ARTICLE

PRIVACY AND SECURITY IN THE IMPLEMENTATION OF HEALTH INFORMATION TECHNOLOGY (ELECTRONIC HEALTH RECORDS): U.S. AND EU COMPARED

JANINE HILLER
PROFESSOR OF BUSINESS LAW
PAMPLIN COLLEGE OF BUSINESS
VIRGINIA TECH

MATTHEW S. MCMULLEN
PARTNER, MARTINELLI AND MCMULLEN PROFESSIONAL SERVICES

WADE M. CHUMNEY
CECIL B. DAY ASSISTANT PROFESSOR OF BUSINESS ETHICS AND LAW
GEORGIA INSTITUTE OF TECHNOLOGY

DAVID L. BAUMER
DEPARTMENT HEAD, PROFESSOR OF LAW AND TECHNOLOGY
NORTH CAROLINA STATE UNIVERSITY

ABSTRACT

The importance of the adoption of Electronic Health Records (EHRs) and the associated cost savings cannot be ignored as an element in the changing delivery of health care. However, the potential cost savings predicted in the use of EHR are accompanied by potential risks, either technical or legal, to privacy and security. The U.S. legal framework for healthcare privacy is a combination of constitutional, statutory, and regulatory law at the federal and state levels. In contrast, it is generally believed that EU protection of privacy, including personally identifiable medical information, is more comprehensive than that of U.S. privacy laws. Direct comparisons of U.S. and EU medical privacy laws can be made with reference to the five Fair Information Practices Principles (FIPs) adopted by the Federal Trade Commission and other international bodies. The analysis reveals that while the federal response to the privacy of health records in the U.S. seems to be a gain over conflicting state law, in contrast to EU law, U.S. patients currently have little choice in the electronic recording of sensitive medical information if they want to be treated, and minimal control over the sharing of that information. A combination of technical and legal improvements in EHRs could make the loss of privacy associated with EHRs de minimis. The EU has come closer to this position, encouraging the adoption of EHRs and confirming the application of privacy protections at the same time. It can be argued that the EU is proactive in its approach; whereas because of a different viewpoint toward an individual's right to privacy, the U.S. system lacks a strong framework for healthcare

privacy, which will affect the implementation of EHRs. If the U.S. is going to implement EHRs effectively, technical and policy aspects of privacy must be central to the discussion.

I. INTRODUCTION

The United States spends the equivalent of 16% of its Gross Domestic Product (GDP) on healthcare, a larger percentage than any other comparably-sized developed country.[1] As the pressure to reduce ballooning healthcare expenditures continues to rise, information technology, and in particular the implementation of Electronic Health Records (EHRs), is identified as one potential method to create efficiencies and reduce costs. However, "studies suggest that fewer than one-fifth of the doctors' offices in the United States offer EHRs."[2] Other countries have made more significant progress; Denmark, for example, has an e-health records system that almost universally links patients/citizens and medical professionals.[3]

In order to promote progress in EHR adoption, former President George W. Bush announced a proposal for the implementation of health information technology (HIT), setting the ambitious goal of assuring that the majority of Americans will have EHRs[4] by 2014. This 2004 plan set a target for complete healthcare information availability for the majority of Americans at the time and place of care, "designed to share information privately and securely among and between health care providers when authorized by patients."[5] The Obama administration continues to emphasize the use of health technologies, and the timetable for implementing HIT, and in particular EHRs, could be even shorter.[6]

This article describes the potential benefits of EHRs, identifies some of the possible risks to individual privacy, discusses related security issues, and

[1] *HIT or Miss*, ECONOMIST, April 18, 2009, at 3. *See also Heading for the Emergency Room*, ECONOMIST, June 27, 2009, at 75-77.

[2] *HIT or Miss*, *supra* note 1, at 3.

[3] *Id.*

[4] For purposes of this study, Electronic Health Records (EHRs) are defined as a patient's medical record in digital format, accessed by a computer, often over a network.

[5] Transforming Health Care: The President's Health Information Technology Plan, April 2004, http://georgewbush-whitehouse.archives.gov/infocus/technology/economic_policy200404/chap3.html.

[6] K.C. Jones, *Obama Wants E-Health Records In Five Years*, INFO. WK., Jan. 12, 2009, http://www.informationweek.com/news/healthcare/showArticle.jhtml?articleID=212800199 .

critically examines the sufficiency of the existing regulatory matrix to meet these challenges. Next, the article analyzes the European Union (EU) approach to implementing EHRs, one that aims to protect citizen privacy and secure their information. The article considers these issues from a high level, framework approach. As member countries of the EU implement the fundamental principles of regulation, and U.S. regulatory measures are refined, there will be further comparisons to be made. However, the frameworks provide the foundation upon which the future of health information privacy rests, and understanding its design is essential.[7] Finally, this paper gleans lessons by comparing these different approaches.

II. EHR BACKGROUND: THE GOOD, THE BAD, AND THE UGLY

The opportunity to reduce costs and provide safer, more effective healthcare by implementing nationwide EHRs also introduces significant risks. The benefits of imbedding electronic record technology into the U.S. healthcare system should be weighed against the risk that the same technology will decrease the privacy of individuals in the sensitive area of personal health information and treatment. Significant losses of personal health information privacy can be the result of an inadequately configured legal system, defective safeguards by healthcare providers, or negligent technical system design without satisfactory security safeguards from criminal intrusions. Regardless of the reason, legal or technical, the result is that the good aspects of EHRs can be undermined by the bad consequences of poor privacy practices and the ugly effects of inadequate security.

A. The Good: Benefits of an Electronic Health Records System

Among the potential benefits of EHRs are: (1) significant reduction in healthcare costs, (2) reduction of medical errors, and (3) improved quality of care.[8] Examination of the data by some healthcare cost experts suggests that the exchange of health information contained in EHRs and other related HIT activity "will have a substantial impact on the health care system's costs, saving approximately $80 billion annually."[9] A significant part of the savings could be achieved through the exchange of health information. The National

[7] While efforts were made to include current information in this article, the speed with which regulatory comments, updates, and positions change should be noted.

[8] Ashish K. Jha & Julie Adler-Milstein, *Chapter 5: Regional Health Information Organizations and Health Information Exchange, in* HEALTH INFORMATION TECHNOLOGY IN THE UNITED STATES: WHERE WE STAND 73 (David Blumenthal et al. eds., 2008), *available at* http://www.rwjf.org/files/research/3297.31831.hitreport.pdf.

[9] *Id.* *See also* Robert Malone, *Health Information Technology: Transforming the Healthcare Industry for the 21st Century* 3 OKLA. J. L. & TECH. 36, 36-37 (2007) (one-third of healthcare costs are wasted on paper processing and the like).

Health Information Network (NHIN),[10] under development through a public – private partnership, will be used to provide "anytime, anywhere health care information and decision support. . .via a comprehensive knowledge-based network of interoperable systems."[11] The RAND Corporation examined the potential cost benefits of NHIN and health information technology (HIT) in a 2005 study.[12] The analysis predicted that if 90% of hospitals and doctors in the U.S. adopted HIT over fifteen years, the healthcare system could save almost $77 billion a year from efficiency gains, a result consistent with other studies.[13] It is important to note that these huge potential savings in healthcare costs are only achievable if all, or nearly all, healthcare organizations participate in sharing EHRs.[14] If health and safety benefits are added to that estimate then

[10] Kevin Puscas, *National Health Information Network (NHIN) Operational Infrastructure Architecture Document*, National Health Information Network, 2 (July 10, 2009), http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910399_0_0_18/NHINInfrastructureArchitectureDocument.doc (The Nationwide Health Information Network (NHIN) is being developed to "provide a secure, nationwide, interoperable health information *infrastructure* that will connect providers, consumers, and others involved in supporting health and healthcare." (emphasis added));

Robert Hudock, *Open Source Programmers Collaborate to Improve the CONNECT Gateway*, LAW BLOG 2.0 (August 31, 2009), http://law2point0.com/wordpress/2009/08/31/open-source-programmers-collaborate-to-improve-the-connect-gateway/

> To promote a more effective marketplace, greater competition, and increased choice through accessibility to accurate information on healthcare costs, quality, and outcomes, the Office of the National Coordinator (ONC) is advancing the NHIN as a "network of networks" which will connect diverse entities that need to exchange health information, such as state and regional health information exchanges (HIEs), integrated delivery systems, health plans that provide care, personally controlled health records, Federal agencies, and other networks as well as the systems" to which they, in turn, connect.

See also Barbara J. Evans, *Congress' New Infrastructural Model of Medical Privacy*, 84 NOTRE DAME L. REV. 585, 586-88 (2009) (describing the FDA Sentinel System, the first step in creating this network).

[11] Ashish K. Jha & Julia Adler-Milstein, *supra* note 8, at 75 (quoting William A. Yasnoff, *The Ehealth Trust(Tm) Path to Implementing Health Information Infrastructure*, Tampa, FL, 2005 (PowerPoint Presentation)).

[12] *HIT or Miss*, *supra* note 1, at 5.

[13] *Id*.

[14] This result has been validated in studies of the economics of networks. The really significant gains are only achievable if nearly all healthcare facilities can transmit and receive electronic health records. *See* S. J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8.2 J. OF ECON. PERSPECTIVES 133, 134 (Spring 1994); *see also* John W. Hill et al., *Law, Information Technology, and Medical Errors: Toward A National Healthcare Information Network Approach to Improving Patient Care and*

the efficiency gains could double, resulting in savings of approximately 6% of the almost $3 trillion spent on healthcare annually.[15]

A potential secondary health benefit of EHR adoption is the reduction of care variability by use of data to define and disseminate best practices, therefore helping to deliver more effective care to a broader patient base.[16] In addition, consumer and patient interfaces with EHR systems may yield valuable data which might provide additional benefits such as: "determining provider (hospital and physician) performance outcomes, monitoring chronic diseases, monitoring medication adherence, promoting safety metrics, determining patient satisfaction, promoting more informed clinical decisions, and improving patient-physician communication tracking."[17]

Implemented and utilized properly, EHRs can lead to these significant benefits by reducing variability of healthcare treatment and resulting in improved care. It is conceivable that reducing variability in healthcare treatment could reduce both the incidence of medical malpractice and the excessive use of defensive medical practices, including unnecessary tests ordered primarily to avoid malpractice litigation.[18]

B. The Bad: Risks to Individual Privacy

Despite the benefits of widespread EHR adoption, its acceptance and implementation will not be achieved unless its risks are mitigated. Perhaps the most complex set of risks is to patient privacy and security. In fact, a significant obstacle to public acceptance of EHRs is the concern over the privacy and security of personal health information.[19] In a 2006 survey, 62%

Reducing Malpractice Costs, 2007 U. ILL. J.L. TECH. & POL'Y 159 (2007) (arguing that state privacy laws are too restrictive and that a preemptive federal law is needed in order to implement HIT and reduce medical errors).

[15] *HIT or Miss*, *supra* note 1, at 5.

[16] Ashish K. Jha & Julia Adler-Milstein, *supra* note 8, at 76.

[17] Karen Donelan & Paola D. Miralles, *Chapter 4: Consumers, EHRS and PHRs: Measures and Measurement*, *in* HEALTH INFORMATION TECHNOLOGY IN THE UNITED STATES: WHERE WE STAND 56, 57 (David Blumenthal et al. eds., 2008), *available at* http://www.rwjf.org/files/research/3297.31831.hitreport.pdf.

[18] *Cf.* Johnny Benjamin, *Healthcare Reform and Defensive Medicine*, THE HUFFINGTON POST, July 23, 2009, http://www.huffingtonpost.com/johnny-benjamin/healthcare-reform-and-def_b_243537.html (reduced variability in treatment could limit a physician's freedom to conduct defensive medicine via assurance and avoidance behavior by limiting the acceptable range of treatment).

[19] The following definitions of privacy and security have been used in this report: "Privacy"- The claim of individuals and the societal value representing that claim, to control the use and disclosure of their information. Ruth Faden, *Keynote Speech*, *in* HEALTH RECORDS: SOCIAL NEEDS AND PERSONAL PRIVACY (Feb. 1993), *available at* http://aspe.hhs.gov/pic/reports/ahrq/4441.pdf. "Security"- The safeguards (administrative,

of the public said "the use of electronic medical records makes it more difficult to ensure patients' privacy," however "similar proportions recognized the potential for EHRs in cost and error reductions and increased patient safety."[20] Asked about a "network to provide people with access to personal health information online," respondents said they were "very concerned" about the following: 80% about medical identity theft, 77% about marketing firm access, 56% about employer access, and 53% about insurance company access to the information.[21] Additional concerns expressed by the public include the loss of sensitive health information, increased sharing of information without patients' knowledge, inadequate data security, and the possibility that medical errors could increase.[22]

The disparity between patient desires for privacy and what is provided by some electronic health record systems, is illustrated by the results of a 2007 study commissioned by HHS, which found that the privacy policies of Personal Health Record (PHR) vendors, a type of health record controlled by the patient, generally "lacked the standard components of privacy notices."[23] Revealing a lack of attention to individual privacy, "only two of thirty PHR vendors described what would happen to consumer's data if the vendor were sold or went out of business, and only one had a policy with respect to accounts terminated by the consumer."[24]

---

technical, physical) in an information system that protect it and its information against unauthorized disclosure (as well as ensure its availability and maintain its integrity) and limit access to authorized users in accordance with an established policy. Willis Ware, *Lessons for the Future: Privacy Dimensions of Medical Record Keeping*, *in* HEALTH RECORDS: SOCIAL NEEDS AND PERSONAL PRIVACY (1993), *available at* http://aspe.hhs.gov/pic/reports/ahrq/4441.pdf. *See* Sean T. McLaughlin, *Pandora's Box: Can HIPAA Still Protect Patient Privacy Under a National Healthcare Information Network?*, 42 GONZ. L. REV. 29, 31 (2006) ("To succeed in digitalizing American medicine, the Bush administration must first inspire the trust and confidence of lawmakers, patients, and other health care participants. While providing participatory incentives to the healthcare industry, the federal government also needs to vigilantly protect individual privacy against foreseeable abuse and threats.").

[20] Karen Donelan & Paola D. Miralles, *supra* note 17, at 66.

[21] *Id*. at 67.

[22] *Id*. at 66. These concerns are not unfounded, as "[T]here is unequivocal evidence of unlawful sales" of healthcare data. Angela Ferneding, Note, *Regional Health Information Organizations: Lower Health Care Costs, Fewer Iatrogenic Illnesses, and Improved Care-What are We Waiting For*, 22 J.L. & HEALTH 167, 182 (2009).

[23] *Personal Health Records Need a Comprehensive and Consistent Privacy and Security Framework*, CTR. FOR DEMOCRACY & TECH., June 9, 2009, http://www.cdt.org/policy/personal-health-records-need-comprehensive-and-consistent-privacy-and-security-framework.

[24] *Id*.

C. The Ugly: Medical Identity Theft

Medical identity theft (MIT) is generally defined as the theft of personally identifiable health information[25] in order to gain access to health treatment or to fraudulently file for reimbursements for false medical treatment.[26] The consequences of MIT are similar across stakeholder groups; with the common themes of both diminished healthcare quality and financial loss as the primary risks.[27] Based upon self-reported cases to the Federal Trade Commission (FTC), it is estimated that MIT comprises 3% of all reported identity theft cases.[28] However, the FTC figure is likely low since the U.S. Department of Health and Human Services, the most likely agency to which complaints of health care theft are reported, had not previously kept specific records on MIT.[29]

There are two common types of MIT: when an internal employee steals a patient's information (often sold to another party), or an individual uses another's identity to receive medical services or goods.[30] Traditionally, when MIT occurred via the theft of paper records, the physical nature of paper records limited the extent of the theft. The transition to EHRs and the storage of information in electronic databases will exponentially increase the number of patient records obtainable by MIT thieves, also making notification to victims more difficult.[31] It is also clear that MIT can result in life threatening damage if the medical records of an individual are changed, absent, or erroneous as a result of the theft. In a well-known case, a medical office

---

[25] Personally identifiable information (PII) is any information about an individual that can be used to distinguish or trace an individual's identity. Examples include: Social Security Number, Date of birth, Name and address, and Medicare/Medicaid ID or Healthcare/Insurance ID. Booz Allen Hamilton, *Medical Identity Theft Environmental Scan*, DEP'T OF HEALTH & HUM. SERVS., 1 (Oct. 15, 2008), *available at* http://healthit.hhs.gov/portal/server.pt?open=18&objID=850701&parentname=CommunityPage&parentid=1&mode=2&in_hi_userid=10741&cached=true.

[26] Id. at 4.

[27] *Id*. at 8.

[28] *Id*. at 7. For an update to this report, see Booz Allen Hamilton, *Medical Identity Theft Final Report*, DEP'T OF HEALTH & HUM. SERVS., (Jan. 15, 2009), *available at* http://healthit.hhs.gov/portal/server.pt/document/848096/medidtheftreport011509_pdf (this report argues that health information technology can also help to avoid medical identity theft Id. at 4.).

[29] Interview by Matt McMullen with William Gould, Deputy Dir. of Program Integrity Unit, Ctr. For Medicare and Medicaid Serv., at The Centers for Medicare and Medicaid Services, Baltimore, Md. (Aug. 23, 2009).

[30] See Booz Allen Hamilton, supra note 25, at 5-7.

[31] See Pam Dixon, MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You, WORLD PRIVACY FORUM, at 42-44 (May 3, 2006), available at http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

worker stole the electronic records of over 1,000 patients, selling them to a relative who made nearly three million dollars by filing false medical claims.[32] As a result of these types of incidents, some medical offices require their patients to provide photo ID.[33] This identification procedure is not universally implemented.[34]

III. THE U.S. LEGAL FRAMEWORK FOR HEALTHCARE PRIVACY

The Fourth Amendment to the U.S. Constitution is the fundamental source for the protection of privacy, and as the preamble to the Privacy Rule adopted to enforce HIPAA states:

> [T]he existence of a generalized right to privacy as a matter of constitutional law suggests that there are enduring values in American law related to privacy. For example, the need for security of 'persons' is consistent with obtaining patient consent before performing invasive medical procedures. Moreover, the need for security in 'papers and effects' underscores the importance of protecting information about the person contained in personal diaries, medical records or elsewhere.[35]

In particular, in Whalen v. Roe, "the U.S. Supreme Court recognized a limited Constitutional right to individual privacy with respect to information held in governmental databases. The question of constitutional protection of health information privacy remains largely unresolved because attempts to apply Whalen to informational privacy more generally have been inconsistent."[36] Privacy and confidentiality of health records have traditionally been governed by state common law, however outcomes in state cases have been inconsistent.[37] Common law in many states includes actions based on an

---

[32] Walecia Konrad, Medical Problems Could Include Identity Theft, N.Y. TIMES, 13 June 2009, at B1 available at http://www.nytimes.com/2009/06/13/health/13patient.html.

[33] Id.

[34] Interview with William Gould, Deputy Director of Program Integrity Unit, Ctr. For Medicare and Medicaid Serv. at The Centers for Medicare and Medicaid Services, Baltimore, Md. (Aug. 23, 2009).

[35] Melissa Goldstein, Lee Repasch, & Sara Rosenbaum, *Chapter 6: Emerging Privacy Issues in Health Information Technology*, *in* HEALTH INFORMATION TECHNOLOGY IN THE UNITED STATES: WHERE WE STAND 95 (David Blumenthal et al. eds., 2008), *available at* http://www.rwjf.org/files/research/3297.31831.hitreport.pdf.

[36] *Id*. at 96; *see also* Whalen v. Roe, 429 U.S. 589, 603-04 (1997).

[37] Ilene N. Moore et al., *Confidentiality and Privacy in Health Care From The Patient's Perspective: Does HIPAA Help?*, 17 HEALTH MATRIX 215, 217 (2007); *See also* Daniel J. Oates, *HIPAA Hypocrisy and the Case for Enforcing Federal Privacy Standards Under State Law*, 30 SEATTLE U. L. REV. 745, 767-68 (2007) (recommending that HIPAA standards should be adopted in common law to address inconsistencies of state law and HIPAA's shortcomings in the lack of a private cause of action). For further discussion of

injury to privacy interests.[38] Employers may be held liable for invasions of privacy under theories of respondeat superior, if their employees' actions lead to private medical information being made "public."[39] Several states extend liability to health organizations based on a confidentiality statute.[40] However, a review of state laws prior to HIPAA found that instead of providing for broad privacy protection, that the state provisions were relatively reactive and limited to unique factual circumstances.[41]

In relation to privacy protection and identity theft, states have addressed the important area of information security by enacting security breach notification laws.[42] California was the leader in passing a data breach notification requirement, subsequently modified to include breaches of data held by a health care provider or insurer.[43]

Variation and lack of uniformity in state privacy law, however, hinders the widespread adoption of EHRs. Federal regulation, with the potential to harmonize protections throughout the nation, has expanded, however.[44] Federal laws protect health information in specific programs, such as Medicaid[45]and federal substance abuse treatment programs.[46] In addition, the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 contains protection for financial information held by health insurers.[47] Broader federal laws include the Privacy Act of 1974[48] and the Health Insurance Portability

state laws, see Benjamin J. Beaton, *Walking the Federalist Tightrope: A National Policy of State Experimentation for Health Information Technology*, 108 COLUM. L. REV. 1670 (2008); Kari Bomash, *Privacy and Public Health in the Information Age: Electronic Health Records and the Minnesota Health Records Act*, 10 MINN. J. L. SCI. & TECH. 117 (2009).

[38] Moore et al, *supra* note 37, at 226.

[39] *Id*.

[40] *Id*. at 224.

[41] *Id*. at 227.

[42] Booz Allen Hamilton, *supra* note 25, at 19, 29-30.

[43] S. 1386, 2001-2002 Leg. (Cal. 2003). State laws usually apply to entities if they do business in the state and maintain information about residents. Many state statutes provide an individual right of action for damages based on the breach. *See* Booz Allen Hamilton, *supra* note 25, at 19, 29-30.

[44] The relationship between state and federal health information protection laws is complex and beyond the scope of this article. HIPAA generally does not preempt state law. However, *see infra* Part III (A)(3), discussing HIPAA's relationship to state law with regards to disclosures.

[45] Goldstein et al., *supra* note 35, at 96.

[46] *Id*.

[47] Gramm-Leach-Bliley (Financial Services Modernization) Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338.

[48] Privacy Act of 1974, 5 U.S.C. § 552a.

and Accountability Act of 1996 (HIPAA),[49] as amended in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH).[50] The Privacy Act of 1974 applies to federal agencies that hold individuals' personal information within any "federal government records."[51] Because the Privacy Act is limited to records held by federal agencies, this article will focus on HIPAA, as amended by HITECH, which applies to all health providers.[52]

A. Privacy of Health Care Information: HIPAA and HITECH

HIPAA is the primary law that establishes the U.S. legal framework for health information privacy. Although passed in 1996, HIPAA took several years to function to protect individual privacy. The law originally gave Congress three years to pass explicit privacy rules; when Congress failed to act within the three years, the Department of Health and Human Services (HHS) automatically became the authority for adopting privacy regulations.[53] Thus, the HIPAA final Privacy Rule ("Privacy Rule") establishing standards for the privacy of individually identifiable health information, was adopted by HHS in 2003.[54] The Privacy Rule applies to covered entities, defined as health care plans, health care providers and clearinghouses.[55] The Privacy Rule delineates when and how these covered entities can disclose protected health information. In addition to the Privacy Rule, the HIPAA Security Rule ("Security Rule")[56] requires covered entities to safeguard protected health information through the use of administrative, technical, and physical measures.[57] In 2009, HITECH strengthened HIPAA's privacy and security guidelines[58] by imposing new privacy obligations on covered entities, expanding and clarifying business

[49] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[50] Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13402, Pub. L. No. 111-5, 123 Stat 115 (2009).

[51] Goldstein et al., *supra* note 35, at 96.

[52] See 45 C.F.R. §§ 160.102, 162.100, 164.104 (2009).

[53] Samuel J. Miller, Electronic Medical Records: How the Potential for Misuse Outweighs the Benefits of Transferability, 4 J. HEALTH & BIOMEDICAL L. 353, 359-60 (2008).

[54] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. §§ 160, 164).

[55] 45 C.F.R. § 160.103(ii)(3) (2010).

[56] Security and Privacy, 45 C.F.R. § 164 (2001).

[57] Health Insurance Reform: Security Standards Final Rule, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. §§ 160, 162, 164).

[58] Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat 115 (2009).

associates requirements; it also added provisions related to EHR, health information exchange (HIE), and personal health records (PHR).[59] HITECH increased enforcement and monetary civil penalties.[60] Highlights of HITECH are discussed in the following sections when relevant to HIPAA and the protection of health information privacy.

1. Protected Information: Covered Entities and Business Associates

HIPAA originally regulated protected health information (PHI) in the hands of "covered entities," defined as health plans, health care clearinghouses, and health care providers who transmit health information electronically in certain health information transactions.[61] This initial definition excluded significant numbers of entities who were involved in electronic health information exchanges, such as personal health record (PHR) vendors, thus not universally protecting the privacy of personal health information. On June 21, 2007, the National Committee on Vital and Health Statistics (NCVHS) submitted a letter to the Secretary of HHS expressing concern that "many of the new entities essential to the operation of the National Health Information Network (NHIN) fall outside HIPAA's statutory definition of a 'covered entity.'"[62] Specifically, the advisory panel pointed to "health information exchanges, regional health information organizations, record locator services, community access services, system integrators [and] medical record banks" as outside the law's purview, and thus recommended that the scope of the law be expanded to cover these entities.[63] Subsequent legislation, HITECH, addressed this concern and required HHS and the Federal Trade Commission (FTC) to make recommendations by 2010 regarding certain health records not already covered under HIPAA.[64]

---

[59] Diane Manos, *HHS Issues Rule on EHR Breach Notification*, HEALTHCARE IT NEWS (Aug. 19, 2009), *available at* http://www.healthcareitnews.com/news/hhs-issues-rule-ehr-breach-notification.

[60] *See* Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13410, Pub. L. No. 111-5, 123 Stat. 115 (2009).

[61] 45 C.F.R. §160.103 (2010) (definition of covered entity); Goldstein et al., *supra* note 35, at 96, 100.

[62] Letter from Simon P. Cohn, Chairman, Nat'l Comm. on Vital and Health Statistics, to Michael O. Leavitt, Sec'y, U.S. Dep't of Health & Hum. Servs. (June 21, 2007), *available at* http://www.ncvhs.hhs.gov/070621lt2.pdf; *accord* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-988T, HEALTH INFORMATION TECHNOLOGY: EFFORTS CONTINUE BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY, at 4, 18 (2007), *available at* http://www.gao.gov/new.items/d07988t.pdf.

[63] Letter from Simon P. Cohn, *supra* note 62.

[64] *See* HITECH § 13424 (b), 42 U.S.C. § 17953(b) (2006); *see also* FED. TRADE COMM'N, FTC FILE NO. R911002, FTC ISSUES FINAL BREACH NOTIFICATION RULE FOR ELECTRONIC HEALTH INFORMATION (Aug. 17, 2009), *available at*

In reality, many health care providers engage outside contractors to perform non health functions such as computer systems work or billing. Those secondary entities can receive personal health information in the performance of their duties, and are addressed in the Privacy Rule under the category of "business associates."[65] A "business associate" is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information."[66] In order to disclose PHI to business associates, a covered entity must have assurances that the use of the information will be limited to that for which it was transferred, that the entity has sufficient security to protect the information, and that it will cooperate with the covered entity to protect the information as required under the Privacy Rule.[67] Those assurances must be included in the agreement between the covered entity and the business associate.[68]

Before HITECH, there was some confusion regarding whether an entity that processed information as a conduit, but was not using that information for other purposes, would be subject to the same privacy requirements as a covered entity. HITECH clarified and extended the regulation of business associates by providing that they are subject to the same privacy regulations applied to covered entities.[69] In summary, HITECH sought to put business associates under the same umbrella as covered entities in the protection of privacy and security of protected health information.

2. Information Collection and Patients' Rights

There is an ongoing debate among privacy experts, consumer advocates and the medical profession about the extent of control patients should have over their electronic health records. Some contend that policies that require too much patient control "could hamper a patient's health in a medical emergency," while on the other side, it is "said that not enough control could put their lives at risk in other ways."[70] Patient Privacy Rights, an advocacy

http://www.ftc.gov/opa/2009/08/hbn.shtm; *see also infra* Part III.A.2 (discussion of individual access to electronic health records).

[65] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., at 3 (May 2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[66] 45 C.F.R. § 160.103 (2009); *see supra*, note 66, at 3 ("Business associate functions or activities . . . include claims processing, data analysis, utilization review, and billing. Business associate services . . . are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services").

[67] 45 C.F.R. §§ 164.308(b), 164.502(e) (2004).

[68] 45 C.F.R. § 164.504(e)(2) (2004).

[69] Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13404(a), Pub. L. No. 111-5, 123 Stat 115 (2009).

[70] Diana Manos, *Privacy Experts Debate Patient Consent*, HEALTHCARE IT NEWS (Sept.

organization dedicated to ensuring that Americans control access to their health records, argues that "[a] lack of safeguards. . . poses risks to a person's well-being, livelihood and financial stability," and because of this "patients should have total control over their personal health records. . . to ensure that information that a patient wishes to be kept private is kept that way."[71] On the other hand, the Center for Democracy and Technology's Health Privacy Project argues, "patients intuitively want control of their data, but requiring consent for every exchange of health information is sometimes not the best approach for ensuring privacy."[72]

The federal government attempted to address privacy concerns through HIPAA and the Privacy Rule. The rule establishes individual rights, including rights to access and the potential to amend personal health information, to obtain a record of when and why PHI has been shared with others for certain purposes, to receive a privacy notice, and to file a complaint.[73] Under HIPAA a patient has a right to receive notice of the privacy policies of a covered entity, including how they use and disclose PHI and the respective rights and duties of the patient and the entity.[74] The patient's right to know if their information has been disclosed improperly is addressed by the recent change in law. HITECH established a federal health care data breach notification requirement.[75] HITECH clearly includes a breach notification procedure for both "covered entities" and "business associates;" it also sets out various obligations and a timeframe for the notification,[76] and addresses security breaches by personal health record vendors.[77]

The American Health Information Management Association (AHIMA), however, called for additional protection of patient health information, arguing that the additional measures in HITECH were insufficient to provide consumers with adequate protection.[78] AHIMA proposed a national Health

21, 2009), *available at* http://www.healthcareitnews.com/news/privacy-experts-debate-patient-consent.

[71] *Id*.

[72] *Id*.

[73] 45 C.F.R. §§ 160.306, 164.520, 164.524, 164.526, 164.528 (2004); For a discussion of enforcement issues related to the Privacy Rule, *See* Tobi M. Murphy, *Enforcement of the HIPAA Privacy Rule: Moving From Illusory Voluntary Compliance to Continuous Compliance Through Private Accreditation*, 54 LOY. L. REV. 155 (2008).

[74] 45 C.F.R. § 164.520(a).

[75] Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13402, Pub. L. No. 111-5, 123 Stat 115 (2009).

[76] Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13402(a), (b) and (d), Pub. L. No. 111-5, 123 Stat 115 (2009).

[77] Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13407(a), Pub. L. No. 111-5, 123 Stat 115 (2009).

[78] Bernie Monegain, *AHIMA charts course for protecting patient data*, HEALTHCARE IT

Information Bill of Rights, including seven essential protections for patient health information.[79] The principles address "the protection of consumer health information from three basic standpoints: appropriate access, optimal accuracy, and the highest standards of privacy and security for everyone."[80] The AHIMA bill of rights includes cost-free access to health information, information accuracy and completeness, accountability, and the right to a legal recourse in the event that a breach of information causes harm.[81] The introduction to the proposed bill of rights acknowledges that the recommendations represent a "major paradigm shift from current practice" however it considered these steps essential to "allow healthcare consumers to become more proactive in managing their health and their health information."[82]

3. Information Disclosure and Sharing

Under HIPAA, a patient's ability to restrict electronic health record access is significantly limited. The HIPAA framework defines two categories of potential disclosures, required and permissive. There are only two types of disclosures within the required category; "a covered entity's provision of a patient's own PHI to the patient or to the patient's representative, and requests by the HHS Secretary for PHI for audit or other enforcement purposes."[83] Any other disclosures "are considered permissive or 'allowed' but not 'automatic'- even disclosures that may be required by other federal or state laws."[84] Permissive disclosures are further categorized as; "(1) those that require patient authorization, and (2) those that can be made without patient authorization."[85] However, "if a covered entity desires to disclose PHI it generally can find a way to do so. . . HIPAA essentially permits covered entities to substitute their own institutional practices and policies for variable state disclosure laws."[86] In

NEWS (Oct. 6, 2009), *available at* http://www.healthcareitnews.com/news/ahima-charts-course-protecting-patient-data.

[79] *Id*.

[80] *Id*.

[81] AHIMA Health Information Bill of Rights, http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045343.pdf (last visited Nov. 27, 2010); *See also* Patricia Sanchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, 6 NW. J. TECH. & INTELL. PROP. 244, 269-76 (2008) (suggesting a patient's bill of rights that includes an architecture of privacy, informed consent, control of disclosure, transparency, accessibility and portability, due process, dispute resolution, protection of minors, and anonymity).

[82] AHIMA, *supra* note 81.

[83] Goldstein et al., *supra* note 35, at 97.

[84] *Id*.

[85] *Id*.

[86] *Id*. at 99.

essence, the health care provider has more control than the patient over what information will be disclosed.

a. No Patient Prior Authorization Required

Patient authorization is not required to share health information when it is being used for treatment, payment or health care operations, and the entity has taken steps to secure the information in a reasonable way, which depends on the method used to communicate that information.[87] Communication methods include oral, written, telephone or fax communication.[88]

For example, guidance provided by the Centers for Medicare and Medicaid Services states that patients are not required "to sign consent forms before doctors, hospitals or ambulances can share information for treatment purposes."[89] Furthermore, patient prior authorization is not required when information is shared for purposes of: public health, payment, treatment, healthcare operations, research, and support of a healthcare exchange.[90]

The amount of information disclosed is required to be limited to the "minimum necessary." However, HIPAA allows a covered entity to rely upon the determination by another covered entity as to what amount of information is the minimum necessary for the stated purpose.[91] Lastly, no patient authorization is required to share aggregated and de-identified health information used to advance public understanding of the quality of health care or the process of quality improvement.[92]

b. Patient Authorization Required

Under HIPAA, a covered entity or business associate may not disclose PHI

---

[87] 45 C.F.R. § 164.506(a) (2010).

[88] *See HIPAA – Frequently Asked Questions*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/hipaafaq/providers/smaller/482.html (last updated Aug. 8, 2005).

[89] *See Medical Privacy of Protected Health Information*, U.S. DEP'T OF HEALTH & HUM. SERVS., 1 (Revised June 2009), http://www.cms.hhs.gov/MLNproducts/downloads/SE0726FactSheet.pdf; *See also Understanding Health Information Privacy*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding (last visited Oct. 16, 2010).

[90] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., 4-5 (May 2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. *See infra* Part V.B.2.; *see also* Goldstein et al., *supra* note 35, at 97 ("Indeed, health plans often require such disclosure for financial reimbursement.").

[91] 45 C.F.R. § 164.514(d)(3)(ii)(B)(iii)(B) (2010).

[92] Goldstein et al., *supra* note 35, at 97; *see also* Samuel J. Miller, *Electronic Medical Records: How the Potential for Misuse Outweighs the Benefits of Transferability*, 4 J. HEALTH & BIOMEDICAL L. 353, 365-70 (2008) (noting that the broad means of disclosure can lead to potential misuse and ease of abuse during undefined emergency situations).

when it directly or indirectly receives remunerations for the exchange, unless the patient authorizes such exchange.[93] Under HITECH, there are further circumstances requiring a patient's authorization to sell the information if the information is used for marketing or fundraising.[94] However, exceptions provide that patient authorization is not needed if the marketing related remuneration is for: transfer of data for public health research, treatment, the sale, transfer, merger, or consolidation of all or part of the covered entity, due diligence related to a business entity transfer, or in connection with payment for services under a business associate agreement.[95]

4. Security and Security Breach Notification

HIPAA requires covered entities to establish and maintain administrative, physical, and technical safeguards for healthcare information.[96] These safeguards cover a range of possible procedures, and establishing standards to which the industry can adhere has taken time.[97] With the increased desire to implement electronic health records and other HIT measures, the need to address challenges in privacy and security also increased. On September 15, 2009, the Health IT Standards Committee[98] endorsed security and privacy standards for EHR systems with the explanation that acceptable levels of protection "would get progressively tougher without holding back wider health information sharing."[99] The Committee's proposed standards "cover access control, authentication, authorization and transmission of health data. . .. Under the standards approved . . . EHR systems would have to meet several standards for access control, including technical requirements of the security and privacy rules. . .." [100]

In addition to strengthening existing requirements, HITECH also instituted a new security requirement: a breach notification procedure that applies to both

[93] U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 65, at 9-10.

[94] Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13405(d), Pub. L. No. 111-5, 123 Stat 115 (2009).

[95] *Id*. at § 13405(d)(2)(A)-(G) (2009).

[96] 45 C.F.R. § 164.530(c) (2010).

[97] See Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 335-42, 372-82 (2007) (discussing the potential for vendor and certification roles for security).

[98] The Standards Committee makes recommendations to the Office of the National Coordinator for Health IT on standards, implementation guidelines and certification criteria for Health IT policies developed by the Health IT Policy Committee.

[99] Mary Mosquera, *Federal Panel Approves EHR Security, Privacy Standards*, GOVERNMENT HEALTH IT NEWS (Sept. 16, 2009), http://www.healthcareitnews.com/news/federal-panel-approves-ehr-security-privacy-standards (requirements increase in 2013).

[100] *Id*.

covered entities and business associates.[101] The final interim rule adopted requires covered entities to provide the Secretary of HHS, the affected individuals, and the media with notice of a breach of unsecured protected health information when over 500 victims are identified.[102] In addition, PHRs and other non-covered entities are regulated by similar rules adopted by the FTC.[103]

5. Enforcement

HHS has jurisdiction to bring a civil action to enforce HIPAA and to seek penalties for violations. However, an individual has no direct action right under federal law; any possible individual action is found in state law.[104] While individuals may be able to benefit from the penalties collected by HHS,[105] they will nonetheless be unable to directly seek the repair of an information loss or to pursue a change in health information practices.

HITECH increased the penalties for violations[106] and imposed mandatory penalties for those due to "willful neglect."[107] Business associates are also

[101] 42 U.S.C. § 17932 (2006)*; See also HITECH Breach Notification Interim Final Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html (last visited Nov. 27, 2010) (HHS regulates the covered entities under HIPAA, and the FTC regulates those health records not covered by HIPAA, however the two agencies coordinated their rule adoption).

[102] 45 C.F.R. § 164.408 (2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf; *See Instructions for Submitting Notice of a Breach to the Secretary*, U.S. DEP'T OF HEALTH & HUM. SERVS., www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html (last visited Oct. 18, 2010) (if there are fewer than 500 persons affected by the breach then that information should be reported in an annual report to the HHS).

[103] *Id*.; *see* Federal Trade Commission, Health Breach Notification Rule, 16 C.F.R. 318 (2009), *available at* http://www.ftc.gov/os/2009/08/R911002hbn.pdf.

[104] *See* 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, 302, 309 (2010). For a discussion of the lack of enforcement by HHS, *see* Cicely N. Tingle, *Developments in HIPAA and Health Information Technology*, 3 I/S J. L. AND POL'Y INFO. SOC'Y 677 (2007).

[105] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., 17 (May 2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[106] *See* 42 U.S.C. § 1320d-5 (2006).

[107] The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, sec. 13410(a), 123 Stat. 115.

liable under this section.[108] Additionally, HHS is required to formally investigate any complaints that are preliminarily determined to involve potential willful neglect.[109] In addition, state attorneys general may bring civil actions for violations of the HIPAA privacy and security standards on behalf of a resident consumer.[110] The Department of Justice may bring criminal charges for a knowing violation of the Privacy Rule, which could potentially result in a sentence of up to ten years in an egregious case.[111] Viewed together, the increased civil and criminal penalties, state attorney general actions, and business associate liability significantly strengthen the previous enforcement framework.[112]

IV. EU PRIVACY PROTECTION FOR HEALTH INFORMATION

The protection of the privacy and security of health data is essential for any Electronic Health System to reach its full potential. How to implement privacy and security in this unique environment is not evident however, as balancing individual and societal interests can be difficult. The EU has addressed, and is continuing to examine, how privacy and security of health data can co-exist with a robust EHR system. In order to learn from and compare the choices to be made, the following sections review the overarching framework of EU policy and the regulatory approach addressing privacy and security in an EHR environment.

A. International Privacy Principles Background

Historically, the European environment for privacy has been uniquely different from that of the United States. The 1950 Council of Europe Convention identified individual privacy as a fundamental value.[113] Article 8 of the European Convention for the Protection of Human Rights and

[108] *Id*. at sec. 13401(b).

[109] *Id*. at sec. 13410(a)(1).

[110] *Id*. at sec. 13410(e)(1).

[111] *See* Peter S. Rank, *Co-Regulation of Online Consumer Personal Health Records: Breaking Through the Privacy Logjam to Increase the Adoption of a Long-Overdue Technology*, 2009 WIS. L. REV. 1169, 1185 (2009).

[112] *See Improvements and Challenges in Health Privacy Law*, CENTER FOR DEMOCRACY & TECHNOLOGY (March 27, 2009), http://www.cdt.org/policy/improvements-and-challenges-health-privacy-law.

[113] *See* Francesca Bignami, "Constitutional Patriotism and the Right to Privacy" in NEW TECHNOLOGIES AND HUMAN RIGHTS 135 (Thérèse Murphy ed., 2009). For a parallel discussion of the application of the fundamental right to health care and the authority of the European Union, see Christina Simpson, *Policy as a Process: The Pedagogical Role of the EU in Health Care*, 33 N.C. J. INT'L L. & COM. REG. 293, 316-19 (2007)(discussing the sovereignty issue and the relationship to health regulation).

Fundamental Freedoms states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[114] In 1981, the Council of Europe specifically addressed automated information collection and processing in its Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Data Convention). The Data Convention states that countries shall "respect. . .rights and fundamental freedoms, and in particular [the] right to privacy" for all individuals, regardless of nationality.[115] The Data Convention has been described as the set of first international legal principles to protect data privacy.[116] Summarized, the principles include: fair information collection for a specific purpose, limitation to the specified purpose, accuracy, storage for no longer than necessary for the purpose, accessibility by the subject, and reasonable security.[117] The Council of Europe adopted more specific medical privacy recommendations in 1981, which addressed the treatment of automated medical data banks.[118] These recommendations were replaced in 1997 by a recommendation covering medical data in general.[119] Furthermore, in 1991 the Council adopted recommendations covering transborder data flows.[120]

Furthermore, international declarations of privacy standards are also relevant, and show a correlation between the development of privacy recognition in the EU and the international stage. There is an evident historical connection between the adoption of the first individual privacy principles at the end of World War II and the advent of technology and automated information

---

[114] *See* Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

[115] *See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[116] *See* Data Protection Legislation, EUROPEAN DATA PROTECTION SUPERVISOR, http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2.

[117] See Convention, *supra* note 115.

[118] *Recommendation No. R (81) 1 of the Committee of Ministers to Member States on Regulations for Automated Medical Data Banks*, COUNCIL OF EUROPE (Jan. 23, 1981), http://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=599521&SecMode=1&DocId=670452&Usage=2.

[119] *Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data*, COUNCIL OF EUROPE (Feb. 13, 1997), http://www1.umn.edu/humanrts/instree/coerecr97-5.html.

[120] *Recommendation No. R (91) 10 of the Committee of Ministers to Member States on the Communication to Third Parties of Personal Data Held by Public Bodies*, COUNCIL OF EUROPE (Sept. 9, 1991), http://www.coe.int/t/e/legal_affairs/legal_co-operation/administrative_law_and_justice/Texts_&_Documents/Conv_Rec_Res/Recommendation(91)10.asp.

collection in the early 1980s.[121] The 1949 U.N Universal Declaration of Human Rights, Article 12, states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. . ."[122] In 1980, the Organization for Economic Cooperation and Development (OECD) issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines).[123] These guidelines contain, in summary, these principles: limitation of data collected, maintenance of data quality, specification of the collection purpose, limitation of data use to that specified purpose, adequate security, transparency, individual access to and control of data collected, and accountability.[124] In 1998, the OECD reviewed the guidelines in light of the enormous changes in electronic communication, and confirmed the application of these basic principles to that environment.[125] The OECD continues to work towards international standards in data privacy, and in recent work expanded its policy to the cross-border flow of information.[126]

B. European Union Privacy Principles

The current EU treatment of individual privacy builds upon these international and supranational foundational principles and policy documents, and is found primarily in two directives: the 1995 Directive on protection of individuals with regard to the processing of personal data and on the free

---

[121] *See* David L. Baumer et al., *Internet Privacy Law: A Comparison Between the United States and the European Union*, 23 COMPUTERS & SECURITY 400, 401 (2004); *see also* Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 374-75 (2005) (privacy protections developed after World War II); *see also* Tracy B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 423-24 (2002).

[122] *See* Universal Declaration of Human Rights, G.A. Res. 217A, at 71, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948), *available at* http://www.un.org/en/documents/udhr/.

[123] Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris 1981), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html; *see also* Baumer, *supra* note 121, at 402.

[124] *See* Baumer, *supra* note 121, at 402.

[125] *See* The Organization for Economic Co-operation and Development, *Protection of Privacy and Personal Data*, http://www.oecd.org/document/26/0,3343,en_2649_34255_1814170_1_1_1_1,00.html (last visited on Oct. 18, 2010).

[126] *30 Years After: The Impact of the OECD Privacy Guidelines*, THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, http://www.oecd.org/document/39/0,3343,en_2649_34255_44946983_1_1_1_1,00.html (last visited on Oct. 18, 2010).

movement of such data (Data Directive),[127] and the 2002 Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector.[128]

The Data Directive created the Article 29 Working Party, or the Article 29 Board, as an independent advisory board on data protection.[129] In 2007, the Article 29 Board issued the *Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records* [hereinafter EHR Report].[130] The EHR Report provides an interpretation of the application of privacy principles to electronic health records, and recommends adoption of eleven specific legal protections to protect individual health privacy. A detailed review of this document is essential to understanding the way in which fundamental privacy protection will be applied to electronic health records in the EU.

C. Translating General Data Privacy to Health Privacy

The EHR Report states unequivocally that "[a]ny processing of personal data in EHR systems has to fully comply with the rules for the protection of personal data."[131] Hence, any data controller collecting individually identifiable health information must: limit data use to the purpose for which it was collected (purpose principle), ensure data quality (relevancy and accuracy), limit data retention (and not further process the data), provide individuals with data collection information and access to the information collected (with rights of correction), and provide appropriate data security measures.[132] The report indicates that the Data Directive gives health

---

[127] Bignami, *supra* note 113, at 139-41. *See also* Council Directive 95/46/EC art. 1, 1995 O.J. (L 281) 10, 11 (EC).

[128] Bignami, *supra* note 113, at 139-41. *See also* Council Directive 2002/58/EC art. 5, 6, 9, 2002 O.J. (L 201) 11, 12, 14 (EC).

[129] Council Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, art, 30, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0047:EN:HTML.

[130] Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records* 2 (Article 29 Working Party, Working Paper No. 131, 2007) *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.

[131] *Id*. at 6.

[132] *Id*. at 6-7. According to Article 10 of the 1995 EU Information directive, a "controller" is "the natural or legal person, public authority, agency or any other body which alone or with others determines the purposes and means of the processing of personal data." Council Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, art, 2, 1995 O.J. (L281) 31.

information greater protection because it is a "sensitive" category of personal information. Article 8(1) of the Data Directive mandates that "Member States shall prohibit the processing of. . .data concerning. . .health."[133] While certain information, such as a particular injury or drug use, may clearly fall in the category of health data, the Working Party specifies that "if [data] were not relevant in the context of the treatment of the patient, they would and should not have been included in a medical file."[134] Therefore, "all data contained in medical documentation, in electronic health records and in EHR systems should be considered to be 'sensitive data.'"[135] The global categorization of all health information collected by a data collector as sensitive data is a hallmark of individual privacy protection; it provides the bedrock upon which individuals are given control over health information collected by health professionals.

a. Limited Health Data Derogations

While the prohibition on processing health data is overarching, it is not draconian. The Data Directive contains several mandatory derogations and one optional derogation. States must allow for derogations to process health information when the individual gives explicit consent if it is "necessary to protect the vital interests"[136] of either the individual or on behalf of one incapable of giving consent and in limited circumstances when the data is collected by health professionals. In addition, states may, but are not required to, allow data to be collected when there is a "substantial public interest."[137] Each of these derogations is discussed in detail in the EHR Report, and is summarized below.

1. Explicit Consent

The first possible derogation is that an entity may collect and process health information when the affected individual grants explicit consent. The consent must be given by a positive communication of consent, an opt-in procedure rather than an insufficient opt-out procedure. In addition, the consent must be specific, voluntary, informed, and not coerced in any way. In that respect, consent that is obtained because of a "threat of non-treatment or lower quality treatment in a medical situation"[138] would be coercive and illegitimately obtained. In addition, if information is collected before consent is granted,

[133] Article 29 Data Protection Working Party, *supra* note 130, at 7.

[134] *Id.*

[135] *Id.*

[136] *Id.* at 9.

[137] *Id.* at 1.

[138] *Id.* at 8.

later consent may not "legitimize" the previous processing.[139]

Lastly, because of the sensitive nature of health information collection and processing, a country may adopt an absolute prohibition on processing specified health information, which cannot be overcome by consent.[140]

2. Vital Interests

A derogation based on the vital interests of the patient or on behalf of another who is "physically or legally incapable of giving his consent" will only apply to a "small number of cases."[141] The example given is when medical treatment and access to information is given to an unconscious patient, thus illustrating the narrow nature of this exception.[142]

3. Health Professionals

For health professionals to process health information as a derogation to the general rule, (1) processing must be required for the purpose of "preventive medicine, medical diagnosis" (2) for the "provision of care or treatment or the management of health-care services," and (3) the health professional processing the information must be bound by law or professional rules to professional secrecy or the "equivalent."[143] This derogation specifically states that it does not enable health research, insurance reimbursement processing, discovery or other aspects of evidence in a lawsuit, or processing of information for public health.[144]

The report emphasizes that the derogation for health professionals "must be interpreted in a restrictive way" and that it does not, in and of itself, validate an overall EHR system.[145] A further comment warns that many purposes of an EHR system, such as sharing health information among medical professionals, inherently conflict with privacy.[146] An EHR system will challenge the presumption of privacy preservation, especially applied to internet records and exchanges, and new, additional safeguards may be needed to address the fundamental conflicts and dangers of exchanging information in an electronic environment.[147]

---

[139] Article 29 Data Protection Working Party, *supra* note 130, at 8.

[140] *Id*. at 9.

[141] *Id*.

[142] *Id*. at 10.

[143] *Id*.

[144] *Id*.

[145] Article 29 Data Protection Working Party, *supra* note 130, at 11.

[146] *Id*.

[147] *Id*. at 11-12.

4. Public Interest

As seen, it would be difficult, if not impossible, to institute widespread and comprehensive EHRs under the foregoing derogations of explicit consent, vital interests, or health professionals. Importantly, with suitable safeguards, the optional public interest derogation may provide the basis for a national EHR system. This derogation is allowed "[f]or public health and social protection," Data Directive 8(4) reasons, if three requirements are met: (1) there must be a "[s]pecial legal basis" that establishes the need and foundation for the EHR system, (2) information processed under this system must be necessary and proportional to the need, and (3) the system must include "specific and suitable safeguards" for fundamental privacy.[148] The European Convention on Human Rights applies to any EHR system that interferes with family and private life. Therefore, any system must be "necessary in a democratic society" and protections must be provided for within the law.[149]

In conclusion, the Report notes that an EHR may be adopted under the public interest exemption, yet it warns that careful compliance with the Directive requirements is necessary.[150] As a result, the report proceeds to describe elements of the "suitable legal framework for EHR systems"[151] that are needed in order to preserve privacy and security.

D. Legal Framework for EHR

Rules for the protection of health information privacy and related security requirements "should preferably be laid down in a special comprehensive legal framework."[152] The Article 29 Report outlines eleven areas that should be included in this legal framework, which would preferably be contained in a unique legal section. The following sections summarize the substantive areas that the Report advises should be addressed in the law.

a. Self Determination

Patient control (self determination) is always appropriate, even when collection of the information is not based on consent. In fact, it is stated that a patient should "always" have the ability to prohibit the sharing of information, even with another health professional.[153] Indeed, it is stated that "nobody could be forced to take part in an EHR system."[154] However, the Report

[148] *Id*. at 12-13.

[149] *Id*. at 12.

[150] *Id*. at 13.

[151] Article 29 Data Protection Working Party, *supra* note 130, at 13.

[152] *Id*.

[153] *Id*. at 14, III(1)(c).

[154] *Id*. at 14, III(1)(d). The report leaves open whether the individual must be completely

outlines a continuum for the type of consent or agreement that is necessary for the collection of health information. While an opt-out procedure may be appropriate for ordinary health processing, opt-in would be required for the processing of more sensitive health information such as mental health treatment or sexually related treatment.[155]

b. Identification and Authentication

Identification and authentication requirements apply to both patients and healthcare professionals. While patient identification is "crucial" in order to provide proper treatment, healthcare professionals must also be identified in order to protect against unauthorized persons gaining access.[156] The Report anticipates electronic forms of identification and authentication.[157]

c. Authorized Access Safeguards

The Report identifies general access safeguards and special access safeguards. General safeguards are needed to ensure that only those professionals who are immediately treating the patient have access to the records; the creation of a tiered or "modular" access system that further segments types of information and its accessibility to certain healthcare professionals is recommended.[158] Special safeguards are described as those involving patient agreement to information access; these might include sealing certain information in an electronic "envelope" to restrict access, or giving the patient direct access to the system in order to make determinations about access.[159]

d. Third Party Use of Information

The Working Party incorporates the requirements of the Data Directive Article 8, including certain prohibitions on sharing, and the possibility of anonymizing information in the case of use for research or government purposes.[160]

e. System Design

The Report identifies three options for system design that could be legally

deleted from the system or whether preventing access to the information is sufficient.

[155] *Id*. at 14, III(1)(b).

[156] *Id*. at 14-15, III(2)(a)-(b). It is important to emphasize the absoluteness with which the Report states the conclusion that no unauthorized person be allowed access to health records.

[157] Article 29 Data Protection Working Party, *supra* note 130, at 14-15, III(2)(b).

[158] *Id*. at 15, III(3)(a).

[159] *Id*. at 15, III(3)(b).

[160] *Id*. at 16, III(4).

mandated. Control by the patient is not recommended because of security and accuracy concerns.[161] A decentralized system wherein each provider keeps information and the information is searchable in some manner by others would require the establishment of "one central body to be responsible for steering and monitoring the whole system" to ensure privacy and system compatibility.[162] Lastly, the centralized system, with one data controller who operates as a repository for information from all the healthcare professionals, might pose a higher risk for unauthorized access and security. Additional security measures, such as increased encryption requirements, might be necessary if a centralized system is implemented.

f. Data Storage

This section of the legal framework addresses what information should be collected and for how long it should be stored. It states that a complete health record is nearly "impossible" and also undesirable.[163] While the choice is primarily a medical one, the Report espouses the view that it is also a privacy choice as well. In order to protect the privacy of the data, data modules may be created containing different kinds of information. The report uses the example of a "vaccination data module" as a kind of useful categorization; when vaccination information is needed then only that module would be accessible.[164] In essence, this complexity allows for privacy protection by segmenting information, and then allowing for access by others only to that particular segment of information. A patient might decide that vaccination information could be shared with public health officials, employers, or even schools. At the same time, granting access to the vaccination information would still protect all other health information not in that module. Limited access to information modules by insurance companies could be particularly helpful.[165]

g. International Transfer

The Report is clear that no identifiable health data should be transferred or stored outside the EU unless there is an "adequate legal framework"[166] to protect the data. Anonymizing health records for second opinions, for example, could address this problem.[167]

---

[161] *Id*. at 17, III(5)(a)-(c).

[162] *Id*. at 17, III(5)(b).

[163] Article 29 Data Protection Working Party, *supra* note 130, at 18, III(6)(a).

[164] *Id*. at 18, III(6)(b).

[165] *Id*. at 18, III(6)(c). "Granting access to private insurance companies to the EHR of a patient seems unacceptable." *Id*.

[166] *Id*. at 19, III(7).

[167] *Id*.

h. Data Security

The security of a system is emphatically required. The Report states that "[a]ccess by unauthorised persons must be virtually impossible. . .."[168] Thus, the legal framework must include technical and organizational elements.[169] The report mentions: encryption of data and other privacy enhancing technologies, electronic identification and authentication, internal documentation and control of access, backup and recovery systems, personnel policies, individual competence requirements, and auditing.[170]

i. Transparency

Transparency of the content and functioning of an EHR, by means of public notification and easily accessible and free information for patients, is required to create trust and effective use of the system.[171]

j. Liability

Rather than adopt standards for liability for failure to protect health information, the Report advises that member states should:

> [I]n advance conduct in-depth, expert civil and medical law studies and impact assessments to clarify the new liability issues likely to arise in this context, e.g. regarding the accuracy and completeness of data entered in EHR, defining how extensively a health care professional treating a patient must study an EHR, or about the consequences under liability law if access is not available for technical reason, etc.[172]

k. Process Control Mechanisms

The Working Party recommends that an overarching institution be established to respond to data access questions, and that free and accessible arbitration be used to settle conflicts between data controllers and subjects (patients).[173] In addition, an access trail should be available to the patient,[174] and "[r]egular internal and external data protection auditing of access protocols must take place."[175]

---

[168] *Id*. at 19, III(8).

[169] Article 29 Data Protection Working Party, *supra* note 130, at 19, III(8).

[170] *Id*. at 20.

[171] *Id*. at 20, III(9).

[172] *Id*. at 20, III(10).

[173] *Id*. at 21, III(11)(a)-(b).

[174] *Id*. at 21, III(11)(c).

[175] Article 29 Data Protection Working Party, *supra* note 130, at 21, III(11)(d).

E. Privacy of Cross-Border EHR Systems

Subsequent to the Article 29 Working Party guidance, the European Commission released the *Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems* [hereinafter Cross-border Recommendation].[176] The section "Protection of Personal Data" is the relevant portion of the recommendation dealing with privacy of health information in an electronic health system that crosses national boundaries.[177] The Cross-border Recommendation reaffirms that collection of health data is particularly sensitive, is covered by the Data Protection Directive, and that a specific legal framework is necessary for addressing the privacy of this sensitive data. The Cross-border Recommendation particularly notes that,

> When implementing interoperability of electronic health record systems, it should be pointed out that EHR systems create a significant new risk scenario for processing of personal data concerning health, which calls for new, additional safeguards and counterbalances: maintaining the legal standard of confidentiality suitable within a traditional paper record environment may be insufficient to protect the privacy interests of a patient once electronic health records are put online.[178]

Furthermore, the recommendations note that "[m]ember states should be aware that interoperable electronic health record systems increase the risk that personal data concerning health could be accidentally exposed or easily distributed to unauthorized parties, by enabling greater access to a compilation of the personal data concerning health, from different sources, and throughout a lifetime." [179]

The Cross-border Recommendation requires adoption of a "comprehensive

---

[176] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems, document number C(2008) (3282); (2008/594/EC), *available at* http://www.epractice.eu/files/media/media2134.pdf. "In Community law, a Recommendation is a legal instrument that encourages those to whom it is addressed to act in a particular way without being binding on them. A recommendation enables the Commission (or the Council) to establish non-binding rules for the Member States or, in certain cases, Union citizens." *Glossary*, EUROPEAN JUDICIAL NETWORK IN CIVIL AND COMMERCIAL MATTERS, EUROPEAN COMMISSION, http://ec.europa.eu/civiljustice/glossary/glossary_en.htm#Recommendation (last visited on Oct. 18, 2010).

[177] Commission Recommendation, *supra* note 176, at 18-20, Paragraphs 10-15.

[178] *Id*. at 9.

[179] *Id*. at 18, Paragraph 12. For an overall discussion of health information and offshore data processing, *See* Nicolas P. Terry, *Under-Regulated Health Care Phenomena in a Flat World: Medical Tourism and Outsourcing*, 29 W. NEW ENG. L. REV. 421, 440-41 (2007) (discusses outsourcing and medical tourism and argues for a flat world of health information regulation).

legal framework"[180] that includes protection of personal privacy in electronic health record systems. The one dozen specific legal recommendations for protecting personal health data are shorter and more general than the standards set out by the Article 29 EHR Report, however, they incorporate the fundamental principles of the earlier document. Summarized, they call for:

- consideration of alternatives for systems and storage of records to reflect best practices,[181]
- utilization of easy to use technology for a patient to exercise control and freely make decisions about health information storage and disclosure,[182]
- requiring systems to be designed for limited data collection, or no collection, and the inclusion of an option for anonymization,[183]
- risk assessments for security breaches prior to implementation,[184]
- delineation of what health information may and may not be electronically stored or processed, and if a subset of information is subject to stricter controls,[185]
- limitation of the processing of data to health professionals who are clearly identified and subject to secrecy under professional or state regulations,[186]
- policy, security, and technical rules for access to and use of health information by entities other than the individual, enforceable by national data protection authorities and technology,[187]
- notice to patients about the implementation of EHR systems, including options for accessing understandable information about the system,[188]
- procedures for the prevention of inappropriate pressure for an individual's participation,[189]
- limiting data to jurisdictions that abide by the Directive,[190]
- auditing procedures for compliance, and[191]
- security measures and breach notification procedures to "guarantee

[180] Commission Recommendation, *supra* note 176, at 10.

[181] *Id*. at 18.

[182] *Id*. at 19.

[183] *Id*.

[184] *Id*.

[185] *Id*.

[186] Commission Recommendation, *supra* note 176, at 19.

[187] *Id*.

[188] *Id*.

[189] *Id*.

[190] *Id*.

[191] *Id*. at 20.

confidentiality of electronic health record systems."[192]

F. Future Steps: The Prague Declaration

On February 19 and 20, 2009, European Union Health Ministers met at the conference, "eHealth for Individuals, Society and Economy,"[193] to discuss eHealth implementation across the EU. As a result, the participants adopted the Prague Declaration,[194] identifying areas that needed attention for the realization of the potential of eHealth, and outlining three areas for special attention.[195] Patient safety and empowerment was one of the three areas singled out as essential for future development of communications technologies and health systems. Member states were exhorted to pay close attention to "legal and ethical issues" including "data protection and privacy issues. . .[in pursuit of] a common approach to optimize existing directives on data protection and privacy."[196] While lacking particulars, the Prague Declaration embodies the policy and intent of EU Health Ministers to pay close attention to matters of patient privacy. The declaration is a clear signal that the technical integration of health systems is insufficient by itself. Systems must also include processes for protecting the security and privacy of individual health information.

V. COMPARISONS AND LESSONS

The U.S. and EU approaches to balancing the promotion of EHRs to improve health care efficiency on the one hand, with personal privacy and security on the other hand, are vastly different. Yet, they do contain some fundamental similarities. The next section compares EU and U.S. health privacy protection beginning with a discussion of overarching approaches. The comparison is then framed by using the fair information privacy principles adopted by the Federal Trade Commission.[197] Within the comparisons of

---

[192] Commission Recommendation, *supra* note 176, at 20.

[193] Press Release, Czech Health Minister Daniela Filipiová opens European conference of Health Ministers entitled "eHealth for Individuals, Society and Economy" in Prague (Feb. 19, 2009), *available at* http://www.ehealth2009.cz/file.aspx?id=107&name=press%20release.doc.

[194] *Id*.

[195] eHealth 2009 Conference; The Prague Declaration, Feb. 20, 2009, http://ec.europa.eu/information_society/activities/health/docs/events/2009/ehealth2009/prague_declaration.pdf.

[196] *Id*. at 3. For an example of how one EU country has proceeded to implementation, *See* Klaus M. Brisch & Claudia E. Haupt, *Information Technology meets Healthcare: The Present and Future of German and European E-Health Initiatives*, 12 DEPAUL J. HEALTH CARE L. 105 (2009).

[197] It could be argued that a broader set of privacy principles should be used.

differences and similarities is discussion of the following questions: Do the regulations protect the same breadth of personal health information? What are a patient's rights of notice and control over health information collection? What are the implications for the broad sharing of health information across a national health network with third parties? And are security and enforcement mechanisms sufficient to protect the rights of patients? The comparisons and answers to those questions will reveal how the balance is struck between electronic health records and personal privacy and security.

A. Summary Comparison

U.S. and EU assumptions for implementing privacy within an EHR system are worlds apart. A fundamental reason for these differences could be the differing foundations of individual privacy; whereas the U.S. established the right of an individual to health information privacy through a specific statute, in the EU this basic privacy right already existed under a human right to privacy, even before the adoption of the directives. This opposing jurisprudence leads to several distinguishing features.

Procedurally and substantively, the passage of HIPAA, as amended by HITECH, was necessary for the protection of individual health information in the U.S., and while not using the exact words, in a sense it identified personal health information as a category of sensitive information worthy of heightened protection.[198] In comparison, in the EU, health information was identified as a unique and sensitive category of information in the Data Protection Directive.[199] While in the U.S. further detailed regulation is adopted by HHS and to a lesser extent the FTC, in the EU the Article 29 Working Party has authority for policy and guidance. HIPAA allows for more detailed rules at the federal level by regulatory process than the Article 29 Working Party, which leaves detailed implementation to member states.

Thus, essential differences between U.S. and EU law are crucial to understanding the potential functioning of an EHR system. HIPAA can be interpreted as based on the assumption that health information will be collected from the individual; its focus is on the subsequent protection, use, and sharing of that information. The EU framework begins with detailed considerations about whether the information may be collected and how to protect patients in the original collection process. As a corollary, patients in the U.S. have no real choice as to whether to participate in the system, whereas EU policy contemplates that protections should be implemented to prevent coercion of a patient into participation.

In addition, it should be noted that emerging rulemaking and standard setting in the U.S. as well as the EU member state integration of health privacy

[198] *See supra* Section III.

[199] *See supra* section IV (B).

must temper the comparisons described in the next section.

B. Under the Microscope: Fair Information Principles

The following sections utilize the Fair Information Practice Principles as adopted by the Federal Trade Commission in order to compare the EU and U.S. approaches in more detail.[200] The five principles are a subset of international principles to protect individual privacy, and are shared by the EU and U.S.[201]

1. Notice and Awareness of How Information is Shared

Individuals are unable to protect themselves or make informed decisions about whether to share information if they are neither aware that the information is being collected nor aware of how the information will be used once collected. The U.S. emphasizes that information must be given to individuals in a covered entity's privacy notices. Notices must contain: basic information about how information is used and disclosed to other parties, the entity's duty to protect patient privacy, how the entity accomplishes this, a patient's right to complain to HHS, and contact information for filing complaints.[202]

The EU Data Protection Directive contains detailed information that a data processor must make available whenever any individually identifiable information is used.[203] In addition, transparency of health systems, notice, and ease of information are also contained in the Working Party EHR Report.[204] The Cross-border Recommendation includes: use of alternate means of notification, the implementation of easy to use technology to facilitate access, and the consideration of notice that is appropriate for "persons with special needs."[205] The EU emphasis on actual patient understanding of information collection and sharing, depending on individual circumstances, sets it apart from the less specific U.S. requirements.

2. Choice and Consent to Share Health Information

Since the U.S. and EU have diametrically opposed starting points for what health information may be collected, direct comparison of the subsequent sharing of that information is difficult and must be understood within the varying frameworks. The differences continue when making comparisons

---

[200] Federal Trade Commission, *Fair Information Practice Principles*, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007).

[201] Federal Trade Commission, PRIVACY ONLINE: A REPORT TO CONGRESS 7-11 (1998).

[202] 45 C.F.R. § 164.520 (2009).

[203] *See* Baumer, *supra* note 121 and accompanying text.

[204] *See generally* Article 29 Data Protection Working Party, *supra* note 130, at 6.

[205] *See* Commission Recommendation, *supra* note 176, at 14(h).

between the frameworks for a patient's choice and consent to share personally identifiable health information with third persons. HIPAA contains so many exceptions to when a patient's consent is needed to share information, that in practice it offers limited instances for patient choice; instead it is argued that HIPAA should "empower patients to assert control"[206] of their health information.

The public interest exception is the only true avenue for implementing an EHR in the EU. This exception requires an explicit legal basis that is tailored to the circumstances and that always allows the right of the patient to either limit sharing or withdraw completely from the system. Thus, the EU and U.S. approaches to consent and sharing are strikingly dissimilar, as the following chart illustrates.

SHARING INFORMATION	U.S. REGULATION	EU REGULATION
Required disclosure; no consent or authorization needed	• To individual upon request • To HHS; audit, law enforcement	• To individual*

Permitted disclosure; no authorization needed	• To individual
	• For treatment
	• For payment
	• For healthcare operations
	• Incident to other permitted disclosure
	• In the public interest (12 specific instances)
	• Limited data set
	• Whenever individual given an opportunity to agree/object
		• For a substantial public interest
		  • Under law or regulation &
		  • Limited scope and proportional
		  • With safeguards (see below: subject to patient's right to prohibit disclosure)

Optional disclosure;written	• Psychotherapy notes • Marketing	(see below: members can proscribe)

[206] Moore, *supra* note 37, at 258-61. "In short, HIPAA is guilty of duplicity. While purporting to provide something that people value, it actually prioritizes the health care team's function over individuals' preferences and shields health care workers and institutions from liability for disclosures related to those functions. . . . Patients' 'privacy rights' under the regulations describe procedural rights, not substantive rights." *Id.* at 251; *see also* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 681 (2007).

authorization required	(with exceptions)	
Prohibited disclosure	Any other situation not listed above**	• Patient withdraws completely from EHR • Patient limits forward sharing • Patient limits sharing of specific information • Patient fails to opt-in when particularly sensitive • Patient opts-out • Member countries may completely prohibit sharing certain information in domestic implementation

* with identification

** HIPAA states that protected health information may not be shared except by written authorization or under provisions of the Privacy Rule. Also note that fundraising efforts must include an opt-out provision.

3. Patient Access and Participation in Accuracy of Data

Subject to exceptions, HIPAA provides a patient the right of access to his or her health records. Copies may be made subject to reasonable costs borne by the patient. Although the patient may request changes to the record, the entity is not required to implement those changes. Procedures are established for the patient to pursue the request; if it is ultimately denied, then the patient has the right to include a statement in the record disagreeing with the information.[207]

The EU emphasis on patient control of health information underpins its approach to access and accuracy. Therefore the policy emphasizes security aspects such as ensuring that the person requesting the information is properly identified as the patient. In addition, it is recommended that a unique institution handle access requests so as to simplify the process for patients in a complex technical system with multiple participants.[208]

4. Integrity and Security of Data

The U.S. requires the implementation of administrative, physical and technical standards for security; those requirements are contained primarily

[207] 45 C.F.R. § 164.524 (2009) and 45 C.F.R. § 164.526 (2009).

[208] Article 29 Data Protection Working Party, *supra* note 130, at 21.

within the HIPAA Security Rule.[209] While the Security Rule contains a rather comprehensive framework, it does not require specific technical solutions but rather allows entities to find multiple avenues to ensure security.[210] The U.S., through the implementation of HITECH, also has more detailed breach notification rules that are recently being developed in the EU.[211]

The EU does not address security in the more detailed manner of the Security Rule. It does address requirements for organizational, process and technical protection. Policy also addresses the need for general and special safeguards for authorized access, including anticipation of electronic methods of identification and auditing of systems.[212] The unique aspect of EU security as compared to the U.S. is a consideration of both overall system choices and of particular opportunities for designing for privacy. The Article 29 EHR Report discusses whether an EHR system should be centralized or de-centralized; it does not require that one choice be adopted, but identifies

---

[209] *See* Health Insurance Reform, *supra* note 57.

[210] The Security Rule, 45 C.F.R. pts. 160, 164(a), (c) (2009).

"The general requirements of the HIPAA Security Rule establish that covered entities must do the following:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
4. Ensure compliance by the workforce.

Covered entities have been provided flexibility of approach. This implies:

1. Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications.
2. In deciding which security measures to use, a covered entity must take into account the following factors:
   i. The size, complexity, and capabilities of the covered entity.
   ii. The covered entity's technical infrastructure, hardware, and software security capabilities.
   iii. The costs of security measures.
   iv. The probability and criticality of potential risks to electronic protected health information."

HIPAA Security Rule Overview, HIPAA ACADEMY (Oct. 4, 2010, 1:22 PM), *available at* http://www.hipaaacademy.net/consulting/hipaaSecurityRuleOverview.html; *see* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 337 (2007).

[211] *See supra* Section III(A)(4).

[212] *See supra* Section IV(D)(e).

privacy considerations for each type.[213] In addition, both the EHR Report and the Cross-border Recommendation express preferences for particular methods of system design that would facilitate privacy and security, including: anonymization, and separate information modules for different types of information subject to varying security and authorization protocols. The Cross-border Recommendation also includes breach notification, but leaves details for further development.[214]

5. Enforcement and Redress

One of the most criticized aspects of HIPAA is its lack of individual redress for violations.[215] Although civil and criminal sanctions are possible, they are rare.[216] However, HITECH increased enforcement and criminal and civil penalties, thereby emphasizing the focus being placed in these areas.[217]

EU enforcement mechanisms are contained under the general purview of Article 8; enforcement is required but specifics are left to member countries. Data protection authorities in member countries serve to enforce the Directive as implemented internally.[218] The EHR Report further states that each member state should study and implement remedies for the violation of health information protection.[219] Furthermore, the Cross-border Recommendation limits international transfer without adequate protection, and identifies breach notification for inclusion within domestic law.[220]

C. Recommendations for the U.S.

As the driver behind EHR adoption, the U.S. federal government has an important role in establishing rules to protect the privacy and confidentiality of healthcare information. As the discussion highlights, the protections provided by U.S. law are increasing, but are still limited in comparison with the EU. Patients have no control, absent withholding information, over the initial collection of sensitive health information, and considering the large number of exceptions they have strikingly little control over the information that can be

---

[213] *See* Article 29 Data Protection Working Party, *supra* note 130, at 17, (IV)(D)(e).

[214] *See supra* sections IV(D)(e) and IV(E).

[215] Joshua D.W. Collins, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 201 (2007). Although HITECH strengthened the enforcement features of HIPAA, there is no private right of action. *See supra* section III(A)(5).

[216] Collins, *supra* note 215, at 202.

[217] *See supra* Section IIIA (5).

[218] Council Directive 95/46, art. 24, 1995 O.J. (L 281) 31, 45 (EC), *available at* http://aspe.hhs.gov/DATACNCL/eudirect.htm.

[219] *See* EHR Report, *supra* note 122, at 20.

[220] *See generally*, Article 29 Data Protection Working Party, *supra* note 130.

shared down the line with other health and insurance entities. A series of Government Accountability Office (GAO) reports addressed the need for attention to questions of privacy in the realm of health information.[221] Although subsequently addressed in part by HITECH, in one report, the GAO recommended improvements in a wide swath of privacy protections, including standards for obtaining patient consent, enforcement, and disclosure standards.[222]

In fundamental ways, EU law has made more significant progress towards the dual goals of effective implementation of EHRs and the protection of individual privacy through enabling patient control. The regulatory body used to promote and guide uniformity in the EU, the Article 29 Working Group, has described a framework for health privacy protections as they relate to electronic health record systems. In comparison, the regulatory structure in the US, while becoming clearer, is still adapting to technological changes. The FTC, while becoming more involved with the problems of medical identity theft, is recently establishing its jurisdiction, and tackling the tough policy questions related to individual privacy concerns in health information technology.[223] It is yet to be seen if the HITECH framework will sufficiently enhance their authority, and increase their participation in healthcare privacy in a way that bolsters consumer trust. Thus, the lack of stronger governmental protection mechanisms, exacerbated by the lack of a private cause of action, may not inspire patient/citizen confidence and trust in EHRs.[224] As a result, it seems clear that the security of health information, while always a critical component to an effective system and protection of the patient becomes exponentially more important in a system that allows for the wide sharing of that information electronically.

---

[221] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-238, HEALTH INFORMATION TECHNOLOGY: EARLY EFFORTS INITIATED BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY (2007); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-400T, HEALTH INFORMATION TECHNOLOGY: EARLY EFFORTS INITIATED BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY (2007); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-988T, HEALTH INFORMATION TECHNOLOGY: EFFORTS CONTINUE BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY (2007); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-499T, HEALTH INFORMATION TECHNOLOGY: HHS IS PURSUING EFFORTS TO ADVANCE NATIONWIDE IMPLEMENTATION BUT HAS NOT YET COMPLETED A NATIONAL STRATEGY (2008).

[222] Goldstein et al., *supra* note 35, at 94-95.

[223] *See, e.g.*, Health Breach Notification Rule, 16 C.F.R. § 318, *available at* http://www.ftc.gov/os/2009/08/R911002hbn.pdf (2009).

[224] *See* Nicholas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 730-31 (2007) (suggesting an independent regulatory entity).

VI. CONCLUSION

The U.S. legal framework for healthcare privacy is a combination of constitutional, statutory, and regulatory law at the federal and state levels. Differing and conflicting state privacy laws led to enactment of the 1996 Health Insurance Portability and Accountability (HIPAA) Act of 1996. More recently the Health Information Technology for Economic and Clinical Health Act (HITECH) Act of 2009 amended HIPAA. Regulatory promulgations from the U.S. Department of Health and Human Services resulted in the Privacy Rule and the Security Rules. These Rules define the rights of patients with regard to protected health information and the obligations of firms (covered entities and business associates) that possess such information. Regardless of the statutory and regulatory laws enacted to protect the privacy of health information, there is an inevitable tension between ease of access to EHRs for effective treatment of patients and the efficient operation of the health care system on the one hand, and protecting personal privacy of medical records on the other hand. Further, due in part to the interests of medical research, public health issues, and law enforcement, a plethora of socially beneficial uses can compete with the argument for patient control of medical information.

EU privacy protection for health information was shaped by historical events. Specific protections for medical information were passed by the Council of Europe in 1981 and further protections ensued. The current protection of information privacy in the EU was crucially augmented in 1995 with passage of the Data Directive and the 2002 Directive Concerning Personal Data and the Protection of Privacy in the Electronic Communications Sector. The 1995 Data Directive created an Article 29 Working Party that, in 2007, issued a working document on the processing of personal data in electronic health records (EHR Report). The EU protection of privacy, including the classification of personally identifiable medical information as “sensitive”, has generally granted individuals a higher degree of protection. The standard is that the patient should always have the right to prohibit transfer of health information that is in an electronic system. Another significant privacy safeguard found in EU law regarding cross-border transmissions is the requirement that foreign recipients of EHRs must agree to abide by the basic rules of EU protection of personally identifying health records.

Direct comparisons of U.S. and EU medical privacy laws can be made with reference to the five Fair Information Practices Principles (FIPs). In sum, the U.S. notice and awareness of data collection can be satisfied through the privacy practices statement of the company collecting the information, and this information can appear in the company’s web site. In the EU, notices to the patient must state that information has been collected, how the information will be used, the entity’s obligation to protect privacy, and contact information for complaints by the patient. The exception-riddled HIPAA effectively undermines patient control, as there are many legal avenues for collecting,

processing, and transmitting protected health information without obtaining patient consent or authorization. In the EU, the public interest exception is the only avenue for obtaining and transmitting patient medical information via EHRs without consent of the patient, and the patient can always object to the sharing of information. The patient in both EU and U.S. law has access to their health records. In the U.S. the patient can object to information in his or her health records, but the covered entity is not required to make changes requested by the patient. If the patient appeals through several levels, he or she can issue additions to his or her medical record. Therefore, while in both the U.S. and the EU a patient has access to the record and may view the disclosures, this right is more limited in the U.S. Although federal protection of health record privacy in the U.S. seems to be a gain over conflicting state law, in comparison to the basic framework of rights in the EU, patient rights in the U.S. are more limited. It is clear that the ability of EHRs to save a significant amount of money depends on public acceptance and effective implementation of those new systems. To the public, EHR vulnerabilities appear to be the potential loss of privacy and threats to information security, thus making a comparison of U.S. and EU fundamental frameworks for health privacy particularly relevant. The EU framework begins with the presumption of privacy for sensitive health records. In a sense an electronic health system of collection and sharing must then prove itself to meet those privacy standards. That presumptive privacy protection could serve to calm consumer concerns about the implementation of new systems. In comparison, the U.S. framework, while making progress in the protection of health information, lacks the historical presumption of privacy and thereby may not earn consumer confidence as easily. The same might be said of the technical choices that will be made as health systems are implemented; however more study is necessary to follow these developments.

A combination of privacy enhancing technical choices and improved legal requirements for EHRs could make the loss of patient trust associated with EHRs de minimis. It seems that EU countries have come closer to this position, having both adopted EHRs and reaffirmed commitments to patient privacy principles. If electronic health records in the U.S. are to gain widespread use and provide the predicted substantial benefits, the issue of privacy and security for personal health information must be a continuing part of the discussion and a central feature of implementation frameworks.