Safeguarding patient privacy in electronic healthcare in the USA: the legal view

Diana Walsh* and Katia Passerini
School of Management
New Jersey Institute of Technology
Newark, NJ 07102, USA
E-mail: WalshD@njit.edu
E-mail: pkatia@njit.edu
*Corresponding author

Upkar Varshney
Computer Information Systems
Georgia State University
Atlanta, GA 30302, USA
E-mail: uvarshney@gsu.edu

Jerry Fjermestad
School of Management
New Jersey Institute of Technology
Newark, NJ 07102, USA
E-mail: Fjermestad@adm.njit.edu

Abstract: The conflict between the sweeping power of technology to access and assemble personal information and the ongoing concern about our privacy and security is ever increasing. While we gradually need higher electronic access to medical information, issues relating to patient privacy and reducing vulnerability to security breaches surmount. In this paper, we take a legal perspective and examine the existing patchwork of laws and obligations governing health information in the USA. The study finds that as Electronic Medical Records (EMRs) increase in scope and dissemination, privacy protections gradually decrease due to the shortcomings in the legal system. The contributions of this paper are (1) an overview of the legal EMR issues in the USA, and (2) the identification of the unresolved legal issues and how these will escalate when health information is transmitted over wireless networks. More specifically, the paper discusses federal and state government regulations such as the Electronic Communications Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA) and judicial intervention. Based on the legal overview, the unresolved challenges are identified and suggestions for future research are included.

Keywords: electronic healthcare; privacy; security; confidentiality; electronic medical records; EMRs; electronic health records; EHRs; Health Insurance Portability and Accountability Act; HIPAA.

Copyright © 2008 Inderscience Enterprises Ltd.
1 Introduction

1.1 Privacy and security issues in electronic healthcare

Personal privacy is sacred within most cultures around the world but today’s technology and digital repositories have led to a significant invasion of what heretofore was privately possessed and guarded information (including our needs, tastes, and monetary status). This is especially evident with personal medical information and patient records,
which are accessible to thousands of outsiders such as physicians, hospitals, Health Maintenance Organizations (HMOs), insurers, pharmacies, government agencies, pension funds, and employers who generate and/or process it.

The desire to protect individual privacy is a worldwide phenomenon. Almost all countries have enacted laws dovetailing privacy principles espoused by the Organization for Economic Cooperation and Development (OECD) guidelines, the Council of Europe, and the European Union (EU). In the USA, privacy, as a legal concept, can be traced to a Harvard Law Review (HLR) article published in 1890. The essence of the HLR article is that an individual has the right not to have one’s thoughts, statements or emotions be made public without his consent (Thomas, 1946; Culnan, 2006; Culnan and Armstrong, 1999). The notion of ‘consent’ is therefore inherently connected to that of privacy.

Closely allied to the issue of privacy is that of the installation and maintenance of security of the information systems that create, store and transfer sensitive patient data. In the world of the internet, the interconnectivity of computers makes security particularly vulnerable to invasion by traceable and, at times, non-traceable sources. Within seconds, a computer virus may seriously affect enormous numbers of computers globally. System overloads, hardware and software malfunctions, the ordinary difficulties brought about by weather, fire, floods, and the many other physical occurrences that can damage essential records, contribute to this vulnerability. Questions arise on which entity is responsible for data rescue or replacement. Is the responsibility of the network connectivity provider? Is the computing equipment provider responsible?

While security is mostly a technical problem, the establishment of privacy rules, policies and practices is a prerequisite for safeguarding personal data. In fact, highly secure systems may not safeguard privacy if they are not built in compliance with privacy principles. This is why it is important to understand the legal framework before dealing with technological issues. In this paper, we do just that by identifying the general rules and regulations that are currently in place to protect the security of personal medical information. We focus on Electronic Medical Records (EMRs) and their extensions. The overview of fundamental and evolving US legislation constitutes the basis for better understanding the technological implications of managing patient information in healthcare. The objective is to understand the legislative shortcomings not addressed by current regulations. These shortcomings can then be used to inform improved design, implementation, adoption and use of EMR and other e-health systems. The contributions of this paper are:

• an overview of legal EMR issues in the USA
• identification of the unresolved legal issues and how these will impact as health information is being transmitted over wireless and mobile networks.

More specifically, the material includes federal and state government regulations such as the Electronic Communications Privacy Act (ECPA), Health Insurance Portability and Accountability Act (HIPAA), and judicial intervention. Based on the legal overview, unresolved challenges are identified and suggestions for future research are included. It is our sincere hope that this work will motivate researchers to conduct further research in addressing the open challenges identified in this paper. As a result, the government, regulatory bodies and healthcare entities may also move to address these shortcomings more effectively.
1.2 Electronic medical records privacy and security issues

In our study of privacy and security issues, we specifically focus the discussion on EMRs because of the increasing roles that digital databases of patient information are playing both in the USA and other healthcare markets (notably in Europe). EMRs are records that contain digitally stored medical healthcare information of individuals, including the history of the individual’s contacts with the healthcare system. EMR systems are usually managed within a single hospital information system and its connected entities. EMRs are somewhat different from Electronic Health Records (EHRs). EHRs are made up of information systems incorporating personal information records from multiple healthcare facilities and include a history of the patient interactions with the healthcare system. It is anticipated that by the year 2014, EHRs will replace EMRs. The goal of EHRs is to merge medical history of patients into electronic information system records and to make that information available nationally regardless from where patients receive treatment. In this way, health professionals have online access to comprehensive and current health records (HIMSS, 2007; Dunlop, 2007; Garets and Davis, 2006).

According to the California Telemedicine & eHealth Center (CTEC), the term EHR is largely replacing the older term EMR and the two can be used interchangeably. In this paper, we maintain our focus primarily on EMRs. This is because the transition to a national health record is still ongoing and many of the legislative loopholes herein identified are slowing the establishment of EHRs. In contrast, the development of EMRs is reaching plateau. Some European countries are reporting EMRs penetration of about 90%, while others are currently hitting the same mark with an 8%–9% growth rate each year. EMRs are regarded as one of the ‘most important’ health information technology developments in the next five to seven years (Frost & Sullivan, 2007). Figure 1 shows the estimated market growth of EMR revenues for Europe through the average compounded annual growth rate (Kem and Jaron, 2003).

Figure 1 European EMR market revenue forecasts 2006–2013 (see online version for colours)

<table>
<thead>
<tr>
<th>Year</th>
<th>Revenues ($ Million)</th>
<th>Growth Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>200</td>
<td>18</td>
</tr>
<tr>
<td>2007</td>
<td>400</td>
<td>16</td>
</tr>
<tr>
<td>2008</td>
<td>600</td>
<td>14</td>
</tr>
<tr>
<td>2009</td>
<td>800</td>
<td>12</td>
</tr>
<tr>
<td>2010</td>
<td>1000</td>
<td>10</td>
</tr>
<tr>
<td>2011</td>
<td>1200</td>
<td>8</td>
</tr>
<tr>
<td>2012</td>
<td>1400</td>
<td>6</td>
</tr>
<tr>
<td>2013</td>
<td>1600</td>
<td>4</td>
</tr>
</tbody>
</table>

Note: All figures are rounded; the base year is 2006.

Source: Frost & Sullivan (2007, p.37)
In order to achieve the growth identified in Figure 1, a number of issues need to be addressed. For example, the creation of unique patient identities that can be carried across nations; the protection of privacy through secure systems; the training and certifications of the people involved in EMR implementations, and the adoption of supra-national standards to ensure the portability of the records. Among these issues, privacy and security appear the most complicated, given the high standards of privacy protection and various regulations that characterise EU member countries.

For example, in 1995 the EU Directive on the Protection of Personal Data was passed (European Parliament and Council Directive 95/46/EC 24 October, 1995). The directive requires that EU Member States bring their national laws, regulations and administrative provisions into alignment with the framework of established principles presented in the directive itself. Beyond the EU, the Code of Fair Information Practices is another internationally recognised set of privacy principles developed by the OECD. Furthermore, the international application of tort liability is growing in significance and controversy. US plaintiffs may sue foreign or US entities for torts that these entities have allegedly committed overseas. The Alien Tort Claims Act, 28 USC §1350, adopted in 1789, allows even foreign citizens to bring civil suit in US courts for injuries caused by violations of the law of nations or a treaty of the USA. The principles embedded in these regulatory enactments generally safeguard personal privacy and require that only information that is really needed be collected directly from the individual to whom it pertains.

2 Legal EMR issues in the USA: overview

Unlike the healthcare systems of many western countries, the US system is composed of private, independent individual and group providers, hospitals, ambulatory care and long term care centres that compete with one another. It is not centralised but has multi-payers of insurance bills and multi-health providers, all subject to different rules and laws. Moreover, many competing vendors, each with their own products, exist. Additionally, large private data collection agencies, such as ChoicePoint and Acziom, can obtain, analyse, and sell individuals’ data.

In this context, information technology intervenes to support a transition from a single patient health record (or a collection of patient information) to a multi-function health data repository which is to be designed ‘to protect and to promote population health for the greatest good of society at large’. As a result of this transition, the right of individuals to control the use and circulation of their personal information is gradually diminished, while potential risks for the inappropriate management of private personal information are increased through access and/or disclosure of medical information. For example, decisions about the adoption of information technology are made independently and there are few – if any – incentives to share information concerning patient care.

The USA has a confusing, sometimes conflicting, patchwork of federal and state laws, as well as administrative agencies that deal with the protection of information. In the next sections, we provide an overview of the legal framework involving federal and state regulations, and discuss the judicial decisions that defined the boundaries of individual privacy rights protection of the privacy rights of individuals, and notably personal medical information, over the years.
2.1 The US Constitution and the right of privacy

There is no right of privacy explicitly stated in the Constitution of the USA and this might be one of the reasons for the development of a complex legal framework dealing with privacy in the US legal system. Since the Constitution is a legal contract between the people and their government, individuals have absolute rights only against their government. In essence, governmental intrusion is more constitutionally scrutinised than private conduct. As a result, the legislative branches of federal and state governments are struggling to balance the need to guarantee the accessibility of information when it involves private individuals’ data, especially when the data has been misused and has caused personal damages against the ‘common good’. On the other hand, private individuals, a natural person or a legal entity, do not have the same absolute rights against each other and judicial intervention settles disputes. It is then up to the court to decide, case by case, what degree of intrusion upon personal privacy will be constitutionally permissible.

Courts have increasingly examined the conflict between governmental authority and individuals’ right of privacy. In a line of judicial decisions, the US Supreme Court endorsed the view that the Constitution protects individual privacy rights. In *Griswold v. Connecticut*, 381 US 479 (1965), the Supreme Court held that a constitutional right of privacy was implied by the First, Third, Fourth, Fifth, and Ninth Amendments. The Ninth Amendment establishes that the people have rights in addition to those specified in the Constitution.

What about ‘personal security’? Under the Due Process Clause of the Constitution, the Sixth Circuit in *Akella v. Michigan Department of State Police* (1999) noted in the *Kallstrom* case that “individuals have a clearly established right to personal security and to bodily integrity and this right is fundamental where the magnitude of the liberty deprivation that the abuse inflicts upon the victim strips the very essence of personhood”. The *Kallstrom* case involved the City of Columbus disclosure of personal information contained in a police officer’s personnel file to defense counsel during a criminal trial in which the officer testified against the defendants. When personal information is already a matter of public record, the Supreme Court held that such personal information needs not to be protected. This decision applies to related EMRs issues as well, and opens a number of unanswered questions:

- Are medical records a matter of public record when they are available at governmental agencies or health entities?
- Does a privacy right of an individual outweigh the greater good for society that may come from the collection of such data, or does it risk targeting individuals for any medical reason?
- Which outweighs what: individual privacy or efficiency and quality of care for an increasing number of people?

2.2 Federal regulations

Congress members are elected by the people to provide protection by enacting statutes or laws that will reflect and enforce social responsibility for the common good of society at large. Hence, federal laws may intervene to protect the rights of the people. In the late
1960s, society was concerned by the accumulation of personal information in government files and the Congress was pressured to pass legislation permitting individuals to access their files. The Congress responded in 1966 with the Freedom of Information Act that allows any person or citizens to request copies of any information contained in federal government files. In 1974, the Congress passed the Privacy Act giving individuals the right to examine their information held by federal agencies.

In Whalen v. Roe (1977), a New York court held in favour of the Health Commissioner of the State of New York who centrally recorded the names and addresses of persons who had obtained, pursuant to a doctor’s prescription, certain curative drugs. In this case, the prescription of the drugs (such as opium, cocaine and other drugs used to assist in the treatment of a number of disorders) required completing triplicate forms that gave detailed information including the identity of the patient. The forms were filed with the Department of Health, New York State. They were sorted, coded, logged, and recorded on a magnetic tape for retention for a five-year period. Patients and two doctors’ associations sued alleging an unconstitutional invasion of their rights of privacy. As a result of this judicial decision in favour of the Health Commissioner, the privacy provisions enacted by Congress in 1974 to regulate the handling of patients’ information have had limited effect.

Finally, in 1996, the US Congress enacted the HIPAA to address the growing need to safeguard the privacy of individuals’ health records, particularly computerised electronic records. HIPAA requires healthcare providers and healthcare plans, including certain employers who sponsor health plans, to inform patients of their privacy rights and how their personal medical information may be used. Before HIPAA, federal legislation tried to address the financial, technical and confidentiality concerns associated with privacy protection with a series of acts described next.

2.2.1 Privacy Act of 1974

The Privacy Act ensures that federal agencies use fair information practices with regard to the collection and dissemination of any medical information from a system of records. It protects the kind of information collected, the use to which the information is put, the people who have access to the information, the disclosure, the means used to gain the information, the steps taken to ensure the accuracy and completeness of the information and the access that individuals have to information about themselves. After the Privacy Act, the Computer Matching and Privacy Protection Act of 1988 was enacted, which further regulates an agency’s disclosure of records “for use in a computer matching program… [by another] agency or non-Federal agency” (USC 552a 2000).

The Privacy Act prohibits the disclosure of personal information to another person or agency without ‘written consent’ of the individual to whom the information relates. An individual is allowed to review, copy, and correct mistakes in records belonging to that individual. Agencies are allowed to keep information that is necessary for the purpose of the agency. In addition, there are substantial exceptions to enforcement activities. The Privacy Act regulates only the use of medical information by federal agencies and their contractors. The Privacy Act does little to protect the privacy of medical information that is not stored by governmental agencies. The Privacy Act does not cover a private entity that plans to store medical information in computerised systems at a centralised location nor defines security measures to protect the privacy of medical information.
during transfer from one governmental agency to another. Even though a written consent is required before disclosure, nothing in the Privacy Act regulates how such information should be disclosed to protect privacy.

2.2.2 The Electronic Communication Privacy Act of 1986

The ECPA prohibits any person from knowingly revealing to any other person the contents of an electronic communication while that communication is in transmission (and not in electronic storage). Electronic communications through devices ‘furnished to the subscriber or user by a provider of wire and electronic communication services’ and used by the subscriber or by the provider of the service ‘in the ordinary course of its business’ are excluded from coverage. In *Frazer v. Nationwide Mutual Insurance Co.* (2004), an independent contractor named Frazer worked in his own office from a separate location, but Nationwide provided Frazer with an e-mail address and server. Nationwide terminated Frazer’s contract. In the lawsuit that followed, the appellate court ruled that Nationwide had not violated ECPA. To violate the statute an intercept must occur ‘contemporaneously with transmission’ that is, at the same time that it is sent. In addition, Nationwide was the entity that provided the e-mail service and had maintained the information in electronic storage. Therefore, there was no privacy invasion under the ECPA. This legislation only protects individuals while the personal medical information is ‘in transmission and in digital form’ and not in storage or printed form.

2.2.3 Americans with Disability Act of 1990

The Americans with Disabilities Act (ADA) also does very little to protect medical information. The ADA keeps employers from pre-screening prospective employees through the use of medical information and from discriminating against individuals because of their disability. The covered entities under ADA may only inquire about the job applicants’ medical information in reference to their ability to perform job-related functions and not whether applicants are disabled (42 USC 12101–12112 (2000)). Upon an offer of employment, covered entities may also demand medical examinations and, during the course of employment, conduct medical examinations. The act is also limited to what is classified as ‘disabilities’ and not health information. The ADA does not regulate computerised medical information that employers can request to electronic data holders. It does not require any security measures to protect the privacy of the medical information during transmission from any healthcare providers to the employers.

2.2.4 Health Insurance Portability and Accountability Act of 1996 Privacy Rule

Responding to the growing need to protect the privacy of individuals’ health records, particularly computerised records, in 1996, Congress passed the HIPAA, which took effect on April 2003. HIPAA defines and limits the circumstances in which an individual’s ‘Protected Health Information (PHI)’ may be used or disclosed.

The HIPAA and its Privacy Rule could be defined as the first comprehensive Federal protection for the privacy of personal health information. HIPAA is a statute designed to establish a set of basic federal guidelines to limit the use and disclosure of PHI. PHI is individually identifiable health information that is transmitted by electronic media,
maintained in electronic media, or transmitted or maintained in any other form or medium. Although typically used to refer to medical history, PHI also includes any data that may reasonably identify a patient.

HIPAA’s federal rules specify a series of administrative, technical, and physical safeguards, organisational and documentation requirements to assure the availability, confidentiality, and integrity of electronic protect health information. HIPAA directly governs ‘covered entities’, which may be anyone who provides, furnish or receive payment for medical services (Gerberry, 2002). An objective of HIPAA Privacy Rule is to ensure confidentiality, integrity and availability of all electronic PHI a ‘covered entity’ creates, receives, maintains, or transmits. In HIPAA, the meaning of privacy is the ability of an individual or group to exclude others from accessing one’s own personal information, and thereby reveal personal information only selectively. In contrast, confidentiality prevents any disclosure, to others than authorised individuals, of individual’s or group’s proprietary information, investigation findings, or of an individual’s identity unless previously consented by the individual (Dunlop, 2007).

HIPAA also contains provisions that affect employer-sponsored group health plans. HIPAA specifically provides that group health plans and health insurers may disallow coverage for preexisting conditions only if:

- the exclusion related to a condition for which medical advice, care, and the like was given within the preceding six months
- the exclusion does not extend beyond a twelve month period
- the said period of exclusion is reduced by the aggregate of the period of creditable coverage.

Genetic information in the absence of a condition having arisen as a result of the predisposition may not be a basis for denial of insurance coverage. Exceptions to privacy protection are:

- public health activities
- disclosure for health oversight purposes
- use for judicial and administrative proceedings and for use by coroners and medical examiners
- disclosure to law enforcement
- government health data systems and health directories
- disclosure for banking and payment purposes
- medical research (Girasa, 2002).

Covered entities must formulate written privacy policies, designate privacy officials, limit access to computerised health data, physically secure medical records with lock and key, train employees and volunteers on their privacy policies, and sanction those who violate the policies (Clarkson et al., 2006). HIPAA mentions ‘business associates’. These business associates perform activities for, or provide services to, covered entities. Business associates must provide covered entities with ‘satisfactory assurance’ regarding PHI use and disclosure. Should the relationship expire, the business associates must
destroy or return the covered entity’s PHI (45 C.F.R.45 CFR §164.502(e) (2006)). However, HIPAA does not directly regulate ‘business associates’. The statute only requires covered entities to monitor business associates behaviour, uncover potential wrongdoing, and safeguard confidentiality.

In summary, while this legislation finally addresses the issue of computerised health records more holistically than previous acts, it seems more focused on articulating procedures that ultimately protect ‘covered entities’ (insurance companies, health providers, health plans) from liability rather than protecting the individual patients. The patient no longer enjoys a patient-doctor relationship nor has any control over his or her personal medical information. Recent reports describe a widespread frustration with the unintended consequences of HIPAA, which is being interpreted so restrictively by healthcare providers that deny access to medical information also to family members inquiring about patients’ surgical outcomes. While HIPAA has made ‘confidentiality’ a priority in the computerised-medical records era, its attempt to safeguarding electronic privacy have led to overly complex procedures that may actually deny effective access to medical information even to members of the same household (Gross, 2007).

2.3 State regulations

The Fourteenth Amendment to the Constitution provides that states shall not deprive any person of life, liberty or property, without due process of law. Today, most of the rights and liberties set forth in the Bill of Rights apply to state government. Therefore, state legislation is also needed to protect individuals’ privacy rights. Federal laws will only supersede state laws, when ‘covered entities’ cannot comply with both federal statutes and state laws at the same time. However, state laws can and must be more stringent than federal laws. For example, HIPAA will not supersede more stringent state laws. Rigid state laws usually contain tougher restrictions and may allow individuals broader rights to access or amend their records.

To deal with the problem of conflicting state laws, the National Conference of Commissioners on Uniform State Laws proposed the Uniform Health Care Information Act (UHCIA) for adoption by the states. This statute is designed to serve as a model for state regulatory protections of disclosure of medical information. Adopting UHCIA will make protection uniform but not necessarily provide privacy of the individuals’ medical records. The UHCIA requires healthcare providers to have ‘reasonable safeguards’ but the Act does not define what ‘reasonable safeguards’ are. Very few states have adopted the UHCIA to date. Some states simply follow the protection of medical information guidelines implied in federal regulations.

2.4 Judicial intervention

Privacy rights are also protected under tort and contract laws. The basic purpose of these laws is to provide compensation for the invasion and breach of various protected interests. These protected interests include certain intangible interests such as personal information privacy, family relations, confidentiality reputation, and dignity. State tort law for example, safeguards privacy rights through the tort of invasion of privacy and may vary significantly from state to state (Clarkson et al., 2006). Under tort law, unlawful invasion of privacy is expressed four ways:
1 “The use of a person’s name, picture, or other likeness for commercial purposes without permission.”
   - Using without permission someone’s picture to advertise a product or someone’s name to enhance a company’s reputation invades the person’s privacy.
     a With reference to EHRs, if a hospital used a picture of a patient retrieved from EHR without the consent of the patient to demonstrate EHR advancements and the state-of-the-art health information system of the hospital to prospective patients, this would fall under tort law protection.

2 “Intrusion on an individual’s affair or seclusion.”
   - For example, invading someone’s home or illegally searching someone’s briefcase is an invasion of privacy. This tort has been extended to eavesdropping by wiretap, unauthorised scanning of a bank account, compulsory blood testing, and window peeping.
     a In the EHR context, this would include unauthorised access to an individual health records as in the example listed next in the Korntved v. Advanced Healthcare, S.C., and Midwest Medical Insurance Company. In this case, an employee of a health provider accessed EHR records for purposes outside the scope of employment. More specifically to verify the legitimacy of health insurance claims and the related amount of spousal support being charged by the patient to her ex-husband, now remarried to an employee. Several other examples could apply to unauthorised screening EHR records for the purposes of employment or the like.

3 “Publication of information that places a person in a false light.”
   - This could be a story or any information attributing to someone’s ideas not held or actions not taken by that person.
     a It could include listing a patient into an infectious diseases national database by virtue of an error in the patient EHR. The patient may be prevented from travelling or enjoying other rights until the error is recognised and amended, which may also take a significant amount of time.

4 “Public disclosure of private facts about an individual that an ordinary person would find objectionable.”
   - For example, disclosure of personal medical information of a private citizen could be an actionable invasion of privacy.
     a This may be limited to ‘ordinarily objectionable data’ (i.e., list of patients who underwent gender-change operations) or any private information that an individual would have not consented to disclose and whose disclosure could be challenged under tort law.

In 2005, a published opinion by the appellate state courts of Wisconsin, demonstrates the complexity of state laws and liabilities applied to individual cases decided by judges. The plaintiffs in Korntved v. Advanced Healthcare, S.C., and Midwest Medical Insurance
Company, filed a complaint against Advanced Healthcare and Midwest Medical Insurance Company, listing several claims: breach of confidentiality; breach of right of privacy; breach of physician-patient privilege; breach of contract; negligent supervision and/or hiring and/or training; and failure to maintain the standard of care under HIPAA. Breach of confidentiality is a violation of Wis. Stat. §146.82 which provides that patients’ healthcare records shall remain confidential and may be released only to designated persons or persons authorised by the patient.

The plaintiff contended that there were material facts in dispute as to whether the Advanced Healthcare’s employee was acting within the scope of employment as defined by the state statutes, when she accessed medical information of her spouse’s ex-wife. Both the trial and the Appellate court ruled in favour of Advanced Healthcare, which was held not liable for its employee access of the plaintiff’s medical records. Access was committed outside the scope of employment as Advanced Healthcare had an express policy forbidding the retrieval of patients’ medical records for non-work related purposes. The rights of an individual were superseded against general economic/business needs (or in other cases, public health needs) even in a case when the provider (Advanced Healthcare) was unable to demonstrate due care in protecting health records or due care in supervising their employees’ access to the same. The mere issuance of a policy was deemed a sufficient ‘reasonable measure’ to forego Advanced Healthcare’s liability.

2.5 Summary of the legal overview

A centralised healthcare information network offers an abundance of promises. It will empower authorised users to access health information from anywhere and at anytime, especially at the moment of need. It will revolutionise how patients, providers, and others interact within the healthcare system. This will improve efficiency and quality and may reduce costs and medical errors. However, the centralised network will also present federal and state governments with grave challenges, most notably in privacy protection. Individuals perceive the increased use of electronic information system as one of the greatest threats to their privacy. Unfortunately, our review of the legal framework, which is summarised in Figure 2, reveals various shortcomings. Starting from the US Constitution and moving through federal, state and tort laws, the protection of the rights of individuals, especially in the area of health information, seems to remain a patchwork of conflicting laws that vary from state to state.

Many legislative bills have been enacted, from 1974 onwards, to address the need for patient safety and privacy. However, all these federal legislative measures have not eliminated the risks and the harm that may be caused to the individual when personal health information may need to be surrendered in case of economic and public health concerns (i.e., infectious diseases, etc.). In order to guarantee the individual right to the protection of personal information, current shortcomings need to be overcome and a patient-centric rather than a provider-centric view of data needs to be espoused. We discussed some of the relevant regulatory measures dealing with privacy of patient data, as well as their limitations. Our analysis identifies a number of unresolved issues.
3 Unresolved issues

Patients’ health information will cross many departmental barriers. Health information may include x-rays, diagnostic test results (e.g., HIV status), medical procedures such as abortions, psychological testing results, even genetic invasion, and many other aspects that patients perceive as private. Having as a requisite the ‘consent’ of a patient before health providers can include a patient’s information in an EMR information system record and/or releasing it to others indiscriminately may be helpful to individuals who desire to maintain some control over their personal health information (Dunlop, 2007). However, EMRs may not be secure. Many EMR systems are web-based and hackers may merely need some sniffing equipment to access wireless networks and alter the information while in transmission. From the patients’ view, enforcement is placed in the hands of those who are primarily interested in ensuring efficiency and lower costs, more than attending individual interests.

Furthermore, under the new HIPAA amendments to the Privacy Rule there is no requirement for healthcare “providers in direct treatment relationships” to require formal consent, “before using or disclosing medical information for treatment payment or healthcare operations” (Sarraille and Spencer, 2004). Administrative policies need to be put in place to define the types of information considered confidential; who has access to the medical information; procedures that must be followed to release information; and severe disciplinary sanctions imposed upon those that have access to the medical information and breach security measures (Gerberry, 2002). Mandatory safeguards are needed to decrease risks of privacy invasions. Persons or healthcare entities that violate mandatory safeguards are to be subject to severe criminal and civil penalties. Only severe penalties and jail time, when enforced, will efficiently deter violations.
The problem is that the current HIPAA provisions are somewhat lenient. HIPAA provides that a person who ‘knowingly’ obtains individually identifiable health information has to pay a fine of not more than $50,000 and to serve up to one year imprisonment under criminal law. These penalties increase to $250,000 and up to ten years in prison if the wrongful behaviour involves “intent to sell, transfer, or use the individual health information for commercial advantage, personal gain or malicious harm” (42 USC 1320d-6(b) (2000)). Additional penalties may apply when medical information is ‘negligently’ misused (Piller, 1999). Healthcare entities and covered entities that fail ‘negligently or knowingly’ to comply with safety provisions may be subject to penalties. Surprisingly, HIPAA imposes only $100 fine per failure not to exceed $25,000 per year for multiple violations of the identical requirement.

These shortcomings are even more evident with the rapid move toward wireless communication systems, whereby nurses and doctors will update and access patient medical information through portable computers (Datamonitor, 2001; Varshney, 2006). Wireless networks utilise radio frequency that are shared in order to move data, thus security concerns are high (Delio, 2001). Federal and state regulations must protect personal medical information from invasion by regulating the use of wireless communications systems and mandating the use of security devices. The regulations must establish electronic security measures prior to the use of wireless communication systems and protect the transmission and storage of medical information. The regulations have to outline minimum security procedures, rather than leaving the definition of ‘reasonable’ security actions to the covered entities, which as seen in the 2005 Korntved v. Advanced Healthcare were limited to a mere policy statement. However, from the providers’ view, HIPAA regulations have only added another layer of detailed rules, yet they have not substantial efficiency. This barrier to implement EMRs may disappear overtime as security mechanisms become more sophisticated, but it is currently an issue that needs to be addressed uniformly and with the same/comparable standards across providers.

4 Conclusions and future research

With the advancement of technology, EMRs will become the norm of storing and sharing health information across many healthcare providers, facilities, including those engaged in health system planning and research. This trend provides a great benefit to patients’ healthcare by reducing the probability of medical errors, but may impact privacy protection. In the USA, it is up to the state courts through tort law and, ultimately, the Supreme Court to determine the point at which legislations have violated an individual’s privacy rights. The judicial system is increasingly asserting that information should be treated as ‘property’ since it is produced, modified, disseminated, and could be used as an economic activity domestically and globally. If information is treated as ‘property’ issues of ownership emerge on who owns the individual’s health or medical records and their value. Due to the inexorable advances in technology and the data portability advantages, it is becoming less clear who are the ultimate owners of medical information. The only requirement is that individuals voluntarily choose to release to healthcare providers their personal information. This choice occurs through the signing of an ‘informed consent’. Paradoxically, without the patient’s consent, healthcare providers either cannot or will not provide services.
Also federal and state regulations are behind technological advances. The federal government is asserting its role as a broker of information which flows within healthcare settings and, therefore, public law is assuming greater prominence within health law but its efficacy is still limited. This role is also stirring additional controversy, especially when there is a lack of national uniformity in regard to regulations that apply to collection, use and disclosure of health information, including EMR systems.

As we grow comfortable with the instant convenience that computers and wireless technologies provide, issues of privacy, particularly in data accumulation, continue to cause concern. EMRs are transforming healthcare delivery. Stricter regulations that address privacy concerns and minimum security standards (for example, similar to the Sarbanes-Oxley regulations) are indispensable. In addition, higher legal safeguards and sanctions concerning those who are involved in establishing privacy rules, consent processes and security systems must be implemented. Without these essential changes EMRs may put at risk the societal and constitutional pillar of personal privacy. To address these challenges, we presented and discussed legal EMR issues in the USA and identified several unresolved legal issues. We hope that the summary of the legal overview and the unresolved challenges may become the basis for both new research in this area as well as improvements in privacy and security in e-health by governments and healthcare entities.

Additional future research can span from several of the unresolved issues and may also pose new challenges. For example, we focused this analysis on the legal system of the USA, with brief references to international legislative interventions in other countries. Issues faced within the EU with regard to trans-border data flows would also be relevant when exchanging data across countries (i.e., US citizens travelling abroad and in need of emergency access to medical data contained in a US-database). The legal and technical ramifications of sensitive data breaches across countries, and the applicable jurisdiction, are open to extensive review. This is a particularly timely problem with the rise of ‘medical tourism’ which is the practice to travel to a developing country to obtain treatment that would be cost-prohibitive in the USA. Health insurance providers are still struggling to define policies that may accommodate the various repercussion of treating patients in multiple countries and across multiple legal systems.

Another interesting stream of research refers to design science and application development whereby we need to understand the complexities of global electronic health data management (already in place for military personnel) and design specific systems that may be able to address several of the technical challenges of global health information systems that may be further complicated by the spotty legal developments discussed in this paper. These issues and more open interesting avenues for future research.

References


