of a Threshold Scheme in e-Health," in *Proceedings of the Third International Conference on Availability, Reliability and Security*, 2008, pp. 39–46.

[14] C. Thielscher, M. Gottfried, S. Umbreit, F. Boegner, J. Haack, and N. Schroeders, "Patent: Data processing system for patient data," *International Patent, WO 03/034294 A2*, 2005.

[15] T. Thornburgh, "Social engineering: the "Dark Art"," in *Proceedings of the 1st annual Conference on Information Security Curriculum Development*, 2004, pp. 133–135.

[16] K. Pommerening and M. Reng, "Secondary use of the Electronic Health Record via pseudonymisation," *Medical Care Compunetics*, vol. 1, pp. 441–446, 2004.

[17] M. Hendry, *Smart Card Security and Applications, Second Edition*. Artech House, Inc., 2001.

[18] D. Marco, *Building and managing the Meta Data Repository: A Full Life-Cycle Guide*. John Wiley & Sons, Inc., 2000.

[19] R. B. Elson and D. P. Connelly, "Computerized patient records in primary care. their role in mediating guideline-driven physician behavior change," *Family Medicine*, vol. 4, pp. 698–705, 1995.

[20] E. A. McGlynn, S. M. Asch, J. Adams, J. Keesey, J. Hicks, A. DeCristofaro, and E. A. Kerr, "The Quality of Health Care Delivered to Adults in the United States," *The New England Journal of Medicine*, vol. 348, pp. 2635–2645, 2003.

[21] T. Adams, M. Budden, C. Hoare, and H. Sanderson, "Lessons from the central Hampshire electronic health record pilot project: issues of data protection and consent," *BMJ*, vol. 328, pp. 871–874, 2004.