Notre Dame Journal of Law, Ethics & Public Policy

Volume 25
Issue 2 *Symposium On Health Care: Health, Ethics, & the Law*

Article 11

January 2014

Exploring the Barriers to the More Widespread Adoption of Electronic Health Records

Jacqueline Klosek

Recommended Citation

Jacqueline Klosek, *Exploring the Barriers to the More Widespread Adoption of Electronic Health Records*, 25 Notre Dame J.L. Ethics & Pub. Pol'y 429 (2012).
Available at: http://scholarship.law.nd.edu/ndjlepp/vol25/iss2/11

EXPLORING THE BARRIERS TO THE MORE WIDESPREAD ADOPTION OF ELECTRONIC HEALTH RECORDS

JACQUELINE KLOSEK*

Sally has been suffering from a number of troubling medical problems. The quality of her work and personal life has been impacted negatively by intermittent digestive distress, migraines, sinus trouble, and most recently, tingling sensations in her extremities. Despite earnest efforts, she has not been able to find a lasting solution to what ails her. The wide range of her symptoms has prompted her to see her primary care physician as well as a gastroenterologist, ear, nose and throat specialist, neurologist, and a psychiatrist. While she searches for a diagnosis and treatment that will bring her some relief she has been frustrated by the need to repeat her medical history to each new doctor she sees. At each new appointment with a specialist, Sally attempts to provide the new doctor with a rapid verbal download of not only her current symptoms but also a quick summary of the doctors she has already seen, the tests that have been performed, and the treatments she has tried.

Inevitably, this undertaking has left Sally and her specialists frustrated. At some appointments, Sally has forgotten the key details of her prior tests and procedures. In other appointments, her physicians have run out of time to take down the long, convoluted verbal history, or have wanted to commence his or her own physical examination of Sally, with a request that Sally follow-up with a copy of her previous doctors.

To her credit, Sally has attempted to improve this process by arranging for copies of her previous medical records to be sent to her new specialists. This, too, has usually proven to be ineffectual. Sometimes, the records would fail to arrive in sufficient time to allow the specialist to review them before Sally's consultation. Other times, the notes were incomplete or illegible and still other

* Jacqueline Klosek is Senior Counsel with Goodwin Procter LLP in New York and is the author of five books, including the recently published PROTECTING YOUR HEALTH PRIVACY: A CITIZEN'S GUIDE TO SAFEGUARDING THE SECURITY OF YOUR MEDICAL INFORMATION (2010). She may be reached for comment at: jklosek@goodwinprocter.com. The opinions and positions expressed in this Article are solely those of the author and in no way reflect the opinions and/or positions of Goodwin Procter LLP.

times, the specialist did not have the time to go through Sally's voluminous medical file, no matter when it arrived.

Sally, still not feeling well, has grown increasingly frustrated with her efforts to get treatment. She speculates that her specialists would be able to care for her with access to a more complete medical file for her. She wonders why there hasn't been more progress towards the development of a centralized system of electronic medical records so that with a touch of a button her doctors could quickly pull up her complete medical history and see the results of tests performed, the medications prescribed to her, and the treatments attempted.

I. INTRODUCTION

Sally is not the only one to wonder about the lack of a comprehensive, digitized electronic medical record system. Although the United States enjoys automation and interconnectivity in a number of other important aspects of our economy, we have not been able to experience this in a meaningful way with respect to our medical information. With limited exceptions, each time we visit a new doctor, it is as if our medical history is taken anew, typically with our doctors relying upon our verbal descriptions of our previous illnesses, treatments, and current medications. This practice inevitably leads to lost time and wasted resources, and may increase the risks of medical errors and raise the likelihood of duplicative tests and procedures. For years, scholars, researchers, and practitioners have highlighted the problem of a lack of medical information automation.[1]

Other countries have enjoyed a much greater level of success in making the transition to electronic medical records. The United Kingdom, New Zealand, and the Netherlands, in particular, have emerged as leaders in this area, with high rates of electronic health record (EHR) adoption.[2] In the Netherlands, for example, ninety-eight percent of physicians utilize EHRs.[3] By contrast, in the United States, only twenty-eight percent of physicians do.[4]

[1] *See, e.g.*, Edward H. Shortliffe, *Strategic Action in Health Information Technology: Why The Obvious Has Taken So Long*, 24 HEALTH AFF. 1222 (2005); INST. OF MED., THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE (1991).

[2] *See* Rich Daly, *Europe Teaches Lessons on Electronic Records*, PSYCHIATRIC NEWS, Dec. 1, 2006, at 9.

[3] *Id.*

[4] *Id.*

Given the drawbacks of paper-based systems and fragmented electronic systems and the potential advantages of EHRs, this Article examines the possible obstacles to the broader adoption of EHRs in a comprehensive, interconnected way. In doing so, it also explores possible ways to improve the rate of EHR adoption.

II. THE POTENTIAL BENEFITS OF EHRS

The current administration is a strong proponent of EHRs. President Obama has himself declared that EHRs will "reduce error rates, reduce our long-term cost of health care and create jobs."[5] While such a statement might very well reflect a somewhat overly optimistic view of the potential advantages of EHRs in the near future, it is undeniable that more widespread use of EHRs can have a number of positive effects.[6]

EHRs can help to improve the quality of patient care.[7] Just as technology has improved access to information and opened communication channels in other areas, it can generate similar benefits in the area of health care services. When medical professionals have more information about their patients' histories and are better positioned to communicate rapidly and electronically with other medical professionals and with the patients themselves, their ability to provide their patients with the most appropriate care may be improved. Certain studies have confirmed this theory. For example, one recent study by Kaiser Permanente demonstrated that e-mail use between patients with diabetes and hypertension and their physicians resulted in markedly improved quality of care scores.[8]

EHRs may also help to reduce medical errors. According to Dr. Gordon D. Schiff and Dr. David W. Bates, the use of EHRs

[5] Press Release, President Barack Obama, Press Conference by the President (Feb. 9, 2009), *available at* http://www.whitehouse.gov/the_press_office/PressConferencebythePresident.

[6] For a discussion of the potential positive consequences of more widespread implementation and utilization of electronic medical records, see Rodney A. Hayward, *Access to Clinically-Detailed Patient Information: A Fundamental Element for Improving the Efficiency and Quality of Healthcare,* 46 MED. CARE 229 (2008).

[7] *See* CONG. BUDGET OFFICE, EVIDENCE ON THE COSTS AND BENEFITS OF HEALTH INFORMATION TECHNOLOGY 6 (2008), http://www.cbo.gov/ftpdocs/91xx/doc9168/05-20-HealthIT.pdf [hereinafter COSTS AND BENEFITS]; Richard Hillestad et al., *Can Electronic Medical Records Systems Transform Health Care? Potential Health Benefits, Savings, and Costs,* 24 HEALTH AFF. 1103 (2005).

[8] *See* Rob Merkel, *Commentary: Your Stake in Electronic Medical Records,* CNBC (Sept. 2, 2010, 11:36 AM), http://www.cnbc.com/id/38973121/commentary_your_stake-in_electronic_medical-records.

can help to reduce areas of medical error in seven key ways.[9] First, EHRs can help with the filtering, organization, and provision of access to information that physicians and diagnosticians need.[10] Second, EHRs can serve as a platform where medical professionals can document evaluations, develop diagnoses, and note any questions.[11] Third, EHRs can also help medical professionals to document a patient's "evolving history and ongoing assessment."[12] Fourth, if new and improved features develop, EHRs may provide a better mechanism for managing problem lists.[13] Fifth, EHRs can improve medical testing by ensuring a system for fail-safe communication.[14] Sixth, with the use of checklist prompts, EHRs can help to ensure that medical professionals ask key questions and consider all relevant diagnoses.[15] Finally, EHRs can improve patient follow-up and oversight of feedback on diagnostic accuracy.[16]

EHRs may also help to improve the efficiency of health care and to reduce the costs of health care services. One well-cited report claims that effective EMR (electronic medical record) implementation can save more than eighty billion dollars annually.[17] While the aforementioned report has drawn criticism for the magnitude of its claims of cost savings,[18] evidence suggests that EHRs have the potential for generating cost savings in a number of different parts of the health care system.[19] Some of the aspects of EHRs most promising for cost savings may be their abilities to improve access to information and reduce the need for duplicative tests and procedures.

III. Challenges to EHR Adoption

Despite the fact that researchers and practitioners have identified a number of possible benefits to EHRs, a number of factors have challenged the widespread adoption of EHRs. The following sections explore the primary obstacles to EHR adoption:

[9] *See* Gordon D. Schiff & David W. Bates, *Can Electronic Clinical Documental Help Prevent Diagnostic Errors?*, 362 New Eng. J. Med. 1066, 1066–69 (2010).

[10] *Id.* at 1066.

[11] *Id.* at 1067.

[12] *Id.* at 1068.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *See* Costs and Benefits, *supra* note 7, at 4.

[18] *See, e.g.*, David U. Himmelstein & Steffie Woolhandler, *Hope and Hype: Predicting the Impact of Electronic Medical Records*, 24 Health Aff. 1121, 1122 (2005).

[19] *See* Costs and Benefits, *supra* note 7, at 6–17.

financial costs of system acquisition and implementation, implementation challenges, and privacy and data security concerns.[20]

A. *Financial Costs*

One of the most significant barriers to more widespread EHR adoption has been cost. The average cost for setting up a new EHR system in a physician's office is $38,000.[21] Of course, costs are higher for larger organizations, such as multi-physician practices, clinics, and hospitals. Furthermore, in addition to the initial costs of the system, physicians have start-up costs, such as those of data conversion and lost productivity, plus ongoing costs, such as those related to software maintenance and data storage.

In recognition of the potential benefits of EHRs, the Obama Administration has taken a number of steps intended to stimulate the use of more widespread adoption of EHRs. The most significant recent development in this regard has been the enactment of the American Recovery and Reinvestment Act of 2009 (ARRA).[22] In the ARRA, Congress has charged the Office of the National Coordinator for Health Information Technology (ONC) with encouraging physicians to adopt EHR technology.[23]

The Health Information Technology for Economic and Clinical Health Act (HITECH Act)[24] provisions of ARRA created several incentives for medical providers to transfer their medical records to electronic form. The incentives given to providers differ depending on if they are sought under Medicare or Medicaid. A provider may choose to receive the benefits under either one, but not both, Medicare and Medicaid. In order to receive the incentive, a physician must make "meaningful use" of EHRs. To receive benefits under the HITECH Act, this includes three requirements: (i) the EHR must be certified and have the capa-

[20] Other possible barriers to EHR implementation, not discussed herein, include cultural barriers between physicians and patients, standard-setting issues, and issues related to network externalities. *See, e.g.*, Daniel J. Gilman & James C. Cooper, *There is a Time to Keep Silent and a Time to Speak, the Hard Part is Knowing Which is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279, 284 (2010).

[21] Merkel, *supra* note 8.

[22] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115.

[23] *About ONC*, HEALTH IT, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__onc/1200 (last modified Dec. 12, 2010).

[24] Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 115, 226 (codified in scattered sections of 42 U.S.C.).

bilities to ePrescribe (obtain prescriptions on the Internet), (ii) the information in the EHR must be exchangeable with other systems, and (iii) this information must transfer in reports produced pursuant to several clinical and quality metrics.[25] The Department of Health and Human Services has enacted a rule that further explains the criteria for "meaningful use" of EHRs (the "Meaningful Use Rule").[26] The Meaningful Use Rule, which is the first step in an incremental approach to adopting standards, implementation specifications, and certification criteria to enhance the interoperability, functionality, utility, and security of health information technology and to support its meaningful use, is beyond the scope of this Article. However, it is important to note that the Meaningful Use Rule establishes numerous detailed requirements that providers must meet.

Pursuant to the HITECH Act, Congress has set aside seventeen billion dollars for incentive payments to providers who implement a qualifying EHR.[27] Hospital-based professionals do not receive any incentive payments for switching over to EHRs since the hospitals themselves receive these payments for switching over.[28] Something else to note is that doctors who collect incentives can only receive incentives under either Medicaid or Medicare, not both.[29] A doctor who receives the incentive under Medicare receives a predetermined flat amount for each year after he or she puts the EHR into place.[30] Incentives received under Medicaid, on the other hand, can be up to eighty-five percent of allowable EHR costs, not to exceed sixty-five thousand dollars over five years.[31] In order to be eligible for Medicaid incentives, a doctor must waive his or her right to the Medicare incentives.[32]

[25] Medicare and Medicaid Health Information Technology; Miscellaneous Medicare Provisions, Pub. L. No. 111-5, § 4101, 123 Stat. 115, 467 (2009).

[26] *See* Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 75 Fed. Reg. 44314 (July 28, 2010) (to be codified at 42 C.F.R. pt. 412, 413, 422).

[27] *See* ROBERT HUDOCK & PATRICIA WAGNER, EPSTEIN BECKER & GREEN, P.C., ANALYSIS OF THE HITECH ACT'S INCENTIVES TO FACILITATE ADOPTION OF HEALTH INFORMATION TECHNOLOGY, HEALTH CARE & LIFE SCIENCES CLIENT ALERT 2 (2009), http://www.ebglaw.com/files/28043_ClientAlertHITECH.pdf.

[28] Medicare and Medicaid Health Information Technology; Miscellaneous Medicare Provisions, § 4101, 123 Stat. at 468; HUDOCK & WAGNER, *supra* note 27, at 2–3.

[29] *See* HUDOCK & WAGNER, *supra* note 27, at 2.

[30] *Id.* at 3.

[31] *Id.* at 5.

[32] *Id.* at 4.

To be eligible for the Medicaid incentives, a professional must fall into one of the following categories. The first category includes, as mentioned above, professionals who are not hospital-based and whose practices consist of at least thirty percent Medicaid patients.[33] The second category includes professionals who are pediatricians and whose required percentage of Medicaid patients is accordingly lowered to twenty percent.[34] The third category consists of professionals who practice predominantly in federally qualified health centers and have at least thirty percent of their practice attributable to needy individuals.[35] Professionals who are in the Medicaid program will not be the subjects of a punitive incentive that the Medicare program has set in place, which will begin to cut payments to professionals who do not switch to EHRs by the year 2015.[36]

The financial incentives that the HITECH Act provides, while helpful in some respects to certain health care providers, have not been sufficient to motivate a full-scale transition to EHRs among the majority of providers. We have been seeing EHR implementation in hospitals, institutes, and large clinics, but for smaller practices, the adoption of complex EHR systems has often been cost prohibitive. These smaller practices, however, provide the majority of medical services in the country.[37] Accordingly, we cannot have true and complete EHR adoption without getting these smaller providers on board.

B. *Implementation Challenges*

In addition to costs, it appears that a number of implementation challenges may have limited the effective adoption of EHRs. Literature has identified physician reluctance as a factor in the delays in EHR adoption.[38] A number of factors can influence physician reluctance, including questions about the data input process and concerns about the lost productivity that can result from the implementation process.[39] Physicians have also

[33] *Id.* at 5.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] This is particularly important given that researchers have concluded that the support and involvement of general practitioners is critical to wider acceptance and utilization of electronic records. *See* Daly, *supra* note 2.

[38] *See* Gienna Shaw, *EMR Adoption: Starting to Evolve or Still Stuck in the Past?*, HEALTHLEADERS MEDIA (Feb. 23, 2010), http://www.healthleadersmedia.com/print/TEC-246979/EMR-Adoption-Starting-to-Evolve-or-Still-Stuck-in-the-Past.

[39] *Id.*

reported concerns about the future obsolescence of the software and systems that they elect to implement.[40]

C. *Privacy and Data Security*

1. Patient Fears and Expectations

Many medical consumers remain concerned about the use of electronic medical records. As one journalist put it, "Patients' worries about the privacy and security of their health records today are similar to the concern people had about Internet shopping and banking five or ten years ago."[41]

Unfortunately, the data does show that there are reasons for concerns. The reality is that medical information remains vulnerable to a number of threats. For example, the loss and theft of laptops and other data-storage devices continue to be major sources of data breaches both inside and outside of the health care sector. There are many cases where an employee of a covered entity left the entity's premises with a laptop containing private health information, only to have the laptop lost or stolen, thereby jeopardizing the privacy and security of the private health information stored on the laptop. There have also been many instances where lost or stolen laptops and other devices compromised individual patient data, including the following:

- In February 2009, a researcher's laptop, which contained the health information of 2,500 subjects who were participating in a study conducted by the National Institutes of Health (NIH), was stolen.[42]
- In March 2009, personal information from more than 14,000 patients at a North Carolina hospital was compromised when a laptop was stolen from a facility in Canton, Georgia, that was reviewing the information to help the hospital improve care and reduce costs.[43] Although the laptop was stolen on March 9, the hospital was not alerted of the breach until March 14.[44]

[40] *Id.*

[41] Merkel, *supra* note 8.

[42] *See* Editorial, *Safeguarding Private Medical Data*, N.Y. TIMES, March 26, 2008, at A2.

[43] *See* Joe Killian, *Stolen Laptop Has Information on 14,000 Moses Cone Patients*, NEWS & REC., Apr. 14, 2009, at A1.

[44] *Id.*

- In August 2009, a laptop was stolen from a hospital employee's car; it contained the private billing information for 33,000 patients of a Florida hospital.[45]
- Most recently, on November 30, 2009, a laptop containing sensitive patient information, including 4,400 patient records, was stolen from an employee of the University of California, San Francisco School of Medicine and was not found until January 8, 2010.[46]

Of course, these are only some of the numerous breaches of health information that have occurred in the past few years.

Insider criminal actions also present a serious risk to the security of electronic medical information. It has been estimated that more than ninety percent of all medical identity theft is attributable to insider theft.[47] The fact that data has become a highly valuable commodity may make the theft and resale of such data far too tempting for some employees.

There are a number of notable examples of data theft by medical workers. Recently, five individuals were charged for their involvement in a credit card scheme resulting from the fraudulent access of information, namely the records of patients of Johns Hopkins Medicine.[48] One of the charged individuals was an employee of Johns Hopkins and reportedly accessed electronic patient records to obtain patient names, social security numbers, dates of birth and addresses.[49] The medical worker then shared the information with other defendants who used the data to apply for credit at various retail establishments and make fraudulent purchases.[50]

Another instance occurred in 2008, when a former admissions department employee of a New York hospital confessed to stealing and selling the personal information of close to 40,000

[45] *See* Angela Moscaritolo, *Stolen Daytona Beach Hospital Laptop Contained Patient Info*, SC MAG. (October 23, 2009), http://www.scmagazineus.com/stolen-daytona-beach-hospital-laptop-contained-patient-info/article/156050.

[46] *See* Chris Rauber, *UCSF Says Laptop With 4,400 Patient Records Stolen, Then Recovered*, SAN FRAN. BUS. TIMES (January 28, 2010, 11:26 AM PST), http://www.bizjournals.com/sanfrancisco/stories/2010/01/25/daily54.html.

[47] *See* Walecia Konrad, *Medical Problems Could Include Identity Theft*, N.Y. TIMES, June 12, 2009, at B1.

[48] *See* Pamela Lewis Dolan, *5 Charged with Fraud Involving Johns Hopkins Patients*, AM. MED. NEWS (Oct. 20, 2010), http://ama-assn.org/amednews/2010/10/18/bise1020.htm.

[49] *Id.*

[50] *Id.*

patients.[51] Over a period of more than two years, he obtained lists of patient names, phone numbers, and Social Security numbers.[52] According to news reports, an individual seeking personal information for patients born between 1950 and 1970 approached the employee.[53] The employee then sold an initial batch of data for $750 and later, a second batch for $600.[54]

A further example of insider medical identity theft involved a case at the Cleveland Clinic in Weston, Florida, where a front-desk office coordinator pled guilty to selling information involving more than 1,000 patients.[55] Although the hospital had browser controls to limit the number of records that employees could view, no one noticed the woman was exceeding that limit regularly. The case resulted in $2.8 million in Medicare fraud.[56]

As we make the transition to electronic records, will these problems get worse? Possibly. Technology can help, but if not used correctly, it can also exacerbate current problems. An important factor underlying data insecurities plaguing the health care community can be found in the massive amounts of data and paperwork the health care industry produces in treating an individual, as well as the number of different individuals and entities that may have access to the information. Technology can assist by controlling access, as well as by monitoring, recording, and auditing access in ways that go well beyond what is possible with paper-based files. And yet, if not used correctly, technology can also facilitate greater access to medical records by unauthorized parties.

It appears likely that Americans are willing to support EHRs but do have concerns about the privacy and security of their information when stored in such electronic systems. A recent report by the Agency for Healthcare Research and Quality[57] is particularly illustrative in this regard. Dr. Deborah Peel, founder of Patient Privacy Rights,[58] concluded that the "findings [of the

[51] *See N.Y. Hospital Employee Admits Stealing, Selling Patient Data*, CAMPUS SAFETY MAG. (April 14, 2008), http://www.campussafetymagazine.com/News/?NewsID=1851.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *See* Liz Freeman, *Florida Health Fraud Case Breaks New Legal Ground*, NAPLES DAILY NEWS, September 15, 2006, at A1.

[56] *Id.*

[57] AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, U.S. DEP'T OF HEALTH & HUMAN SERVS., NO. 09-0081-EF, CONSUMER ENGAGEMENT IN DEVELOPING ELECTRONIC HEALTH INFORMATION SYSTEMS: FINAL REPORT (2009).

[58] *See* PATIENT PRIVACY RIGHTS, http://patientprivacyrights.org/ (last visited Jan. 28, 2011).

study covered by this report] solidly confirm Americans' desires to control their personal health information."[59] Dr. Peel further contends that: "Americans are generally supportive of health IT, but they want to be well informed about the consequences of disclosure and have the ability to restrict access and use of their information."[60]

2. The Impact of Differences in Applicable Legislation

i. Overview of Legal Framework

Ironically, just as there is evidence to suggest that patient concerns over privacy and security may be impacting the adoption of EHRs, there is also evidence that demonstrates that privacy regulation could be impacting the rate of EHR adoption as well. Significantly, the impact does not appear to be coming from the existence of privacy legislation, but from the fact that there are differences in legal and regulatory requirements, particularly at the state level, but also at the federal level.[61] This can make it difficult for institutions to adopt and implement unified systems that will meet these varying requirements.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[62] plays a significant role in the regulation of medical privacy. However, it is not the only law that regulates health privacy. Beyond HIPAA, there are several federal laws that impact the privacy and confidentiality of health information, including: (i) the Privacy Act of 1974;[63] (ii) the Confidentiality of Alcohol and Drug Abuse Patient Records Regulations;[64] (iii) Family Educational Rights and Privacy Act (FERPA);[65] (iv) the Americans with Disabilities Act (ADA);[66] and (v) the Genetic Information Nondiscrimination Act of 2008 (GINA).[67]

[59] DEBORAH C. PEEL, PATIENT PRIVACY RIGHTS, THE CASE FOR INFORMED CONSENT: WHY IT IS CRITICAL TO HONOR WHAT PATIENTS EXPECT—FOR HEALTH CARE, HEALTH IT, AND PRIVACY 6 (2010), http://patientprivacyrights.org/wp-content/uploads/2010/08/The-Case-for-Informed-Consent.pdf.

[60] *Id.*

[61] *See* Stephen J. Weiser, *Breaking Down the Federal and State Barriers Preventing the Implementation of Accurate, Reliable and Cost Effective Electronic Health Records*, 19 ANNALS HEALTH L. 205 (2010).

[62] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in various sections of 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

[63] 5 U.S.C.A § 552a (2007 & West Supp. 2010 & 2011).

[64] 42 C.F.R. § 2.1-.67 (2010).

[65] 20 U.S.C.A. § 1232g (2006 & West Supp. 2010).

[66] 42 U.S.C. § 12101–213 (2006 & Supp. II 2008).

[67] Pub. L. No. 110-233, 122 Stat. 881 (2008) (codified in various sections of 29 U.S.C. and 42 U.S.C.).

HIPAA's Privacy Rule[68] establishes the minimum privacy protection for health information, while at the same time allowing more protective laws to exist at the state level. Covered entities are required to comply with both HIPAA and state law whenever possible, but HIPAA preempts some state provisions. However, HIPAA does *not* preempt state law in the following circumstances: (i) when state law is necessary for regulation of insurance or health plans, prevention of fraud and abuse, or reporting on health care system operations and costs; (ii) when it addresses controlled substances; (iii) when it relates to reporting of disease or injury, child abuse, birth, death, public health surveillance, or public health investigation or intervention; and (iv) when a provision of state law is more stringent than similar requirements in the HIPAA Privacy Rule.[69]

The most difficult of these exceptions to understand is the stringency exception. Generally, a provision of state law is more stringent if it prohibits or restricts use or disclosure of protected health information that the HIPAA Privacy Rule would permit. Specifically, a more stringent state law: (i) permits greater access and amendment rights to individuals; (ii) provides individuals with more information about use, disclosure, rights, and remedies; (iii) makes the requirement of legal permission for use or disclosure of PHI more lenient; (iv) increases the duration or requires more detailed accounting of disclosures; and (v) provides greater individual privacy protection.

State law is an increasingly important part of health privacy regulation. State laws cover: health insurance regulation; the regulation of organizations that perform certain administrative functions (such as utilization review or third-party administration); licensure requirements for various medical specialties and medical organizations (including requirements for recordkeeping and disclosure); access to medical records; reporting of information to the state and local authorities; use of information for quality assurance and health care operations; issuance of notices of privacy practices; and reporting and providing access to law enforcement authorities. In addition, many states have passed confidentiality laws related to specific conditions or types of health information. Examples include laws related to mental health records, HIV/AIDS, reproductive rights, and genetic testing. States may have laws concerning privacy in connection with insurance, workers compensation, public health, or research. Meanwhile, states are also becoming increasingly involved with

[68] 45 C.F.R. §§ 164.500–.534 (2009).

[69] 45 C.F.R. § 160.203 (2009).

data security. Most states now have laws mandating the disclosure of breaches involving certain data and information useful in committing identity theft or other harm. While all of these state laws extend to financial data, such as social security numbers and bank account numbers, a smaller number of states are beginning to extend their laws to cover breaches of medical and health information.[70] In addition, certain states, including, most notably, Massachusetts, have enacted comprehensive information security laws.[71]

ii. The Impact of Differences in Law

The differences in state laws can impact the implementation and use of EHR systems.[72] In one survey of states, officials reported that laws concerning information regarding mental health, substance abuse, HIV/AIDS, communicable diseases, genetic testing, and disability present the greatest challenges to the release of health information through an electronic data interchange.[73] However, differences in the procedural or substantive requirements regarding medical information, including its disclosure, storage, and security, can impact the structure and implementation of EHR systems. Consider, as one example, state regulations concerning the disclosure of information regarding HIV/AIDS. To ensure the privacy and security of patients suffering from HIV/AIDS, many states have enacted stringent confidentiality laws concerning such information. In Massachusetts, state law requires that physicians, health providers, and health care facilities obtain a patient's written consent prior to the release of any data revealing that the patient has AIDS.[74] Moreover, the law lays out in great detail the scope of the consent and the format required.[75] Many other states have

[70] Julie A. Heitzenrater, Note, *Data Breach Notification Legislation: Recent Developments*, 4 ISJLP 661, 666 (2008).

[71] *See* 201 MASS. CODE REGS. §§ 17.01–17.05 (2011).

[72] *See, e.g.*, Linda Dimitropoulos & Stephanie Rizk, *A State-Based Approach to Privacy and Security for Interoperable Health Information Exchange*, 28 HEALTH AFF. 428, 428–29 (2009) ("An interoperable system of HIE [health information exchange]—that is, one in which various parties can share and exchange data among them—will have difficulty accommodating the current range of variation in policy requirements.").

[73] Vernon K. Smith et al., *State E-Health Activities in 2007: Findings From a State Survey* (The Commonwealth Fund, Publ'n No. 1104, 2008), *available at* http://www.commonwealthfund.org/Content/Publications/Fund-Reports/2008/Feb/State-E-Health-Activities-in-2007—Findings-From-a-State-Survey.aspx (follow "Fund Report" hyperlink).

[74] MASS. ANN. LAWS ch. 111, § 70F (LexisNexis 2004).

[75] *Id.*

enhanced regulations regarding the protection of this sensitive information, but there are differences from state to state. One can imagine how this might impact the implementation of a system for electronic records for use both within and outside of Massachusetts. While the use of technology can accommodate differences such as these, the existence of such differences will complicate the implementation.

Research supports the notion that differences in state laws concerning patient confidentiality may be impacting the extent to which EHRs are being adopted. In fact, researchers have concluded that state privacy regulation restricting hospital release of health information reduces aggregate EHR adoption by hospitals by more than 24%.[76] Significantly, these researchers found that states that eliminated some of their regulation experienced a 21% increase in hospital EHR adoption rates around the years in which the changes were made, while in those states where there were not similar eliminations of legal requirements, there was only an 11% increase in EHR adoption rates.[77]

On the other hand, others, such as privacy specialist Dr. Deborah Peel, and Deven McGraw, director of health privacy at the Center for Democracy and Technology,[78] have expressed skepticism about these findings, contending that the delays in EHR adoption have not resulted from the existence of differences in how states regulate health privacy.[79]

Still, as Miller and Tucker have pointed out, nearly half of the states have their own health privacy requirements.[80] Thus, it does not seem implausible that these differences could be affecting the implementation and adoption of EHRs. In this author's view, however, these differences do not argue for the abolishment of state laws that are more protective than the requirements of HIPAA—a concern of Dr. Peel's.[81] Rather, as discussed further in the next section, which examines suggestions for possi-

[76] Amalia R. Miller & Catherine Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records*, 55 MGMT. SCI. 1077, 1077 (2009).

[77] *Id.* at 1089.

[78] *See Deven McGraw*, CTR. FOR DEMOCRACY & TECH., http://www.cdt.org/personnel/deven-mcgraw (last visited Apr. 11, 2011).

[79] Chris Silva, *EMR Adoption Higher in States With Fewer Privacy Laws*, AM. MED. NEWS (May 4, 2009), http://www.ama-assn.org/amednews/2009/05/04/gvsc0504.htm.

[80] *See* Miller & Tucker, *supra* note 76, at 1083 (identifying the following states as having their own health privacy requirements: Arizona, California, Florida, Georgia, Illinois, Indiana, Maine, Maryland, Massachusetts, Minnesota, Nevada, New Hampshire, New Jersey, Rhode Island, Tennessee, Texas, Vermont, Virginia, Wisconsin, and Wyoming).

[81] Silva, *supra* note 79.

ble ways forward, the data regarding the impact of the differences in state law may be a basis for calling for greater coordination on existing law, which may include raising, rather than lowering, the bar of protection.

IV. WAYS FORWARD

Given that there are numerous advantages to the use of electronic health records and fairly broad support for their adoption, it is important to understand how to overcome some of the primary obstacles to EHR adoption. With this in mind, this section will examine some possible solutions to the current privacy obstacles to broader EHR adoption. This Article has observed that there are other obstacles to EHR adoption—most notably cost and implementation challenges. While these factors are significant obstacles, the solutions to these challenges lie outside of the legal arena and, accordingly, are outside the scope of this Article.

A. *Increased Coordination on Privacy Laws*

Because a variety of researchers and experts have identified differing legislative requirements as an obstacle to the broader adoption of EHRs, it may be prudent to examine how increased harmonization could help improve the adoption and implementation of EHR systems. The creation of uniform, protective federal health privacy law applicable to all states may help reduce physician trepidation about the challenges of adopting an EHR system that will function well for all offices and patients, irrespective of residency. It may also help reduce the costs of implementation by allowing for systems that require less customization.

This is not to suggest that legislatures should eradicate enhanced protections currently in existence at the state level. Rather, scholars and legislators should direct their efforts to examining how to modify existing federal privacy laws to provide a more uniform system of protection for the privacy and security of health information.

B. *Enhancement of Existing Laws and Enforcement*

In addition to providing incentives for the adoption of EHRs, the HITECH Act also modified certain aspects of HIPAA to provide enhanced protection for the privacy and security of medical information. While the changes are notable, arguably, more work is necessary. Despite the changes in law, data breaches in the health sector continue to occur.[82] Recent data exemplify this very point. Since January 1, 2009, regulators have required health care organizations in California to notify them in the event of a breach involving health information. In the several months since that law entered into force, organizations have reported more than 800 data breaches involving medical information.[83] This figure, large by any estimation, is truly astounding when one considers that this number concerns only one state and only a six-month time period. In addition, in the nine-month period between September 22, 2009, and June 11, 2010, organizations reported over 100 breaches, each impacting more than 500 people.[84]

Enhancing existing privacy protections can also help to assuage the fears of medical consumers and the concerns of privacy advocates. There are a number of areas of regulation that are ripe for improvement, and scholars and legislators should take care to ensure that the modifications implemented are those most likely to improve patient privacy protections and expand the use of EHRs. One area ready for improvement is the enforcement of existing privacy laws. Although HIPAA establishes a number of stringent requirements, HIPAA enforcement actions have been few and far between. This reality may be leading some entities that are subject to HIPAA to question whether they need to take their obligations under HIPAA very seriously since the risk of an enforcement action may appear relatively low.

In addition to increasing the number of enforcement actions, some experts have suggested that we may wish to increase the penalties for violations of health privacy.[85] Of course, the HITECH Act did substantially increase the amount of civil and monetary penalties that can be assessed for HIPAA violations.[86] However, it may make sense to study whether further

[82] *Healthcare Hacks on the Rise*, INFOSECURITY (Jan. 26, 2010), http://www.infosecurity-us.com/view/6806/healthcare-hacks-on-the-rise.

[83] Kim Zetter, *New Law Floods California with Medical Data Breach Reports*, WIRED (July 9, 2009, 3:24 PM), http://www.wired.com/threatlevel/2009/07/health-breaches/#ixzz0fc9ffk6r.

[84] *Breaches Affecting 500 or More Individuals*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html (last visited Apr. 11, 2011).

[85] *See* Weiser, *supra* note 61, at 211 ("Criminal and civil penalties would need to be substantially increased to serve as a deterrent to employer, health insurer, or health care provider that improperly discloses sensitive health information.").

[86] *See* Melissa M. Goldstein et al., *Recent Federal Initiatives in Health Information Technology*, *in* HEALTH INFORMATION TECHNOLOGY IN THE UNITED STATES:

enhanced penalties are needed across the board, or at least in the area of EHRs.

We may also wish to consider whether a private right of action under HIPAA is in order. Entities that violate HIPAA may be subject to civil and monetary penalties and, in some cases, may even be subject to criminal sanctions. However, individuals upon whose rights a covered entity's violation of HIPAA has infringed do not have any right to bring private causes of action against the applicable entities. It is worth examining whether the introduction of a private right of action for HIPAA violations might improve medical consumers' confidence in EHRs.

V. Conclusion

There are a number of potential benefits of EHRs. To reap these benefits, we, as a society, need to ensure that EHRs are implemented more broadly. To implement EHRs on a scattered basis is to miss out on the full potential of EHRs. While the use of EHRs in a single medical office may generate efficiencies in that medical office, we need a concerted national effort to truly benefit from digitization in this area. As the former National Coordination for Health Information Technology has explained, "fragmentation . . . results in errors, duplication, lack of coordination, and many other problems."[87]

Through ARRA, the Obama Administration has taken an important step toward encouraging national adoption of EHRs. While the financial incentives will not solve all of the financial challenges for all medical practices, they are likely to make important contributions for many practices. It is now time to focus on the numerous other obstacles to EHR adoption and work on making the changes necessary to ensure that we all can benefit from a cohesive, integrated electronic health record system.

On the Cusp of Change, 2009, at 50, 59 (Robert Wood Johnson Found. et al. eds., 2009), *available at* http://www.rwjf.org/files/research/hitfullreport.pdf.

[87] David Brailer, *Interoperability: The Key to Future Heath Care Systems*, W5 Health Aff. Web Exclusive 19, 19 (2005), http://content.healthaffairs.org/content/early/2005/01/19/hlthaff.w5.19.citation.