Implementation of Data Security Requirements in a Web-based Application for Interactive Medical Documentation

Anja Perlich, Andrey Sapegin and Christoph Meinel
Hasso Plattner Institute, University of Potsdam
Prof.-Dr.-Helmert-Str. 2-3, 14440 Potsdam, Germany

Keywords: Medical Documentation, Information Security, Mental Health Care, Client-Server Application, Patient Data.

Abstract: Keeping data confidential is a deeply rooted requirement in medical documentation. However, there are increasing calls for patient transparency in medical record documentation. With Tele-Board MED, an interactive system for joint documentation of doctor and patient is developed. This web-based application designed for digital whiteboards will be tested in treatment sessions with psychotherapy patients and therapists. In order to ensure the security of patient data, security measures were implemented and they are illustrated in this paper. We followed the major information security objectives: confidentiality, integrity, availability and accountability. Next to technical aspects, such as data encryption, access restriction through firewall and password, and measures for remote maintenance, we address issues at organizational and infrastructural levels as well (e.g., patients' access to notes). With this paper we want to increase the awareness of information security, and promote a security conception from the beginning of health software research projects. The measures described in this paper can serve as an example for other health software applications dealing with sensitive patient data, from early user testing phases on.

1 INTRODUCTION

Keeping data confidential is a deeply rooted requirement in medical documentation. Nowadays, when patient records are increasingly kept in electronic form, the number of data access paths rise. An analysis of security breaches by industry in the United States shows that in the health care sector, breaches of data security have become common. Over a three-year period, 115 breaches were reported (Curtin and Ayres, 2008).

Increasing calls for patient transparency in medical documentation and trends of sharing patient data between medical institutions impose new challenges of data security (van der Linden et al., 2009).

A recent literature review about security and privacy in electronic health records (EHR) shows that more work needs to be done in terms of adopting to security and privacy standards and directives. Even though the sharing of medical data between stakeholders is an integral part of the concept of EHR, some 25% of the selected articles had no indication on data encryption (Fernández-Alemán et al., 2013).

We want to tackle the challenge of data security from the beginning along with our research on the proof-of-concept of an interactive medical documentation system — Tele-Board MED. Its fundamental idea is to let the patient co-document treatment sessions together with the doctor. We investigate if digital whiteboards are a suitable medium for this purpose. Giving the patient the right to actively contribute to and manipulate the documentation system also raises additional questions on data security.

Therefore, we have analyzed and implemented security measures to provide a secure environment for both patients and doctors using our system and to ensure the compliance with existing patient data privacy laws. In particular, this paper describes the security measures of the interactive documentation system Tele-Board MED by taking into account legal obligations as well as typical information technology security objectives.

With this paper we want to increase awareness of information security among health informatics researchers, and promote a security conception from the beginning of research projects. The measures described in this paper were motivated from the setting of an application server located in the network of an ambulant psychotherapeutic clinic. Nonetheless, the exemplary implementations of security guidelines can

Perlich A., Sapegin A. and Meinel C..
Implementation of Data Security Requirements in a Web-based Application for Interactive Medical Documentation.
DOI: 10.5220/0005204503520359
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2015), pages 352-359
ISBN: 978-989-758-068-0

serve as a general example for health software applications dealing with sensitive patient data.

This paper is organized as follows. Section 2 provides details on the Tele-Board MED system and its setup in the clinic network. In section 3 we analyze security criteria for this setup. Based on this, we provide details on the implementation of the security policies in section 4; while section 5 describes security measures for connected systems. Finally, the paper closes with future work and conclusions in sections 6 and 7.

2 TELE-BOARD MED

During a treatment session at the doctor's office the patient usually does not get to see the notes which are taken. Often they can only get a glimpse at illegible handwriting or at the back of a computer screen.

In the scope of the research project Tele-Board MED, we investigate how medical documentation can be turned from a necessity taken care of by the doctor, into a task that supports the patient's recovery. More specifically we try out whether digital whiteboards can be a suitable medium for joint documentation for both patient and doctor, and we investigate if this leads to higher personal engagement by the patient.

2.1 Therapist-patient Documentation in Behavior Psychotherapy

The domain of application and testing is behavior psychotherapy, since here the patient's verbal contribution is higher compared to, e.g., cancer treatment. Moreover, the treatment outcome very much depends on the patient's personal engagement and the patient-therapist relationship (Lambert, 2013).

Tele-Board MED is being developed as an adjunct to the traditional face-to-face therapy to allow a joint documentation of the session's therapeutic content. Figure 1 shows a user scenario with a digital whiteboard to display and operate the documentation panel via touch gestures. Additionally, tablet computers are used as input devices.

The system is being tested at a major German outpatient clinic for psychotherapy with about 200 therapists.

2.2 General Setup and Software Components

Tele-Board MED is a web-based application accessible from common web browsers. It is designed

Figure 1: A doctor-patient scenario: Using Tele-Board MED in a therapy session.

to enable interactions with digital whiteboard panels, e.g., drawing with digital pens, erasing pen strokes, and writing, posting, arranging and clustering sticky notes. Nonetheless, it can be used on a normal screen with mouse and keyboard input as well.

With Tele-Board MED we build upon Tele-Board, a whiteboard system designed to support remote collaboration in distributed design thinking teams (Gumienny et al., 2011). In Tele-Board, there are four main software components: the web portal, the whiteboard client, the sticky note pad application and the server component. The web portal is a web application which serves as the user's entry point to the system. It provides a platform to manage the whiteboard panels. The actual work on a panel happens in the whiteboard client, a Java application launched from the web portal via Java Web Start. The sticky note pad app allows sending digital sticky notes from mobile devices, e.g., tablets, to the whiteboard. The server component contains the database (MySQL[1]), a web server (Apache HTTPD[2]), and a collaboration server for the synchronization of the whiteboard panel elements (Openfire[3]).

The system architecture with the different devices linked to the software components is shown in figure 2. The whiteboard client can be operated on digital whiteboards as well as on a laptop. Sticky notes can also be created and sent to the whiteboard via the web portal and the sticky pad app.

[1] http://www.mysql.com
[2] http://httpd.apache.org
[3] http://www.igniterealtime.org/projects/openfire

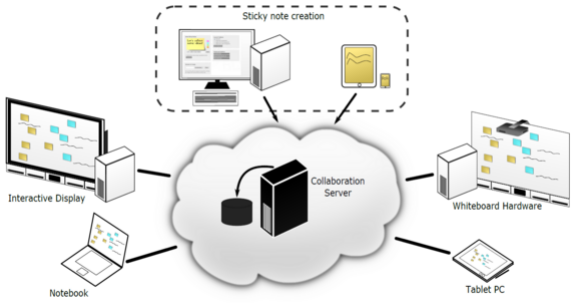

Figure 2: Software system architecture, adapted from (Gumienny et al., 2013).

In order to allow collaboration over distances, Tele-Board is accessible via the World Wide Web. For the pilot application in psychotherapy sessions however, we do not make use of the remote collaboration feature. That is, patient and therapist are in one room and they are the only persons documenting on the whiteboard panel.

2.3 Integrating the Tele-board MED Server in the Clinic Network

Protecting the patient data is the clinic's topmost priority. This is why it was no option to locate the server in a remote location, such as the research institution. Though this setup would have had the advantage of performing the technical maintenance locally.

In any case, in order to test Tele-Board MED with patients, the server holding the data had to be located in the clinic's premises and not be publicly available through the internet. Therefore, we have set up a dedicated Tele-Board MED server and connected it to the clinic network. Our setup includes the physical server (running Ubuntu GNU/Linux 12.04 Server) and the Tele-Board MED server component, including the database (cf. subsection 2.2). Additionally there is a NAS[4] for data backups. Figure 3 shows the integration of our setup into the network.

The Tele-Board MED components are located in a dedicated subnet, where all connections can be controlled. In order for therapists to log into the Tele-Board MED application they need to be connected to the clinic network. However, for security reasons, connections initiated by the Tele-Board MED server into the internal network are blocked using a router with a firewall.

Thus, our setup is separated from the main network, but allows connections from the therapists' computers as well as remote maintenance for administrators (cf. section 5). In the following sections the security measures of this setup are discussed in greater detail.

3 DATA SECURITY CRITERIA

The need for the protection of private patient data has its roots in the medical profession itself. The professional code of secrecy states that everybody who works in health services has to keep strictly confidential all information obtained concerning the patient. Data privacy shall guarantee that everybody can decide which data is gathered about him or her, for which purpose, and to whom it is transferred (Leiner et al., 2009).

Since patient cases are documented with Tele-Board MED, the protection against information security breach is crucially important. In the results of a feedback study about Tele-Board MED with therapists, we found one skeptical group of therapists, mainly concerned about data security issues (von Thienen et al., 2015). The dialogue with the cooperating clinic's directors also disclosed general worries concerning data security.

Therefore, in our project we strictly adhere to the legal obligations and ensure that our setup meets the general information security objectives, as described in the following subsections.

In this context, it is worthwhile mentioning the standardization of security measures according to the ISO 27000 series. The ISO 27001 standard in particular is the specification for an information security management system and its integration into business processes. The standard implies not only the presence of properly configured security tools, but also careful planning and implementation of security policies within different departments of a company. (Pelnekar, 2011). Yet, this goes beyond the mandatory requirements and is out of proportion to our research project.

3.1 Legal Obligations

In countries of the European Union, the statutory regulations are geared to the data protection directive (European Parliament and the Council of the European Union, 1995). Every documentation system especially in the sensitive healthcare domain has to comply with the demands on confidentiality and data security.

In Germany, the legal foundation is the Federal Data Protection Act[5]. Based on this law, the German

[4]Network-attached storage

[5]German: Bundesdatenschutzgesetz, BDSG, 1990

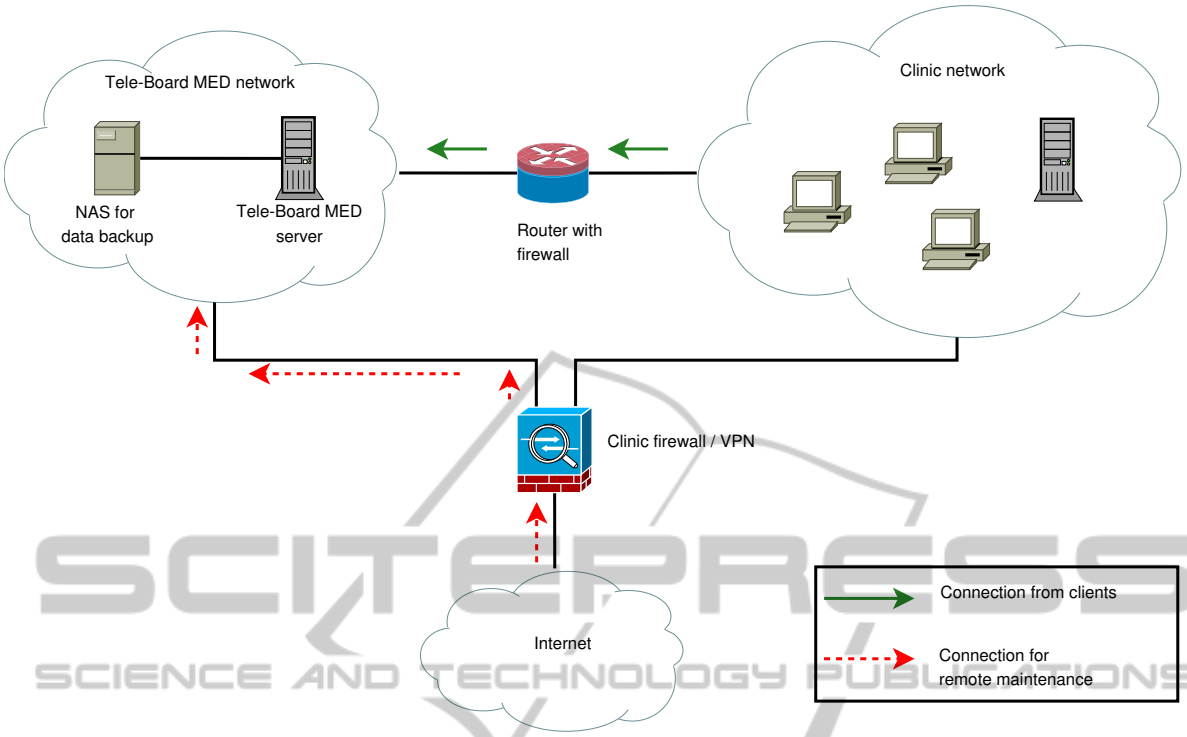

Figure 3: Connection of the Tele-Board MED server to the clinic network.

Medical Association[6] issued recommendations about data privacy and data processing in a doctor's office. Specifically the technical appendix (German Medical Association, 2008) provides an overview of the security measures to be set up in medical practices.

3.2 Information Security Objectives

General security objectives and measures with regard to web-based health care applications are described by (Roehrig and Knorr, 2000). In addition to the so-called CIA requirements for communication security (confidentiality, integrity, availability), they also emphasize accountability as the fourth major security objective of computerized health care applications.

- **Confidentiality.** To keep data confidential means to protect it from unauthorized disclosure. In healthcare, confidentiality is considered the most important information security objective since medical data is highly sensitive.
- **Integrity.** Integrity means making sure that data is not tampered with and that it is what it is supposed to be. Compromised data integrity in health care can, for instance, lead to medical malpractice.
- **Availability.** A system is called available when the required data and services are delivered within an acceptable period of time. A computerized system taking too long to respond, e.g., due to overload or collapse, can delay the therapy and at worst be life-threatening for a patient.
- **Accountability.** If the accountability of a system is guaranteed, every participant of a communication can be sure that the partner (e.g., person or machine) is the one purported to be. In healthcare it is important to know who performed which service at which time in order to hold users responsible for their actions.

4 REALIZATION OF SECURITY MEASURES

The starting point for the implementation of security measures was the technical appendix of the recommendations (German Medical Association, 2008) (cf. section 3.1). We have implemented these recommendations in our setup and provide an overview in table 1. It shows the relevant excerpts of the recommendations together with short descriptions of the practical application.

At this point we want to briefly comment on

[6]German: Bundesärztekammer

how the therapists' perception of data security risk changed. In a feedback study carried out in 2013 concerns about data security were particularly pronounced (von Thienen et al., 2015). After a follow-up presentation to the therapists on the system development progress and the implemented security measures, they were asked to fill in a feedback questionnaire. The results show that none of the therapists had concerns about data security. We can conclude that the awareness about and actions taken for higher data security led to a more confident feeling about using Tele-Board MED in treatment sessions.

We now describe the implemented measures in more detail according to the information security objectives listed in section 3.2.

4.1 Confidentiality Measures

Technical confidentiality measures have been implemented at application as well as at hardware-near levels.

To ensure security of the data transferred to and from users, the web portal only allows SSL[7] connections, which are encrypted. The login to the web portal and the sticky pad application requires user name and password, and is implemented using the form-based authentication mechanism by the CakePHP framework[8]. Access control lists (ACLs) are used to regulate more specific access to parts of the web portal.

In order to prevent physical access to the data, the server's hard disk's data partition is encrypted[9] (cf. table 1, #9).

To separate patient records from each other, the web portal provides a treatment session mode with restricted view (cf. table 1, #1). When a session is running for a certain patient, the files of other patients are hidden in the web portal. Every action is logged, such as starting and stopping a treatment session, or operating the whiteboard panel content.

In addition to technical measures, we also implemented organizational confidentiality measures, namely the non-disclosure agreement signed by the researchers (cf. table 1, #4), the instructions on requirements of password characteristics (cf. table 1, #7), and the limitation of the application's user accounts to therapists. Therefore, the patient does contribute to the documentation, but only if the therapist is present. However, there are export features so that patients can receive a copy of their data (cf. table 1, #2). Accounts are given out to therapists at the clinic only after personal introduction.

4.2 Integrity Measures

The integrity of the patient data could be harmed by unauthorized manipulation through the web portal and whiteboard client, or at database level. Each transaction in the Tele-Board MED application is logged in the database. Furthermore, a former whiteboard panel state can easily be recovered with the help of the history function. Deleted elements are only marked as deleted but are never completely erased.

In order to prevent data manipulation at database level the server itself and the database are password-protected.

4.3 Availability Measures

The server's configuration was chosen according to the maximal expected capacity utilization. To prevent the server from being attacked, and services and data from being unavailable, we set up a firewall (cf. table 1, #8). The only ports which are open for requests from outside of the server are the ones for the protocols SSH[10] (for remote maintenance), HTTPS[11] (for access to web portal), and XMPP[12] with SSL (for the synchronization of panel elements in whiteboard client sessions). The database port is only open for requests from inside of the server.

In case of a data loss on the server, the backup can be used to reconstitute the data availability (cf. table 1, #11). Backups of the database and other personal data, e.g., images, are done on a daily basis in an automated way using a backup script. Every time the complete data is packed in an archive and encrypted using the asymmetric encryption method RSA[13].

Another measure for redundancy in data storage on the server is RAID 1[14]. In case of disk failure, the server could continue operating in degraded mode using the mirrored hard disk until the failed one is replaced.

Finally, the server has a dual power supply and is connected to a Uninterruptible Power Supply (UPS) unit to resist short-term power interruptions.

[7] Secure Sockets Layer

[8] http://www.cakephp.org

[9] We used the Advanced Encryption Standard (AES) with a 256-bit key, and RIPEMD-160 hash algorithm.

[10] Secure Shell

[11] Hypertext Transfer Protocol Secure

[12] Extensible Messaging and Presence Protocol

[13] named after the inventors Rivest, Shamir and Adleman

[14] redundant array of independent disks – mirroring

Table 1: Translated excerpt from the recommendations (German Medical Association, 2008) and corresponding security measures in Tele-Board MED.

#	Recommendation excerpt	Realization
1	"Patient files should in no case be placed in a way that patients can view files of other patients." (section 4.2)	A treatment session mode was implemented. Switching to this mode requires an additional authentication. When a doctor starts a session for a patient in the web portal, the other patient files are hidden, and only documents are shown which belong to the current patient.
2	"In no case should the patients by themselves have the possibility to operate the doctor's computer. Nonetheless, printouts or a digital copy of the doctor's notes transferred via secure electronic communication should be provided." (s. 5.1)	Patients do not get login credentials, and can only access the data in the presence of the doctor. The doctor has the possibility to export data (e.g., as a picture or into common office formats) and hand over printouts (or digital copies) to a patient.
3	"As far as there is no authorization or justification, a transmission of personal data is only allowed if there is an explicit or implicit patient consent. This consent must refer to the concrete transmission process." (s. 5.2)	The patient is informed in a written form about the project Tele-Board MED and signs a patient consent for explicitly described purposes of data handling.
4	"In a contractual relationship the contractor and authorized co-workers have to commit their confidentiality in a written consent." (s. 6)	The researchers involved in the Tele-Board MED project sign the privacy policy of the cooperating clinic.
5	"All (remote) maintenance activities as well as the name of the performing person have to be documented." (s. 6)	Log files are created automatically on the server. A log file contains the timestamps, types and authors of every access.
6	"In remote maintenance, the data transfer between the doctor's computer and the technician's computer has to be encrypted and should only be done via a secured connection." (technical appendix, s. 10)	The remote maintenance is done via a password-protected VPN connection and the SSH protocol which allows encrypted connection only.
7	"A password should be longer than seven characters, should not be listed in dictionaries and should not consist of names or personal data (e.g., date of birth). Furthermore it should contain special characters (e.g., $, #, ?, *, &) and/or numerical digits. If special characters or numerical digits are used, common variations, such as adding them at the beginning or end, should be avoided." (technical appendix, s. 2.1)	The Tele-Board MED web portal is only accessible via HTTPS, and the access is password-protected. The users are instructed to change the default password as soon as possible and to choose a password according to the requirements.
8	"For individual computers, the installation of a so-called personal firewall [...] provides a basic protection; Unix-like systems (e.g., Linux or Mac OS X) should be run with their own firewall mechanisms." (technical appendix, s. 3.1.3)	The server's firewall was configured so that only those ports are opened which are absolutely necessary.
9	"The storage media used in the doctor's practice holding patient data, e.g., notebooks and PDAs, must be completely encrypted, in order to avoid abuse of sensitive data in the case of a theft." (technical appendix, s. 5)	The Tele-Board MED server's hard disk was encrypted. In case of a theft the data on the server cannot be read without the possession of the encryption key, which is stored on a data carrier in a physically safe place.
10	"The doctor's notes have to be retained for a period of ten years after the treatment's completion." (s. 4.3)	The duration of the research cooperation is limited. The responsibility for the long-term storage resides with the psychotherapy clinic. There are several possibilities of downloading data from the Tele-Board MED server, e.g., as a database dump, or as a Word or image file export.
11	"In order to ensure the protection of patient data, daily backups should be created on suitable external media." (s. 6)	The Tele-Board MED server creates encrypted database backups daily and stores them on the network-attached storage.

4.4 Accountability Measures

Accountability measures concern the communication at operating system and application level.

In order to guarantee that the machine the client is communicating with is the Tele-Board MED server and no other machine, an X.509 certificate is used. The certificate not only makes it possible to verify the server's identity, but also to establish an encrypted communication channel between the server and the client via HTTPS. This certificate was issued by a certificate authority (CA) being part of a public key infrastructure (PKI). The CA is the affiliated university which is in turn trusted by the German National Research and Education Network[15].

The whiteboard client code is signed with a code signing certificate, which makes it possible to verify that the source code originates from the declared developers. A combination of the code's verified origin and its encrypted transmission give evidence of the code's authenticity.

The crucial factor for accountability at client side is a conscious handling of login data. If the user credentials fall into the wrong hands, anybody can pretend to be a certain user. An accountability breach of unauthorized web portal access using someone else's user name and password, can be detected based on database entries. The IP address, the web browser and operating system version of the accessing computer together with timestamps of start and end of the connection are saved. Access to the server is also logged at operating system level (cf. table 1, #5).

5 SECURING THE PERIMETER

The mentioned measures are related to securing the Tele-Board MED server itself. But the security of the data stored on the server also depends on the security of the clients. For example, if the doctor's computer is compromised, one could connect through it to the Tele-Board MED server and access the data. Another example would be a physical access to the server hardware. In spite of the hard disk encryption, an attacker could steal the server and influence its availability. Finally, the computers used by the researchers for server maintenance could also be an entry point for the attacker.

In order to protect the data stored on the server against unauthorized access we also ensured the security of the network perimeter:

- **Network Security and Physical Access.** Since the Tele-Board MED server is located in the clinic building and connected to the clinic network, the security of the network and prevention of physical access to the hardware was delegated to the clinic's information technology department.
- **Security of Remote Maintenance Connection.** To ensure that the data cannot be leaked during the remote maintenance procedure, we secured the connection to the server. Via an encrypted VPN[16] connection we connect to the server over SSH with public-key authorization. The remote maintenance is only allowed from a dedicated laptop[17] and the VPN connection can only be established from a specific range of IP addresses (from inside the research institute's network). Besides that, all researchers involved in the project have signed the clinic's privacy policy.

6 FUTURE WORK

The steps offered for securing patient data ensure only a minimal level of data security. However, this basic implementation complies with the legal regulations of the Federal Data Protection Act and provides an adequate environment for short-term testing of medical information systems such as Tele-Board MED.

For a long-term operation a higher security level is recommended. The following measures can be used to enhance the security:

- **Database integrity checks** can be realized via checksums. Periodically, checksums from the database tables containing patient data are calculated (using a cryptographic hash function) and stored on an external medium. To check the integrity, a checksum of the current database state is recalculated, and compared to the latest stored one. If they match, there is a high probability that no change has occurred.
- **Password brute-force protection** tools such as Fail2ban[18], allow to automatically block users, who try to guess the password for the web application repeatedly.
- **Continuous monitoring** allows ensuring the availability of all critical services. Tools such as Nagios periodically check running services for their status and availability (Josephsen, 2007).

[15]German: Deutsches Forschungsnetz (DFN)

[16]Virtual Private Network

[17]The laptop also has a configured firewall and is used only for the maintenance of Tele-Board MED.

[18]http://www.fail2ban.org

The Tele-Board MED server's availability could be checked by a request from inside the clinic network. Incidents of e.g., hard disk failure, can then be reported automatically by using an internal mail server.

- **Automated security scans** performed with a special software, e.g., Nessus,[19] allow to check the infrastructure for vulnerabilities on a regular basis. These checks provide feedback for the person responsible for security updates of the involved systems.

The mentioned measures and tools allow an automated prevention and detection of security threats, and therefore improve the protection and simplify the management of security events for the monitored system. However, the presence of such tools still does not guarantee that a system is fully secure.

7 CONCLUSION

In this paper we illustrated the realization of security measures in our system Tele-Board MED in order to create conditions which shall enable user tests involving patients in a psychotherapy clinic.

The described security issues concern technical, infrastructural, personal as well as organizational levels. In order to cover these aspects as comprehensively as possible we took into account several references such as legal obligations and general information security objectives.

The more comprehensive the security measure catalogue gets, the higher the security level is. Yet, an absolute guarantee can never be reached.

The focus in research projects on new applications or concepts of human computer interaction, is often on functional features and their usage. Nevertheless, if such projects involve sensitive data, an integrated security concept is recommended from the beginning. Even if it is about early user tests, sensitive personal data is worthwhile protecting.

We hope that the measures described in this paper can serve as an example for other health software research projects dealing with sensitive patient data.

ACKNOWLEDGEMENTS

The work of this project was funded by the HPI-Stanford Design Thinking Research Program.

[19] http://www.nessus.org

REFERENCES

Curtin, C. M. and Ayres, L. T. (2008). Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry. *I/S: A Journal of Law and Policy for the Information Society*, 4:566–598.

European Parliament and the Council of the European Union (1995). 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 Union*, L281:0031–0050.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3):541–562.

German Medical Association (2008). Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis - Technische Anlage. http://www.bundesaerztekammer.de/downloads/Schweigepflicht_Tech_Anlage_2008.pdf.

Gumienny, R., Gericke, L., Quasthoff, M., Willems, C., and Meinel, C. (2011). Tele-Board: Enabling efficient collaboration in digital design spaces. *Proceedings of the International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pages 47–54.

Gumienny, R., Gericke, L., Wenzel, M., and Meinel, C. (2013). Supporting creative collaboration in globally distributed companies. CSCW '13, pages 995–1007. ACM.

Josephsen, D. (2007). *Building a Monitoring Infrastructure with Nagios*. Prentice Hall PTR, Upper Saddle River, NJ, USA.

Lambert, M. J. (2013). *Bergin and Garfield's Handbook of Psychotherapy and Behavior Change*. John Wiley & Sons.

Leiner, F., Gaus, W., Haux, R., Knaup-Gregori, P., and Pfeiffer, K.-P. (2009). *Medizinische Dokumentation: Grundlagen einer qualitätsgesicherten integrierten Krankenversorgung ; Lehrbuch und Leitfaden*. Schattauer.

Pelnekar, C. (2011). Planning for and Implementing ISO 27001. *ISACA Journal*, 4:28–35.

Roehrig, S. and Knorr, K. (2000). Towards a Secure Web Based Health Care Application. *Proceedings of the European Conference on Information Systems (ECIS)*, pages 1323–1330.

van der Linden, H., Kalra, D., Hasman, A., and Talmon, J. (2009). Inter-organizational future proof EHR systems. A review of the security and privacy related issues. *International journal of medical informatics*, 78(3):141–60.

von Thienen, J. P. A., Perlich, A., and Meinel, C. (2015). *Design Thinking Research. Building Innovators*, chapter Tele-Board MED: Supporting Twenty-First Century Medicine for Mutual Benefit. Springer.