Journal of Biomedical Informatics 46 (2013) 541–562

Contents lists available at SciVerse ScienceDirect

Journal of Biomedical Informatics

journal homepage: www.elsevier.com/locate/yjbin

Methodological Review

Security and privacy in electronic health records: A systematic literature review

José Luis Fernández-Alemán, Inmaculada Carrión Señor *, Pedro Ángel Oliver Lozoya, Ambrosio Toval

Department de Informatics and Systems, Faculty of Computer Science, University of Murcia, 30100 Murcia, Spain

ARTICLE INFO

Article history:
Received 1 February 2012
Accepted 16 December 2012
Available online 8 January 2013

Keywords:
Electronic health records
Systematic review
Privacy
Confidentiality
Security
Standards

ABSTRACT

Objective: To report the results of a systematic literature review concerning the security and privacy of electronic health record (EHR) systems.
Data sources: Original articles written in English found in MEDLINE, ACM Digital Library, Wiley InterScience, IEEE Digital Library, Science@Direct, MetaPress, ERIC, CINAHL and Trip Database.
Study selection: Only those articles dealing with the security and privacy of EHR systems.
Data extraction: The extraction of 775 articles using a predefined search string, the outcome of which was reviewed by three authors and checked by a fourth.
Results: A total of 49 articles were selected, of which 26 used standards or regulations related to the privacy and security of EHR data. The most widely used regulations are the Health Insurance Portability and Accountability Act (HIPAA) and the European Data Protection Directive 95/46/EC. We found 23 articles that used symmetric key and/or asymmetric key schemes and 13 articles that employed the pseudo anonymity technique in EHR systems. A total of 11 articles propose the use of a digital signature scheme based on PKI (Public Key Infrastructure) and 13 articles propose a login/password (seven of them combined with a digital certificate or PIN) for authentication. The preferred access control model appears to be Role-Based Access Control (RBAC), since it is used in 27 studies. Ten of these studies discuss who should define the EHR systems' roles. Eleven studies discuss who should provide access to EHR data: patients or health entities. Sixteen of the articles reviewed indicate that it is necessary to override defined access policies in the case of an emergency. In 25 articles an audit-log of the system is produced. Only four studies mention that system users and/or health staff should be trained in security and privacy.
Conclusions: Recent years have witnessed the design of standards and the promulgation of directives concerning security and privacy in EHR systems. However, more work should be done to adopt these regulations and to deploy secure EHR systems.

1. Introduction

The paper-based health records currently in use may generate an extensive paper trail. There is consequently a great interest in moving from paper-based health records to electronic health records (EHRs). These efforts are principally being made by independent organisations. However, recent proposals suggest that integrated health records provide many benefits [1], some of which include: a reduction in costs, improved quality of care, the promotion of evidence-based medicine and record keeping and mobility. In order to achieve these benefits, EHR systems need to satisfy certain requirements in term of data completeness, resilience to failure, high availability, and the consistency of security policies [2]. Four great obstacles limit the deployment of EHR systems: funding, technology, attitude and organisational aspects [3]. Many governments rely on integrated EHRs because of the benefits expected from them. One example of this interest is that of the US government. In 2004, the US President decided that the majority of Americans would be connected to EHRs by 2014 [4]. In February 2009, the US President signed The American Recovery and Reinvestment Act, which included the investment of 19,000 million dollars in the digitalisation of medical records in the USA [5]. The Member States of the European Union also intend to make their health systems compatible before 2015, as the Vice-President of the European Commission announced at the High Level eHealth Conference 2010. The EU's objective is to share patients' EHR data with the objective of "Free Movement" and of obtaining quality and efficient health care [6].

However, there has been very little activity in policy development involving the numerous significant privacy issues raised by a shift from a largely disconnected, paper-based health record system to one that is integrated and electronic [7]. Moreover, the advances in Information and Communications Technologies have led to a situation in which patients' health data are confronting new

* Corresponding author. Fax: +34 868 884151.
E-mail addresses: aleman@um.es (J.L. Fernández-Alemán), mariainmaculada.carrion@um.es (I.C. Señor), pedroangel.oliver@um.es (P.Á.O. Lozoya), atoval@um.es (A. Toval).

1532-0464/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jbi.2012.12.003

security and privacy threats [8].The three fundamental security goals are [9] confidentiality, integrity and availability (CIA). The protection and security of personal information is critical in the health sector, and it is thus necessary to ensure the CIA of personal health information. According to the ISO EN13606 standard [10], confidentiality refers to the "process that ensures that information is accessible only to those authorised to have access to it". Integrity refers to the duty to ensure that information is accurate and is not modified in an unauthorised fashion. The integrity of health information must therefore be protected to ensure patient safety, and one important component of this protection is that of ensuring that the information's entire life cycle is fully auditable. Availability refers to the "property of being accessible and useable upon demand by an authorised entity". The availability of health information is also critical to effective healthcare delivery. Health informatics systems must remain operational in the face of natural disasters, system failures and denial-of-service attacks. Security also involves accountability, which refers to people's right to criticise or ask why something has occurred.

Health information is also regarded by many as being among the most confidential of all types of personal information. Protecting this confidentiality is therefore essential if the privacy of subjects of care is to be maintained. Privacy involves access control versus any party not authorised to access the data, and has been defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [11].

Security and privacy in EHRs can be seriously threatened by hackers, viruses, and worms. Many reports of accidental loss or the theft of sensitive clinical data have appeared in recent years [12,13]. Knowing the security and privacy features that EHR systems have could be critical if these risks are to be confronted and measures to increase the data protection of EHRs are to be adopted. According to studies carried out in several countries, concerns regarding data security and privacy have appeared. A recent study estimated that each year there are 25 million compelled authorisations for the disclosure of health records in the United States [14]. In studies conducted in Denmark, Germany and New Zealand [15–17], respondents stated their data security concerns as regards EHRs. Citizens are also aware of the potential risks that shared EHRs may have. In Austria, individuals can even decide whether or not their health-related data should be shared with institutions and health care professionals [18]. In order to mitigate these concerns, organisations such as the Certification Commission for Healthcare Information Technology (CCHIT) offer a certified program which covers a rigorous inspection of, among other things, security aspects based on existing standards [19], which is primarily relevant for the United States. CCHIT has been certifying EHR technology since 2006.

Providing access to EHRs is a vital next step in activating patients in their care and improving the health system [20]. However, this opens new security threats. There is a real concern about both people's and entities' access levels to patients' EHRs. A patient's EHR might be fragmented and accessible from several sites (by visiting different doctors' offices, hospitals, providers, etc.). Security defects in some of these systems could cause the disclosure of information to unauthorised persons or companies, and health data therefore need protection against manipulations, unauthorised accesses and abuses, which includes taking into account privacy, trustworthiness, authentication, responsibility and availability issues [21,22]. EHRs also have difficulties in maintaining data privacy [23], to the extent that administrative staff could for example access information without the patient's explicit consent [24].

Our objective is to perform a systematic literature review (SLR) related to the security and privacy of EHR systems. This article analyses security and privacy based on the ISO 27799 standard [25] in order to answer the following research question:

RQ1. What security and privacy features do current EHR systems have?

We have carried out an in-depth analysis of all issues related to the security and privacy features of EHR systems reported in published literature using a comparative framework extracted from the ISO 27799 standard. It could be argued that EHR solutions purchased from vendors often come with a pre-set of privacy and security capabilities, and this question can only be answered properly by analysing real solutions that are being used as EHRs. Nevertheless, we believe that if the security and privacy proposals found in published literature are identified and analysed, they could be used as a proxy for what may or may not be the real EHR security and privacy proposals. The review could be a useful contribution for stakeholders in the development, Implementation, selection and use of EHRs. This article is also intended for custodians who are responsible for overseeing health information security, together with security consultants, auditors, vendors and third-party service providers.

2. Methods

2.1. Systematic review, protocol and registration

This article has used a systematic review to ensure that both the search and the retrieval process have been accurate and impartial. A systematic review is defined as a research technique that attempts to collect all empirical evidence in a particular field, to assess it critically and to obtain conclusions that summarise the research. The objective of an SLR is not only to collect all the empirical evidence of a research question but to support the development of guidelines which can then be used by professionals. This systematic review has followed the quality reporting guidelines set by the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) group [26]. A review protocol describing each step of the systematic review, including eligibility criteria, was therefore developed before beginning the search for literature and the data extraction. This protocol was reviewed and approved by one of the authors and is described in Section 2.4.

2.2. Eligibility criteria

The following inclusion criteria were used: articles published in English (IC1) and articles that deal with the privacy and security in EHR systems (IC2). Only articles written in English (IC1) were included since this language is favoured by the Scientific Community in the publication of research studies. Finally, IC2 was included to answer the research question.

2.3. Information sources

The search was applied to MEDLINE, ACM Digital Library, Wiley InterScience, IEEE Digital Library, ScienceDirect, MetaPress, ERIC, CINAHL and Trip Database, and was run between July 2012 and August 2012. We also scanned the reference lists included in articles in order to ensure that this review would be more comprehensive.

2.4. Study selection

The study selection was organised in the following four phases:

1. The search for publications from electronic databases related to health and computer science. This phase was performed by

using the following search string: (“electronic health record” AND (“privacy” OR “security”)), which was adapted to the databases’ search engines.
2. Exploration of title, abstract and key words of identified articles and selection based on eligibility criteria.
3. Complete or partial reading of articles that had not been eliminated in the previous phase to determine whether they should be included in the review, in accordance with the eligibility criteria.
4. Scanning the reference lists of articles to discover new studies which were then reviewed as indicated in phases 2 and 3, but these articles had to satisfy the inclusion criteria.

The activities defined in the aforementioned phases were carried out independently by three authors. Any discrepancies were resolved by a fourth member of the team. The study selection was developed in an iterative process of individual assessments until the interrater reliability was acceptable (0.92).

2.5. Data collection process

Data collection was carried out by using a data extraction form. Each potentially relevant article was assessed by one of the authors of the work presented herein, who read the full text, signifying that only one reviewer extracted data while another checked it. Any disagreements were resolved through a discussion between the two authors who had reviewed the study.

2.6. Data items

The ISO 27799 [25] is a standard which has been specifically tailored to healthcare and which defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002. This standard addresses the information security management needs of the health sector. Implementing this guidance allows healthcare organisations to reduce the number and severity of their security incidents and to ensure a minimum level of confidentiality, integrity and availability of personal health information. This standard provides clear, concise and healthcare-specific guidance on the selection and implementation of security controls for the protection of health information, and is adaptable to the wide range of sizes, locations, and service delivery models found in healthcare. The ISO 27799 considers 11 security areas containing a total of 39 main security categories. Each category contains a description of one or more security controls.

We designed a template based on the requirements defined in the ISO 27799 standard containing the characteristics to be analysed in each article. These characteristics are related to five of the eleven original security areas of the standard. The justification for considering these characteristics is as follows: On the one hand, the protection of patients’ privacy can be achieved with two different techniques, anonymisation and encryption [27]. On the other hand, with regard to the key security goals (CIA), access control policy, user access management and monitoring can significantly help to ensure the confidentiality and integrity of personal health information [25]. We have additionally considered compliance with legal requirements owing to the importance of the applicable legislation and standards when dealing with sensitive data [28], such as medical records. Finally, education, training and awareness were selected because they are the greatest non-technical measures available for the purpose of security [29]. Other important ISO 27799 security areas such as information security policy, organising information security, asset management, physical and environmental security, information security incident management and information security aspects of business continuity management, are outside the scope of this work.

Table 1 shows the areas and the security controls identified from the ISO 27799 (prefix 7 refers to Chapter 7 of the standard, in which these concepts are detailed), along with the questions formulated to consider each security control. Security controls define what is required in terms of information security in healthcare but not how these requirements are to be met. Our review attempts to understand this second issue.

3. Results

3.1. Study selection

A total of 49 articles were selected in the review. The search of databases provided a total of 775 studies, although four were discarded because they were not written in English (IC1). The title, abstract and keywords of the remaining 771 articles were examined and 657 of these were discarded because they did not meet the criterion of IC2. The full text of the remaining 114 studies was examined in greater detail. 70 articles were discarded because they did not meet the criterion of IC2, and a total of 44 articles were therefore included in the review. Another five articles were also included after

Table 1
Association between security and privacy categories identified in the ISO 27799 and research questions.

Area	Security control	Questions
7.12. Compliance	7.12.3 Compliance with security policies and standards and technical compliance	What standards and regulations do EHRs satisfy?
	7.12.2.2. Data protection and privacy of personal information	Do EHRs use pseudo anonymity techniques?
7.9. Information systems acquisition, development, maintenance	7.9.3.1. Policy on the use of cryptographic and key management	Are the users’ data encrypted?
7.8. Access Control	7.8.1.2 Access control policy	What authentication systems are used?
	7.8.2.1 User registration	What access control models are deployed?
	7.8.2.2 Privilege management	Can access policies be overridden in the case of an emergency?
	7.8.2.3 User password management	If the system needs user roles, who defines them? Who grants access to the data?
	7.8.5.1 Information access restriction	
7.7. Communications and operations management	7.7.8.1 Health information exchange policies and procedures and exchange agreements	What kind of information is exchanged?
	7.7.10.2 Audit logging	Are there audit logs?
7.5. Human resources security	7.5.2.2. Information security awareness, education and training of employees	Are the EHR users trained in security and privacy issues?

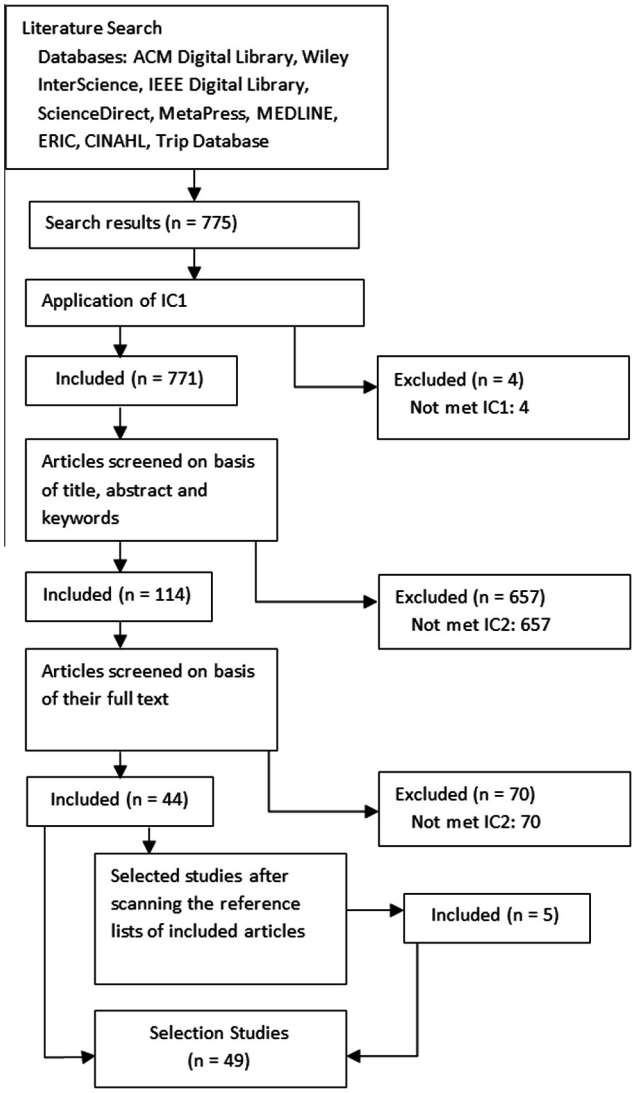

Fig. 1. PRISMA flow diagram.

scanning the reference lists of these articles. Fig. 1 shows a PRISMA flow diagram in which this process is summarised.

3.2. Study characteristics

In this section we describe the most important features of the studies included in the review. Table 2 in Appendix A provides a summary of the privacy and security characteristics related to applied standards and regulations, whether users' data is encrypted, pseudo anonymity techniques and system audit-logs. Table 3 in Appendix A shows the characteristics related to authentication, the access control models deployed, who manages EHR access, what occurs in the case of an emergency, the training of EHR system users and information exchange techniques.

3.2.1. Compliance

What standards and regulations do EHRs satisfy?

In total, 26 of the articles reviewed used standards or regulations concerning privacy or security to design their EHR systems. Of these, 17 studies use the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [8,9,27,30–43], and this is therefore the regulation which is most frequently used. The HIPAA defines the privacy rules of USA health informatics. The studies reviewed also included the EU Data Protection Directive 95/46/EC. This directive, which is employed in four articles [9,33,34,44], regulates the protection of individuals with regard to the processing of personal data and the free movement of this data. It is applied to personal data privacy in general, and is therefore applied to EHR data.

Other standards and regulations also appeared: the Role Based Access Control Standard of the "American National Standard for Information Technology" [45], The National Institute of Standards and Technology (NIST) RBAC reference model [46], the ISO TS 22600 "Health informatics – Privilege management and access control" [47], the ASTM E1986–98 "Standard Guide for Information Access Privileges to Health Information" [47], the ISO DTS 21298 "Health Informatics: roles of persons" [47], the "Recommendations for the Interpretation and Application of the Personal Information Protection and Electronic Documents Act" [35], the Recommendation R (75) in Europe "On the Protection of Medical Data" [36], the ENV 13729:2000 (Health informatics. Secure user identification. Strong authentication microprocessor cards) [48], and the Privacy Code in New Zealand [36].

Do EHRs use pseudo anonymity techniques?

Only 13 articles [27,34,37,49–58] present the pseudo anonymity technique, which allows third parties to access patients' health data without disclosing patients' personal data (for example, an identifier is shown rather than patients' personal data). Of these, eight studies [37,49,51–56] propose collecting all of a patient's EHR data with a patient identifier hash. This identifier hash is a token which is derived from applying a hash function to the patient's identifier. A hash function ensures that it is difficult to compute the patient's identifier from the token when this is on the Net.

Elger et al. [34] use an approach for reversible pseudonym generation. The standard symmetric encryption algorithm AES (Advanced Encryption Standard) was used to generate the pseudonym. Integrity protection is also incorporated into the pseudonym in order to have proof that the pseudonym is unaltered before reverting it. To support future inter-clinic patients, a dual-pass pseudonymisation scheme was developed, signifying that a patient's identity will result in the same pseudonym, regardless of which participating study centre collects that patient's data.

Quantin et al. [49] use a robust cryptographic hash function to anonymise information related to the patient's identity. A reversible pseudonym generation method is used. The authors propose a list of pseudonymous partial identifiers for each patient. The risk of collision is solved by giving a linkage probability level (high, medium or low) to each record. This level is obtained from the probabilistic modelling performed on observed data.

Riedl et al. [54–56] propose the possibility of sharing pseudonyms based on the threshold scheme of Shamir [59], and provide a mechanism with which to recover lost or destroyed keys. Alhaqbani and Fidge [58] define a pseudonym tree for each patient. Each patient can therefore have a different pseudonym in each health provider.

3.2.2. Information systems acquisition, development, maintenance

Are the users' data encrypted?

A total of 36 articles [5,8,9,27,30–38,41,44,47,49–56,60–71] report that systems must encrypt EHR data in order to increase security. In addition to data, identifiers (pseudonyms), keys and data attributes (metadata) are also encrypted [27,34,50–56,63–67,70]. Eight articles [5,27,31,35,36,49,56,57] use both symmetric key and public key schemes to store encrypted data, seven articles

Table 2
Number of selected studies, by source of publisher.

Source	Selected studies	Quality JCR 2011
International Journal of Medical Informatics	13	Q1
Journal of Biomedical Informatics	3	Q2
Journal of Medical Systems	3	Q3
Computer Methods and Programs in Biomedicine	2	Q1
Computers & Security	2	Q3
IEEE Transactions on Parallel and Distributed Systems	1	Q1
Computer Standards & Interfaces	1	Q2
Methods of Information in Medicine	1	Q2
Electronic Notes in Theoretical Computer Science	1	Q3
		Quality SJR 2011
IT Professional	1	Q2
German Medical Science	1	Q2
Studies in Health Technology and Informatics	1	Q2
International Journal of Bio-Medical Computing	1	–
		Quality CORE
IEEE International Conference on Availability, Reliability and Security	2	B
ACM workshop on Cloud Computing Security	2	–
International e-Health Networking, Application and Services Conference	2	C
Annual Hawaii Int. Conf. System Sciences	1	A
International Digital Information Management Conference	1	–
Annual Computer Security Applications Conference	1	A
Digital Rights Management Workshop	1	C
International Congress Series	1	–
ACM International Health Informatics Symposium	1	C
IEEE International World of Wireless Mobile and Multimedia Networks (WoWMoM) Symposium	1	–
IEEE International Cloud Computing (CLOUD) Conference	1	B
IEEE Consumer Communications and Networking Conference	1	B
Pacific Rim Int. Symposium on Dependable Computing	1	B
World Congress Privacy, Security, Trust and the Management of e-Business	1	C
AMIA Symposium	1	–

store [37,38,64–67,71] only public key schemes, and eight articles [34,51–55,62,69] store only symmetric key schemes, while three of the latter [34,62,69] use the AES, a symmetric-key algorithm adopted by the US government in 2001. Encryption keys are encrypted and stored along with encrypted EHR [69] or are stored in a separate database [27].

Communications are securely encrypted, and the server's authentication, using a mutually trusted certification authority, is achieved via SSL (Secure Sockets Layer) [5,8,31,35,37,41,51–53,63,65,66], via TSL (Transport Layer Security) [37,54,56,69], or via other secure protocols [9].

Three studies [9,35,37] tackle encryption in the Cloud. Haas et al. [9] and Zhang and Liu [37] consider that patients should not trust that the Cloud provider cannot access their EHR data, particularly when the Cloud provider is unrelated to patient or health institutions. Narayan et al. [35] propose the use of ciphertext-policy attribute-based encryption (cp-ABE) [72] to ensure that the Cloud provider cannot see (or copy) EHR data.

3.2.3. Access control

What authentication systems are used?

Eleven studies [31,38,49,58,64–66,69–71,73] propose the use of a digital signature scheme based on PKI. Jafari et al. [71] use DRM (Digital Rights Management) to control access to EHRs by licenses. Two certificates are employed: a security processor certificate that contains a key-pair which is used for the cryptographic authentication of the machine and is bound to its unique hardware features, and a separate certificate called a rights management account certificate which contains a key-pair used for the authentication of the user and is bound to the user's unique identifier and email address. Other access mechanisms presented in the studies are: username/password [5,27,32,35,50,62,74], login/password combined with a digital certificate [27,62,63,67,68], password and PIN [51–53], a smart card and its PIN [32,54–56,67,75], a smart card, its PIN and a fingerprint [36] and access policy spaces [40]. Daglish and Archer [61] use a username and a key by employing one of the following methods: (1) physical location as part of authentication; (2) the use of the Web and a security certificate of a trusted organization. Hu et al. [31] propose a PKI based authentication protocol, but a biometric authentication system can also be embedded for stronger security.

Authentication in distributed EHR systems has been also considered. Sun [38] proposes cross-domain authentication based on hierarchical identity-based public key infrastructure (HIB-PKI) to take advantage of the benefits of identity-based PKI in entities from the two domains. HIB-PKI avoids certificate-based PKI induced costs such as revocation, storage, distribution, and certificate verification [76]. van der Linden et al. [47] propose two means of authenticating external access in inter-organisational EHR systems: (1) user identification credentials are registered in the system, thus implying a separate procedure to register the credentials; (2) the system relies on credentials that are issued by systems from a different organisation. Choe and Yoo [60] have designed a multi-agent architecture which permits access to authorised users and the safe exchange of patients' data based on Web services.

Zhang and Liu [37] advocate the use of anonymous digital credentials in healthcare Clouds. The authors use a signature scheme, called a group signature, to allow a member of a group to anonymously sign an EHR.

Table 3
Summary of SLR studies assessing applied standards and regulations, whether users' data is encrypted, pseudo anonymity techniques and system audit-logs.

Authors	Year	Standards and regulations	Users' data encrypted	Pseudo anonymity techniques	Audit-log
Win et al. [32]	2006	HIPAA	A 128-bit strong encryption is used to make interpretation and interference of information extremely difficult	Not indicated	Yes
Rostad and Edsberg [77]	2006	Not indicated	Not indicated	Not indicated	Yes, audit-log is performed in order to define better access policies
Lovis et al. [75]	2007	Not indicated	Not indicated	Not indicated	Not indicated
Agrawal and Johnson [33]	2007	European Union Directive on Data Protection of 1995 and HIPAA	Commutative encryption	De-identification of personal health data using an optimal method of k-anonymisation	Not indicated
Falcão-Reis et al. [44]	2008	EuroSOCAP, European Directive 95/46/EC (personal data protection) and the Guidelines of OECD (privacy protection)	Encryption of data	Not indicated	Yes, auditing who accesses EHR and with what aim
Röstad [45]	2008	Role Based Access Control Standard of "American National Standard for Information Technology"	Not indicated	Not indicated	Yes, accessible and understandable by patients
Kahn and Sheshadri [30]	2008	HIPAA, "Standard Specification for Continuity of Care Record (CCR)" of ASTM	Encryption of data	Not indicated	Not indicated
Choe and Yoo [60]	2008	Not indicated	Architecture that uses XML for user authentication, data trustworthiness and selective encryption of patient's data. The user authentication is based on public key infrastructure (PKI) and a certificate. For encryption, the Rivest, Shamir, and Adleman(RSA) algorithm is used to protect the session key during session initiation between the client and the CAC, and the triple data encryption standard (3-DES) algorithm is used for selective data encryption	Not indicated	Not indicated
Daglish and Archer [61]	2009	Not indicated	Encryption of data	Not indicated	Not indicated
Benaloh et al. [5]	2009	Authors detect the lack of interoperability standards	The EHR system encrypts health records. The authors propose a design for secure and private storage of patients' EHR data. Hierarchical encryption system and partitioned record in which patient distributes keys for decryption of each part. Communications are securely encrypted via SSL. Both symmetric key and public key schemes are used to store encrypted data	Not indicated	Not indicated
Farzandipour et al. [8]	2009	HIPAA	Encryption of data and communications	Not indicated	Not indicated
Hu et al. [31]	2009	HIPAA	Encryption for health-data confidentiality during storage and transmission. Hybrid public key infrastructure (HPKI) solution in order to satisfy HIPAA rules. Both symmetric key and public key schemes are used to store encrypted data	Not indicated	Yes
van der Linden et al. [47]	2009	CEN/TC215 13606, ISO TS 22600, ASTM E1986–98 and ISO DTS 21298	Data encryption with the patient's key	Not indicated	Not indicated
Elger et al. [34]	2010	Data Protection Directive 95/46/EC and HIPAA	Authors use the symmetric encryption standard of AES algorithm and pseudonym generation systems dual-pass in their project, @neurIST. They indicate that a hybrid security model is the basis of a combination of local and distributed models because each health institution has a security	Authors deal with pseudo anonymity method and a classification of pseudonym generation systems, depending on whether or not they are reversible and the number of steps required to generate a pseudonym	Not indicated

Table 3 (*continued*)

Authors	Year	Standards and regulations	Users' data encrypted	Pseudo anonymity techniques	Audit-log
			system, an access right management and privacy protection policies according to user role. Authors argue some vulnerabilities of @neurIST project related to security assessment		
Narayan et al. [35]	2010	HIPAA, "Recommendations for the Interpretation and Application of the Personal Information Protection and Electronic Documents Act"	EHR data are stored in Cloud. EHR data and metadata are encrypted using attribute-based encryption (ABE) scheme that uses public and private keys. These keys are managed by Trusted Authority (TA) which can access all encrypted EHRs. The safe keyword search is permitted by an encrypted scheme, PEKS. The data is encrypted using efficient symmetric key cryptography, and the attribute-based encryption is used to make the symmetric keys accessible to authorised users. The private key is communicated to the users via a secure link such as SSL thereby preventing eavesdropper from learning anything about the key	Not indicated	Not indicated
Hembroff and Muftic [36]	2010	HIPAA, the Recommendation R (75) in Europe and the Privacy Code in New Zealand	Authors design an EHR system in which patient's EHR data are encrypted and stored on health smart card. A 256 bit key length AES cipher is used to encrypt software on the SAMSON card and AES cipher used within hardware components of smart card. The PIV applet, which supports RSA encryption using public keys, RSA signing using user's private key, and RSA key generation, creates three pairs of RSA keys in the card	Not indicated	Yes, system audits each reading, update or deletion on each card and who performs them
Zhang and Liu [37]	2010	HIPAA	Authors describe a security model for healthcare application Clouds. They consider that it is necessary to verify authenticity and trustworthiness for each EHR, maintaining them encrypted and using EHR owner's public key. The EHR owner is the health professional that created it	Each EHR is linked to an identifier the patient has in order to maintain his/her anonymity. A hash table is used. To provide authenticity, integrity and non-repudiation, authors use an anonymous signature scheme, called group signature, threshold signature and a digital credential scheme	Yes, person who accesses EHR is audited
Sun and Fang [38]	2010	HIPAA	Patients' health data are encrypted using the PEKS scheme. The delegatee's access right is restricted to only those data that are actively and effectively required	Not indicated	Yes, the delegator, delegatee, policy servers and storage servers need to maintain an audit trail recording interaction histories
Faresi et al. [39]	2010	HIPAA	Not indicated	Not indicated	Yes, authors perform an audit-log to comply with HIPAA
Ardagna et al. [40]	2010	HIPAA	Not indicated	Not indicated	Yes, every access granted must be recorded to prevent or discover possible abuses later. This process allows the supervisor to analyse access requests to identify common practice that should be explicitly permitted or denied by defining appropriate policies
Jafari et al. [71]	2010	Not indicated	The cryptographic key with which the content is encrypted. This key is in turn encrypted with the recipient's public-key so that it can only be used by the particular user	Not indicated	Not indicated
Haas et al. [9]	2011	HIPAA, IMIA Code of Ethics for Health Information Professionals and European data protection	EHR data are transmitted through secure connections when the receiver authenticates them and	Not indicated	Yes, authors propose to audit access to health data and its disclosure to third parties

(*continued on next page*)

Table 3 (*continued*)

Authors	Year	Standards and regulations	Users' data encrypted	Pseudo anonymity techniques	Audit-log
		directive 95/46/EC	are stored encrypted		
Quantin et al. [49]	2011	Not indicated	All communications are encrypted. Asymmetric encryption algorithm To ensure transmission security, confidential medical information such as the hashed patient identity H(PI) and the patient's medical record are asymmetrically encrypted with the medical practitioner public key	Patient's anonymity is maintained throughout all communications. Each EHR in a hospital is associated with a patient's ID hash, H(ID), to maintain his/her anonymity. Each health care institution must sign its EHRs to verify their authenticity and integrity	Not indicated
Horvath et al. [41]	2011	All developers were trained in HIPAA regulations regarding patient privacy	All data transfers are subject to encryption via SSL certificates	Not indicated	All data created in the course of a query are stored electronically on servers belonging to the DUHS, and all login activities in addition to the SQL executed are logged in perpetual audit trails
Jian et al. [62]	2011	Not indicated	The PHR data is kept secure by encrypting the zip files using a 256 bit symmetric Advanced Encryption Standard key	Not indicated	Not indicated
Dekker and Etalle [42]	2007	The HIPAA act stresses that patients have the right to justifications of past disclosures of their medical records	Not indicated	Not indicated	Audit Logic, an a posteriori access control framework, is used in an EHR setting. Once an action is executed, its occurrence is safely stored in an audit trail along with time-stamping of actions
Lemaire et al. [63]	2006	Not indicated	128-bit SSL encryption was used for all data transmissions. Encrypted passwords were used for all users	Not indicated	Service provider access to the system was logged and timestamped. These logs included information on when a user viewed and edited client records and program information
Peleg et al. [43]	2008	Legislation concerning healthcare privacy preservation (US Privacy Rule), which resulted primarily from the requirements of the1996 (HIPAA)	Not indicated	Not indicated	Not indicated
Bos [64]	1996	Digital Signature Guidelines of the American Bar Association (ABA)	RSA, is an algorithm for public-key cryptography	Not indicated	Not indicated
Bakker [80]	2004	Not indicated	Not indicated	Not indicated	In situations of medical audit, law suits, quality control and self-assessment it may be necessary to be able to replay the EHR output as it was or would have been at a certain moment in the past
Jin et al. [79]	2011	Not indicated	Not indicated	Not indicated	Not indicated
Tsiknakis et al. [78]	2004	The National Institute of Standards and Technology (NIST) RBAC reference model	Not indicated	Not indicated	Audit control is necessary
Sucurovic [65,66]	2007, 2010	MEDIS to meet the requirements of CEN ENV 13606 and CEN ENV 13729 standards	TripleDES, SSL and WSS4 J (for client–server communication), digital signature (RSA). The MEDIS project implements Web service security between the clinical and central server and SSL between the central server and a client	Not indicated	Not indicated
Kalra et al. [50]	2005	Security – policies and technical measures for the supervision and maintenance of the pseudonymous EHR repository as if it contained identified patient records, in conformance with NHS and international standards including privacy enhancing techniques and methods to reduce the risk of re-	Security of data transmissions	Pseudonymisation and, depersonalization	Reliable identification and traceability

Table 3 (*continued*)

Authors	Year	Standards and regulations	Users' data encrypted	Pseudo anonymity techniques	Audit-log
		identification			
Ueckert et al. [51–53]	2002, 2003, 2004	Not indicated	SSL-encryption is applied in the kind of storage and transport of data. All data in the two databases are encrypted with symmetric keys	User authorisation table. Only the version encoded by a one-way hash function is stored. Akteonline has been split into two different logical databases: The first database contains patient identification and demographic data (name, address, etc.) and links it to an internally generated patient ID, but no sensitive clinical information. The second contains the actual clinical information, indexed by the patient's ID but without any personal data	All of the data updates (user and date) are logged
Huang et al. [57]	2009	Following HIPAA guidelines, the method is designed to protect, recover and verify patients' identifiers in portable EHRs	A smartcard to input the key for the encryption and decryption work. Both symmetrical and asymmetrical algorithms are used	De-identification and pseudonymity. The recovery process includes re-identification and verification	Not indicated
Neubauer and Heurix [27]	2011	Not indicated	The client-side cryptographic operations required for the challenge/response style authentication procedure are carried out with a user-owned secured (contact) micro controller smart card acting as secure keystore for the authentication credentials and as trusted client-side cryptographic module. Both symmetric key and public key schemes are used to store encrypted data	Shared pseudonyms are shared between the data owner and the authorised person and are encrypted with both their inner symmetric keys so that both are able to decrypt this authorisation relation	Not indicated
Reni et al. [74]	2004	De facto standards	Not indicated	Not indicated	An audit trail of all accesses to any clinical record is kept by marking the name of the person accessing the record in addition to the date and time, regardless of whether any information is altered
Ruotsalainen [73]	2004	Not indicated	Not indicated	Not indicated	Audit of defined services (PKI, TTP) is performed
France et al. [67]	2007	Not indicated	Encrypted data and passwords. An asymmetric cryptographic system is used	Not indicated	Needed to control emergency situations
Al-zharani et al. [68]	2006	Not indicated	Encrypted data	Not indicated	Not indicated
Yu and		Chekhanovskiy [69]	2006	Not indicated	Encrypted data with AES (Advanced Encryption Standard). Secure communication protocol using TLS
Not indicated	Not	indicated			
Riedl et al. [54–56]	2008, 2007	Not indicated	Data, identifiers (pseudonyms), keys and data attributes (metadata) are encrypted. Secure communication protocol using TLS. Both symmetric key and public key schemes are used to store encrypted data	Pseudonymisation. A hash-algorithm to compute a unique identifier for the patient is used	Not indicated
Bouwman [70]	2008	Not indicated	Encrypted data	Not indicated	Audit logs is included
Alhaqbani and Fidge [58]	2008	Not indicated	Not indicated	A pseudonym tree for each patient is defined. Each patient can have a different pseudonym in each health provider	Accesses are audited

What access control models are deployed?

A total of 35 articles use access control models, of which 27 refer to RBAC [27,30,33,34,36–39,41,44,45,47,54–56,60,61,63,65,66,69–71,74,75,77,78] which is, therefore, the access control model par excellence. Each of the users who access the system thus has a role which defines his permissions and restrictions. One article [43] presents a superset of RBAC named SitBAC model which defines scenarios in which a patient's data access is permitted or denied. This is the outcome of analysing the 129 scenarios that the authors had elicited via qualitative research. The main concept underlying this model is the Situation Schema, which is a pattern consisting of the entities along with their properties and relations.

Ardagna et al. [40] introduce an access control system that regulates access to medical data based on policies that are modelled as a set of authorisations stating who can or cannot execute which action on which resource. Policies can be further combined to define complex policies regulating access to resources. Their proposal is

aimed at limiting accesses that break the glass, by classifying (a subset of) these access requests as abuses or planned exceptions and by defining specific policies regulating them.

Jin et al. [79] present a unified access control scheme that supports the patient-centric selective sharing of virtual composite EHRs using different levels of granularity, accommodating data aggregation and privacy protection requirements.

Can access policies be overridden in the case of an emergency?

Sixteen of the articles included in our review [9,27,31,36,40,43,44,51–53,58,67,70,74,77,79] indicate that in the case of an emergency, when the patient's life is at risk, it is necessary to override defined access policies. Two articles [67,74] indicate that a security committee must verify access properness to ensure that the confidentiality of the personal health data in the health system is being respected.

Hembroff and Muftic [36] propose two methods to ensure the patient's safety and security in the case of an emergency. The first method was created to have a read access open to anyone who is in possession of a card. Medical information for emergencies (emergency contacts, allergies, medications, and existing conditions) can be obtained using this method. The second method is used when a patient cannot provide her PIN, for example, when the patient is disoriented or unconscious. In these cases, fingerprint-only authentication protocol along with another security smart card issued to medical personnel that have proper emergency authorisation credentials to access patients' medical data must be used.

Ardagna et al. [40] propose the definition of four different policy spaces: authorised accesses, denied accesses, planned exceptions and unplanned exceptions. The planned exceptions space allows the definition of policies which are used to regulate emergency requests that include all the accesses that are necessary to preserve patients' health, and are inherently different from normal routine.

Rostad and Edsberg [77] analyse an installation of DocuLive EPR, a product of Siemens Medical Solutions. In this system, which is used by many of the largest hospitals in Norway, there is an extensive use of exception-based access control. Emergency access is assigned to users as roles, and not all documents in the EHR are accessible through emergency access. Since there are no predefined reasons for using emergency access, the user always has to manually provide a reason. The time interval in which the document remains accessible after using emergency access is established beforehand.

Peleg et al. [43] presents an emergency authentication process in two levels: (1) the system verifies the authenticity of the emergency situation; (2) it authenticates a person (responder) for each activity in the mitigation process, such that the person can assume the default situation role for the emergency based on his credentials.

If the system needs user roles, who defines them?

Eleven articles deal with who must define the roles, i.e., patients or health organisations, and what roles are created in an EHR system [30,37,38,41,44,45,47,60,61,71,75]. Of these, eight studies propose that roles should be previously defined by institutions, hospitals or some institutional committee [30,37,38,41,47,60,61,75], although five articles [44,45,47,61,75] propose that the patient should be able to include refinements or restrictions in order to customize the roles. Røstad [45] affirms that a complete history in both user-defined and system-defined roles should be maintained to ensure that the user can perform auditing and examine who had what permission to access her information at any given time. Røstad presents an access control model for Indivo in which a role assignment is labelled with a start time and an end time. Jafari et al. [71] suggest that the leader of the project should establish the roles of researcher or assistant in a health research facility.

Who grants the access to the data?

A total of 33 studies deal with EHR data access [5,9,27,31,33–40,44,45,47,51–56,58,60–62,67,69–71,74,75,78,79]. Of these, 25 articles indicate that the patient should grant access permissions [5,9,27,31,33–36,39,40,44,45,51–56,60,62,69–71,78,79].

Three articles [37,38,75] indicate that access is granted by authorised health professionals. Narayan et al. [35] propose that health professionals should be able to delegate access to other health professionals if they have previously obtained the patient's authorisation, and Faresi et al. [39] indicate that there should be data guardians (i.e., doctors, nurses) who are responsible for the micromanaging of data, deciding whether the patient's preferences can be applied on the basis of the HIPAA.

In one study [61] patients and administrative staff define what kind of data are available to what kind of user, and another describes two approaches [47]: implicit consent, which signifies that the patient consents to predefined rules unless otherwise indicated, and explicit consent, which signifies that the patient forbids access unless he grants it. In two articles [58,74] patients and health providers grant access to health information, whereas in one article [67] only health providers grant access to health information.

3.2.4. Communications and operations management

What kind of information is exchanged?

A total of 16 studies [36–38,49,51–56,58,60,64,67,71,73] show that health data are exchanged between organisations, one of these by using the Cloud [37]. Pseudonyms [54–56] and even policies [58] can also be interchanged by using a script language. Choe and Yoo [60] propose a multi-agent architecture based on Web services to access the authoritative data and to exchange patients' data safely.

van der Linden et al. [47] identify and analyse the privacy and security related to problems that occur when health data are exchanged between health organisations. According to these authors, a standardisation of security measures that goes beyond organisational boundaries is required, such as global definitions of professional roles, global standards for patient consent and semantic interoperable audit logs.

Sun and Fhan [38] have designed an EHR system that allows data sharing between health institutions whilst protecting patient privacy. Their EHR system incorporates advanced mechanisms for fine-grained access control, and on-demand revocation, as enhancements to the basic access control provided by the delegation mechanism, and the basic revocation mechanism, respectively. Quantin et al. [49] have designed a search engine for a distributed database belonging to several health institutions. The EHR system can gather together the different parts of a patient's medical record that are located in different hospitals without any risk of breaching confidentiality. This system allows patient anonymity to be achieved in all communications.

Are there audit logs?

Twenty-five articles [9,31,32,36–42,44,45,50–53,58,63,67,70,73,74,77,78,80] believe that it is important to include audit logs. These logs included information on who [36,37,44] accesses EHR, with what aim [36,44], and the time-stamping of actions [42,51–53,63,74]. Two articles [44,45] claim that the audit logs should be accessible and understandable to the patient. Four articles [36,40,67,77] indicate that it is necessary to audit the access when access policies are overridden in the case of an emergency. In this case, the patient is notified in order to avoid malicious use. Audit trail is also used to comply with the HIPAA and existing laws

[39,80], to prevent or discover possible abuses later and misuse exception mechanisms [9,40,77], and to define better access policies [40,77].

Some authors [45] advocate that audit logs should be accessible and understandable by patients. Falcão-Reis et al. [44] argue that each patient should have the capacity to monitor her own audit data, and determine who has accessed her EHR, what information has been accessed, for how long and for what purpose. Patients should have information related to the creation of the record, specific instances of how the record is used, the process or processes by which the record is updated and eventually deleted. Haas et al. [9] propose auditing EHR accesses and all data flows in order to allow the patient to be able to verify whether privacy policies are being enforced. In the case of unwanted information flow, patients are able to identify the data source or leak. The SAMSON system [36] provides the patient with the ability to view audit logs which display names, roles, dates/times, and fields of data that have been read, written, or deleted. When a physician initiates a break-the-glass procedure in emergency circumstances, that physician's data (name, national provider identifier, name of health care organisation) is copied from the physician's card into the patient's medical card audit log. The architecture proposed by Faresi et al. [39] includes a component named audit logger which logs every request/response of patients' health data. Patients can access audit logs of their records saved in a repository.

Audit in distributed EHR systems is also tackled. Sun and Fang [38] propose maintaining an audit trail in order to record interaction histories (authentication, delegation, proxy signing, searchable public key encryption and retrieval, and revocation) between the EHR system and other entities. Zhang and Liu [37] propose maintaining a log of every access to and modification of data in their EHR security reference model for managing security issues in healthcare Clouds.

3.2.5. Human resources security

Are the EHR users trained in security and privacy issues?

Staff training in security and privacy rarely appears in the articles reviewed: four studies indicate that it is necessary [8,30,34,44]. Three of these propose that only health staff training is necessary [8,30,34], while Falcão-Reis et al. [44] point out that system user training is necessary for both health staff and patients. Patients should be provided with a general education in their privacy rights and duties, including clinical data privacy [44]. Farzandipour et al. [8] also propose that all third-party users of an organisation's information should be trained in security procedures. Specification and guidelines for handling patients' medical records should include the requirements of using content encryption and secure key management solutions [69]. Healthcare professionals must also receive affordable security guidance. Kahn and Sheshadri [30] consider that the best solution for security compliance in a digital ambulatory medical practice is to offer healthcare professionals educational tools with which to implement security policies and procedures.

3.2.6. Quality assessment

In order to assess the quality of the studies reviewed, we have considered where they were published (Table 4). In total, 31 of the studies reviewed were published in journals. A total of 27 articles were published in journals indexed in the Journal Citation Report (JCR) [81], 16 of which appeared in first quartile journals in 2011, 5 appeared in second quartile journals in 2011, and 6 appeared in third quartile journals in 2011. Three studies were published in second quartile journals indexed in the SCImago Journal Rank (SJR) [82] in 2011.

The remaining 18 articles were presented in conferences. According to the COmputing Research and Education (CORE) conference classification which appeared in 2010 [83], two articles were published in CORE A conferences, five in CORE B conferences and another five in CORE C conferences. Six articles were presented in conferences which are not indexed but were published by IEEE and ACM and are in other ranks of computer science conferences.

As is shown above, the quality of the review studies is high, since 88% of them appertain to top category journals and conferences.

4. Discussion

4.1. Summary of evidence

The main characteristics included in the studies reviewed are summarised and discussed below. These characteristics answer our research question:

Q1. What security and privacy features do current EHR systems have?

4.1.1. Compliance

What standards and regulations do EHRs satisfy?

About half of the studies reviewed in this article are based on standards or regulations, which shows that the application of standards and regulations is necessary in any EHR system that guarantees the privacy and security of patients' data. The most frequently referenced regulation is the HIPAA, which is used in the US. The HIPAA is a federal law which protects health information and ensures that patients have access to their own medical records, while giving new responsibilities to those in charge of protecting this information. Another very important standard in Europe is the CEN/ISO EN13606-Part IV, which includes privacy and security directives in Chapter Four. This is an incipient standard that was developed by the CEN in 2008, approved by the ISO and updated in 2010. Its objective is not to describe how EHR systems must be developed but rather to propose common rules for all in order to achieve interoperable EHR systems. Based on the findings of our study, we have noted that the use of CEN/ISO EN13606 and ISO 27799 is low. This can be explained by observing that these standards were published in 2008 and thus, from our point of view, not enough time has elapsed for it to have been widely adopted.

There are practical reasons for using standards, including expectations of efficiency, cost saving, and risk avoidance, since standards summarise the relevant aspects of security and privacy process clearly and concisely in a structured manner [84]. However, the lack of (1) a harmonised policy on trust, privacy and confidentiality and (2) common security standards are important barriers for secure inner-organisational and cross-organisational communication [73].

New challenges in privacy and security emerge when genetic/genomic data are collected for research purposes. Genetic/genomic data access should also be treated as sensitive information in the EHR [85]. The Personalized Health Care Workgroup of the American Health Information Community has provided materials that discuss confidentiality, privacy, and security issues related to genetic/ genomic test information in the EHR [86].

Do EHRs use pseudo anonymity techniques?

De-identification is the process of removing (or modifying) identifiers from the health personal data so that identification is not reasonably possible. This technique is used to prevent the mis-

Table 4
Summary of SLR assessing authentication, access control models deployed, access management, what occurs in the case of an emergency, the training of EHR system users and information exchange techniques.

Authors	Authentication	Access control models deployed	Access management	Case of an emergency	User training	Techniques of information exchange
Win et al. [32]	PIN, username/password, credentials	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
Rostad and Edsberg [77]	Not indicated	RBAC	Not indicated	Not indicated	Not indicated	Not indicated
Lovis et al. [75]	Use of a personal smartcard coupled with a personal identification number	RBAC	Access permissions are granted by health professionals. Roles are defined by an international committee but the patient is able to grant or forbid access to some health professionals in a future trans-institutional network	Not indicated	Not indicated	Not indicated
Agrawal and Johnson [33]	Not indicated	RBAC	The patient grants access permissions in accordance with health organisations' policies	Not indicated	Not indicated	Not indicated
Falcão-Reis et al. [44]	Not indicated	RBAC. Roles are hierarchical following three rules: assignment, authentication and authorisation	The patients grant permission to access their EHR	Health staff with a special role could bypass access policies in the case of an emergency	Yes, system users in general	Not indicated
Röstad [45]	Not indicated	RBAC. There are two kinds of roles: system roles (patient, provider and researcher) and user roles (defined by user)	The patients have the control over who accesses their data	Not indicated	Not indicated	Not indicated
Kahn and Sheshadri [30]	Not indicated	RBAC. Employees, administrative staff, health staff, IT staff. Roles are created by health care organisation. Individual and non-shared identification	Not indicated	Not indicated	Yes, the training of professionals is necessary	Not indicated
Choe and Yoo [60]	Digital certificate. Public key infrastructure (PKI) is used to issue and revoke public keys and public key certificates	RBAC. Roles are assigned based on security policies of each hospital	The patients grant permission to access parts of their EHR	Not indicated	Not indicated	A multi-agent architecture based on Web services is proposed to access the authoritative data and to exchange patients' data safely
Daglish and Archer [61]	Username and key using one of following methods: 1) physical location as part of authentication; 2) use of Web and security certificate of a trusted organisation	RBAC. Previously defined roles: researcher, patient, primary care, second care, emergencies and administration. The patient may define refinement rules for roles	Patients and administrative staff define what kind of data are available to what kind of user	Not indicated	Not indicated	Not indicated
Benaloh et al. [5]	Username and password	Not indicated	The patients share their EHR selectively and choose with whom to do so	Not indicated	Not indicated	Not indicated
Farzandipour et al. [8]	Not indicated	Not indicated	Not indicated	Not indicated	Yes, staff training	Not indicated
Hu et al. [31]	Not indicated	Not indicated	The patient grants access to health provider	Not indicated	Not indicated	Not indicated
van der Linden et al. [47]	Not indicated	RBAC. Creation is not indicated explicitly, but it seems that roles are defined by health organisation although the patient can include restrictions to specific users	There are two approaches: implicit consent where it is assumed that patients have consented unless otherwise indicated; and explicit consent where patients forbid access unless otherwise indicated	Not indicated	Not indicated	Not indicated
Elger et al. [34]	Authentication mechanism based on tokens	RBAC	The patient grants access permissions but exceptions exist	Not indicated	Yes, it is necessary	Not indicated
Narayan et al. [35]	Mutual authentication	Each user has a *username* used to define access policies that are managed by patient	The patient adds and revokes permissions. Health professionals can delegate access to other health	Not indicated	Not indicated	Not indicated

			professionals			
Hembroff and Muftic [36]	Health card PIN and patient's fingerprint	RBAC. The patients grant permission to access their data by entering PIN and allowing fingerprints to be read	Not indicated	Access is allowed in the case of an emergency by using PIN of health professional's health card and patient's fingerprint	Not indicated	Health data are exchanged between organisations because the patient takes the card to different health institutions
Zhang and Liu [37]	Anonymous digital credentials in healthcare Clouds	RBAC. Roles are not indicated explicitly but are related to the kind of health professional	Access permission is granted by authorised health professional, usually the creator of EHR	Not indicated	Not indicated	The data exchange is performed through secure connection (SSL, TSL or IPSec)
Sun and Fang [38]	Authors achieve data authenticity and integrity with the hierarchical ID-based signature (HIDS) and standard ID-based signature (IBS)	RBAC. Authors use an approach based on roles to access delegation and revocation and use proxy signature to achieve a fine-grained access control	Roles define the function of the kind of health professional that can access EHRs. A health professional delegates access to qualified professionals	Not indicated	Not indicated	Authors design a distributed EHR system that allows data to be shared to permit institutions to cooperate and to protect data privacy
Faresi et al. [39]	Not indicated	Modified RBAC based on purpose of access and HIPAA privacy regulations	Patients manage the access to their data. The data guardians (doctors, nurses) perform a micromanagement of data to decide whether patient's preferences are to be applied based on HIPAA regulations (when the decision cannot be automated)	Not indicated	Not indicated	Not indicated
Ardagna et al. [40]	Not indicated	RBAC. Access control using policy spaces	The patients should be able to access their health data and to manage access control by a proper notification mechanism, prior approval and explicit consent	To guarantee the Care Comes First (CCF) principle, it is necessary to provide a means to bypass the access control models in cases of emergency (“break the glass”)	Not indicated	Not indicated
Jafari et al. [71]	Not indicated	RBAC and licenses that indicate access permissions. Leader, researcher and assistant are the roles defined	Patients have to give their explicit consent for their data to be used in research by use of a list of keywords	Not indicated	Not indicated	Authors propose use of digital rights management (DRM) to share EHRs in research scenarios
Haas et al. [9]	Not indicated	Not indicated	Each patient declares privacy policies and checks that they are being complied	Access policies are bypassed in the case of emergencies	Not indicated	Not indicated
Quantin et al. [49]	Digital signature	Not indicated	Not indicated	Not indicated	Not indicated	Authors design a search engine for a distributed database between health care institutions
Horvath et al. [41]	DEDUCE authenticates using Microsoft Windows Server 2003 (Redmond, WA, USA) Active Directory accounts, as these are employees' primary means of accessing workstations and clinical applications	RBAC. When logging into the system, users must choose one of four user role types:	Roles are pre-established in the EHR system	Not indicated	Not indicated	Not indicated
Jian et al. [62]	The patients are given an initial password that allows them to access the files from the TMT-viewer. In addition to being password protected the zip file also contains a digital signature from the hospital and a checksum	Not indicated	Persons unauthorized by the patient are not able to view the data	Not indicated	Not indicated	Not indicated
Dekker and Etalle [42]	Authentication of users and objects. an authorisation request or an authentication credential corresponds to a logical formula and the authorisation or authentication decision corresponds to a proof of the formula	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
Lemaire et al.	Password and individual 128-bit	RBAC. The kind of access or roles:	Roles are pre-established in the	Not indicated	Not indicated	Not indicated

(*continued on next page*)

Table 4 (*continued*)

Authors	Authentication	Access control models deployed	Access management	Case of an emergency	User training	Techniques of information exchange
[63]	digital certificates were generated from Windows 2000 Server and installed in all service providers' computers. Certificate authentication was performed upon log-in	Access granted to Client Profile, Access granted to Client Profile data, No access to Client Profile data	EHR system			
Peleg et al. [43]	Not Indicated	Situation-Based Access Control (SitBAC) model	Based on situations which are dependent on the context (the same task to be performed by the same user can require different authorisations	Mentioned as a situation	Not indicated	Not indicated
Bos [64]	Digital signature in information exchange	Not indicated	Not indicated	Not indicated	Not indicated	The use of digital signature is performed in information exchange context between EHRs
Bakker [80]	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
Jin et al. [79]	Not indicated	Unified access control scheme that supports patient-centric selective sharing of virtual composite EHRs using different levels of granularity, accommodating data aggregation and privacy protection requirements	Unified access control scheme that supports patient-centric selective sharing of virtual composite EHRs using different levels of granularity, accommodating data aggregation and privacy protection requirements	In order to accommodate the emergency situations, a "break-of-glass" policy ("BG" policy for simplicity) can be specified to allow staff in emergency rooms to access the patient's medical information without the patient's explicit authorisations	Not indicated	Not indicated
Tsiknakis et al. [78]	Not indicated	RBAC	Patients can grant access to their EHRs	Not indicated	Not indicated	Not indicated
Sucurovic [65,66]	Digital signature, PKC (public key certificate), RSA. Open source API for X.509 authentication and authorisation	XML as the language for developing constrained hierarchical role based access control (RBAC) and, at the same time, has its focus on decomposing policy engines into components	Authorisation policy for hierarchy. It defines hierarchies of how, when, where, why and who attributes (hierarchy of roles, professions, regions, etc.)	Not indicated	Not indicated	Not indicated
Kalra et al. [50]	Login/password	Assignment of GRID access control levels	Not indicated	Not indicated	Not indicated	Not indicated
Ueckert et al. [51–53]	Password and PIN	Granular access control mechanisms	The user authorises persons or institutions to read and/or write data in his personal EHR	Read access to an "emergency subset" of patient's EHR can be enabled and defined	Not indicated	The European Union's (EU) 'Directive', Canada's response Personal Information Protection and Electronic Documents Act (PIPEDA), and more recently the final privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) in the USA which became enforceable on 14 April 2003
Huang et al. [57]	Authentication digital signature and login/password	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
Neubauer and Heurix [27]	Login/password	RBAC. Three roles are pre-established in the EHR system: the data owner, the affiliated, and the authorised person	The patient who is in full control of her health data in that she can create data access authorisations for specific health records (for authorised users) in addition to granting full access rights equivalent to root access (for affiliated users)	A private ticket toolkit is generated for each entry relying on an asymmetric keypair stored on an emergency card (e.g., a relative's card)	Not indicated	Not indicated
Reni et al. [74]	Login/password	RBAC	The Chief Medical Officer (CMO)	Emergency read-only access is	Not indicated	Not indicated

			defines the roles. Patient and CMO grant access to personal health information	always allowed. In the case of someone gaining emergency access, a warning message is issued to the CMO, who must then investigate to verify access properness		
Ruotsalainen [73]	PKI-services for authentication	Not indicated	To make it possible for external (dynamic) users to access any of the EHRs inside connected domains, the platform offers automatic security negotiation services.	Not indicated	Not indicated	Different health applications can run securely and exchange sensitive data by using PKI
France et al. [67]	Digital signature and electronic identification card,	Not indicated	Health providers grant access to health information	The patient record is open from 5 days before a planned admission to 15 days after discharge. There is a security committee to check that the confidentiality of the personal health data in the health system is being respected	Not indicated	Exchange of health information concerning identifiable patients by using digital signature
Al-zharani et al. [68]	Authentication digital signature and login/password	Access control module but type is not indicated	Not indicated	Not indicated	Not indicated	Not indicated
Yu and Chekhanovskiy [69]	Authentication digital signature and PKI	RBAC	Patients can grant access to their EHRs	Not indicated	Not indicated	Not indicated
Riedl et al. [54–56]	User authentication using a security token that contains the access keys (for example a smart card and PIN)	RBAC	Health provider defines the roles. Not indicated explicitly, but it seems that the patient grants access permissions	Not indicated	Not indicated	Exchange of pseudonyms
Bouwman [70]	Digital certificate	RBAC	Patients can grant access to their EHRs	A specific role is defined for emergencies	Not indicated	Not indicated
Alhaqbani, and Fidge [58]	Authentication digital signature and PKI	Not indicated	Patients and health providers grant access to health information	Emergency access policy defined between patient and health provider is used	Not indicated	Information exchange between health organisations. Data and policies are interchanged by using a script language

use of health data. For example, employers or insurance companies could use health information to refuse employment or health coverage.

Pseudonymisation [27] consists of transforming and then replacing personal data with a pseudonym that cannot be associated with the identification data without knowing a certain secret. Pseudonymisation therefore allows the data to be associated with a patient under specified and controlled circumstances, thus allowing both primary use of the records by health care providers and secondary use for clinical research.

Although the confidentiality of medical data can be improved through de-identification, de-identified data does not guarantee confidentiality [87]. Complete anonymisation of the extract of clinical records is unlikely to be feasible while the original clinical record exists [34]. The anonymity in EHR databases can be reversed through the disambiguation process [88]. Nevertheless, de-identification should be as complete as possible such that the extract in isolation from the original clinical record would be reasonably anonymised.

Important ethical and legal consequences are associated with de-identification when using data for the purposes of research. Depending on the kind of research network and its requirements, distinct procedures for pseudonymisation are appropriate [89]. The ''one-way single-pass'' pseudononymisation method places non-reversible codes on the data for research use, and yet still allows researchers to update the research record. However, there are cases in clinical research in which the research subject must be re-contacted, and reversible systems are therefore often preferred (e.g. reversible single-pass, reversible dual-pass). A rigorous review of strategies for the generation and reversal of pseudonyms can be found in [90].

Data that is reversibly coded is viewed as personal data in the majority of countries, and must therefore be protected. Independent Trusted Third Parties (TTPs) could apply a code to the data and hold the pseudonyms [91]. The European Medicines Agency (EMEA) suggests that the TTP could be ''an external entity, such as a governmental agency, legal counsel, or other qualified third party not involved with the research'' [92].

There is a growing body of literature investigating the risks of person re-identification through data mining and probabilistic techniques [93] and a similarly expanding set of algorithmic techniques have been proposed for the profiling and monitoring of serial queries and result sets to detect attempts to triangulate towards unique person characteristics [94,95]. A social engineering approach can also be used by an attacker to gain illegal access to the pseudononymisation algorithm or the patient list, thus compromising the system [96].

New methods are being investigated and developed that can further protect identifiable information. One innovative approach [97] aims to protect the data from being viewed by others while the user reads it. A hiding function allows identifiable information to be made invisible, thus preventing the disclosure of any personal and sensitive information while an EHR is being viewed. The pre-processing of common pattern matching, dictionary and predefined area searches to recognise identifiers in the free-form condition are used in the application of this method.

True anonymisation is challenging, and further work is needed in the areas of de-identification of datasets and protection of genetic information [98], and in those scenarios in which the EHR storage is in the Cloud in order to prevent the Cloud provider from being able to see patients' data.

4.1.2. Information systems acquisition, development, maintenance

Are the users' data encrypted?

A proper encryption scheme must be introduced in order to achieve confidentiality in an EHR system. Both symmetric key and public key schemes are equally used in the studies reviewed. In general, public key operations are slower than symmetric key primitives, and when searchability or hidden labels are required they appear to have inherent privacy weaknesses [5]. On the other hand, if the server itself holds the private key, then key symmetric schemes are also vulnerable, as the key might be stolen along with the encrypted data. Encryption keys can be also hosted on a separate physical server to prevent decryption of patient data if the data storage machine is ever compromised [61].

In most of the studies reviewed [27,38,41,51–57,67,69] the data is encrypted in the servers and the provider itself stores the encryption keys. Moreover, in order to guarantee data trustworthiness and authentication, the review articles advocate that the health staff who create or update the EHR should sign it digitally. However, some proposals [5,31,35] enable patients to generate and store encryption keys, and patients can therefore control the access to their PHI (Personal Health Information). In these EHR systems, each patient grants access to specific portions of his EHR data. Benaloh et al. [5] claim that if the server holds the decryption keys then it will be vulnerable to theft. They therefore propose that each patient generates her own decryption key, and uses that key to encrypt her records. Encryption schemes will guarantee that the patient's privacy is protected, assuming that the patient stores the key safely. Choe and Yoo [60] also propose the selective encryption of patient data to reduce the computational burden. The encryption is then applied only to those items selected by the patient.

A number of desired features for appropriate key management are proposed [37]: (1) the number of keys held by both patients and doctors should not be large; (2) the keys should be easy to store and consume low space complexity; (3) the updating of keys should be convenient and efficient in terms of time complexity; (4) none of the keys should contain any private information of any parties; (5) all the keys should be traced and revoked when they expire or when a user leaves the group.

When data volume is large (e.g. data image), asymmetric cryptography may be inefficient. This problem can be particularly severe if health records with imaging data are accessed through a low performance computing device, such as a portable digital assistant (PDA) [60]. A symmetric cryptography method is thus advised for the purpose of efficiency. This is the case of Hu et al. [31] who present a hybrid public key infrastructure solution (HPKI) to comply with the HIPAA regulations. They offer the option of using a cryptographically strong PKI scheme for sensitive yet computational non-intensive textual PHI data, while efficient symmetric cryptographic technology is deployed for the storage and transmission of resources demanding PHI image data. The HPKI proposal is contract oriented (a period of time) rather than session oriented. It should be noted that even with an efficient advanced encryption standard scheme and a powerful desktop PC, encryption and decryption of a very high volume of digital medical images within low performance computing devices is still challenging [31]. Promising results concerning encryption theory based on the features of medical images have been reported [99].

The most common communication protocol used to establish a secure connection is secure socket layers (SSLs). This method guaranties the secure low-cost end-to-end transmission of information over the potentially insecure internet [100]. Implementing a firewall and antivirus protection through security policies will further provide a more secure Internet connection [101].

4.1.3. Access control

What authentication systems are used?

Two kinds of authentication have been distinguished: user authentication and data authentication. User authentication can be defined as the way in which users prove their authenticity to the EHR. Username or identity (ID) with an associated password have been the most common user authentication mechanisms in EHRs [102,103]. The process used to ensure the origin of a data source is data authentication. Our findings reveal that the most frequent data authentication method in current EHR systems consists of a digital signature scheme.

It should be noted that when physicians [104], patients [5,61] or other authorised users are able to see or modify EHRs, a privacy and security problem could occur if the user's access data (password or other access mechanism) were to be stolen by unauthorized parties. Most EHR users believe that the password checking included in the system will ensure the system security of EHRs. However, only checking a password to ensure access restriction does not ensure adequate security for EHRs [87]. It has been noted that the use of passwords as authentication mechanisms is exposed to multiple types of attacks, such as "electronic monitoring" to listen to network traffic in order to capture information, or "unauthorized access to the password file". In particular, man-in-the-middle (MITM) attacks are often implemented with authenticating identity, although most cryptographic protocols include some form of endpoint authentication specifically to prevent these attacks [37]. Moreover, passwords can be copied, shared or cracked by using debuggers and disassemblers. Thus, in addition to the password, there should be some other mechanisms to enhance information security.

Logins/passwords have been superseded by other, more robust methods [105]. The HIPAA Security Guidance report advises using two-factor authentication. Designers should therefore incorporate another authentication system in order to provide strong authentication [106]. Two of the following three methods are recommended for inclusion in an identification system: "something a person knows" such as a login ID, email address, password, PIN; "something a person has" such as a key, swipe card, access card, digital certificate; or "something that identifies a person" such as biometrics (face and voice pattern identification, retinal pattern analysis, hand characteristics or automated fingerprint analysis based on pattern recognition). The insertion of an RFID (Radio Frequency IDentification) chip is an invasive identification mechanism, but it can be also used for securing health information.

A sufficiently secure solution to user authentication is a credential system in which only the user who holds a legitimate credential issued by a trusted authority can gain access to the health record [32]. The user who has obtained a credential can perform cryptographic operations, such as signing or decryption.

Authentication solutions based on smartcards combining a token and a PIN are also employed in the studies reviewed. They have a fundamental weakness: the presenter of the token cannot be authenticated. Tokens and PINs can be lost and stolen. Biometrics such as fingerprints can provide stronger authentication mechanisms [107]. However, the mobile biometrics template embedded in the smartcard also runs a high risk of being compromised once the smartcard is stolen or lost. Recent research indicates that the fingerprint minutiae can be used to recover fingerprints [108]. It is currently preferable to use a central matching scheme for the biometric authentication in e-health security systems owing to the fact that a physically secure organisational infrastructure can offer better computing resources.

Cross-organisation authentication can be addressed by means of HIB-PKI or the use of federated identity management such as the Liberty Alliance project [109]. Federation technologies provide secure methods for a service provider to identify users who are authenticated by an identity provider [110]. The Security Assertion Markup Language (SAML) is a federation standard approved by the Organisation for the Advancement of Structured Information Standards (OASIS) and backed by the Liberty Alliance's interoperability testing. SAML defines standardised mechanisms for the communication of security and identity information between business partners.

In order to enable information sharing among a network of healthcare organisations, research should define extensible trust hierarchies and authentication standards [33]. One solution consists of creating central registries that can be used to grant or revoke credentials for a specific professional based on his professional behaviour. However, legal procedures for updating and querying the status of the credentials should be created [47].

What access control models are deployed?

The findings of this review have shown that the majority of the EHRs analysed used the RBAC model, thus confirming previous studies [111–113]. In fact, RBAC is the most common access control model, and is considered to be particularly well-suited to health care systems [114]. An access control system designed to operate in the healthcare scenario should be flexible and extensible. It should not be limited to a particular model or language, should protect the privacy of the patients, and should not allow the exchange of identity data, in compliance with government legislation [40].

One of the main pros of RBAC is the flexibility it provides. Roles are assigned to users to allow them to interact with the system, thus determining what resource can be accessed by the user, and in what situations. In order to update the permissions of many users it is only necessary to change the role to which they are all assigned. An administrator is responsible for role creation. Certain models propose allowing the user some control over role assignment and delegation [115,116], but not over role creation or adaption.

In contrast, EHRs using RBAC are not well-suited to handling unplanned and dynamic events (e.g. doctors asking for second opinions from colleagues or unplanned patient arrivals) [77]. Most of these EHRs therefore have exception mechanisms in addition to the normal role-based access control to handle these situations. However, the use of exceptions leads to security threats and a need to perform regular auditing to ensure that the exceptions mechanism is not misused.

In order to mitigate the complexity of RBAC management it would be convenient for a healthcare worker with a specific role to have access to similar kinds of information in various systems. A universally applicable model of role definitions that is adopted by all health organisations may be an important step forward. The American ASTM E1986–98 standard [117] has defined an American list of roles. ISO DTS 21298 defines a similar set of structural and functional roles which are referred to in the International Labour Organisation [118]. However, these proposals do not provide definitions of each role and its policies.

RBAC has been implemented in many commercial systems [45], and an RBAC-standard has therefore been created to ensure that the main principles remain equal across different implementations [46,119]. Nevertheless, limitations, design flaws, and technical errors have been identified [120]. An alternative to RBAC is Attribute-Based Access Control (ABAC) [121]. This model for EHR offers context-aware authorisation in order to provide the capability to define different policies for different contexts which can be distinguished by contextual data or environmental attributes. ABAC improves the efficiency of search and scalability of policy with regard to RBAC [37]. RBAC has been further extended to a contextual-RBAC and Situation-Based Access Control (SBAC) [43,122].

Can access policies be overridden in the case of an emergency?

Access policies are bypassed in the case of emergencies, when the patient's life is at risk. This is bindingly ruled by the EU Directive 95/46/EC and by the fourth part of the EN 13606 standard which defines emergency procedures with which to override access restrictions [10]. There are undoubtedly some situations in which the bypassing of access policies is justified. For example, EHR systems should be flexible enough to allow for the emergency treatment of minors, in which the parent or legal guardian may be absent, and the usual procedures for consent must therefore change [123].

In emergency situations, policies that apply in normal circumstances can be overridden. Special roles in the EHR access control model are sometimes defined to deal with emergency cases [44]. All these overriding roles must be widely audited and their actions fully justified. However, there are some accesses that should always be prevented [40]. They cannot help in managing such emergency situations and represent abuses that should never be permitted. It should be noted that exception mechanisms increase the threats to patient privacy, and their use should therefore be limited and subject to auditing [77]. Performing an audit-log is extremely important, and it is crucial that the system user checks whether privacy and access policies are being enforced [124].

If the system needs user roles, who defines them?

It is often the case that users' very specific tasks cannot be modelled by generic roles or policies [47]. Adherence to the RBAC model will result in a large number of roles unless an organisational policy to conform to generic roles is defined and rigorously implemented. Several authors [44,45,47,61,75] therefore advocate that roles can be defined or refined by the patient. However, care should be taken that the result does not interfere with good clinical practices, and consensus on the definition of roles and profiles across organisations should be reached in distributed EHRs systems.

Who grants the access to the data?

With regard to the principles, guidelines and recommendations compiled by the OECD (Organisation for Economic Co-operation and Development) protection of privacy and trans-border flow of personal data within health information system development, the patients are the owners of their health records, and should thus have the ability to monitor and control which entities have access to their personal EHRs [44]. While a patient might wish to share her entire record with her doctor, she might not wish to allow pharmacists, billing staff or lab technicians to see any more information than is necessary. This issue is addressed in several studies [5,35] that present a system in which a patient can grant access to specific portions of his health data, using a system based on a hierarchical encryption system [5] or attribute-based cryptography [35]. Other works [71] go one step further, and allow patients to determine the time conditions under which the rights are granted. Moreover, patients can be endowed with a policy manager to view, express and alter privacy policies on the usage of their data and check their enforcement [9,40].

4.1.4. Communications and operations management

What kind of information is exchanged?

Security and privacy issues can often be managed quite simply when dealing with data residing in systems in a single organisation, but in the case of ensuring secure health information exchange across organisations, these categories may be more challenging [47].

Some authors advocate that complex environments such as health would benefit from a policy-driven RBAC [47]. This ISO specification [125,126] extends RBAC by defining a framework to represent and manage computable policy agreements between parties in order to exchange and use information. The policy agreements specify which information can be exchanged and under which security-related circumstances. In this context, the term 'profile' is used as the set of constraints regarding the permissions assigned to users, usually represented through their roles and as a corresponding set of policies.

Are there audit logs?

Audit trails are an important tool for data security in EHR systems [127]. However, audit trails are only a palliative measure, since the confidentiality/integrity of the information can be violated before countermeasures have been taken. Our review shows that many systems rely on the auditing of log data as a security mechanism. Audit trails can serve as proofs when disputes arise regarding serious issues such as abuse of permissions, illegal access attempts, and the improper disclosure of patients' health data [38]. Many countries have brought regulations into force that make their inclusion mandatory, such as the Security Rule of the HIPAA, which requires healthcare organisations to retain access logs for a minimum of 6 years [128].

Some access control models insert exceptional accesses into an auditing log for their analysis a posteriori. An auditing process allows the supervisor to analyse access requests in order to identify common practices that should be explicitly permitted or denied by defining appropriate policies [40]. For example, the analysis of access logs could be a very useful tool for learning how to reduce the need for exception-based access [77].

Audit trails can become a fundamental data security tool, as some security breaches have resulted from the misuse of access privileges by authorised persons [111]. However, one study [77] indicates that these log data are seldom used. Examining access logs is often an overwhelming task. Audit trails may not be practical, since they can exceed the size of the original file by orders of magnitude [129]. Hash chains are currently the most promising approach for storing authentic log files with a reasonably small overhead [9].

The workload can be reduced by distributing this task in order to allow each patient to be responsible for auditing the access log for his own record [45]. Log data should therefore be accessible and understandable by patients [45]. Event histories and an alert system can help the patient focus his attention on potentially illegal access to his data. This system can mark entities or users that have accessed the patient data and were defined as being suspicious by the patient. Monthly reports along with statistics should appear as options in the service interface menu. All features implemented in this service should be customised by the patient.

The current practice of auditing access logs involves identifying suspicious accesses to records based on known and simple patterns. Many research articles that tackle the development of algorithms, modelling and the definition of information sources used to determine the appropriateness of access, architectures for auditing systems, and the application of business intelligence platforms can be found in literature [112].

4.1.5. Human resources security

Are the EHR users trained in security and privacy issues?

All organisations that process personal health information should ensure that information security education and training, along with regular updates in organisational security policies

and procedures, are provided to all professional health staff [25]. As recommended by the ISO 27799 standard [25], some authors [8,30,34,44] consider that it is necessary to train health staff and patients in EHR system security and privacy in order to prevent sensitive data from being exposed. A security official should be responsible for all training activities [8]. HIPAA has also established a set of healthcare provider rules and regulations, requiring that all employees in the entities covered (defined as those organisations that, during the course of providing services, come in contact with or use personal health records) be educated in privacy [30]. However, in the light of the articles reviewed, security and privacy training fades into the background. The reason for this resides in the fact that education is not considered to be as important for security and privacy as is, for example, creating security algorithms for anonymity, authentication and access control.

The findings of a comparative study concerning the EHR information security requirements of Australia, Canada, Britain and the USA showed that it is critical that every computer user be aware of her information security [8]. Studies using semi-structured interviews with ambulatory care network and information systems leadership, medical directors, practice managers and vendors perceived training as pivotal for successful EHR implementation in an academic ambulatory setting [130].

Physicians [131] have also expressed their concern as regards the introduction of medical errors [132] resulting from complex technical capabilities and the level of technical support for clinical information technology solutions. Poor security and privacy training can affect care work [133,134]. In a study [133] of 26 clinicians situated in 3 large Australian hospitals, Fernando and Dawson discovered that the clinicians did not understand how to use specific privacy and security implementations effectively and were not able to identify confidential information. Complex security controls such as fine grained RBAC with emergency access may therefore make this problem worse, thus leading to suboptimal patient care, especially without the existence of appropriate training in the use of complex features such as 'break the glass'.

AHIMA research indicated that 64% of the organisation's new employees were trained in privacy rules in-house by the privacy or education officer [135]. The investment in training the workforce, both at the beginning of employment and during the job, decreases potential risk and damage to the organization [8]. Moreover, standardised educational materials in relation to all elements of the EHR should be adopted [20].

4.2. Limitations

Our study may have several limitations:

- The comparative framework was limited to 11 security controls belonging to 5 of 11 security areas identified in the ISO 27799 standard.
- The search was organised as a manual search process of several databases. The search string may not have included words that would have selected other relevant studies.
- The authors have only included articles in English, signifying that these results must be considered within the scope of English literature.
- The authors have not included studies published after the search date.
- One researcher extracted data from each article and another checked them. The reviewers may have omitted relevant security and privacy data.
- The evaluation criteria used might not have been appropriate.
- The authors reviewed articles published in scientific literature to discover how security and privacy are managed in an EHR. One in-depth endeavour by which to answer the question posed would be to analyse real solutions that are being used in EHR.

5. Conclusions

EHRs allow structured medical data to be shared between authorised health stakeholders in order to improve the quality of healthcare delivery and to achieve massive savings [27]. In these systems, privacy and security concerns are tremendously important, since the patient may encounter serious problems if sensitive information is disclosed. In this article, we have identified and analysed critical privacy and security aspects of the EHRs systems, based on the study of 49 research articles.

From the articles in our review, and based on the five security areas analysed, we can conclude the following:

- Compliance. Eleven different standards and regulations related to security and privacy have been used in the EHR systems found in 26 (53%) articles. Harmonisation is required to resolve possible inconsistencies and conflicts among standards.
- Information systems acquisition, development, maintenance. Various encryption algorithms have been proposed in 23 (46%) articles. It is advisable to use an efficient encryption scheme that is easy to use by both patients and healthcare professionals, is easily extensible to include new EHR records, and has a reduced number of keys held by each party [37].
- Access control. The preferred access control model in EHR systems is RBAC (55%). The most common authentication mechanisms are digital signature schemes based on PKI (22%) and logins/passwords (26%). In order to support patient empowerment [53,136], 3 (6%) EHR systems allow patients to grant access to specific portions of their health data.
- Communications and operations management. The recording of communications with the electronic health record system is found in 25 (51%) articles. It was observed that audit is particularly useful to identify suspicious accesses and common access practice.
- Human resources security. Health staff training in security and privacy rarely appears – in only 4 (8%) of the articles reviewed. However, it is recognised that educational programs which address issues of privacy and security for healthcare professionals and health organisations should be developed [137].

We have also perceived that most of the articles in the review defined EHR system security controls, but these are not fully deployed in actual tools. An example of this has been provided by a recent survey conducted in Spain [138], which illustrates a gloomy state of patient information security. 45% of state hospitals do not include on their forms the standard legal wording which explains how and why patients' data is stored. More than 30% of public hospitals do not have measures in place to prevent unauthorised access to patients' data while they are being transported. The number of state hospitals which do not carry out a security audit on their records is as high as 66%.

Centralised European and American health record systems will become a reality in the near future. A centralised supranational central server which stores electronic medical records from different health providers will make sensitive data more easily and rapidly accessible to a wider audience, but this also will increase the risk that health data could be accidentally exposed or easily distributed to unauthorised parties [138]. Security and privacy related issues are thus becoming even more important in such a cross-organisational environment [47].

Finally, although communications in a wireless environment are not within the scope of our review, the increasing use of wireless and Internet technologies in healthcare delivery is an unquestionable fact [25]. A problem with security could therefore occur if the Net is not protected when users access health data using wireless devices. In the future, we hope to carry out a systematic review concerning the privacy and security in wireless devices connected to EHR systems.

Acknowledgments

This work has been partially financed by the Spanish Ministry of Science and Technology, project PEGASO, TIN2009-13718-C02-01 and PANGEA, TIN2009-13718-C02-02.

Appendix A

The features of the 49 studies included in the review are summarised in Tables 2 and 3.

References

[1] Greenhalgh T, Hinder S, Stramer K, Bratan T, Russell J. Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. BMJ 2010;341:c5814.
[2] Allard T, Anciaux N, Bouganim L, Guo Y, Folgoc LL, Nguyen B, et al. Secure personal data servers: a vision paper. PVLDB 2010;3(1–2):25–35.
[3] Sainz-Abajo B, La-Torre-Díez I, Bermejo-González P, García-Salcines E, Díaz-Pernas J, Díez-Higuera JF, et al. Evolución, beneficios y obstáculos en la implantación del Historial Clínico Electrónico en el sistema sanitario. RevistaeSalud.com 2010;6(22):1–14.
[4] Hesse BW, Hansen D, Finholt T, Munson S, Kellogg W, Thomas JC. Social participation in health 2.0. Computer 2010;43(11):45–52.
[5] Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: ensuring privacy of electronic medical records. In: Proc ACM workshop on cloud computing security; 2009. p. 103–14.
[6] Los países europeos compartirán las historias clínicas de sus pacientes antes de; 2015. <http://www.europapress.es/> [accessed 07.12.12].
[7] Rothstein MA. Health privacy in the electronic age. J Leg Med 2007;28(4):487–501.
[8] Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: lessons learned from a comparative study. J Med Syst 2010;34(4):629–42.
[9] Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller N. Aspects of privacy for electronic health records. Int J Med Inform 2011;80(2):e26–31.
[10] ISO/EN 13606. <http://www.iso.org/iso/home.htm/> [accessed 07.12.12].
[11] Westin AF. Privacy and freedom. New York: Atheneum; 1967.
[12] NHS Lothian Communications Office. NHS Lothian staff member loses patient data. <http://www.nhslothian.scot.nhs.uk/MediaCentre/PressReleases/2008/Pages/0307PatientData.aspx/> [accessed 07.12.12].
[13] Department of Veterans Affairs Office of Inspector General. Review of issues related to the loss of VA information involving the identity of millions of veterans; 2006. <http://www.va.gov/oig/apps/info/OversightReports.aspx?igRT=ai/&igPG=4/> [accessed 07.12.12].
[14] Rothstein MA, Talbott MK. Compelled authorizations for disclosure of health records: magnitude and implications. Am J Bioeth 2007;7(3):38–45.
[15] Zurita L, Nøhr C. Patient opinion–EHR assessment from the users perspective. Stud Health Technol Inform 2004;107(2):1333–6.
[16] Kirchner H, Prokosch H, Dudeck J, Jöckel KH, Lehmacher W, Gesenhues S. Querschnittsbefragung von 8.000 BARMER-VersichertenzuErwartungen und EinsatzeinerelektronischenGesundheitsakte [Survey on expectations and implementation of an electronic health record, in German]. In: Proc of the annual meeting of the GMDS; 2009.
[17] Chhanabhai P, Holt A. Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. Med Gen Med 2007;9(1):8.
[18] Hoerbst A, Kohl CD, Knaup P, Ammenwerth E. Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens. Int J Med Inform 2010;79(2):81–9.
[19] HIT Standards Committee. Privacy and security standards applicable to ARRA requirements; 2009. <http://healthit.hhs.gov/> [accessed 07.12.12].
[20] Wiljer D, Urowitz S, Apatu E, DeLenardo C, Eysenbach G, Harth T, et al. Patient accessible electronic health records: exploring recommendations for successful implementation strategies. J Med Internet Res 2008;10(4):e34.
[21] Brigade T. The new threat: attackers that target healthcare (and what you can do about it). <http://www.infosecwriters.com/text_resources/pdf/New_Threat_Brigade.pdf/> [accessed 07.12.12].
[22] Mellado D, Fernández-Medina E, Piattini M. Security requirements engineering framework for software product lines. Inform Softw Technol 2010;52(10):1094–117.
[23] Liu LS, Shih PC, Hayes GR. Barriers to the adoption and use of personal health record systems. In: Proc of iConference; 2011. p. 363–70.
[24] Anderson R, Brown I, Dowty T, Inglesant P, Heath W, Sasse A. Database state. Joseph Rowntree Reform Trust; 2009. <http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf/> [accessed 07.12.12].
[25] ISO 27799:2008. Health informatics – information security management in health using ISO/IEC 27002. <http://www.iso.org/iso/home.htm/> [accessed 07.12.12].
[26] Liberati A, Altman DG, Tetzlaff J, Mulrow C, Gøtzsche PC, Ioannidis JPA, et al. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. J Clin Epidemiol 2009;62(10):e1–34.
[27] Neubauer T, Heurix J. A methodology for the pseudonymization of medical data. Int J Med Inform 2011;80(3):190–204.
[28] Deutsch E, Duftschmid G, Dorda W. Critical areas of national electronic health record programs—is our focus correct? Int J Med Inform 2010;79(3):211–22.
[29] Colwill C. Human factors in information security: the insider threat – who can you trust these days? Information Security Technical Report 2009;14(4):186–96.
[30] Kahn S, Sheshadri V. Medical record privacy and security in a digital environment. IT Professional 2008;10(2):46–52.
[31] Hu J, Chen HH, Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards & Interfaces 2010;32(5–6):274–80.
[32] Win KT, Susilo W, Mu Y. Personal health record systems and their security protection. J Med Syst 2006;30(4):309–15.
[33] Agrawal R, Johnson C. Securing electronic health records without impeding the flow of information. Int J Med Inform 2007;76(5–6):471–9.
[34] Elger BS, Iavindrasana J, Lo Iacono L, Müller H, Roduit N, Summers P, et al. Strategies for health data exchange for secondary, cross-institutional clinical research. Comput Methods Programs Biomed 2010;99(3):230–51.
[35] Narayan S, Gagné M, Safavi-Naini R. Privacy preserving EHR system using attribute-based infrastructure. In: Proc ACM workshop on cloud computing security; 2010. p. 47–52.
[36] Hembroff GC, Muftic S. SAMSON: Secure access for medical smart cards over networks. In: Proc IEEE int world of wireless mobile and multimedia networks (WoWMoM) symp; 2010. p. 1–6.
[37] Zhang R Liu L. Security models and requirements for healthcare application clouds. In: Proc IEEE 3rd int cloud computing (CLOUD) conf; 2010. p. 268–75.
[38] Sun J, Fang Y. Cross-domain data sharing in distributed electronic health record systems. IEEE Trans Parallel Distrib Syst 2010;21(6):754–64.
[39] Faresi AAL, Wijesekera D, Moidu K. A comprehensive privacy-aware authorization framework founded on HIPAA privacy rules. In: Proc ACM international health informatics symposium; 2010. p. 637–46.
[40] Ardagna CA, di Vimercati SDC, Foresti S, Grandison T, Jajodia S, Samarati P. Access control for smarter healthcare using policy spaces. Comput Secur 2010;29(8):848–58.
[41] Horvath MM, Winfield S, Evans S, Slopek S, Shang H, Ferranti J. The DEDUCE guided query tool: providing simplified access to clinical data for research and quality improvement. J Biomed Inform 2011;44(2):266–76.
[42] Dekker M, Etalle S. Audit-based access control for electronic health records. Electron Notes Theoret Comput Sci 2007;168:221–36.
[43] Peleg M, Beimel D, Dori D, Denekamp Y. Situation-based access control: privacy management via modeling of patient data access scenarios. J Biomed Inform 2008;41(6):1028–40.
[44] Falcão-Reis F, Costa-Pereira A, Correia ME. Access and privacy rights using web security standards to increase patient empowerment. Stud Health Technol Inform 2008;137:275–85.
[45] Rostad L. An initial model and a discussion of access control in patient controlled health records. In: Proc conf availability, reliability and security ARES; 2008. p. 935–42.
[46] Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM Trans Inf Syst Secur 2001;4(3):224–74.
[47] van der Linden H, Kalra D, Hasman A, Talmon J. Inter-organizational future proof EHR systems. A review of the security and privacy related issues. Int J Med Inform 2009;78(3):141–60.
[48] ENV 13729:2000. Health informatics. Secure user identification. Strong authentication microprocessor cards. <http://www.freestd.us/soft/144932.htm/> [accessed 07.12.12].
[49] Quantin C, Jaquet-Chiffelle DO, Coatrieux G, Benzenine E, Allaert FA. Medical record search engines, using pseudonymised patient identity: an alternative to centralised medical records. Int J Med Inform 2011;80(2):e6–11.
[50] Kalra D, Singleton P, Milan J, Mackay J, Detmer D, Rector A, et al. Security and confidentiality approach for the clinical e-science framework (CLEF). Methods Inf Med 2005;44(2):193–7.
[51] Ueckert F, Prokosch HU. Implementing security and access control mechanisms for an electronic healthcare record. In: Proc AMIA symp; 2002. p. 825–9.
[52] Ueckert F, Müller ML, Bürkle T, Prokosch HU. An electronic health record to support patients and institutions of the health care system. Ger Med Sci 2004;2.

[53] Ueckert F, Goerz M, Ataian M, Tessmann S, Prokosch HU. Empowerment of patients and communication with health care professionals through an electronic health record. Int J Med Inform 2003;70(2–3):99–108.
[54] Riedl B, Grascher V, Neubauer T. Applying a threshold scheme to the pseudonymization of health data. In: Proc 13th Pacific rim int symp dependable computing PRDC; 2007. p. 397–400.
[55] Riedl B, Grascher V, Fenz S, Neubauer T. Pseudonymization for improving the privacy in e-health applications. In: Proc annual Hawaii int conf system sciences; 2008. p. 1–9.
[56] Riedl B, Neubauer T, Goluch G, Boehm O, Reinauer G, Krumboeck A. A secure architecture for the pseudonymization of medical data. In: Proc int conf availability, reliability and security ARES; 2007. p. 397–400.
[57] Huang LC, Chu HC, Lien CY, Hsiao CH, Kao T. Privacy preservation and information security protection for patients' portable electronic health records. Comput Biol Med 2009;39(9):743–50.
[58] Alhaqbani B, Fidge C. Privacy-preserving electronic health record linkage using pseudonym identifiers. In: Proc int conf e-health networking, applications and services healthcom; 2008. p. 108–17.
[59] Shamir A. How to share a secret. Commun ACM 1979;22(11):612–3.
[60] Choe J, Yoo SK. Web-based secure access from multiple patient repositories. Int J Med Inform 2008;77(4):242–8.
[61] Daglish D, Archer N. Electronic personal health record systems: a brief review of privacy, security, and architectural issues. In: Proc world congress privacy, security, trust and the management of e-business congress; 2009. p. 110–20.
[62] Jian WS, Wen HC, Scholl J, Shabbir SA, Lee P, Hsu CY, et al. The Taiwanese method for providing patients data from multiple hospital EHR systems. J Biomed Inform 2011;44(2):326–32.
[63] Lemaire ED, Deforge D, Marshall S, Curran D. A secure web-based approach for accessing transitional health information for people with traumatic brain injury. Comput Methods Programs Biomed 2006;81(3):213–9.
[64] Bos JJ. Digital signatures and the electronic health records: providing legal and security guarantees. Int J Biomed Comput 1996;42(1–2):157–63.
[65] Sucurovic S. An approach to access control in electronic health record. J Med Syst 2010;34(4):659–66.
[66] Sucurovic S. Implementing security in a distributed web-based EHCR. Int J Med Inform 2007;76(5–6):491–6.
[67] France FHR, Bangels M, De-Clercq E. Purposes of health identification cards and role of a secure access platform (be-health) in Belgium. Int J Med Inform 2007;76(2–3):84–8.
[68] Al-zharani S, Sarasvady S, Chandra H, Pichappan P. Controlled EHR access in secured health information system. In: Proc int digital information management conf; 2007. p. 63–8.
[69] Yu WD, Chekhanovskiy MA. An electronic health record content protection system using SmartCard and PMR. In: Proc int e-health networking, application and services conf; 2007. p. 11–8.
[70] Bouwman B, Mauw S, Petkovic M. Rights management for role-based access control. In: Proc 5th IEEE consumer communications and networking conf CCNC; 2008. p. 1085–90.
[71] Jafari M, Safavi-Naini R, Saunders C, Sheppard NP. Using digital rights management for securing data in a medical research environment. In: Proc digital rights management workshop; 2010. p. 55–60.
[72] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proc IEEE symp security and privacy; 2007. p. 321–34.
[73] Ruotsalainen P. A cross-platform model for secure electronic health record communication. Int J Med Inform 2004;73(3):291–5.
[74] Reni G, Molteni M, Arlotti S, Pinciroli F. Chief medical officer actions on information security in an Italian rehabilitation centre. Int J Med Inform 2004;73(3):271–9.
[75] Lovis C, Spahni S, Cassoni N, Geissbuhler A. Comprehensive management of the access to the electronic patient record: towards trans-institutional networks. Int J Med Inform 2007;76(5–6):466–70.
[76] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proc ASIACRYPT; 2003. p. 452–73.
[77] Rostad L, Edsberg O. A study of access control requirements for healthcare systems based on audit trails from access logs. In: Proc annual computer security applications conf; 2006. p. 175–86.
[78] Tsiknakis M, Katehakis D, Orphanoudakis S. A health information infrastructure enabling secure access to the life-long multimedia electronic health record. In: Proc computer assisted radiology and surgery; 2004. p. 289–94.
[79] Jin J, Ahn GJ, Hu H, Covington MJ, Zhang X. Patient-centric authorization framework for electronic healthcare services. Comput Secur 2011;30(2–3):116–27.
[80] Bakker A. Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. Int J Med Inform 2004;73(3):267–70.
[81] ISI Journal Citation Reports (JCR); 2011. <http://www.accesowok.fecyt.es/jcr/> [accessed 07.12.12].
[82] SCImago Journal Rank (SJR); 2010. <http://www.scimagojr.com/journalrank.php/> [accessed 07.12.12].
[83] CORE. COmputing Research and Education; 2010. <http://core.edu.au/index.php/categories/conference/%20rankings/1/> [accessed 07.12.12].
[84] Bouhaddou O, Cromwell T, Davis M, Maulden S, Hsing N, Carlson D, et al. Translating standards into practice. Experience and lessons learned at the Department of Veterans Affairs. J Biomed Inform 2012;45(4):813–23.
[85] Glaser J, Henley DE, Downing G, Brinner KM. Advancing personalized health care through health information technology: an update from the American Health Information Community's Personalized Health Care Workgroup. J Am Med Inform Assoc 2008;15(4):391–6.
[86] McGuire AL, Fisher R, Cusenza P, Hudson K, Rothstein MA, McGraw D, et al. Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. Genet Med 2008;10(7):495–9.
[87] Win KT. A review of security of electronic health records. HIM J 2005;34(1):13–8.
[88] Dreiseitl S, Vinterbo S, Ohno-Machado L. Disambiguation data: extracting information from anonymized sources. J Am Med Inform Assoc 2002;9(6 Suppl. 1):s110–4.
[89] Lo-Iacono L. Multi-centric universal pseudonymisation for secondary use of the EHR. Stud Health Technol Inform 2007;126:239–47.
[90] Gulcher JR, Kristjánsson K, Gudbjartsson H, Stefánsson K. Protection of privacy by third-party encryption in genetic research in Iceland. Eur J Hum Genet 2000;8(10):739–42.
[91] Pommerening K, Reng M. Secondary use of the electronic health record via pseudonymisation. In: Bos L, Laxminarayan S, Marsh A, editors. Medical care compunetics 1. Amsterdam: IOS Press; 2004. p. 441–6.
[92] European Agency for the Evaluation of Medical Products (EMEA) Committee for Proprietary Medicinal Products. Position paper on terminology in pharmacogenomics. Report No. EMEA/CPMP/3070/01, London; 2002.
[93] Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzzy Knowl-Based Syst 2002;10(5):557–70.
[94] Ferris TA, Garrison GM, Lowe HJ. A proposed key escrow system for secure patient information disclosure in biomedical research databases. In: Proc AMIA symp; 2002. p. 245–9.
[95] De-Moor GJE, Claerhout B, De-Meyer F. Privacy enhancing techniques – the key to secure communication and management of clinical and genomic data. Methods Inf Med 2003;42(2):148–53.
[96] Thornburgh T. Social engineering: the "Dark Art". In: Proc annual conference on Information security curriculum development; 2004. p. 133–5.
[97] Huang LC, Chu HC, Lien CY, Hsiao CH, Kao T. Embedding a hiding function in a portable electronic health record for privacy preservation. J Med Syst 2010;34(3):313–20.
[98] Kushida CA, Nichols DA, Jadrnicek R, Miller R, Walsh JK, Griffin K. Strategies for de-identification and anonymization of electronic health record data for use in multicenter research studies. Med Care 2012;50:S82–S101.
[99] Hu J, Han F. A pixel-based scrambling scheme for digital medical images protection. J Netw Comput Appl 2009;32(4):788–94.
[100] van-der-Haak M, Mludek V, Wolff AC, Bülzebruck H, Oetzel D, Zierhut D, et al. Networking in shared care-first steps towards a shared electronic patient record for cancer patients. Methods Inf Med 2002;41(5):419–25.
[101] Ball E, Chadwick DW, Mundy D. Patient privacy in electronic prescription transfer. IEEE Secur Privacy 2003;1(2):77–80.
[102] Horst H. How to tamper with electronic health records. <http://www.gnumed.net/gnotary/tampering.html/> [accessed 07.12.12].
[103] Allaert F, Le-Teuff G, Quantin C, Barber B. The legal knowledge of the electronic signature: a key for a secure direct access of patients to their computerised medical record. Int J Med Inform 2004;73:239–42.
[104] Alban RF, Feldmar D, Gabbay J, Lefor AT. Internet security and privacy protection for the health care professional. Current Surgery 2005;62:106–10.
[105] Sax U, Kohane I, Mandl KD. Wireless technology infrastructures for authentication of patients: PKI that rings. J Am Med Inform Assoc 2005;12(3):263–8.
[106] Park MA. Embedding security into visual programming courses. In: Proc information security curriculum development conference; 2011. p. 84–93.
[107] Wang Y, Hu J, Phillips D. A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing. IEEE Trans Pattern Anal Mach Intel 2007;29:573–85.
[108] Ross A, Shah J, Jain AK. From template to image: reconstructing fingerprints from minutiae points. IEEE Trans Pattern Anal Mach Intel 2007;29:544–60.
[109] Liberty Alliance Project 2009. <http://www.projectliberty.org/> [accessed 07.12.12].
[110] Smith D. The challenge of federated identity management. Network Security 2008;2008(4):7–9.
[111] Barrows RJ, Clayton P. Privacy, confidentiality and electronic medical records. J Am Med Inform Assoc 1996;3:139–48.
[112] Boxwala AA, Kim J, Grillo JM, Ohno-Machado L. Using statistical and machine learning to help institutions detect suspicious access to electronic health records. J Am Med Inform Assoc 2011;18(4):498–505.
[113] Ferreira A, Cruz-Correia R, Antunes L, Chadwick D. Access control: how can it improve patients' healthcare? Stud Health Technol Inform 2007;127:65–76.
[114] Blobel B. Authorisation and access control for electronic health record systems. Int J Med Inform 2004;73(3):251–7.
[115] Zhang L, Ahn GJ, Chu BT. A role-based delegation framework for healthcare information systems. In: Proc ACM symposium on Access control models and technologies; 2002. p. 125–34.
[116] Na S, Cheon S. Role delegation in role-based access control. In: Proc ACM workshop on Role-based access control; 2000. p 39–44.
[117] Standard Guide for Information Access Privileges to Health Information, ASTM E1986–98; 2005. <http://www.astm.org/DATABASE.CART/HISTORICAL/E1986-98R05.htm/> [accessed 07.12.12].

[118] ISO DTS 21298 Functional and structural roles. <http://www.iso.org/iso/home.htm/> [accessed 07.12.12].
[119] American National Standard Institute (ANSI). American National Standard for information technology: role based access control. Technical Report ANSI INCITS 359-2004; 2004. <http://www.csrc.nist.gov/rbac/EDACcompliance.pdf/> [accessed 07.12.12].
[120] Li N, Byun JW, Bertino E. A critique of the ANSI Standard on role-based access control. IEEE Security Privacy 2007;5(6):41–9.
[121] Mohan A, Blough DM. An attribute-based authorization policy framework with dynamic conflict resolution. In: Proc symposium on identity and trust on the internet; 2010. p. 37–50.
[122] Motta GH, Furuie SS. A contextual role-based access control authorization model for electronic patient record. IEEE Trans Inf Technol Biomed 2003;7(3):202–7.
[123] Bates GW. Special requirements of electronic medical record systems in obstetrics and gynecology. Obstet Gynecol 2010;116(4):994.
[124] Rissanen E, Firozabadi BS, Sergot MJ. Discretionary overriding of access control in the privilege calculus. In: Proc formal aspects in security and trust; 2004. p. 219–32.
[125] ISO/TS 22600-1 Health informatics—Privilege management and access control—Part 1: Overview and policy management. ISO 2006. <http://www.iso.org/iso/home.htm/> [accessed 07.12.12].
[126] ISO/TS 22600-2 Health informatics—Privilege management and access control—Part 2: Formal models; 2006. <http://www.iso.org/iso/home.htm/> [accessed 07.12.12].
[127] Bilykh I, Bychkov Y, Dahlem D, Jahnke JH, McCallum G, Obry C, et al. Can GRID services provide answers to the challenges of national health information sharing? In: Proc conference of the centre for advanced studies on collaborative research; 2003. p. 39–53.
[128] US Department of Health and Human Services, Office for Civil Rights. Standards for protection of electronic health information; final rule. Federal Register 45 cfr: pt. 164; 2003.
[129] Win KT. Web-based personal health record systems evaluation. Int J Healthcare Technol Manage 2006;7(3–4):208–17.
[130] Yoon-Flannery K, Zandieh SO, Kuperman GJ, Langsam DJ, Hyman D, Kaushal R. A qualitative analysis of an electronic health record (EHR) implementation in an academic ambulatory setting. Inform Prim Care 2008;16(4):277–84.
[131] McAlearney AS, Chisolm DJ, Schweikhart S, Medow MA, Kelleher K. The story behind the story: physician skepticism about relying on clinical information technologies to reduce medical errors. Int J Med Inform 2007;76(11–12):836–42.
[132] Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR, Kimmel SE, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA 2005;293(10):1197–203.
[133] Fernando J, Dawson L. The health information system security threat lifecycle: an informatics theory. Int J Med Inform 2009;78(12):815–26.
[134] Fernando J, Dawson L. Clinician assessments of workplace security training—an informatics perspective. eJHI 2008;3(1):e7.
[135] AHIMA. The state of HIPAA privacy and security compliance, April 2006. <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022739.pdf/> [accessed 07.12.12].
[136] Masys D, Baker D, Butros A, Cowles KE. Giving patients access to their medical records via the internet: the PCASSO experience. J Am Med Inform Assoc 2002;9(2):181–91.
[137] Patel VL, Arocha JF, Shortliffe EH. Cognitive models in training health professionals to protect patients' confidential information. Int J Med Inform 2000;60(2):143–50.
[138] Kierkegaard P. Electronic health record: wiring Europe's healthcare. Comput Law Security Rev 2011;27(5):503–15.