Yuan et al. Security Informatics (2015) 4:3
DOI 10.1186/s13388-015-0017-9

Security Informatics
a SpringerOpen Journal

REVIEW Open Access

Emerging issues for education in E-discovery for electronic health records

Shuai Yuan*, Raghav H Rao and Shambhu Upadhyaya

Abstract

In order to provide a foundation for education on e-discovery and security in Electronic Health Record (EHR) systems, this paper identifies emerging issues in the area. Based on a detailed literature review it details key categories: Development in EHR, E-discovery policy and strategy, and Security and privacy in EHR and also discusses e-discovery issues in cloud computing and big data contexts. This may help to create a framework for potential short course-design on e-discovery and security in the healthcare domain.

Keywords: Electronic Health Record; E-discovery; Security and Privacy

Introduction

Electronic Health Record (EHR) systems are the aggregate electronic record of health-related information on individuals "created and gathered cumulatively across more than one health care organization and managed and consulted by licensed clinicians and staff involved in the individual's health and care" (National Alliance for Health Information Technology (NAHIT[a]) [1]. EHR has been strongly recommended for adoption in the healthcare industry in the U.S. The increased use of EHR systems has assisted health care professionals in medical practices by storing patients' medical and diagnosis information, exchanging laboratory reports and radiologic images, and also providing decision support tools for the physicians and communication methods with patients [2,3]. The American Recovery and Reinvestment Act of 2009 (ARRA)'s goal was to computerize all Americans health records by 2014 by dedicating nineteen billion dollars to the promotion of health information technology [4,5]. However, EHR systems also bring new liability and litigation risks such as the inappropriate use of the systems, privacy breaches, and inadvertent data disclosures, which in turn may impose heavy costs in terms of preservation of electronic information and potential litigation issues [6].

E-discovery refers to discovery of information, often for civil litigations, that is stored in electronic format, known as Electronically Stored Information (ESI). In 2006, amendments were made to federal rules to facilitate ESI discovery. This resulted in changes to traditional e-discovery rules [7]. To comply with the new rules, healthcare providers are required to establish and update policies and procedures in terms of information governance and EHR systems along with advanced technologies that may also be needed to be developed to facilitate e-discovery.

EHR adoption will require significant efforts with regard to workforce since it is a complex and large initiative in healthcare industry. This calls for expansion of today's education system to cover topics of security, security technology and policy, and privacy issues. The primary purpose of this study is to lay a foundation for topics in both security issues and e-discovery challenges involving EHR system use. To achieve this purpose, we categorize the emerging issues based on in-depth literature review, into three categories: Development in EHR, E-discovery policy and strategy, and Security and privacy in EHR. We also discuss some key issues related to e-discovery raised from the new technologies of cloud computing and big data contexts. A major contribution of this paper is the development of a framework for education. The outcome of this study can be used to design short courses on security and e-discovery regarding EHR systems in the healthcare domain.

The rest of the paper is organized as follows. Section 2 provides discusses three categories- Development in EHR, E-discovery policy and strategy, and Security and privacy in EHR. Section 3 studies new and emerging

* Correspondence: shuaiyua@buffalo.edu
SUNY at Buffalo, Buffalo, NY 14260, USA

issues associated with e-discovery when cloud computing and big data are becoming prevalent. Section 4 concludes with a discussion on the course-design framework for faculty members.

Literature review of E-discovery in EHR

Developments in EHR

EHR systems that contain patients' medical data and information, have not only been used in healthcare delivery, but are relevant to litigation and are subject to ESI discovery due to amendments that were passed in 2006. As the adoption of EHR systems in hospitals and other healthcare sectors is increasing, providers and legal counsel must be aware of the advances in EHR technology, get a better understanding of the information they can acquire and retrieve from EHR systems, and prepare e-discovery provisioning requirements [8]. The development of techniques in EHR systems would facilitate e-discovery. In addition, healthcare providers naturally have a wide choice as to how engaged their medical practice will be with EHR technology and which EHR system will be used [8]. With national benchmarks to measure EHR systems in terms of certification and meaningful use, the quality of the system outcomes as well as the functionalities associated with e-discovery request need to be guaranteed. Furthermore, particular EHR technologies, for instance, metadata search algorithms, are necessary to facilitate the review process for e-discovery use. Healthcare providers and legal counsel might not be technology experts in EHR development, however, the knowledge of where relevant ESI exists and how to preserve such information to satisfy e-discovery obligations is a necessary requirement.

Techniques in EHR systems to facilitate e-discovery

Advanced techniques in EHR systems to facilitate e-discovery process are needed, otherwise e-discovery will be inefficient and costly, leading to heavy burden to stakeholders involved. For instance, the 2006 amendments have expanded the use of a "legal hold" for preservation of paper documents as well as ESI document. Healthcare organizations should suspend routine document retention and destruction policy to ensure the preservation of all forms of relevant information avoiding sanctions for ESI spoilage, at the time when the organization receives a notice of litigation [9]. There is a documented lack of efficient technology in EHR systems to establish a legal hold on patients' records and it is costly to put a legal hold on one particular patient in EHR systems [10]. Further, sometimes legal counsels do not have sufficient knowledge in techniques to acquire valuable data from EHR systems. This calls for education about functions of EHR systems.

Information sharing and data interoperability

There is an increasing need to build a national health information infrastructure (NHII) to connect users and manage knowledge of healthcare so that provides functions for information sharing among different EHR systems. There are three main reasons why the NHII is required [11]: First, professionals and researchers face substantial growth and much more complex health data about patients as they encounter more types of illnesses and simultaneously improving diagnostic capabilities; Second, data standardization fulfilled by NHII will facilitate data manipulation so that costs and turnaround times are reduced and last but not least, a platform is needed to assure the benefits of cutting edge technology and method diffuse to different stakeholders in healthcare domain. For instance, large datasets are needed to acquire the knowledge regarding the molecular underpinning of disease through intensive computing capabilities. Such data sets can be one feature of the NHII. In order to achieve the goal to build a NHII connected participants in healthcare, series of agreements on standardization of technology, data, processes and rules need to be reached as well. The quantity and quality of data to support decision-makings in health care delivery are important for implementation of a complete NHII [8]. Each of these issues is critical for system related education.

Data interoperability is a key ability in NHII implementation that two or more EHR systems can exchange and share information. This feature has also been indicated in "meaningful use" stage 1 requirements such that key patient data can be exported to a common format. Currently two formats have been developed: Continuity of Care Records (CCR) and Continuity of Care Documents (CCD) but neither of them has been used to export entire patient's EHR records, since abbreviations and terminology vary among practice [12]. In order to facilitate e-discovery, first, the format used by the export feature must be able to provide a complete record of a patient for production during discovery. In addition, the EHR data should be viewable by a lawyer in a similar layout as viewed by medical professionals since, "A party must produce documents as they are kept in the usual course of business..." Finally, it is necessary for the feature to be able to export specific data required for production such that the lawyer is capable to produce only relevant data for discovery purposes [12].

Metrics for EHR systems quality control

Without appropriate mechanisms and metrics to control the quality of diverse EHR systems in the market, healthcare organizations are at risk of investing large amounts on poorly designed systems which may not improve the outcomes. Therefore, developing national benchmarks to

measure not only the technology but systems in terms of certification, meaningful use, and implementation specification, etc. are mandatory [13,14].

Here, it is also worth noticing the difference between certification and meaningful use on EHR systems [15]. Certification of EHR systems ensures that the particular system meets functionality standards. In June 2010, the Office of the National Coordinator for Health Information Technology (ONC) defined the temporary criteria for testing and certifying EHRS functionality [16]. Subsequently in January 2011, ONC issued the final rule on a Permanent Certification Program for Health Information Technology, for functional testing requirement, cases and tools. Meaningful use implies "providers need to show they're using certified EHR technology in ways that can be measured significantly in quality and in quantity", corresponding to quality of the adoption of EHR systems [17]. Identification of these issues is important for educational programs.

Clinical practice guidelines to optimize EHR system use

Clinical practice guidelines (CPG)s assist in decisions about special circumstances in healthcare. CPGs in terms of diagnostic and treatment practices have been developed by professional societies over a long time period. The standard of care is a key to successful defense in medical malpractice litigation since it reveals whether the defendant "proceed [ed] with the reasonable caution that a prudent man would have exercised under such circumstances" [13]. Compliance with well-established CPGs, similar to expert testimony, can be utilized as proof that the defendant met the standard of care, "at least as evidence of a practice that is accepted by a respectable minority". However, at the early age of EHR system development and adoption, few authoritative CPGs exist regarding the design and use of EHR systems, and even less in the litigation context [13]. Any educational program related to e-discovery in health needs to include such CPGs.

Audit trails/ metadata search techniques

Audit trails are the records about "who did what and when" in order to meet requirements on "system integrity, recoverability, auditing, and requirements". Effective audit trails on EHR systems should keep all relevant system input and output not only for the purpose of system validation and problem diagnosis, but also to understand how EHR systems are operating. The audit trails can then serve as unbiased evidence of medical practice for potential litigation use [13].

A key component of the functioning of audit trails is Metadata - which is generated to track how an electronic document has been manipulated. Metadata has been viewed as non-hearsay evidence by the courts because it can be considered to have integrity - it is automatically generated without human intervention [10]. Metadata can also be used as a tool to reveal what documents have been actually created, reviewed, modified and deleted. Federal courts have held that when an electronic document is discoverable, it is to be produced "in native format…with their metadata intact" [10]. E-discovery with metadata would generate a huge amount of ESI. This calls for effective search techniques and strategies to facilitate the review process [13]. Therefore, search techniques for metadata and an understanding of metadata need to be covered in e-discovery courses.

Advances in health 2.0

Health 2.0. has been defined as the phenomenon in which Web 2.0 Technologies provide members of the health community–health professionals, health consumers, and health science students–with new and innovative ways to create, disseminate, and share information both individually and collaboratively. It is a new concept of health care that employs social software and other Web-based tools to promote collaboration between patients, their caregivers, medical professionals, and other stakeholders in health care to create a better, more knowledgeable and cost effective environment for better well-being [18]. Health 2.0 is the use of a set of Web tools (blogs, Podcasts, wikis, etc.) in health care by doctors, patients, and scientists. For example, websites like PatientsLikeMe [19] use knowledge from users the network from social media to personalize health care and promote health education [20].

One key difference between traditional models of medicine and Health 2.0 is the knowledge of patient records and related control. In traditional models, patients' records could only be kept and accessed by medical professionals; while in newer models patients obtain more control and deeper insight into their own information. Web 2.0/technology, patients, professionals, social networking, health information/content, collaboration, and change of health care are the topics closely related to the definition of Health 2.0 [18].

Therefore, any curriculum for Health 2.0 should also include, for instance: 1) the stakeholders involved, e.g. patients/consumers, professionals/caregivers, and biomedical researchers, 2) the emerging methods and technology, e.g. web 2.0 and virtual-reality tools, 3) the change of relationship between stakeholders, such as the improved collaboration and communication between professionals and patients, and 4) the impact on the development of health care system like improvement on safety, efficiency and quality of old system. In addition, inaccurate online information is another concern in Health 2.0. Although research has found that online

information is often accurate or can be corrected rapidly, many practitioners believe "the consequences could be disastrous for any inexperienced trainee following the advice" [21]. The use of Health 2.0 raises a challenge for healthcare organizations to serve e-discovery requests. Since the information in Health 2.0 associated with privacy, ethical, and ownership issues is in the scope of discovery as well, failing to preserve relevant information due to un-updated usage and electronic data management policy and techniques could lead to potential sanctions. It is important that students are exposed to each one of these, since these could drive e-discovery lawsuits.

E-discovery policy and strategy

Policies and processes for electronic records management

Electronic health records are composed of types of information within the boundary of the health organization, e.g. email, text messages, and even legacy information systems [22]. Health Information Management and IT professionals need to work together to fulfill the tasks of determining organizational document storage, retention, and destruction schedules as well as for digital information to avoid potential sanctions resulting from failure to preserve relevant documents in e-discovery cases.

For instance, the updated policies and processes should indicate where and in what type of format the electronic health records should be stored, how often to maintain such records, and when to destroy them. Updated policies and processes for electronic medical records are required for healthcare organizations to comply with federal, state requirements to facilitate e-discovery.

Economics of cost

Recently, courts have started to limit ESI discovery based on cost-benefit analysis. Under the Discovery Scope and Limits in Rule 26 of The Federal Rules of Civil Procedure, ESI discovery could be limited if "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issue at stake in the litigation, and the importance of the proposed discovery in resolving the issues". For example, in Lorranie v. Markel American Insurance Co., Judge Grimm denied the parties' competing motions for summary judgment by opining that "it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted [23]". Therefore, it is important for students to understand how organizations should establish a means for determining the actual costs for production of ESI, and for detecting if this production would be over burdensome in which case such ESI would be out of the scope of discovery [10].

Legal hold policies to handle preservation of relevant documents

Legal hold indicates that a party "must suspend its routine document retention/destruction policy" for the purpose of making sure the preservation of relevant document including ESI, once the party receives a notice of litigation [24]. In order to comply with the preservation obligation, in addition to appropriate techniques, healthcare organizations need to understand the legal hold policy to handle this process, e.g. the instructions and corresponding workflow so that the regular automatic retention/destruction policy would not execute automatically. These issues would fit into an understanding of both law and workflow systems.

Security and privacy issues

Information privacy and data confidentiality

For an information system in any area and domain, security is of crucial concern. Further, information privacy is one key issue that has serious influence on the adoption of EHR systems since all the patients' healthcare information are stored, shared and communicated among different EHR systems and healthcare sectors. Any privacy breach and abuse of data may prohibit the intention to use EHR systems in spite of numerous benefits. Privacy issues have not been addressed sufficiently at either technical or business process level, e.g., in a nationwide survey conducted in February 2005 by Harris Interactive of Rochester, N.Y., 70 percent of people were somewhat or very concerned that personal medical information would be leaked due to weak data security [25].

Data is the primary resource in EHR systems thus its confidentiality is significant for information privacy. Personal information obtained in physician-patient relationship should not be revealed to others unless the patient understands and consents to disclosure [26]. The trend of data sharing among EHR systems and healthcare organizations is inevitable, as a result, innovative management techniques and policies on data confidentiality should be taught to keep in step.

Access controls and policies for EHR

While maintaining information privacy matters, obtaining patients' healthcare information on demand from EHR systems for caregivers like hospitals and doctors is critical as well. There is a trade-off between accessibility to patients' information and privacy concerns, especially when some EHR systems are based on web services which make the information more easily to access while

at the same time give rise to potential privacy issues. Therefore, a challenge raised is to develop access control policies that can provide required protection on privacy while keeping flexibility to accommodate authorized users so that only a set of users can access certain level of patient information [27], e.g. which portions of a patient's record can access by whom for a specific period of time. In general, attribute-based access control (ABAC) and role-based access control (RBAC) are the two main approaches to control access to EHR systems [28,29]. ABAC divides the system into subcomponents and for each subcomponent, access policy has been stored as an attribute of the data, while RBAC constructs a hierarchy of roles that can be assigned to each user, through which to authorize privileges to each role instead of each user. Both approaches have their own benefits and shortcomings. Thus understanding existing access control method and policy to ensure both flexibility and security is urgent for any student of e-discovery.

Management of patient consent

As we mentioned earlier, without patient's awareness and consents to disclosure, private information in EHR systems should not be revealed to others, thus consent of patient plays a vital role. Individual patients should know and understand the contents of records in terms of effective notification and truly informed consent for disclosure, which also implies that the particular patient is fully informed of his/her medical status and gives voluntary agreement to permit access to their healthcare information [26]. Failure to truly inform patient's awareness of disclosure, e.g. using implied consent, would lead to unethical issues.

Patients either implicitly or explicitly consent to information disclosure according to different consent models. For example, two types of consent models are considered: General Consent with Specific Denials and General Denial with Specific Consent [30]. Obviously the latter can maintain information at a high level of confidentiality while at the same time, it might hinder the workflow of healthcare providers. Therefore, an understanding of effective consent and control mechanisms are needed that can give patients control for their own healthcare information as well as not impede regular healthcare delivery process.

HITECH and HIPAA privacy and security rules

Significant modifications have been made to Health Information Technology for Economic and Clinical Health Act (HITECH) and Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. For instance, substantial incentives and grants are provided in the HITECH Act for the adoption of EHR systems and information exchange to improve both quality and efficiency of healthcare. On the other hand, for the HIPAA Privacy and Security Rules, mandatory federal security breach reporting requirements, criminal and civil penalties for noncompliance are established [31,32]. These extensions and enforcements are aimed at continually improving the effect of HITECH and HIPAA rules – clearly an important area of knowledge for the student.

Issues on E-discovery in cloud and Big data

The cloud is the place where various users including patients and physicians on EHR systems have started to share resources [33]. E-discovery becomes more complex in the context of the cloud environment. First, the data are preserved by a cloud service provider, which may lead to the consequence that some ESI might be outside the scope of discovery, or alternately, some data may fall under e-discovery but may not be controlled by firms facing a discovery request. The other reason is, since data from various users is intermingled in the cloud controlled only by the service provider, retrieving and placing a hold on one user's information for anticipated litigation request may affect other users who are not involved [34]. Therefore, some unique issues are needed to be understood in the context of e-discovery in cloud as well.

Cloud services support the basic infrastructure and platform for EHR systems, and would be instrumental in the harvesting of big data. Organizations are experiencing exponential growth in the amounts of data they create, capture, and retain within their in-house facilities, as well as that are maintained in the cloud in the current big data world, thus call for advanced analytics techniques dealing with them [35]. E-discovery also relies on high performance analysis tools to reduce the time and cost, but due to the nature of big data more powerful tools will be needed to identify, organize, and analyze big data. In addition to the technical tools, comprehensive policy and strategy according to e-discovery are also required to accommodate the "big" world. Developing guidelines, procedures, and workflows for the creation, storage and destruction of ESI with potential big data involved in litigation procedures for compliance with federal and state regulations has been considered urgent and necessary as well as a big challenge [36].

In addition, cloud computing service and big data interact with each other. Therefore, they have in common some critical issues, e.g. data preservation and analytics techniques in e-discovery, as well as usage policies and "thresholds" of relevancy for evidence to be admissible.

Data analytics

The volume of data, velocity with which data is generated and variety of data-pictures, messages, audio files, text files, in e-discovery procedures, makes it nearly

impossible to review them by humans. Data mining along with predictive analytics plays an important role in e-discovery for legal purposes. For instance, text mining, as well as image mining can discover hidden patterns and relationship between people and events that can be used as evidence in litigations [37].

Predictive coding as the service that can rank and code relevant documents might be used in an anticipated litigation through machine learning algorithms and pattern recognition methods built-in. It is increasingly recognized as a field of inquiry and capability development and could reduce the extent of human involvement in the e-discovery process [38]. A hybrid method combining both predictive coding and data mining techniques with extra attention by human review on the most important ESI would help best practice results in e-discovery. Such skills are important for an e-discovery scholar.

Data preservation and control policies

Data in the cloud provides additional difficulties in data preservation since ESI from one particular user can be stored across multiple physical storage locations due to the nature of cloud. Thus, in order to implement preservation, specific cloud resources need to be isolated [34,39]. Data in the cloud are under custody and control by the cloud service provider which means users may not have actual powerful control over them that can serve as key evidence in litigation [34]. When litigation is anticipated, it is required to put a legal hold on relevant ESI as well in the cloud. Failing to maintain relevant ESI, e.g. deletion by routine operation policy, would result in potential spoliation claims.

Further, the users of EHR data have access and control of their accounts and the information. However, it is possible they may delete some information without realizing that such information could be relevant to anticipated legal issues and should be preserved. Under this circumstance, it is necessary to determine whether the users have a duty to preserve the information and whether it is reasonable to foresee that the information is in the scope of discovery [40].

These issues regarding data preservation in cloud environment by the third party service provider and data control are not taught in many universities as of yet and we suggest that they should be required.

Thresholds of relevancy for evidence to be admissible

Courts are determining on a case-by-case basis whether a person's claim of privacy is reasonable [33]. Courts have continued to be opposed to the notion that any protectable privacy interest exists in material posted on social network websites related to health record, for example, in Fawcett v. Altieri, the court reasoned that, "if you post a tweet, [it is] just like you scream it out the window, [and] there is no reasonable expectation of privacy." Effective and efficient approaches to determine a "threshold" showing of relevancy for evidence to be admissible are required when concerned about the impact of privacy interests.

Review and Conclusions

This review indicates that there are some "common" issues shared with e-discovery in EHR systems, cloud computing and big data, particularly the attention and emphasis on the needs for organizational policy updates for integrating e-discovery requirements into regular operations and workflows while advances on technical and information privacy are the other two sides. Information is the core in any discovery-related procedure, thus information governance composed of technical and managerial issues would be important for students to understand. We summarize the above discussion in a framework (See Table 1). The framework can be used for potential short course-design on e-discovery and security in the healthcare domain.

This study provides a broad view and better understanding of the critical and urgent issues on e-discovery

Table 1 Framework of key issues for e-discovery in EHR

Domains		Key issues
EHR Systems	Development in EHR	Techniques in EHR systems to facilitate e-discovery
		Information sharing and data interoperability
		Metrics for EHR systems quality control
		Clinical practice guidelines (CPGs) to optimize EHR system use
		Audit trails/metadata search techniques
		Advances in Health 2.0
	E-Discovery policy and strategy	Policies and processes for electronic records management
		Economics of cost
		Legal hold policies to handle preservation of relevant documents
	Security and privacy	Information privacy and data confidentiality
		Access controls and policies for EHR
		Management of patient consent
		HITECH and HIPAA privacy and security rules
Cloud Computing and big data		Data analytics
		Data preservation and control policies
		Thresholds of relevancy for evidence to be admissible

and security focusing on EHR systems. The list of issues can also help healthcare industry for better training of personnel.

It is important to mention that this study was not intended to capture "all of the issues" within given contexts. Nevertheless, it offers an opportunity to build consensus on what is significant and what is urgent in this field. Furthermore, this study would also contribute to developing guidelines for design of courses on e-discovery in the healthcare domain. In the long term with the increasing rate of EHR adoption and EHR meaningful use achievement, new issues and challenges would emerge. Experts from healthcare organizations, legal institutes, and IT professions as well as privacy and data management communities should work closely to draw a detailed education map for this field by sharing different ideas from various orientations.

Endnotes

[a]NAHIT ceased operations in 2009, but it concluded several major US health related initiatives before it ceased. (http://www.healthcareitnews.com/news/nahit-no-more).

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

Author SY carried out the review under the guidance of HRR and SU. All authors participated in the writing of the paper. All authors read and approved the final manuscript.

Acknowledgements

The authors thank the guest editors and reviewers for critical comments that have improved the paper. This research was supported in part by the National Science Foundation under grant # DUE-1241709. The usual disclaimer applies.

Received: 10 June 2014 Accepted: 13 March 2015
Published online: 15 April 2015

References

1. Gensinger Jr RA, Introduction to healthcare information enabling technologies. Chicago: Healthcare Information and Management Systems Society (HIMSS); (2010)
2. C Chen, T Garrido, D Chock, G Okawa, L Liang, The kaiser Permanente electronic health record: transforming and streamlining modalities of care. Health. Aff. **28**, 323–333 (2009)
3. JA Handler, CF Feied, K Coonan, J Vozenilek, M Gillam, PR Peacock, R Sinert, MS Smith, Computerized physician order entry and online decision support. Acad. Emerg. Med. **11**, 1135–1141 (2004)
4. D Blumenthal, Stimulating the adoption of health information technology. N. Engl. J. Med. **360**, 1477–1479 (2009)
5. Strobel CD, American recovery and reinvestment act of 2009 (ARRA09). J Corp Account Finance 20(5):83-85 (2009) (111th US Congress)
6. R Kaushal, AK Jha, C Franz, J Glaser, KD Shetty, T Jaggi, B Middleton, GJ Kuperman, R Khorasani, M Tanasijevic, Return on investment for a computerized physician order entry system. J. Am. Med. Inform. Assoc. **13**, 261–266 (2006)
7. G Paul and B Nearon, The Discovery Revolution: e-Discovery Amendments to the Federal Rules of Civil Procedure, American Bar Association, Chicago, Illinois (2006)
8. Fulton-Cavett AM, Electronic Health Records: Federal E-Discovery Rules and Case Law Are Guides for State Litigation. The Brief, 40 (2011)
9. KB-S Reich, E-discovery in healthcare: 2010 and beyond. Annals. Health. L. **19**, 173 (2009)
10. TR McLean, EMR metadata uses and E-discovery. Annals. Health. L. **18**, 75 (2009)
11. DE Detmer, Building the national health information infrastructure for personal health, health care services, public health, and research. BMC. Med. Informatics. Decision. Making. **3**, 1 (2003)
12. JL Masor, Electronic medical records and E-discovery: with New technology come New challenges. Hastings. Sci. Tech. LJ. **5**, 245 (2013)
13. S Hoffman, A Podgurski, E-Health hazards: provider liability and electronic health record systems. Berkeley. Tech. LJ. **24**, 1523 (2009)
14. S Hoffman, A Podgurski, Meaningful use and certification of health information technology: what about safety? J. Law. Med. Ethics. **39**, 77–80 (2011)
15. R Drummond, EHR certification: getting comfortable with the concept. Health. Manag. Technol. **32**, 26 (2011)
16. Certification Process for EHR Technologies. [http://www.healthit.gov/providers-professionals/certification-process-ehr-technologies]
17. Meaningful Use Definition & Objectives. [http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives]
18. Van De Belt TH, Engelen LJ, Berben SA, Schoonhoven L: Definition of Health 2.0 and Medicine 2.0: a systematic review. J. Med. Internet. Res.**12**, 2 (2010)
19. Patientslikeme [http://www.patientslikeme.com/]
20. Health 2.0 in Wikipedia. [http://en.wikipedia.org/wiki/Health_2.0]
21. Hughes B, Joshi I, Wareham J: Health 2.0 and Medicine 2.0: tensions and controversies in the field. J. Med. Internet. Res. 2008, **10**, 3 (2008)
22. C Dimick, E-discovery: preparing for the coming rise in electronic discovery requests. J. AHIMA. **78**, 24 (2007)
23. Lorraine v. Markel American Insurance Company, 241 F.R.D 534 (D.Md. May 4, 2007)
24. RC Goss, Hot issues in electronic discovery: information retention programs and preservation. Tort. Trial. Ins. Prac. LJ. **42**, 797 (2006)
25. Ray P, Wimalasiri J: The need for technical solutions for maintaining the privacy of EHR. In Engineering in Medicine and Biology Society, 2006 EMBS'06 28th Annual International Conference of the IEEE; New York City. IEEE. 4686–4689 (2006)
26. KT Win, A review of security of electronic health records. Health. Information. Manag. **34**, 13–18 (2005)
27. Norman C: Advances and Challenges in Secure EHR Access. CEISARE's Information Assurance Program 2012, (2012)
28. Yuan E, Tong J: Attributed based access control (ABAC) for web services. In Web Services, 2005 ICWS 2005 Proceedings 2005 IEEE International Conference on IEEE; Los Alamitos. IEEE. (2005)
29. Ferraiolo D, Cugini J, Kuhn DR: Role-based access control (RBAC): Features and motivations. In Proceedings of 11th annual computer security application conference. IEEE Computer Society Press; Los Alamitos. IEEE. 241-248 (1995)
30. E Coiera, R Clarke, e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment. J. Am. Med. Inform. Assoc. **11**, 129–140 (2004)
31. MM Richards, Electronic medical records: confidentiality issues in the time of HIPAA. Professional. Psychol. Res. Practice. **40**, 550 (2009)
32. PLC CGSB, Client Alert: HITECH Act Expands HIPAA Privacy and Security Rules. In Book Client Alert: HITECH Act Expands HIPAA Privacy and Security Rules. Coppersmith Gordon Schermer & Brockelman PLC; Phoenix (2009)
33. Ashish S. Prasad, Cloud computing and social media: Electronic discovery considerations and best practices. Metropolitan. Corporate. Counsel. 26–27 (2012)
34. Alberto G. Araiza, Electronic Discovery in the Cloud, 10 Duke Law & Technology Review 1–19 (2011)
35. Singh S, Singh N: Big Data analytics. In Communication, Information & Computing Technology (ICCICT), 2012 International Conference on; 19–20 Oct. 2012. IEEE; Mumbai. IEEE. 1–4 (2012)
36. Ingram B: Controlling E-discovery costs in a big data world. Peer Peer. http://www.lexisnexis.com/pdf/Litigation/ArticleILTAPeer2Peer-ControllingEDSCCostsinaBigDataWorld-Ingram032013.pdf (2013)
37. JG Browning, Digging for the digital dirt: discovery and use of evidence from social media sites. SMU. Sci. Tech. L. Rev. **14**, 465 (2010)
38. A Sanfilippo, N Gilbert, M Greaves, Technosocial predictive analytics for security informatics. Security. Informatics. **1**, 1–3 (2012)
39. C Pham, E-discovery in the cloud Era: what's a litigant to do. Hastings. Sci. Tech. LJ. **5**, 139 (2013)
40. 2013 Year-End Electronic Discovery and Information Law Update. [http://www.gibsondunn.com/publications/pages/2013-Year-End-Electronic-Discovery-InformationLaw-Update.aspx]