Medical Informatics Europe 2002
G Surján et al. (eds)
IOS Press 2002

Data security and protection in cross-institutional electronic patient records

Minne van der HAAK[a], Astrid Corinna WOLFF[a], Volker MLUDEK[a], Peter DRINGS[b], Michael WANNENMACHER[c], Thomas WETTER[a]

[a] *Institute for Medical Biometry and Informatics, Department of Medical Informatics, University of Heidelberg, Germany*
[b] *Department of Internal Medicine and Oncology, Thoraxklinik-Heidelberg, Germany*
[c] *Department of Clinical Radiology, University Medical Center of Heidelberg, Germany*

Abstract. This paper describes data protection and data security requirements of a cross-institutional electronic patient record, and presents possible solutions for meeting these requirements. A comprehensive analysis of literature and legal documents was performed. Beside the general requirements that the EPR of a single institution must meet, specific requirements exist for cross-institutional EPRs. In Germany, patient information may only be revealed to external physicians within so-called "treatment connections". A secure connection between the EPR-systems of two health institutions in Germany, which jointly treat tumor patients, was established using additional SecuRemote™ Software. The development and implementation of a cross-institutional EPR is a complicated process, mainly due to data security regulations. However, its introduction is thought to be valuable, since a cross-institutional EPR will improve communication within shared care processes, and, thus, improve the quality of patient care.
Keywords: Data security, data protection, electronic patient record, shared care

1. Introduction

Modern health care is characterized by the high specialization of health care institutions. These institutions are co-operating in the patient care processes [1-4]. While the health care system has become increasingly distributed and decentralized, care processes center around the patient [5]. Adequate communication between all health institutions involved is a prerequisite for offering high quality care in this new organizational form of health care, often called shared care [1, 6].

An example of such a close cooperation is the Heidelberg/Mannheim Tumor Center, in which the Thoraxklinik-Heidelberg and the Department of Clinical Radiology of the University Medical Center of Heidelberg jointly treat approx. 500 patients per year. The Thoraxklinik-Heidelberg is an academic training hospital of the University of Heidelberg. Mainly patients suffering thoracic and lung diseases are treated in this hospital. While the primary treatment usually takes place in the Thoraxklinik-Heidelberg, the patients are referred to the Department of Clinical Radiology for radiotherapy, usually as out-patients.

Due to several shortcomings of paper-based patient records [7], a transition to electronic patient records has taken place in many health care institutions [8]. However, during shared care processes, patient health information is distributed over several independent, co-operating institutions [9, 10]. These lack possibilities for physicians to view the health information of a shared patient stored at a partner institution. Patient health information, which accumulates during the shared care process of a patient, must be integrated by means

of a shared, cross-institutional EPR to make it available to all responsibly involved participants of the patient care process [11]. Such a patient record is often called *virtual*, since it consists of health data generated by different sources at different locations, but brought together to form one *virtual* record at the time the information is required [5].

A shared, cross-institutional EPR can be set up by means of the Internet or other network technology. However, data security and data protection requirements are a major barrier, especially when the Internet is used as the transfer medium, since it is potentially insecure [12, 13]. This paper describes the data protection and security requirements for setting up a cross-institutional EPR, and offers possible solutions for meeting these requirements.

2. Data security and protection requirements of a cross-institutional EPR

In most developed countries, laws ensure the security and protection of patient data. This is of great importance, since these data are among the most sensitive personal data. Security and protection issues need to be considered carefully, especially in regard to the development and implementation of cross-institutional EPRs accessible via the Internet [12, 13].

The EU has decribed data protection guidelines (95/46/EG) [14] that must be implemented in the national laws of its member states. In Germany, these guidelines have been implemented in several laws. These laws are: the „Strafgesetzbuch" (penal code), the "Bundesdatenschutzgesetz" (federal data protection law), "Landesdatenschutzgesetze" (data protection laws of the federal states), the "Landeskrankenhausgesetze" (hospital laws of the federal states) and the "Ärztliche Berufsordnung" (medical profession code) [14].

For a better understanding of the subject, we shall first present a definition of data security and data protection:

- *Data security* aims to protect an individual's personal data against misuse, unauthorized access or use or change by a third party. It also deals with the security of the data against unintentional change and access by unauthorized individuals.
- *Data protection* ensures the authority of the individual patient to make his/her patient health care data available within the limits of the right of informational self-determination.

Together, data security and data protection aim to ensure the following five fundamental objectives [15]:

1. *Confidentiality* means to ensure that patient data are not made available or disclosed to unauthorized individuals.
2. *Integrity* means to ensure that patient data cannot be changed or deleted by unauthorized individuals or parties.
3. *Authentication* means the corroboration that a person is the one claimed.
4. *Accountability* means that the actions of a person can be traced.
5. *Availability* means that upon demand patient data can be accessed and used by authorized people.

A secure connection between the health institutions is a pre-requisite to ensure the confidentiality and integrity of a cross-institutional EPR. Fixed lines between two health institutions are a way to achieve this. However, they are expensive and not flexible enough. Two alternative solutions for providing a secure connection are secure socket layers (SSL) and by virtual private network (VPN) technology.

1. *SSL* can achieve a low-cost, end-to-end encrypted transmission of information over the Internet [12].
2. Firewalls can offer the functionality of *VPN-technology*. Many health institutions' networks are protected from the outside by means of a firewall. A VPN is a network

that dynamically connects the sites and workstations of several institutions using secure paths, also called tunnels. These tunnels are secured by encryption techniques. A VPN-tunnel can also be set up between a (VPN) server and (VPN) client.

The use of passwords alone to ensure the authentication is insufficient. People forget passwords, write them down or use easily to guess passwords [12]. In addition, passwords can be monitored and then replayed. Two methods for providing secure user authentication are:

1. The *"challenge-response"* procedure uses hardware tokens, or smart cards, in combination with an authentication server. The challenge-response procedure uses encryption techniques, e.g. DES [12], without revealing the actual key. The authentication server has the same key as the hardware token, or smart card. The authentication server sends a combination of numbers (challenge) to the user and calls upon him/her to answer. This challenge is then being encrypted by the authentication server and the hardware token or the smart card. The user sends the result (response) back to the authentication server. That compares both combinations. If they are identical, the authentication has been successful.
2. The *Public Key Infrastructure (PKI)* system [16] authenticates users using digital certificates. PKI makes use of asymmetric cryptography. A corresponding pair of keys, consisting of a private and a public cryptographic key, is used to encrypt and decrypt data, and to generate and attach a digital signature if needed. The authenticity of the pair of keys is ensured by means of a certificate, which associates the public key with the identification data of the key holder. Certification service providers, who fulfill the function of a 'Trusted Third Party', issue the certificates and offer other services surrounding electronic signatures. PKI can be used in combination with VPN software and hardware.

By means of input control, it should be possible to check and identify retrospectively, if and by whom person related data have been entered, changed or deleted, thereby satisfying the requirement of accountability. Therefore, the data processing activities should be recorded. Back up procedures at fixed time intervals can be used to ensure the availability of the data.

In Germany, the confidentiality objective has a special significance. Physicians are not allowed to reveal, or share, health information about a patient with other people, even if these people are also subject to an obligation to maintain confidentiality, e.g. other physicians. A physician is only allowed to share patient information with physicians of other health institutions or medical departments participating in the patient treatment, in the case of a so-called "treatment connection". Shared information should be restricted to such that concerns the treatment case in which the external physician is participating. For shared, cross-institutional EPRs, it is therefore necessary to extend the authorization concepts of health professional information systems to include the "treatment connection" between the case of a specific patient and an external physician.

Furthermore, the written consent, signed by the patient, is needed in which the patient agrees that his/her health information may be stored in a cross-institutional EPR, which can be viewed by the physicians of several health institutions participating in his/her treatment.

If the cross-institutional EPR can be accessed via automatic access procedures, these procedures must be documented in a so-called "index of procedures", and require a pre-check before they can be used in routine.

Special attention has to be paid to results that are not final, i.e. interim results of laboratory tests, since they may change. Such provisional results should either be marked as such, or not be made available to external partners. This is necessary to prevent medical decisions based on incorrect, or provisional results.

3. Solutions for cross-institutional access on the EPR

In the Department of Medical Informatics of the University of Heidelberg a project is underway that aims at a cross-institutional EPR for the Thoraxklinik-Heidelberg and the Department of Clinical Radiology. This shared EPR has to be realized within the existing information system architectures of both institutions. Both the Thoraxklinik-Heidelberg and the Department of Clinical Radiology use the hospital information system IS-H*MED, which offers electronic patient record functionality. Additional department-specific systems are used in both institutions.

As a first step towards a shared, cross-institutional EPR, we proved the functionality of a remote access architecture via ISDN using VPN-1 SecuRemote™ software. This remote access architecture allows a one-way connection. In this way, the hospital information system of the Department of Clinical Radiology can be accessed from the Thoraxklinik-Heidelberg. With the help of VPN-1 SecuRemote™ Software, external users can pass the Firewall-1® of Check Point™ Software Technologies Ltd., which protects the internal network of the University Medical Center of Heidelberg. VPN-1 SecuRemote™ Software establishes VPN-tunnels and allows secure connections using authentication and encryption techniques. In the Thoraxklinik-Heidelberg, only a few computers, placed outside the internal network, have access to the Internet via ISDN. Authentication is performed using an AXENT Technologies'™ Defender Security Server™ and Defender™ Tokens that use the "challenge- response" procedure.

During the weekly radiotherapy consultation that is held in the Thoraxklinik-Heidelberg, the radiologists from the Department of Clinical Radiology can set up a secure connection to the Department of Clinical Radiology from within the Thoraxklinik-Heidelberg using the described approach. They can then can log in to IS-H*MED according to the same procedure as if they were in the Department of Clinical Radiology. Now the radiologists can share the patient information of shared patients with the oncologists from the Thoraxklinik-Heidelberg.

The remote access approach was chosen, because it offered a low-cost, easy method to establish a secure one-way connection between the two institutions. The approach ensured confidentiality, integrity and authentication, and could be realized within the existing information system infrastructure.

In the near future, a bi-directional connection between the two institutions will be set up, by means of a VPN-Tunnel between the firewall of the University Medical Center and a yet to be installed firewall in the Thoraxklinik-Heidelberg. Integration of the two hospital information systems, taking into account the adoption of the "treatment connection" will be the third step towards the shared EPR between the two institutions.

4. Discussion and Conclusion

Many of the data security and protection requirements of single institutional EPRs also apply to shared, cross-institutional EPRs. However, extensions to these requirements are needed, e.g., extensions to the authorization concepts and written consent. In addition, new, specific requirements exist for cross-institutional EPRs, e.g., secure connection and, a German specialty, the adoption of the so-called "treatment connection" into the authorization concept of the EPR.

Due to legal aspects in several countries, especially in Germany, the development and implementation of a cross-institutional EPR is a complicated and difficult process. However, we think that the efforts are reasonable because it will be able to improve the communication between health institutions, medical disciplines and professionals involved

in shared care processes. It will provide them with the complete health information set of jointly treated patients [4] and, thus, is expected to improve the quality of patient care [17].

Acknowledgements

We thank our colleagues in the Thoraxklinik-Heidelberg and in the Department of Clinical Radiology, especially D. Zierhut and D. Oetzel. Special thanks to M. Ehmann and M. Schurer for their assistance in working out the data protection and data security requirements and to K. Horn and U. Thiel for their participation in setting up the remote access.

References

[1] Blobel B, Holena M. *Comparing middleware concepts for advanced healthcare system architectures.* Int J Med Inf, 1997; **46**(2): p. 69-85.
[2] Klimczak JC, Witten DM, Ruiz M, et al. *Providing location-independent access to patient clinical narratives using Web browsers and a tiered server approach.* Proc AMIA Annu Fall Symp, 1996: p. 623-7.
[3] Neame R, Olson M. *How can sharing clinical information be made to work?* Medinfo, 1998; **9**(Pt 1): p. 315-8.
[4] van Bemmel JH. *Toward a virtual electronic patient record.* MD Comput, 1999; **16**(6): p. 20-1.
[5] Forslund DW, Phillips RL, Kilman DG, Cook JL. *Experiences with a distributed virtual patient record system.* Proc AMIA Annu Fall Symp, 1996; **86**(1): p. 483-7.
[6] Blobel B, Pharow P. *Results of European Projects Improving Security of Distributed Health Information Systems. in Medinfo 98.* 1998: IOS Press Amsterdam.
[7] Dujat C, Haux R, Schmucker P, Winter *A. Digital optical archiving of medical records in hospital information systems--a practical approach towards the computer-based patient record?* Methods Inf Med, 1995; **34**(5): p. 489-97.
[8] Safran C, Goldberg H. *Electronic patient records and the impact of the Internet.* Int J Med Inf, 2000; **60**(2): p. 77-83.
[9] Isaac S, Kohanne P, Greenspun J, et al. *Building national electronic medical record systems via the world wide web.* JAMIA, 1996; **3**: p. 191-207.
[10] Forslund D, Kilman D. *An international collaboratory based on virtual patient records.* Comm ACM, 1997; **40**: p. 111-117.
[11] Malamateniou F, Vassilacopoulos G, Mantas J. *A search engine for virtual patient records.* Int J of Med Inf, 1999; **55**: p. 103-115.
[12] Alkhateeb A, Singer H, Yakami M, Takahashi T. *An end-to-end secure patient information access card system.* Methods Inf Med, 2000; **39**(1): p. 70-2.
[13] Anderson JG. *Security of the distributed electronic patient record: a case-based approach to identifying policy issues.* Int J Med Inf, 2000; **60**(2): p. 111-8.
[14] Schurer M, Gesetzestexte, http://www.krz.uni-heidelberg.de/dsb/handbuch.htm, last access: 2002-01-11
[15] Bakker A, Barber B, Moehr J. *Security of the distributed Electronic Patient Record: conclusions, recommendations and guidance.* Int J Med Inf, 2000; **60**(2): p. 227-36.
[16] van Dyk J. *Securing the Exchange of Health Information.* MD Computing, 2000; **16**(5): p. 44-6.
[17] Moehr JR. *Privacy and security requirements of distributed computer based patient records.* Int J Biomed Comput, 1994; **35 Suppl**(2): p. 57-64