

PRIVACY AND E-HEALTH INNOVATION

By: Sharona Hoffman*

INTRODUCTION

The practice of medicine in the United States is undergoing a transformation. Traditional paper medical files are being replaced by electronic health record (EHR) systems. The federal government has allocated 27 billion dollars over ten years to assist health care providers with the purchase and adoption of health information technology.¹

The computerization of medical information has raised significant concerns about privacy. Electronic records may be vulnerable to inappropriate disclosure through hacking, stolen laptops, employee mistakes, or intentional malice.² This short thought piece analyzes the privacy concerns that are particular to health information and the mechanisms by which the government and industry have addressed them. It argues that a focus on privacy is essential to our successful transition to digitized medicine because without it, patients may resent and distrust EHRs. In addition, appropriate technological responses to privacy concerns can, as a side effect, enhance the overall safety and quality of EHR systems. At the same time, however, I caution against radical approaches to privacy protection that might prevent clinicians, researchers, and patients from enjoying the full benefits of health information technology.

THE NEED FOR EHR PRIVACY PROTECTION

Privacy safeguards are vital in the medical arena because individuals' health records contain personal and sensitive information that might be of interest to a large number of parties.³ Employers wish to hire healthy workers who will not have productivity and absenteeism problems or submit costly medical claims for reimbursement. Various types of insurers (e.g. life, disability, long-term care) want to find clients who are low-risk and whose premium payments will exceed claims. Lenders are interested in borrowers who can work and earn sufficiently to pay off their loans. Advertisers and marketers hope to influence doctors' prescribing decisions and patients' medical purchasing choices. Political operators may hope to use health information to disqualify or embarrass candidates, and blackmailers or other criminals may seek financial

* Professor of Law and Bioethics, Co-Director of Law-Medicine Center, Case Western Reserve University School of Law; B.A., Wellesley College; J.D., Harvard Law School; LL.M. in Health Law, University of Houston

¹ David Blumenthal & Marilyn Tavenner, *The "Meaningful Use" Regulation for Electronic Health Records*, 363 N. ENGL. J. MED. 501, 501 (2010).

² See Robert Pear, *tighter Medical Privacy Rules Sought*, N.Y. TIMES, August 22, 2010 (discussing a number of recent privacy breaches).

³ See Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 334-35 (2007).

gain through its possession and use. These few examples illustrate the potential value of personal health data to parties outside the clinician-patient relationship.⁴

THE INTERDEPENDENCE OF PRIVACY SAFEGUARDS AND INNOVATION

Without comprehensive security safeguards to protect patient privacy, the transition to EHR systems may well fail. Patients must believe that use of health information technology is in their best interest and buy into the mammoth effort to transform the practice of medicine through digitization. Any well-publicized privacy leaks could erode patient trust in computerized systems and create political backlash against them, especially if the breaches cause discernable harm, such as embarrassment, loss of employment opportunities, or damage to reputation. Fear of such consequences may cause individuals to forego needed medical care or not to be fully candid with clinicians who treat them.⁵ Patients who worry that their psychiatric records, HIV status, sexual histories, or other sensitive information will fall into the hands of third parties may refuse to disclose important medical facts to their health care providers or avoid seeking routine, preventive and non-emergency medical care.

Fortifying EHR system security and workplace procedures for privacy purposes can also improve the quality of health care in many other ways. For example, authentication and authorization standards, password management, and workforce clearance procedures for those handling EHRs can ensure that unauthorized personnel do not access records and inadvertently or intentionally corrupt medical data. Automatic logoff after a specified period of inactivity can prevent clinicians from erroneously entering information into a record that was left open by another user. In addition, protection against malicious software such as viruses and worms can prevent system failures and downtime.

THE GOVERNMENT'S RESPONSE – THE HIPAA SECURITY RULE

Regulatory Requirements

The U.S. Department of Health and Human Services (HHS) has not ignored the privacy risks associated with EHR systems. In 2005 it enacted the HIPAA Security Rule,⁶ which was later amended by the Health Information Technology for Economic and Clinical Health Act of 2009.⁷ The Rule supplemented the previously enacted HIPAA Privacy Rule, which governs the

⁴ *Id.*

⁵ LYNNE "SAM" BISHOP ET AL., CAL. HEALTHCARE FOUND., NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005: EXECUTIVE SUMMARY 3-4 (2005) (finding that 67% of respondents were concerned about the confidentiality of their medical records and 13% had taken various steps to protect their own privacy (e.g. avoiding medical tests, paying out of pocket, or asking doctors to distort diagnoses)).

⁶ 45 C.F.R. §§ 164.302-318 (2010).

⁷ Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

disclosure of medical information stored in either paper or electronic form and details the rights patients have with respect to their medical records.⁸

The Security Rule applies to most health care providers, health plans, and health care clearinghouses and their business associates.⁹ It does not, however, apply to any other entities, no matter how much private health information they might possess. The Rule delineates the administrative, physical, and technical safeguards that these covered entities must employ to secure electronic health information.

In order to understand the types of technological and organizational interventions that can protect confidentiality, it is useful to detail some of the regulatory requirements. The administrative safeguard standards focus on security management processes, workforce security, information access management, security awareness and training, security incident procedures, and contingency plans. Implementation specifications mandate risk assessment, the establishment of a sanctions policy for non-compliant employees, workforce clearance procedures, log-in monitoring, password management, and many other measures.¹⁰

The physical safeguards section emphasizes facility access controls, workstation use, workstation security, and device and media controls. For example, covered entities are required to develop plans and procedures related to facility security, access control and validation, and data backup and storage.¹¹

The technical safeguards include the establishment of procedures to control access to electronic health information (EHI), to audit activity in information systems that process EHI, to protect EHI from improper modification or elimination, and to obtain authentication from those seeking access to EHI. Appropriate methods to achieve some of these goals are encryption and decryption.¹²

The Shortcomings of the HIPAA Security Rule

Despite its significant achievements, the HIPAA Security Rule suffers from several gaps, which I have discussed at length in prior work.¹³ A very brief summary of my critique is provided below.

First, the HIPAA Security Rule does not reach all parties that might pose privacy threats for patients. Employers, marketers, life insurers, and others who have health information are not bound by the Rule's mandates and thus are not legally required to implement security precautions. Employers, for example often collect significant medical information from workers

⁸ 45 C.F.R. § 164.534 (2010).

⁹ 45 C.F.R. §§ 160.102-160.103 (2010); 45 Fed. Reg. 40912 (2010).

¹⁰ 45 C.F.R. § 164.308 (2010).

¹¹ 45 C.F.R. § 164.310 (2010).

¹² 45 C.F.R. § 164.312 (2010).

¹³ See Hoffman & Podgurski, *supra* note 3 at 359-84.

through pre-employment physicals or periodic exams and storing such data electronically without appropriate security safeguards would create a risk of privacy breaches.¹⁴ Equally troubling is the fact that the HIPAA Privacy Rule applies to the same narrow category of covered entities as the Security Rule, and thus non-covered entities are free of the regulations' restrictions on the disclosure of personally identifiable health information.¹⁵

Second, the HIPAA Security Rule does not provide aggrieved individuals with a private cause of action.¹⁶ Its efficacy is dependent upon HHS having sufficient enforcement resources, and therefore, it may lack the deterrence power that the prospect of private litigation would bestow. In addition, patients whose confidential information is inappropriately disclosed or leaked cannot receive compensation no matter what harm they suffered.

Finally, the Security Rule's standards and implementation specifications lack sufficient guidance. Covered entities without sophisticated information technology departments are unlikely to find that the Rule provides adequate instructions concerning compliance with the various requirements.¹⁷

Nevertheless, by enacting the HIPAA Security Rule, the federal government recognized that without robust privacy protections, there can be no shift to e-health in the U.S. Despite its limitations, the Rule is a laudable and important step in providing patients with comprehensive privacy protection.

A WORD OF CAUTION ABOUT OVERLY ZEALOUS APPROACHES TO PRIVACY

The importance of privacy and security for electronic health information is irrefutable. Nevertheless, some advocates wish to carry the commitment to privacy too far. Some have suggested the implementation of privacy practices that are extreme and inadvisable. These proposals include allowing patients to opt-out of having an EHR, to place portions of their EHRs (e.g. mental health treatment) in "secure envelopes" that can be accessed only with the individuals' specific permission, to control what information is disclosed to which providers, or to access and edit their records as they see fit.¹⁸ Such practices, however, could compromise patient care.

One of the significant advantages of interoperable EHR systems is that patient records can be obtained by authorized personnel even if they are stored by other health care facilities or networks. Thus, if a patient is brought unconscious to the emergency room, doctors can review

¹⁴ Sharona Hoffman, *Employing E-Health: The Impact of Electronic Health Records on the Workplace*, 19 KANSAS J. L. & PUBLIC POL'Y 409, 409-10, 418-20, & 430 (2010).

¹⁵ 45 C.F.R. § 160.103 (2010).

¹⁶ See 45 C.F.R. §160.300-.552 (2010).

¹⁷ See Hoffman & Podgurski, *supra* note 3 at 350-54.

¹⁸ Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 725-30 (2007).

her medical history, drug and allergy lists, and other vital information. Similarly, doctors treating patients who are forgetful or confused about their medical details would not need to rely on the patients' unreliable accounts.

If patients are empowered to opt out of EHR use or to disallow treating physicians' access to their records, they may lose much of the benefit of computerization. Many clinicians would continue to care for patients in ignorance of essential facts that could make the difference between appropriate and inappropriate treatment decisions. For example, it might seem at first blush that most physicians would not need access to a patient's psychiatric records. However, a psychiatric diagnosis may help other specialists better understand the patient's symptoms, and the patient's complete drug list, including psychiatric drugs, is vital for purposes of safely prescribing additional medications.¹⁹

Another benefit of EHRs is that they can enable the creation of general research databases containing millions of deidentified patient records. Such databases could enable researchers to conduct comprehensive observational studies based on the actual clinical experience of patients with diverse demographics and to fill many medical knowledge gaps.

Some experts worry, however, that deidentification is insufficient to protect patient privacy and would prefer that informed consent be obtained each time data will be used or that data subjects be allowed to opt out of each individual research project before it is commenced.²⁰ It is important that deidentification be thorough and responsible²¹ and that patients have the opportunity to consent to the initial inclusion of their records in research databases. However, making database administration and research excessively burdensome because of over-zealous privacy and consent requirements would be ill-advised.²² Investigators who must identify and re-contact millions of patients to ask if they wish to have their anonymized records included in each particular study may find the task impossibly time-consuming or costly and abandon important research initiatives. Furthermore, if, out of an abundance of caution, patients are repeatedly contacted and warned about the risks of inclusion in a research database and consequently opt out in large numbers, research data could become fragmented, making it difficult for investigators to draw general inferences. To illustrate, if individuals who have a particular ancestry, who suffer from a certain disease, or who share certain lifestyle habits opt out disproportionately, research data may become skewed and unreliable.

CONCLUSION

¹⁹ It should be noted that psychotherapy notes are not generally disclosable without patient consent. 45 C.F.R. § 164.508 (2010).

²⁰ Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?* 10 AM. J. BIOETHICS 3–11 (2010).

²¹ See 45 C.F.R. 164.514(b)(2)(i) (2010) for deidentification guidance provided by the HIPAA Privacy Rule.

²² See Sharona Hoffman, *Electronic Health Records and Research: Privacy vs. Scientific Priorities*, 10 AM. J. BIOETHICS 19 (2010).

Careful attention to privacy and security safeguards is vital to the success of EHR system adoption. Such safeguards will reassure patients that computerization will not compromise confidentiality and allow physicians to earn patient trust and cooperation, which will facilitate health information technology implementation. Security precautions may also yield other benefits by improving the overall quality of EHR products and reducing clinician error rates. So long as radical privacy measures are not espoused, privacy protection is in the best interest of all who have a stake in the successful implementation of health information technology: industry, the government, medical professionals, and patients.