Boston College Law Review

Volume 48
Issue 2 *Number 2*

Article 2

3-1-2007

In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information

Sharona Hoffman
sharona.hoffman@case.edu

Andy Podgurski

IN SICKNESS, HEALTH, AND CYBERSPACE: PROTECTING THE SECURITY OF ELECTRONIC PRIVATE HEALTH INFORMATION

SHARONA HOFFMAN*
ANDY PODGURSKI**

Abstract: The electronic processing of health information provides considerable benefits to patients and health care providers while at the same time creating serious risks to the confidentiality, integrity, and availability of the data. The Internet provides a conduit for rapid and uncontrolled dispersion and trafficking of illicitly obtained private health information, with far-reaching consequences to unsuspecting victims. To address such threats to electronic private health information, the U.S. Department of Health and Human Services enacted the Health Insurance Portability and Accountability Act Security Rule, which thus far has received little attention in legal literature. This Article presents a critique of the Security Rule. It argues that the Rule suffers from several defects relating to its narrow definition of "covered entities," the limited scope of information it allows data subjects to obtain about their health information, the vagueness and incompleteness of the Rule's standards and implementation specifications, and the lack of a private cause of action. This Article explores the difficult problem of crafting static regulations to adequately address rapidly changing computer and communications technologies and associated security threats to private health information. In addition, it develops detailed recommendations for improving safeguards for electronically processed health records.

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

** Associate Professor of Electrical Engineering and Computer Science, Case Western Reserve University. The authors wish to thank Jonathan Entin, Max Mehlman, Jennifer Mitchell, and Mark Rothstein for comments on previous drafts. We are also grateful for the skillful research assistance of Cheryl Cheatham, Roselle Ponsoran, and Ian Wilson. Research on this paper was made possible in part by support from the U.S. National Institutes of Health through the Case Western Reserve University Center for Genetic Research Ethics and Law (NIH grant # P50 HG-003390).

Introduction

The electronic processing of health data provides invaluable benefits to patients and health care providers. These benefits include speed and flexibility of information processing, retrieval, and communication; long-term cost savings due to increased efficiency; and the availability of powerful computational techniques that can contribute to improved patient outcomes.[1] Unfortunately, some of these same attributes enable the operation of a market in illicitly obtained private health information. The Internet provides a nearly ideal channel for trafficking in such information because it permits the information to be transmitted anywhere in the world quickly, cheaply, and with relatively little risk of detection.[2] This Article analyzes the threats to electronic health records and the deficiencies of regulations that have been enacted to address them.[3] It also develops recommendations for improving safeguards for these records.[4]

The risks associated with the electronic storage and transmission of personal information in general and health data in particular are indeed grave. A New Year's Day 2006 article in the *New York Times* included the following statement:

> Every week seems to bring reports of a new breach of the computer networks that contain our most intimate personal information. Scores of companies—including Bank of America, MasterCard, ChoicePoint and Marriott International—have admitted to security lapses that exposed millions of people's financial information to potential abuse by identity thieves.[5]

Another article reported that between February and June of 2005 alone, "businesses, universities, and government agencies lost . . . ten million records" and that, according to a Gallup poll conducted in August of 2005, nearly one out of five Americans experienced identity theft.[6] In

---

[1] *See* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. Ill. L. Rev. (forthcoming) (manuscript at 2, on file with authors) (discussing the advantages of electronic health records).

[2] *See* Young B. Choi et al., *Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules*, 30 J. Med. Sys. 57, 60 (2006) (stating that private information can be distributed worldwide within seconds).

[3] *See infra* notes 5–30, 48–193 and accompanying text.

[4] *See infra* notes 194–333 and accompanying text.

[5] John Schwartz, *The Nation: Spy Game; What Are You Lookin' at?*, N.Y. Times, Jan. 1, 2006, § 4, at 1.

[6] Daniel B. Prieto, *Data Mine: Stopping Identity Theft*, New Republic, Dec. 19, 2005, at 17.

May of 2006, a burglary at the home of a Department of Veterans Affairs employee resulted in the well-publicized theft of discs containing names, birthdates, and Social Security numbers of as many as 26.5 million military veterans.[7] Even private cell phone use is vulnerable to public disclosure.[8] Reportedly, dozens of Internet-based companies sell information concerning calls made and received by cell phone users, which they obtain by posing as customers and asking for copies of bills.[9]

The confidentiality of personal health information appears to be compromised with disturbing frequency. A report that focused on discarded hard drives and disk sanitization practices disclosed that in August of 2002, the U.S. Veterans Administration Medical Center in Indianapolis sold or donated 139 of its old computers without removing confidential information contained on their hard drives, including the names of veterans who had AIDS and mental illnesses.[10] An earlier paper published by the British Medical Association reported numerous instances of private health information abuse, including the case of a banker who served on a state health commission and obtained a list of all cancer patients in his state, which he used to single out these individuals and call in their loans.[11] On April 26, 2006, Aetna announced that a laptop computer containing personal information concerning 38,000 consumers had been stolen, and on May 12, 2006, a newspaper article reported that a computer breach may have led to the theft of personal information relating to 60,000 patients who visited Ohio University's health center.[12] Other reported incidents include an inadvertent Internet posting of identifying information and details of the sex lives of ninety psychotherapy patients, an inadvertent posting of sixty children's psychological records on the University of Montana's website, a hacker's illegal downloading of thousands of patients' medical files from a university medical center, and the stealing of health infor-

---

[7] David Stout & Tom Zeller, *Vast Data Cache About Veterans Has Been Stolen*, N.Y. TIMES, May 23, 2006, at A1.

[8] *See* Sheryl Harris, *Are Your Cell Phone Records Safe? Web-Based Companies Offer Data Telling Numbers You Called for as Little as $100*, PLAIN DEALER, Jan. 14, 2006, at A1 (reporting that one company charges only $100 for information about a customer's last 100 calls).

[9] *Id.*

[10] Simson L. Garfinkel & Abhi Shelat, *Remembrance of Data Passed: A Study of Disk Sanitization Practices*, 1 IEEE SECURITY & PRIVACY 17, 17 (2003).

[11] ROSS J. ANDERSON, BRITISH MED. ASS'N, SECURITY IN CLINICAL INFORMATION SYSTEMS 5 (1996) (citation omitted).

[12] Jennifer Gonzalez, *3rd Computer Breach at OU Within 3 Weeks: Records Involve 60,000 Who Used Health Center*, PLAIN DEALER, May 12, 2006, at A1; *see* Press Release, Aetna, Statement of CEO and President Ronald A. Williams on Data Security (Apr. 26, 2006), *available at* http://www.aetna.com/news/2006/pr_20060426.htm.

mation belonging to military personnel and their families from a contractor's database.[13]

Why would anyone want to obtain the health information of others? The reasons are numerous. Private health information can be useful to employers who wish to hire and retain the healthiest employees,[14] lenders and other businesses with a stake in individuals' financial futures and thus in their health statuses,[15] drug companies that wish to influence doctors' prescribing decisions,[16] advertisers and marketers who wish to tailor their material for particular audiences,[17] health insurers making eligibility and premium rate decisions concerning individual insurance policies, and even educational institutions that might wish to recruit and accept students with the greatest potential for success and longevity. In a world in which electronic health information

---

[13] DANIEL J. SOLOVE, THE DIGITAL PERSON 54–55 (2004); *see also* Nicolas P. Terry, *To HIPAA, a Son: Assessing the Technical, Conceptual, and Legal Frameworks for Patient Safety Information*, 12 WIDENER L. REV. 133, 163 (2005) (describing other examples of dysfunctional "privacy and security systems").

[14] ANDERSON, *supra* note 11, at 5 (reporting that as of 1995, "over half of America's largest 500 companies admitted using health records to make hiring and other personnel decisions"). It should be noted, however, that these health records were most likely lawfully obtained because the Americans with Disabilities Act of 1990 (the "ADA") permits medical testing of applicants and employees with some limitations, though it forbids discrimination against qualified employees with disabilities. *See* 42 U.S.C. § 12112 (a), (d) (2000). Employees who are sick or vulnerable to illness are often unappealing to employers because they can cause absenteeism, productivity, scheduling, and morale problems in the workplace and can raise health insurance costs. Questions concerning the meaning of the terms "qualified" and "disability," and thus the ADA's scope of coverage, have generated considerable litigation. *See generally* Sharona Hoffman, *Corrective Justice and Title I of the ADA*, 52 AM. U. L. REV. 1213 (2003).

[15] ANDERSON, *supra* note 11, at 6 (reporting that a network is being built by a credit reference agency to trade health records).

[16] *Id.* at 5 (stating that a U.S. drug company purchased a health systems company and obtained a prescription database for fifty-six million people, which it was planning to search for individuals whose prescriptions suggested that they suffered from depression and could benefit from Prozac, a drug produced by the company); *see also* Robert Steinbrook, *For Sale: Physicians' Prescribing Data*, 354 NEW ENG. J. MED. 2745, 2745 (2006) (reporting that during the last two decades, health care information companies routinely have purchased electronic prescription records from pharmacies and elsewhere, which they then sold to drug manufacturers); Stephanie Saul, *Doctors Object as Drug Makers Learn Who's Prescribing What*, N.Y. TIMES, May 4, 2006, at A1 (describing computerized records with information concerning physicians and the drugs they prescribe that are used by drug sales representatives to influence doctors to write more prescriptions for drugs produced by their companies or fewer prescriptions of a competitor's drugs).

[17] Prieto, *supra* note 6, at 18 (asserting that "[a]s advertisers have sought greater return on their dollar, they are increasingly relying on personal data to target ads" based on particular attributes); *see also* Terry, *supra* note 13, at 162 (stating that PHI is "valuable for secondary uses" such as marketing).

can be easily stolen or accessed, it could also become increasingly appealing to blackmailers and other criminals.[18] For example, after a computer was stolen from a general medical practice, two prominent women received letters from blackmailers who threatened to publicize the fact that the women had undergone abortions.[19] Even potential romantic partners looking for a low-risk mate might try to obtain personal health information if it were easily accessible.

Trafficking in personal health information poses a significant risk to the public. Once the data is dispersed on the Internet, it becomes available to anyone who is willing to pay for it,[20] and it cannot be expunged. Consequently, the harm to an individual from illicit or accidental disclosure of health information is potentially unlimited. It is quite possible for the affected individual to remain unaware of the disclosure and its consequences,[21] and it may be difficult or impossible to establish how the disclosure actually occurred. Loss or corruption of health data can also require the duplication of painful medical tests or even cause serious and life-threatening medical errors.

Americans are aware of these dangers. A 2005 National Consumer Health Privacy Survey, which queried 2000 people, revealed that sixty-seven percent of respondents were "somewhat" or "very concerned" about the confidentiality of their medical records.[22] Furthermore, thirteen percent of respondents claimed that they had attempted to protect their own privacy by avoiding medical tests or visits to their regular physicians, asking doctors to distort diagnoses, or paying for tests out-of-pocket so that no medical documentation would be sent to insurance companies.[23]

To address the data security threats associated with the electronic storage and transmission of private health information, the U.S. De-

---

[18] *See* ANDERSON, *supra* note 11, at 5; COMPUTER SCI. & TELECOMM. BD., NAT'L RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 3 (1997) (stating that hackers may penetrate computerized systems to steal data, destroy it, or damage the system).

[19] ANDERSON, *supra* note 11, at 5.

[20] *See id.* at 6 (reporting that a network is being built by a credit reference agency to trade health records).

[21] *See* Prieto, *supra* note 6, at 17 (stating that the average victim becomes aware of identity theft only after fourteen months, but in some cases discovering the crime takes ten years). This Article does not specifically address the theft of PHI, which could be hidden more easily because the consumer will not see suspicious charges on her credit card or telltale credit reports.

[22] LYNNE "SAM" BISHOP ET AL., CAL. HEALTHCARE FOUND., NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005: EXECUTIVE SUMMARY 3 (2005).

[23] *Id.* at 4.

partment of Health and Human Services ("HHS") enacted the Security Rule under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[24] The Security Rule is part of the larger HIPAA Privacy Rule established in the HIPAA privacy regulations[25] promulgated pursuant to HIPAA's statutory authority.[26]

The HIPAA Security Rule, which became effective on April 20, 2005 for most covered entities,[27] delineates administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information ("PHI").[28] Under the Rule, PHI includes "individually identifiable health information" that is electronically or otherwise transmitted or maintained.[29] "Covered entities" include health plans, health care clearinghouses, and health care providers that transmit health information electronically.[30]

Many have criticized various aspects of the broader HIPAA Privacy Rule,[31] but few have focused specifically on the regulations' Security Rule. It is our view that the HIPAA Security Rule has serious deficien-

---

[24] *See* 45 C.F.R. §§ 164.302–.318 (2006); *see also* Security and Electronic Signature Standards, 63 Fed. Reg. 43,242, 43,242–43 (Aug. 12, 1998) (providing background concerning the Security Rule's purpose).

[25] 45 C.F.R. §§ 160.101–.534.

[26] 42 U.S.C. §§ 1320d to 1320d-8 (2000 & Supp. III 2003).

[27] 45 C.F.R. § 164.318. Small health plans were given an extended adjustment period and were required to comply with the Rule by April 20, 2006. *Id.*

[28] *Id.* §§ 164.308–.312.

[29] *Id.* § 160.103.

[30] 45 C.F.R. § 160.103 (2006). A health care clearinghouse is defined as follows:

> [A] public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:
> (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
> (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Id.

[31] *See* PEW INTERNET & AM. LIFE PROJECT, EXPOSED ONLINE: WHY THE NEW FEDERAL HEALTH PRIVACY REGULATION DOESN'T OFFER MUCH PROTECTION TO INTERNET USERS 6–8 (2001) (discussing the fact that many health-related websites are not covered entities); SOLOVE, *supra* note 13, at 70 (stating that the "HIPAA regulations have apparently pleased nobody" because health care providers "complain that the regulations are too complicated, cumbersome, and expensive to follow" and privacy advocates "find the regulations weak and ineffective").

cies that hinder its efficacy as a mechanism to impede the operation of a market in illicitly obtained PHI.

These deficiencies are of four principal types. First, the HIPAA statute, and thus the Security Rule, do not address trafficking in private health information by businesses and individuals outside of the health industry, such as employers, marketers, and lenders that are not "covered entities."[32] Consequently, these parties are permitted to handle health data without restriction under HIPAA.[33] Second, although the HIPAA Privacy Rule allows patients to inspect and copy their PHI,[34] it does not enable individuals to establish the provenance of the data or verify how the information has been used.[35] Third, the HIPAA Security Rule gives covered entities an excessive amount of discretion in deciding what implementation specifications they will address and how they will do so, and many of its standards and implementation specifications lack sufficient detail and specificity.[36] As a result, careless or unscrupulous covered entities are very likely to become the main source of illicitly obtained PHI.[37] Furthermore, well-meaning but resource-poor covered entities that cannot develop sophisticated expertise with respect to computer security technology are given insufficient guidance as to how to achieve compliance with the Security Rule.[38] Fourth, the HIPAA privacy regulations, including the Security Rule, do not establish a private cause of action for aggrieved individuals.[39] Thus, insufficient enforcement mechanisms significantly diminish the regulations' deterrence and remedial powers.[40]

The remainder of this Article proceeds as follows. Part I describes the relevant Security Rule provisions.[41] Part II critiques the Rule and

---

[32] *See* 45 C.F.R. § 160.103(3) (defining a "covered entity" as a "health plan," "health care clearinghouse," or "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter").

[33] *See id.*

[34] *Id.* § 164.524(a)(1) (establishing that an "individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set").

[35] *See id.*

[36] *See* 45 C.F.R. § 164.306(b) (2006) (establishing that "[c]overed entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications" of the Security Rule in a provision entitled "Flexibility of approach").

[37] *See id.*

[38] *See id.*

[39] *See id.* §§ 160.300–.552; Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 618 (2002).

[40] *See* 45 C.F.R. §§ 160.300–.552.

[41] *See infra* notes 48–91 and accompanying text.

exposes its weaknesses.[42] To address the Security Rule's deficiencies, this Article proposes in Part III a detailed set of recommendations for enhancing PHI security.[43] We acknowledge the challenge of crafting static regulations for an area that is dynamic by nature because both computer technology and security threats are continually changing. We also recognize the potential tension between patients' needs for privacy safeguards and businesses' needs for efficient and profitable operations. We have considered the implications of our proposal in a variety of circumstances and have evaluated them through detailed examples.

Our recommendations include: (1) expanding the definition of "covered entity" to include any person who knowingly stores or transmits individually identifiable health information in electronic form for any business purpose related to the substance of such information;[44] (2) broadening the right of access to PHI so that affected individuals can obtain information concerning its provenance and uses;[45] (3) revising several of the Security Rule's provisions to provide further detail and guidance, and establishing mechanisms that will facilitate compliance;[46] and (4) adding a private cause of action to the law's enforcement scheme.[47] Although we focus our critique on the Security Rule, some of our recommendations, such as changes in statutory definitions and scope, necessarily would extend to the Privacy Rule as a whole.

I. The HIPAA Security Rule

The HIPAA Security Rule establishes general security requirements and provides implementers with broad discretion in choosing appropriate technologies to implement the standards.[48] One of the Rule's guiding principles is "technological neutrality," an approach based on the belief that regulators should not dictate the use of specific technologies, which may be inappropriate in particular settings or superseded by improved technologies.[49] It is clear from the public comments

---

[42] *See infra* notes 92–193 and accompanying text.

[43] *See infra* notes 194–333 and accompanying text.

[44] *See infra* notes 198–212 and accompanying text.

[45] *See infra* notes 239–243 and accompanying text.

[46] *See infra* notes 244–318 and accompanying text.

[47] *See infra* notes 319–333 and accompanying text.

[48] 45 C.F.R. §§ 164.302–.318 (2006); *see also* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8336 (Feb. 20, 2003) (stating that the final Rule was written "to frame the standards in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies").

[49] *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8335 (describing the drafters' "basic assumptions that the entities affected by this regulation are so varied in

received by HHS to the initial proposed version of the Security Rule that industry strongly favored such discretion.[50]

A. *HIPAA Security Requirements*

The Security Rule establishes four general requirements. Covered entities must: (1) ensure the "confidentiality, integrity, and availability" of electronic health information that they produce, obtain, maintain, or transmit; (2) protect the data against reasonably anticipated threats to its security or integrity; (3) safeguard against impermissible use or disclosure of the information; and (4) ensure that their employees comply with the Rule.[51] Covered entities may choose the means by which to "reasonably and appropriately" implement the Rule's standards, so long as they consider their size, complexity, capabilities, and technical infrastructure in making their decisions along with the costs of implementation and the risks of security breaches.[52]

The HIPAA Security Rule features "standards" and then "implementation specifications" that provide instructions concerning how to fulfill the obligations outlined in the standards. There are two types of implementation specifications: required and addressable.[53] Required implementation specifications are mandatory.[54] By contrast, implementers may respond to an addressable implementation specification in one of three ways: (1) by implementing it, (2) by implementing an "equivalent alternative measure," or (3) by doing neither because implementation would not be "reasonable and appropriate."[55] A covered entity that does not implement an addressable implementation specification must document its justification for not doing so,[56] and all covered entities

---

terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be useable by all covered entities").

[50] *Id.* (stating that "[m]any commenters also supported the concept of technological neutrality, which would afford them the flexibility to select appropriate technology solutions and to adopt new technology over time"); *see also id.* at 8336 (explaining that numerous commentators asserted that "the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress").

[51] 45 C.F.R. § 164.306(a). Permissible and impermissible uses of private health information are described in Subpart E of the HIPAA Privacy Rule. *Id.* §§ 164.500–.534.

[52] *Id.* § 164.306(b).

[53] *Id.* § 164.306(d).

[54] 45 C.F.R. § 164.306(d)(2) (2006).

[55] *Id.* § 164.306(d)(3).

[56] *Id.* § 164.306(d)(3)(ii)(B)(1).

must review their compliance and modify their security measures as needed.[57]

1. Administrative Safeguards

Several required implementation specifications are intended to provide administrative safeguards.[58] These safeguards include risk analysis and risk management practices, the establishment of sanctions for noncompliant employees, and information system activity reviews.[59] Covered entities also must identify a "security official" who is responsible for compliance with the Security Rule and establish procedures whereby only authorized individuals have access to electronic PHI.[60] To achieve workforce security, a covered entity should implement authorization and supervision standards, workforce clearance procedures, and termination of authorization procedures, but these are considered addressable implementation specifications.[61]

In addition, a covered entity should implement a security awareness and training program for its workforce and implement measures such as security reminders, mechanisms that protect against malicious software, log-in monitoring, and password management.[62] The Security Rule mandates the creation of response and reporting mechanisms for security incidents[63] and contingency plans that focus on data backup, disaster recovery, emergency mode operation, testing and revision procedures, and analysis of the criticality of the affected data and applications.[64] It also instructs that covered entities should perform periodic evaluations of their compliance[65] and may enter into written contracts or other arrangements with business associates to handle electronic PHI, so long as the associates provide satisfactory assurances that they will appropriately safeguard the data.[66] The Security Rule, however, does not apply to the transmission of electronic PHI to another health

---

[57] *Id.* § 164.306(e).

[58] *Id.* § 164.308(a).

[59] 45 C.F.R. § 164.308(a)(1)(ii).

[60] 45 C.F.R. § 164.308(a)(2)–(3)(i) (2006).

[61] *Id.* § 164.308(a)(3)(ii).

[62] *Id.* § 164.308(a)(5). These are addressable implementation specifications. *Id.*

[63] *Id.* § 164.308(a)(6).

[64] *Id.* § 164.308(a)(7). The development of testing and revision procedures and applications and data criticality analysis are addressable implementation specifications. *Id.* The other safeguards are required. *Id.*

[65] 45 C.F.R. § 164.308(a)(8).

[66] 45 C.F.R. § 164.308(b)(1), (3)–(4) (2006); *see also id.* § 164.314 (listing specifications regarding business associate contracts and other arrangements).

care provider who is treating the patient, a group health plan sponsor, or agencies determining eligibility for government programs providing public benefits.[67]

2. Physical Safeguards

The HIPAA Security Rule next establishes physical safeguards aimed at thwarting unauthorized access to electronic information systems and the facilities in which they are housed while ensuring access to authorized personnel.[68] This subsection describes several "addressable" implementation specifications regarding contingency operations, facility security plans, access control and validation procedures, and maintenance of records concerning repairs and modifications to security-related components of the physical plant.[69]

In addition to safeguarding workstation security,[70] a covered entity must establish procedures that govern the movement of hardware that contains electronic PHI within and outside of the facility in question.[71] These procedures should address electronic media disposal, removal of PHI in cases in which equipment will be reused for other purposes, maintenance of records of the hardware's whereabouts and who is responsible for it, and data backup and storage prior to moving equipment.[72]

3. Technical Safeguards

The required and addressable[73] technical safeguards detailed by the HIPAA Security Rule are designed to ensure that only authorized personnel have access to electronic PHI.[74] These safeguards include assigning unique user identification names or numbers, establishing emergency access procedures, having an automatic logoff after a specific period of inactivity, and implementing encryption and decryption

---

[67] *Id.* §§ 164.308(b)(2), .502(e)(1)(ii)(C).

[68] *Id.* § 164.310(a)(1).

[69] *Id.* § 164.310(a)(2).

[70] *Id.* § 164.310(b)–(c).

[71] 45 C.F.R. § 164.310(d)(1).

[72] 45 C.F.R. § 164.310(d)(2) (2006). The implementation specifications for disposal and media reuse are required, while the record-keeping and data backup and storage requirements are addressable. *Id.*

[73] *See infra* notes 75–76 (indicating which safeguards are required and which are addressable).

[74] 45 C.F.R. § 164.312(a)(1).

mechanisms.[75] This provision also discusses audit controls, authentication mechanisms for electronic PHI and its users, and measures to ensure security when electronic PHI is transmitted electronically.[76]

B. *Enforcement*

The HIPAA legislation authorizes both civil and criminal penalties.[77] Given that HHS is not authorized to conduct criminal prosecutions, however, the privacy regulations only address the civil penalties.[78] Under a Final Rule issued by HHS on February 16, 2006, the HIPAA Privacy Rule's enforcement provisions also are applicable to the Security Rule.[79] Thus, if a covered entity discloses health information in an unauthorized manner for any reason, it can be penalized.[80] In addition, it can be penalized for the absence of appropriate security measures even if no PHI is disclosed.[81]

These provisions establish a primarily complaint-driven enforcement scheme for privacy violations.[82] Persons[83] who believe that a covered entity is violating the Privacy Rule may submit a complaint to the Secretary of HHS, who has discretion as to whether to investigate it.[84] The authority to administer and enforce the Security Rule has been delegated to the Centers for Medicare and Medicaid Services ("CMS"),

---

[75] *Id.* § 164.312(a)(2). Unique user identification and emergency access procedures are required, while automatic logoff and encryption and decryption mechanisms are addressable implementation specifications. *Id.*

[76] *Id.* § 164.312(b)–(e). Mechanisms for information authentication and integrity controls for the transmission of data are designated addressable. *Id.*

[77] 42 U.S.C. §§ 1320d-5 to 1320d-6 (2000). The criminal penalty provision is discussed further *infra* note 88 and accompanying text.

[78] 45 C.F.R. §§ 160.400–.426 (2006).

[79] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390, 8390 (Feb. 16, 2006) (stating that "[t]he final rule amends the existing rules relating to investigation of noncompliance" and the imposition of penalties "to make them apply to all of the HIPAA Administrative Simplification rules, rather than exclusively to the privacy standards"); *see also* 45 C.F.R. § 160.300 (making the enforcement provisions applicable to all HIPAA rules, including the Security Rule). Originally, the enforcement provisions applied only to Subpart E of the Privacy Rule, which limits the circumstances under which covered entities can use and disclose PHI. *See* 45 C.F.R. §§ 164.500–.534.

[80] 45 C.F.R. §§ 164.500–.534.

[81] *Id.* §§ 164.302–.318.

[82] HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. 20,224, 20,226 (Apr. 18, 2005). The regulations, however, also provide that HHS may conduct compliance reviews without receiving a complaint. 45 C.F.R. § 160.308; HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. at 20,226.

[83] A "person" is defined as a "natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private." 45 C.F.R. § 160.103.

[84] 45 C.F.R. § 160.306(a), (c) (2006).

and thus, CMS investigates alleged violations relating to the Security Rule specifically.[85] If a covered entity is found to be noncompliant, it will be informed by the Secretary, who will, if possible, attempt to resolve the matter informally.[86] The Secretary has authority to impose civil penalties for noncompliance in an amount not to exceed $100 per violation, or $25,000 during a calendar year "for all violations of an identical requirement."[87] In addition, violators may be subject to criminal prosecution and fined up to $250,000 and may face imprisonment for up to ten years.[88] A respondent may also request a hearing before an administrative law judge (an "ALJ").[89] As is typical in administrative

---

[85] Statement of Organization, Functions, and Delegation of Authority Notice, 68 Fed. Reg. 60,694, 60,694 (Oct. 23, 2003). On March 25, 2005, CMS issued a notice entitled "Procedures for Non-Privacy Administrative Simplification Complaints Under the Health Insurance Portability and Accountability Act of 1996," which became effective on April 25, 2005. 70 Fed. Reg. 15,329, 15,330–31 (Mar. 25, 2005). The notice states that if CMS finds a violation based on a complaint, it will work with the covered entity "to obtain voluntary compliance." *Id.* In the absence of cooperation, "the Secretary will pursue other options, such as . . . civil money penalties." *Id.* at 15,331.

[86] 45 C.F.R. § 160.312(a)(1).

[87] 42 U.S.C. § 1320d-5(a)(1) (2000); 45 C.F.R. § 160.508. A civil penalty may not be imposed for a violation if it is punishable as a criminal offense under 42 U.S.C. § 1320d-6, which is administered by the Department of Justice. 42 U.S.C. § 1320d-5(b)(1); HIPAA Administrative Simplification: Enforcement, 70 Fed. Reg. at 20,237.

[88] *See* 42 U.S.C. § 1320d-6. This provision, entitled "Wrongful disclosure of individually identifiable health information," states:

> (a) Offense
> A person who knowingly and in violation of this part—
> (1) uses or causes to be used a unique health identifier;
> (2) obtains individually identifiable health information relating to an individual; or
> (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section.
> (b) Penalties
> A person described in subsection (a) of this section shall—
> (1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
> (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
> (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

Id.

[89] 45 C.F.R. § 160.504(a).

proceedings, only limited discovery is permitted,[90] and the ALJ is generally not bound by the Federal Rules of Evidence.[91]

II. A Critique of the Security Rule

The HIPAA Security Rule is characterized by several flaws and deficiencies that greatly detract from its efficacy. These relate to the narrow definition of "covered entity," the limited access individuals have to information concerning their PHI, the Rule's insufficient compliance guidelines, and the lack of a private cause of action for Privacy Rule violations. This Part will analyze all of these shortcomings.

A. *Covered Entities*

The HIPAA Security Rule follows its enabling legislation, the HIPAA statute, and covers only health plans, health care clearinghouses, and health care providers that transmit health information electronically.[92] Consequently, doctors, hospitals, pharmacists, health insurers, and health maintenance organizations ("HMOs") must comply with the HIPAA privacy standards, but not all parties possessing PHI are covered.[93] Thus, websites selling nonprescription medications or dispensing medical advice,[94] employers handling applicants' and employees' medical records, marketers, or any other business entities that obtain PHI are not bound by the requirements of the HIPAA Security Rule.[95] The Rule's narrow scope of coverage compromises its ability to protect Americans against misuse of their PHI. It leaves the vast amount of health information stored on systems maintained by noncovered entities especially vulnerable to theft, destruction, or alteration.[96]

In fact, it is arguable that the greatest PHI-related threats are associated with the acquisition of PHI by non-health-care-related entities.

---

[90] *See* 45 C.F.R. § 160.516 (2006).

[91] *Id.* § 160.540.

[92] *Id.* § 160.102(a).

[93] Solove, *supra* note 13, at 208; Winn, *supra* note 39, at 618 (affirming that the "Rules do not subject to legal sanction any of the numerous entities whose access to personal health information has exploded with the increased use of electronic health information").

[94] *See* Pew Internet & Am. Life Project, *supra* note 31, at 6–8; David L. Baumer et al., *Internet Privacy Law: A Comparison Between the United States and the European Union*, 23 Computers & Security 400, 410 (2004) (emphasizing that websites in the United States are not regulated with respect to most transactions, including those involving health information).

[95] Solove, *supra* note 13, at 208.

[96] Computer Sci. & Telecomm. Bd., *supra* note 18, at 3.

Many commentators have expressed concern that disclosure of health information can lead to loss of various types of insurance; employment and educational discrimination; denial of loans; and severe disadvantages in custody battles, adoption efforts, parole proceedings, and personal injury lawsuits.[97] Blackmail, identity theft, and other crimes perpetrated by those with access to illicitly obtained PHI are also grave dangers.[98]

The European Union (the "E.U.") has tackled the contemporary threat to privacy by non-health-care-related entities very aggressively. The E.U. Privacy Directive provides wide-ranging privacy protection.[99] It binds "Member States"[100] and extends to the processing of all personal data by any party, with few exceptions.[101] Specifically, the Directive's broad language establishes that "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[102] It then delineates exceptions to the rule, which, in the case of health information, relate to the provision of medical care.[103]

By contrast, the United States has a much more segmented approach to privacy, though it has enacted numerous individual laws that address privacy issues. The Privacy Act of 1974, for example, governs all federal agencies.[104] The law forbids the disclosure of personal information (with some exceptions), aims to safeguard the security of records, and allows individuals to review their records and request corrections of errors.[105] Although the law covers only federal agencies, it is in some ways much broader than the HIPAA Privacy Rule because it defines "record" to mean not only medical data, but also identifiable information

---

[97] Janet L. Dolgin, *Personhood, Discrimination, and the New Genetics*, 66 BROOK. L. REV. 755, 764–65 (2001); Joanne L. Hustead & Janlori Goldman, *Genetics and Privacy*, 28 AM. J.L. & MED. 285, 288 (2002); Mark A. Rothstein & Sharona Hoffman, *Genetic Testing, Genetic Medicine, and Managed Care*, 34 WAKE FOREST L. REV. 849, 887 (1999).

[98] *See supra* notes 5–23 and accompanying text.

[99] *See generally* Parliament and Council Directive 95/46/EC, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter E.U. Privacy Directive].

[100] *Id.* art. 1, ¶ 1, 1995 O.J. (L 281) at 38.

[101] *Id.* art. 3, ¶ 2, 1995 O.J. (L 281) at 39. The exceptions include matters such as the processing of information for security purposes or criminal law and processing "by a natural person in the course of a purely personal or household activity." *Id.*

[102] *Id.* art. 8, ¶ 1, 1995 O.J. (L 281) at 40.

[103] *Id.* art. 8, ¶¶ 2–3, 1995 O.J. (L 281) at 40–41.

[104] 5 U.S.C. § 552a (2000).

[105] *Id.* § 552a(b)–(e).

about people's "education, financial transactions, medical history, and criminal or employment history."[106]

Title V of the Gramm-Leach-Bliley Act is devoted to privacy.[107] It requires financial institutions to respect customers' privacy and shield the security and confidentiality of customers' private information.[108] To this end, the law prohibits financial institutions from disclosing "nonpublic personal information" to a nonaffiliated third party if the disclosure is not authorized by the law[109] and requires regulatory agencies to establish standards concerning appropriate "administrative, technical, and physical safeguards" for private information.[110]

A number of other laws also protect privacy in particular realms. The Family Educational Rights and Privacy Act of 1974 governs the accessibility and disclosure of certain student records.[111] The Cable Communications Policy Act of 1984 mandates that cable operators inform subscribers of any personal information that is collected, the disclosure of such information, and the subscribers' right of access to the information.[112] Information cannot be collected or disclosed without the customer's written or electronic consent unless it is needed for a "legitimate business activity."[113] The Electronic Communications Privacy Act governs electronic surveillance and restricts searches and interception of wire, oral, and electronic communications.[114] The Video Privacy Protection Act of 1988 provides that video store operators may not disclose the titles of the videos rented or purchased by any particular customer, though some exceptions apply.[115] The Driver's Privacy Protection Act of 1994 requires states to obtain a driver's consent before divulging personal information contained in motor vehicle records to marketers, unless one of the stated exceptions is applicable.[116] The Children's Online Privacy Protection Act of 1998 establishes that operators of web-

---

[106] *See id.* § 552a(4).

[107] *See* 15 U.S.C. §§ 6801–6827 (2000).

[108] *Id.* § 6801(a).

[109] *Id.* § 6802(a)–(b).

[110] *Id.* § 6801(b).

[111] 20 U.S.C. § 1232g (2000).

[112] 47 U.S.C. § 551(a)–(d) (2000 & Supp. III 2003).

[113] *Id.* § 551(b)–(c). The law further provides that cable operators may not disclose to the government "records revealing cable subscriber selection of video programming from a cable operator" and must destroy personally identifiable information when it is no longer needed. *Id.* § 551(c)(2)(D), (e).

[114] 18 U.S.C. §§ 2511, 2701 (2000).

[115] 18 U.S.C. § 2710(a)(3), (b)(1) (2000).

[116] 18 U.S.C. § 2721 (2000).

sites targeted at children must acquire parental consent to use the personal data of children under the age of thirteen.[117]

The laws discussed above provide varying degrees of privacy protection to individuals with respect to particular kinds of information or particular holders of private information.[118] It is unlikely that the United States will be willing to adopt a privacy law that is as far-reaching as the E.U. Privacy Directive. In the spirit of already existing U.S. legislation, however, we should have at the very least a law that narrowly targets only health information but is broad enough to include within its scope all parties that maintain or transmit such information in electronic form for business reasons related to the substance of the PHI.

This approach already has been suggested in a bipartisan bill introduced by Senator Hillary Clinton and then-Senator Bill Frist, entitled the Health Technology to Enhance Quality Act of 2005.[119] The bill was designed "[t]o reduce healthcare costs, improve efficiency, and improve healthcare quality through the development of a nationwide interoperable health information technology system."[120] The bill provided that the HIPAA privacy regulations be amended to "apply to any health information stored or transmitted in an electronic format."[121] In Part III of this Article, we similarly recommend that the term "covered entity" in the HIPAA Privacy Rule be expanded to include any person who stores or transmits individually identifiable electronic PHI for any business purpose related to the substance of the PHI.[122]

B. *Accessibility*

The HIPAA Privacy Rule allows patients access to their PHI.[123] Specifically, the regulations provide that "an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set," with some exceptions, such as psychotherapy notes and information compiled for purposes of litiga-

---

[117] 15 U.S.C. §§ 6501(1), 6502 (2000).

[118] For a critique of the privacy laws, see SOLOVE, *supra* note 13, at 67–72.

[119] S. 1262, 109th Cong. (2005); *see also* Terry, *supra* note 13, at 138.

[120] S. 1262, 109th Cong. pmbl.

[121] *Id.* § 2907.

[122] *See infra* notes 198–212 and accompanying text.

[123] 45 C.F.R. § 164.524 (2006).

tion or administrative proceedings.[124] Furthermore, the Privacy Rule enables individuals to request amendment of PHI that is incorrect.[125]

If the definition of "covered entity" is expanded to include any person who knowingly stores or transmits individually identifiable electronic PHI for any business purpose related to the substance of the PHI,[126] the right of access to inspect and obtain a copy of PHI should extend to all electronic PHI that is processed by any covered entity. In addition, the right to correct PHI should be similarly extended. Thus, if an employer[127] or a bank obtains PHI in order to make employment or loan decisions, the individual who is the subject of that information should have a right of access to that data and a right to amend it if it is incorrect.

Furthermore, the right of access should be expanded to include a right to establish the provenance of the data and the purpose for which it is used. This approach has been utilized by the Fair Credit Reporting Act, which requires all consumer reporting agencies to disclose to consumers, upon request, not only the information in the consumer's file, but also "the sources of the information."[128] In the case of health care providers, health plans, and many health care clearinghouses, the origins and purposes of the data will be obvious from the documents themselves, and thus, this requirement will add no burden to the covered entity. In the case of other parties, however, establishing the provenance and uses of the information could be essential to determining whether the Security Rule has been breached by any covered entity, by allowing the inappropriate dissemination of PHI. Information concerning the data's origins also will be necessary to ascertain whether criminal prosecution should be pursued, how widely the information has been distributed, and how much harm might be done to the individual at issue.

As discussed above, PHI is already commonly targeted by hackers.[129] It is not unrealistic to expect that a black market will develop for PHI to which businesses, marketers, blackmailers, and others could turn to purchase health information. According to one source, about

---

[124] *Id.* § 164.524(a)(1).

[125] *Id.* § 164.526(a). The provision also specifies the conditions under which a request to amend records can be denied. *Id.*

[126] *See supra* notes 92–122 and accompanying text.

[127] See Americans with Disabilities Act of 1990, 42 U.S.C. § 12112(d) (2000), for details concerning the obligations of employers with respect to medical information.

[128] 15 U.S.C. § 1681g(a)(1)–(2) (2000).

[129] *See supra* notes 5–23 and accompanying text.

$10 billion in U.S. medical transcription business is outsourced to foreign countries.[130] Foreign data processors of PHI are "business associates"[131] of covered entities, and are bound by certain privacy protection requirements under the HIPAA regulations.[132] HHS has admitted, however, that it is unable to regulate effectively offshore business associates or monitor their contracts with U.S. companies.[133] It is entirely possible that businesses or individuals processing PHI in distant locations, far from the direct reach of U.S. regulatory powers, will begin selling PHI to third parties who believe it offers opportunities for profit.

Several databases already sell lists of persons suffering from a large number of ailments.[134] In addition, health care information companies sell individual physicians' prescribing records purchased from pharmacies to pharmaceutical companies that use them to market particular drugs to specific doctors.[135]

These lists are not necessarily compiled by illegal means. Rather, medical and other personal data can often be mined from purchase information, supermarket savings cards, surveys, sweepstakes and contest entries, U.S. Census records, credit card transactions, phone records, credit records, product warranty cards, or public records that are rightfully in the possession of those aggregating the information.[136] Consequently, individuals are vulnerable to manipulation, exploitation, and discrimination by those who have access to their PHI. The patients, in turn, should, at the very least, be empowered to learn the origins and uses of PHI possessed by various parties.

This disclosure approach is consistent with the one adopted by the E.U. Privacy Directive.[137] The Directive provides that each data subject

---

[130] Terry, *supra* note 13, at 164.

[131] 45 C.F.R. § 160.103 (2006) (defining "business associates").

[132] *Id.* § 164.504(e) (establishing standards for "business associate contracts"). The provision mandates that, with some exceptions, contracts between a covered entity and a business associate "may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity." *Id.*

[133] Terry, *supra* note 13, at 165 (citing Letter from Tommy G. Thompson, Sec'y of Health & Human Servs., to Edward J. Markey, Representative, U.S. House of Representatives (June 14, 2004)).

[134] *See* Elec. Privacy Info. Ctr., Privacy and Consumer Profiling, http://www.epic.org/privacy/profiling (last visited Feb. 23, 2007); *see, e.g.*, Hippo Direct, Medical and Healthcare List, http://www.hippodirect.com/ListSubjectN_1.asp?lSubject-11 (last visited Feb. 23, 2007); Med. Mktg. Servs., Inc., http://www.mmslists.org/privacy/profiling (last visited Feb. 23, 2007).

[135] Steinbrook, *supra* note 16, at 2745.

[136] Elec. Privacy Info. Ctr., *supra* note 134.

[137] *See generally* E.U. Privacy Directive, *supra* note 99.

may obtain "confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing," as well as the recipients, contents, and source of the data.[138] The approach is also consistent with the Fair Information Practices (the "FIP") outlined in a report issued by the U.S. Department of Health, Education, and Welfare in 1973.[139] The FIP provide, in relevant part:

- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

. . . .

- Any organization creating, maintaining, using or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[140]

Under these principles, data subjects have a right to know how their PHI is used. They should also have a right to know the source of the information possessed by any party so that they can ensure that their information is not being misused or utilized for purposes for which it was not intended. In Part III, Section B, we discuss mechanisms for allowing meaningful inquiry concerning the origins and uses of electronically stored PHI.

C. *Insufficient Compliance Guidelines*

The Security Rule leaves the mechanisms of implementing the outlined security standards to the discretion of the covered entity.[141] Although flexibility is often a desirable quality, it can also be hazardous in the regulatory context because it can leave those subject to regulation without sufficient guidance as to how to comply with legal require-

---

[138] E.U. Privacy Directive, *supra* note 99, art. 12(a), 1995 O.J. (L 281) at 42.

[139] *See generally* Dep't of Health & Human Servs., Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[140] *See generally id.* The FIP have not been codified into any specific law in the United States, but rather, have served as the basis for some of the privacy laws discussed in this Article. *See* Privacy Rights Clearinghouse, A Review of the Fair Information Principles: The Foundation of Privacy Public Policy, http://www.privacyrights.org/ar/fairinfo.htm (last visited Feb. 23, 2007).

[141] 45 C.F.R. § 164.306(b) (2006).

ments.[142] In the context of the Security Rule, it is unrealistic to expect that every health care provider has the technical expertise and ability to determine on its own how to implement the security standards.

Furthermore, some organizations could use the regulations' vagueness as a justification for establishing minimal PHI security measures. It already appears that information technology is a low priority for the health care industry. As of 2002, only two to three percent of the industry's funding was devoted to the electronic management of PHI, compared to ten to fifteen percent of funding devoted by other industries to advance information technology.[143] Furthermore, the health care industry is "generally considered to be ten to fifteen years behind other industries with regard to security."[144]

A careful reading of just a few of the Security Rule's provisions illustrates its characteristic weaknesses. In a provision entitled "Flexibility of approach," the Rule states, "Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications."[145] The regulations elaborate on the "reasonably and appropriately" standard only by instructing covered entities to take into account the entity's size, complexity, capabilities, and technical infrastructure; the security measures' costs; and the "probability and criticality of potential risks to electronic protected health information."[146] The above language does not define the term "criticality" and fails to provide guidance concerning how to identify "potential risks."[147]

Likewise, in its "Administrative safeguards" section, the Security Rule requires covered entities to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information."[148] No further details are provided concerning how the complex task of risk analysis should be accomplished.

---

[142] Choi et al., *supra* note 2, at 62 (characterizing the HIPAA privacy regulations as a "loosely-worded document that is the current passing standard for privacy" and predicting that covered entities will experience difficulty "interpreting exactly what HIPAA security standards mean to their company and what exactly constitutes compliance").

[143] *Id.*

[144] Nancy A. Lawson et al., *The HIPAA Privacy Rule: An Overview of Compliance Initiatives and Requirements*, 70 DEF. COUNS. J. 127, 147 (2003).

[145] 45 C.F.R. § 164.306(b)(1).

[146] *Id.* § 164.306(b)(2).

[147] *See* 45 C.F.R. § 164.306(b)(2) (2006).

[148] *Id.* § 164.308(a)(1)(ii)(A).

In response to comments received during the proposed Rule's public comment period, HHS explained:

> A thorough and accurate risk analysis would consider "all relevant losses" that would be expected if the security measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures.[149]

This description, however, also lacks sufficient specificity. For example, whose losses are to be considered—those suffered by the data subjects, by covered entities,[150] by business associates, or by other stakeholders? How direct or remote should the potential risks be in order to be considered? Unauthorized disclosure of PHI to various parties can affect insurance coverage, job prospects, family dynamics, and even social opportunities.[151] Should all of these potential consequences be contemplated?

If covered entities are to maintain discretion under the Security Rule's flexible approach,[152] the key to ensuring that they choose effective security measures is a requirement that they implement rigorous risk analysis and management processes. These processes should identify, analyze, and mitigate the particular risks associated with health information disclosure for various stakeholders, and especially for data subjects. The Security Rule fails to provide sufficient guidance for the development of such measures.

Besides exhibiting a low level of specificity in its security standards, the Security Rule entirely fails to address certain important issues. The Security Rule omits an explicit requirement that covered entities, perhaps with the assistance of consultants or vendors,[153] identify the relevant *best current security practices* of the health informatics and computer security communities. Such a requirement is needed to ensure that covered entities are knowledgeable about sound security practices and

---

[149] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8347 (Feb. 20, 2003).

[150] In this response, HHS emphasized the potential losses that could be suffered by a covered entity: "A covered entity that lacks adequate protections risks inadvertent disclosure of patient data, with resulting loss of public trust, and potential legal action." *Id.* at 8344. It is unclear why HHS did not focus on other parties that bear significant risks as well.

[151] *See supra* notes 14–23 and accompanying text.

[152] 45 C.F.R. § 164.306(b)(1).

[153] *See infra* notes 268–292 and accompanying text (discussing the services of security product vendors).

emergent security risks and their countermeasures. The rapid exploitation of newly discovered vulnerabilities in software systems and applications by attackers makes it essential that covered entities be extremely diligent in learning about and responding to vulnerabilities. Covered entities or their agents should utilize the substantial amount of relevant information that is provided by reputable organizations such as the International Organization for Standardization ("ISO"), the Computer Emergency Response Team ("CERT"), the National Institute of Standards and Technology ("NIST"), the National Information Assurance Partnership ("NIAP"), and software vendors.[154]

Another crucial omission from the Security Rule is guidance concerning the risks inherent in the development, operation, and maintenance of the computer software that provides the functionality of systems that process electronic PHI. Such software is often extremely complex, comprising many thousands or millions of program instructions, most of which are executed only under particular conditions. Errors in software development are virtually inevitable. Any software defect, such as a missing or erroneous sequence of instructions, becomes a security vulnerability if an attacker can exploit it to his or her benefit and to the detriment of system stakeholders. Moreover, mistakes in the configuration and operation of software easily can render it insecure,[155] as can errors made during software maintenance,[156] the process of modifying software to correct defects or to enhance its functionality.

Thus, covered entities should be required to consider the risks associated with software as part of their risk analysis process and to follow best current practices for software development, validation, operation, and maintenance. These risks include, among others: incorrect functionality resulting in erroneous output, missing functionality, poor "usability," poor documentation, "crashes" and other critical failures, and excessive costs and delays in development leading to reduced emphasis on product quality and security.[157] All of these risks can adversely affect the security of electronic private health information.

---

[154] *See infra* notes 269–318 and accompanying text.

[155] SANS Inst., The Top 20 Most Critical Internet Security Vulnerabilities (Updated)—The Experts Consensus, http://www.sans.org/top20/2005 (last visited Feb. 23, 2007).

[156] STEPHEN R. SCHACH, OBJECT-ORIENTED AND CLASSICAL SOFTWARE ENGINEERING 7–13, 479–96 (6th ed. 2005).

[157] *See id.*; *see also* PETER G. NEUMANN, SRI INT'L, ILLUSTRATIVE RISKS TO THE PUBLIC IN THE USE OF COMPUTER SYSTEMS AND RELATED TECHNOLOGY (2007), *available at* ftp://ftp.csl.sri.com/pub/users/neumann/illustrative.pdf.

If compliance with the Security Rule's standards is not to be a sham, the Rule's standards and implementation specifications must be augmented, and covered entities must receive further guidance as to how to achieve their obligations. Section C of Part III develops recommendations for elucidating the Security Rule's requirements and facilitating compliance through instruments that limit the costs and burdens it places upon covered entities.[158]

D. *Private Cause of Action*

The HIPAA Security Rule does not provide for a private cause of action.[159] Rather, enforcement is achieved through administrative procedures and hearings before an ALJ.[160] It is noteworthy that under the Clinton Administration, the HHS Secretary's recommendations to Congress included a proposal for a private right of action, but Congress ultimately rejected this approach.[161]

Under the enforcement system established by the regulations, any aggrieved individual has a right to file a complaint with the HHS Secretary.[162] At his or her discretion, the Secretary may investigate the complaint.[163] If a violation is found, the Secretary is to impose a penalty on the offender[164] and collect the money,[165] but no damages are available for persons who are aggrieved or injured by the privacy lapse. At the request of the covered entity, a hearing may be held before an ALJ, but the only parties to participate are the respondent and HHS personnel.[166]

By contrast to the HIPAA Privacy Rule, many other American privacy laws establish a private cause of action.[167] These laws provide ex-

---

[158] *See infra* notes 244–318 and accompanying text.

[159] *See* 45 C.F.R. §§ 160.300–.552 (2006); Winn, *supra* note 39, at 618.

[160] *See* 45 C.F.R. §§ 160.300–.552; Winn, *supra* note 39, at 618.

[161] Sec'y of Health and Human Servs., Recommendations Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996 (Sept. 11, 1997), *available at* http://www.aspe.hhs.gov/admnsimp/pvcrec.htm ("Any individual whose rights under the law have been violated, whether negligently or knowingly, should be permitted to bring an action for actual damages and equitable relief. For knowing violation attorney's fees and punitive damages also should be available.").

[162] 45 C.F.R. § 160.306(a); *see also* U.S. Dep't of Health & Human Servs., Office for Civil Rights—HIPAA, Medical Privacy—National Standards to Protect the Privacy of Personal Health Information, http://www.hhs.gov/ocr/hipaa (last visited Feb. 23, 2007) (listing information concerning the filing of complaints and other matters).

[163] 45 C.F.R. § 160.306(c).

[164] *Id.* § 160.402(a).

[165] 45 C.F.R. § 160.424(a) (2006).

[166] *Id.* § 160.504(a).

[167] *See* Privacy Act of 1974, 5 U.S.C. § 552a(g) (2000) (stating that individuals may bring civil actions against noncompliant agencies for injunctive relief or for damages up to $1000

plicitly for a right to recover attorney's fees and costs so that even plaintiffs with minimal damages resulting from inappropriate disclosure are likely to find attorneys willing to litigate their cases. Like these laws, the E.U. Privacy Directive supports the notion of private litigation and mandates that "Member States shall provide for the right of every person to a judicial remedy for any breach of the rights" embodied in the state's applicable privacy law.[168]

We recommend that the HIPAA Security Rule's enforcement provisions, which apply to the entirety of the HIPAA privacy regulations,[169] be revised to include a private cause of action. Further details concerning suggested procedures and remedies are discussed in Part III.[170] At this point, however, because covered entities surely would object to the prospect of costly and onerous private litigation, it is appropriate to justify our recommendation and analyze the contributions a private cause of action could make to PHI security.

If the HIPAA privacy regulations are intended to protect data subjects, they must provide access to a remedy when individuals' rights are violated and must not leave victims out of the enforcement process. The HIPAA regulations provide little satisfaction for aggrieved persons and discount their potential injuries by failing to include them in enforcement proceedings and provide them with a personal remedy.

Moreover, private litigation is often needed as an adjunct to administrative procedures for deterrence purposes. Aggressive pursuit of governmental enforcement actions may depend upon political priori-

---

in cases of intentional or willful violations, as well as attorney's fees and costs); Electronic Communications Privacy Act, 18 U.S.C. § 2520 (2000) (stating that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate," including actual damages, punitive damages, attorney's fees, and costs); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(c) (2000) (allowing aggrieved persons to bring civil actions for actual damages, punitive damages, reasonable attorney's fees and costs, and equitable relief); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2724 (2000) (establishing that a "person who knowingly obtains, discloses or uses personal information, from a motor vehicle record" for an impermissible purpose will be liable to the individual at issue for actual damages, punitive damages, reasonable attorney's fees and costs, and equitable relief); Cable Communications Policy Act, 47 U.S.C. § 551(f)(1) (2000) (providing that "[a]ny person aggrieved by any act of a cable operator in violation of this section may bring a civil action" in a U.S. district court for actual damages, punitive damages, attorney's fees, and costs).

[168] E.U. Privacy Directive, *supra* note 99, art. 22, 1995 O.J. (L 281) at 45.

[169] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390, 8390 (Feb. 16, 2006) (stating that the regulation's enforcement provisions now apply "to all of the HIPAA Administrative Simplification rules").

[170] *See infra* notes 319–333 and accompanying text.

ties and pressures, such as the degree to which a case is perceived as advancing the general public interest[171] or budgetary and other resource allocation constraints.[172] Thus, clear violations that affect only a single person could be ignored, and cases that would not set important precedents might not be litigated by the government no matter how justified prosecution would be. Such inevitable resource-rationing decisions can leave a significant deterrence void, which can only be filled through private enforcement.

Private litigation features several important advantages over administrative proceedings. It can effectively restrict unlawful conduct through the threat of costly and well-publicized court proceedings, and it can often resolve cases more quickly than administrative enforcement handled by overburdened agencies.[173] Furthermore, careful judicial review that produces published opinions can serve an important rule-making function by setting precedents that interpret vague language in administrative regulations.[174] Cases that capture media attention, as some lawsuits do, have the added advantage of educating members of the public at large concerning their rights and obligations under the law.[175] By contrast, although HIPAA mandates that ALJs issue decisions containing findings of fact and conclusions of law, the decisions are issued only to the parties and are unlikely to be published in any widely accessible format.[176]

In fact, HHS already has been criticized for grossly deficient enforcement of the HIPAA Privacy Rule.[177] Between April 14, 2003 and June of 2006, HHS received 19,420 complaints concerning privacy vio-

---

[171] *See* Arthur Best, *Monetary Damages for False Advertising*, 49 U. PITT. L. REV. 1, 40 (1987) (explaining that "[p]rivate suits do not have to pass a public interest test").

[172] *See* Ann J. Gellis, *Mandatory Disclosure for Municipal Securities: Issues in Implementation*, 13 J. CORP. L. 65, 86 (1987) (stating that "reliance on public proceedings as the prime means of enforcement is subject to the direct political restraints of budget resources and indirect political pressures regarding how those resources are directed").

[173] *See* Best, *supra* note 171, at 40.

[174] *See* Gellis, *supra* note 172, at 81 (discussing judicial rule-making functions).

[175] *See* 45 C.F.R. § 160.426 (2006). If the Secretary imposes a fine on a covered entity, the Secretary is to notify the public "in such manner as the Secretary deems appropriate." *Id.* The Secretary is given no instructions, however, as to which media outlets to utilize, and it is uncertain whether a mere statement concerning the imposition of a penalty will generate the kind of extensive media interest that courtroom drama seems to produce.

[176] *See id.* § 160.546(a), (c).

[177] *See* Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, CENTER FOR AM. PROGRESS, June 7, 2005, http://www.americanprogress.org/issues/2005/06/b743281.html.

lations.[178] No civil fine has been imposed,[179] however, and as of June of 2006, only two criminal actions had been brought under HIPAA's criminal enforcement provision.[180] One case prosecuted a hospital phlebotomist who accessed the medical records of a terminal cancer patient in Seattle and obtained credit cards in his name,[181] and the other resulted in the conviction of a Texas woman who sold the medical records of an FBI agent.[182]

One might argue that several causes of action relating to privacy violations already exist in tort law, rendering a statutory private cause of action under HIPAA unnecessary. The tort of public disclosure of private facts consists of four elements: (1) public disclosure, (2) of a private fact, (3) that would be objectionable and offensive to a reasonable person, and (4) that is not of legitimate public concern.[183] Most courts have found that to support this theory of liability, plaintiffs must prove widespread dissemination of personal information to the public[184] and have deemed this tort theory to fit mostly cases involving publication through the media.[185] In the context of HIPAA violations, however, PHI

---

[178] Rob Stein, *Medical Privacy Law Nets No Fines: Lax Enforcement Puts Patients' Files at Risk, Critics Say*, WASH. POST, June 5, 2006, at A1. The regulations went into effect on April 14, 2003. 45 C.F.R. § 164.534.

[179] Stein, *supra* note 178.

[180] *Id.* The criminal enforcement provision is found at 42 U.S.C. § 1320d-6 (2000).

[181] Swire, *supra* note 177. The defendant had charged over $9000 on the credit card largely for video game purchases. *Id.* He pled guilty and was sentenced to sixteen months in prison. *Id.*

[182] Stein, *supra* note 178.

[183] *See* Diaz v. Oakland Tribune, 188 Cal. Rptr. 762, 765, 767–68 (Ct. App. 1983) (noting that jury found defendant liable for publicizing fact that plaintiff had gender corrective surgery, but overturning award based on erroneous jury instructions). There are three other kinds of invasion of privacy torts, none of which are likely to be relevant in the case of PHI disclosures—intrusion on seclusion, appropriation of name/likeness, and placing someone in a false light. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[184] Winn, *supra* note 39, at 653; *see* Satterfield v. Lockheed Missiles & Space Co., 617 F. Supp. 1359, 1370 (D.S.C. 1985) (stating that "[c]ommunication to a single individual or to a small group of people" will not support liability under a theory of public disclosure of private facts, which requires publicity rather than publication to a small group of people); Beard v. Akzona, Inc., 517 F. Supp. 128, 132 (E.D. Tenn. 1981) (emphasizing that publication to a small number of people will not create liability); Tollefson v. Price, 430 P.2d 990, 992 (Or. 1967) (stating that public disclosure occurs only when the information is communicated to the public generally or to a large number of people); Vogel v. W. T. Grant Co., 327 A.2d 133, 137 (Pa. 1974) (explaining that the tort is established only if disclosure is made to the public at large or the information is certain to become public knowledge); Swinton Creek Nursery v. Edisto Farm Credit, 514 S.E.2d 126, 131 (S.C. 1999) (stating that "publicity, as opposed to mere publication, is what is required to give rise to a cause of action for this branch of invasion of privacy").

[185] SOLOVE, *supra* note 13, at 59–60 (explaining that this tort "appears to be designed to redress excesses of the press").

generally will be delivered to particular interested parties, such as drug representatives, employers, or individuals with criminal intent, rather than to the general public, and thus, the tort of public disclosure of private facts will be inapplicable.

A more fruitful tort theory for plaintiffs might be breach of confidentiality.[186] Courts have based the patient's right of confidentiality upon a variety of sources, including privilege statutes protecting physician-patient communications, licensing statutes prohibiting the disclosure of patient information without authorization, and medical ethics principles articulated in the Hippocratic Oath and other sources.[187] In *Horne v. Patton* in 1973, for example, the Alabama Supreme Court held that a physician breached his duty of confidentiality by disclosing medical information to the patient's employer.[188] The court ruled that a doctor has a duty not to disclose patient information obtained in the course of treatment and that a private cause of action exists in cases where the duty is breached.[189] An action for breach of confidentiality can be maintained regardless of the degree to which the information has been publicly distributed, and there is no requirement to prove the intent of the perpetrator.[190]

Nevertheless, in general, the tort of breach of confidentiality can be established only when the perpetrator and the victim of the breach of confidentiality had a direct relationship.[191] Plaintiffs have also occasionally prevailed against third parties who knowingly induced physicians to reveal confidential information in violation of physician-patient confidentiality responsibilities, but here too, the improper disclosure was made by the doctor.[192] In addition, because breach of confidential-

---

[186] *See* Winn, *supra* note 39, at 652–58 (discussing the common law tort theory of breach of confidentiality and its implications).

[187] *Id.* at 654–55.

[188] 287 So. 2d 824, 829–30 (Ala. 1973).

[189] *Id.*

[190] Winn, *supra* note 39, at 657–58 (comparing the torts of invasion of privacy and breach of confidentiality).

[191] *Id.* at 662; *see* Humphers v. First Interstate Bank, 696 P.2d 527, 527–28, 530, 536 (Or. 1985) (finding that a mother who had given her daughter up for adoption had a cause of action for breach of confidentiality against a doctor who helped her daughter discover her mother's identity and explaining that "only one who holds the information in confidence can be charged with a breach of confidence").

[192] Winn, *supra* note 39, at 661–65; *see* Hammonds v. Aetna Casualty & Surety Co., 243 F. Supp. 793, 795 (N.D. Ohio 1965) (suit brought against a physician's malpractice insurer that had induced the physician to disclose the patient's confidential medical records when no malpractice case was pending); Alberts v. Devine, 479 N.E.2d 113, 116 (Mass. 1985) (suit brought against individuals who obtained information from the plaintiff's psychiatrist and used it to make an adverse employment decision); Biddle v. Warren Gen. Hosp., 715

ity is a common law tort, the standard for establishing liability can vary from state to state.[193]

The breach of confidentiality tort, therefore, will not extend to cases in which insurers or clearinghouses, rather than physicians or hospitals, legitimately possess PHI and disclose it to third parties who are not entitled to the data. Similarly, if the definition of "covered entities" is extended to encompass a large variety of parties in possession of PHI, the breach of confidentiality tort will not apply to disclosures made by employers, data miners, and others who obtained PHI by means other than physician disclosure.

Consequently, a statutory cause of action is needed to capture the many privacy threats that do not fit within the narrow bounds of common law causes of action. A federal statutory cause of action with explicit guidelines regarding damages will diminish inequities and inconsistencies in case outcomes.

III. Recommendations

In this Part, we provide four primary recommendations to enhance the efficacy of the Security Rule in particular, and to some extent, the Privacy Rule in general. These include: (1) expanding the scope of the HIPAA Privacy Rule through revision of the definitions of "covered entity" and "health information"; (2) enabling individuals to receive information concerning the provenance and uses of their PHI; (3) bolstering existing standards and implementation specifications, and providing covered entities with guidance and mechanisms that will facilitate compliance with the Security Rule's requirements; and (4) establishing a private cause of action for aggrieved individuals.[194] Our recommendations are designed to create fixed regulations that are workable in the dynamic and ever-changing realms of computer technology and security vulnerabilities. They also seek to balance patients' needs for privacy protection against businesses' needs to operate efficiently and profitably. We have carefully crafted our definitions to avoid creating unrealistic burdens for those who cannot bear them. We also have considered the

---

N.E.2d 518, 520 (Ohio 1999) (involving a law firm that induced a hospital to allow it to review all patient files to determine whether the patients were eligible for Supplemental Security Insurance Disability benefits, and thus, presumably, might wish to utilize the law firm's services); Morris v. Consolidation Coal Co., 446 S.E.2d 648, 649–50 (W. Va. 1994) (involving an employer who inappropriately obtained information from a physician who treated the plaintiff for injuries for which he claimed workers' compensation).

[193] *See* sources cited *supra* note 192.

[194] *See infra* notes 195–333 and accompanying text.

implications of our proposals in a variety of circumstances, which we illustrate through detailed examples.

A. *Expanding the Regulatory Scope*

In order to expand the scope of the Privacy and Security Rules, two regulatory definitions must be altered. The terms at issue are "covered entity" and "health information." This Section will formulate recommendations for revisions of the definitions,[195] discuss the changes' impact on the Privacy Rule's "uses and disclosures" provision,[196] and critique alternative approaches to the suggested changes.[197]

1. Covered Entities

Because health care providers, insurers, and clearinghouses are by no means the only entities to maintain and transmit PHI, it is illogical to limit the jurisdiction of the Security Rule in particular and the privacy regulations in general to these three types of entities.[198] The threat to electronic PHI reaches far beyond the health care field because a variety of parties, such as marketers, blackmailers, and anyone with a stake in an individual's financial future, might be interested in obtaining health information.[199]

Consequently, the term "covered entity" in the HIPAA Privacy Rule[200] should be expanded to include a fourth component, namely, "any person who knowingly stores or transmits individually identifiable health information in electronic form for any business purpose related to the substance of such information." At the same time, some of the Privacy Rule's "Applicability" sections[201] and the "Applicability" provision of the HIPAA legislation itself[202] would need to be revised to add the above-described fourth covered category.

The term "Person" is defined in the privacy regulations as "a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private."[203] The term

---

[195] *See infra* notes 198–223 and accompanying text.
[196] *See infra* notes 224–235 and accompanying text.
[197] *See infra* notes 236–238 and accompanying text.
[198] *See supra* notes 92–121 and accompanying text.
[199] *See supra* notes 5–23, 92–121 and accompanying text.
[200] *See* 45 C.F.R. § 160.103 (2006) (providing the current definition).
[201] *Id.* §§ 160.102, 164.104.
[202] 42 U.S.C. § 1320d-1(a) (2000).
[203] 45 C.F.R. § 160.103.

"business" should be defined as an "activity or enterprise undertaken for purposes of livelihood or profit."[204]

Admittedly, limiting the scope of regulatory coverage to those who utilize PHI for business purposes related to the substance of the PHI will result in the persistence of some significant security threats. For example, volunteers associated with religious organizations might collect and electronically store large volumes of information about community members who have been hospitalized or have disabilities for purposes of providing them with assistance. If this data is not secured through adequate computer technology and security practices, it could be inadvertently or deliberately disseminated to unwanted sources. Yet, this volunteer activity could not be defined as "business" under the proposed revision and would not be addressed by the Privacy Rule.

Nevertheless, it is inadvisable to extend the regulations beyond this suggested revision because doing so, ironically, could result in increased governmental invasion of privacy rather than enhanced privacy protection. To illustrate, a definition of "covered entity" that included any person who handled electronic PHI for any reason whatsoever would capture private citizens who e-mailed each other about a friend's medical problem. These individuals would be required to purchase costly security technology for their computers and be subject to penalties for disseminating news of the illness to third parties without the data subject's consent. Such a rule would constitute unwarranted government intrusion into purely private matters.

Application of the privacy regulations to volunteer activities also would be undesirable because the cost of compliance and the threat of liability might deter engagement in charitable work and, therefore, hurt rather than promote the interests of those who are sick or have disabilities. It also should be recalled that several relevant causes of action exist under tort theories, such as public disclosure of private facts and breach of confidentiality.[205] Thus, disclosures of private health information by parties not covered by the Privacy Rule's revised definition could, in appropriate circumstances, be addressed through tort law, if they cause injury to the data subject.[206]

Furthermore, limiting covered entities to those that *knowingly* process individually identifiable health information in electronic form for any business purpose related to the substance of such information

---

[204] *Cf.* Flint v. Stone Tracy Co., 220 U.S. 107, 171 (1911) (providing similar definition); BLACK'S LAW DICTIONARY 211 (8th ed. 2004) (same).

[205] *See supra* notes 183–193 and accompanying text.

[206] *See supra* notes 183–193 and accompanying text.

addresses the fact that some parties might unintentionally and inadvertently come to possess health information. For example, a photo shop that develops pictures from digital cameras could handle pictures revealing scars and physical impairments or memorializing hospitalizations, births, and other health-related events. These might be stored for a time on the business's computer even though no employee specifically knows of their existence or uses them for any purpose relating to health and medicine. It would be excessive and impolitic to burden all photo shops with the requirements of the Security Rule and other privacy regulations based on the possibility that some of the pictures they develop will contain medical data.

The final qualification of the definition, which restricts covered entities to those that process PHI for any business purpose *related to the substance of such information*, aims to exclude those who might come to handle some form of PHI in the course of their business but who do not actually use the contents of the information. Thus, the photo shop described above would be excluded from coverage not only for the reasons already discussed, but also because it does not utilize the contents of health information concerning individuals for any business purpose.

To illustrate further, a small "mom and pop" store might sell over-the-counter medications along with food and other items. If a customer pays by credit card, these drugs might be scanned for payment purposes and associated with the customer's credit card number in electronic transaction records. The store operators, however, would retain the information only for purposes of credit card records and would not utilize specific information concerning the customer's health-related purchases for any business purpose.[207] It would be inappropriate to require the mom and pop store to comply with the HIPAA privacy regulations' requirements based solely on its sale of pain relief or cold medications.

By contrast, pharmacies selling prescription drugs that are labeled with the patient's name and doctor's instructions have far more extensive information about patients, including the names of their doctors, histories of their prescription drug purchases, and other details, which they utilize for purposes of refills and identifying repeat customers who fill new prescriptions. Drug stores are thus justifiably covered entities.[208]

---

[207] If, however, the store operators wished to sell individually identifiable information about the purchase of health products to third parties and thereby profit from its processing, they would become covered entities.

[208] *See* SOLOVE, *supra* note 13, at 208.

Under the proposed definition, most if not all "business associates" also will become covered entities because they are hired specifically to process PHI.[209] This coverage is consistent with the existing regulations, which state that a "covered entity may be a business associate of another covered entity" and will provide reinforced protection to data subjects.[210] Business associates will not only be bound by the terms of their contracts with other covered entities, which are governed by the HIPAA Privacy Rule,[211] but also will be themselves subject to all of the Privacy Rule's provisions, HHS investigations and administrative enforcement actions,[212] and private litigation in case of statutory violations.

2. Health Information

The recommended expansion of the definition of "covered entity" will necessitate a parallel expansion of the meaning of "health information," which is found in the privacy regulations' definition section[213] as well as in HIPAA's statutory definition section.[214] "Health information" currently means:

> [A]ny information, whether oral or recorded in any form or medium, that:
>
> (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
>
> (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[215]

This definition excludes PHI that is provided by individuals without the involvement of a health professional and is handled by financial

---

[209] *See* 45 C.F.R. § 160.103 (2006) (defining "business associate"); *see also id.* § 164.314 (stating contractual requirements relating to the processing of PHI by business associates). Under the contractual terms demanded by 45 C.F.R. § 164.314, it would be very difficult for a business associate to claim that it did not know it was processing PHI and thus escape HIPAA responsibilities. To avoid any ambiguity, however, covered entities should state explicitly in their contracts that they are hiring business associates to process PHI.

[210] *See id.* § 160.103.

[211] *Id.* § 164.314 (articulating the standard for business associate contracts).

[212] *See id.* §§ 160.500–.552. Unfortunately, business associates in foreign countries are likely to be beyond the reach of HHS enforcement.

[213] *Id.* § 160.103.

[214] 42 U.S.C. § 1320d(4) (2000).

[215] *Id.*

institutions, marketers, website operators, and many other parties with an interest in individuals' electronic PHI.[216]

A more appropriate definition can be derived from the proposed Health Technology to Enhance Quality Act of 2005,[217] discussed previously.[218] This bill defines "health information" to mean "any information, recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual."[219] This language does not limit "health information" based on who its creator or recipient was.

Although this definition is quite broad, it should be qualified to require a clear association between data and the physical or mental health status of a particular individual. Recall the above example of a grocery store selling nonprescription medication, vitamins, or dietary supplements.[220] Do records of purchases of such items constitute "health information"? On the one hand, data miners may be able to infer the existence of particular diseases from a series of seemingly unrelated purchases.[221] On the other hand, many substances can be utilized for a broad spectrum of conditions, ranging from a headache to post-surgical care, and many items are bought for use by persons other than the purchaser. The fact of the sale does not clearly reveal specific information concerning a particular individual's health status. Consequently, records of sales of nonprescription health-related goods should not be covered by HIPAA even if they are maintained in electronic form.[222] We therefore recommend that "health information" be defined as "any information, recorded in any form or medium, that clearly relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual."

Because we cannot anticipate every circumstance that will arise and require interpretation of the regulatory standards, we cannot pro-

---

[216] *See id.*

[217] *See* S. 1262, 109th Cong. (2005).

[218] *See supra* notes 119–121 and accompanying text.

[219] S. 1262 § 2901(3).

[220] *See supra* note 207 and accompanying text.

[221] Buying a combination of high calorie dietary supplements, pain medication, and particular vitamins could indicate that an individual has AIDS or cancer.

[222] PHI that is inferred by data miners from such records and used for business purposes would, however, be covered under our definition.

vide comprehensive guidance concerning the meaning of "health information" in every hypothetical instance. Further elucidation of the Privacy Rule's requirements will be achieved over time through further guidance by HHS and the courts in response to specific controversies.[223]

3. Uses and Disclosures

The new definition of "covered entity" would render all of the privacy regulations' provisions applicable to anyone who knowingly transmits or maintains electronic PHI for any business purpose related to the substance of the PHI. A particularly significant section of the Privacy Rule is the "uses and disclosures" provision,[224] which prohibits the utilization and dissemination of PHI without the patient's consent except in specific circumstances that generally relate to medical treatment or obligations established by law.[225] With an expanded definition of "covered entity," this provision would have a dramatically greater impact because it would constrain many more parties handling PHI. This consequence is a salutary development that will provide much more meaningful protection for individually identifiable health information. Employers, life insurers, marketers, retailers, and others could not use PHI or disclose it to third parties without obtaining the consent of the data subjects.

The required contents of covered entities' notice of privacy practices, including use and disclosures, are specified in the federal regulations.[226] The regulations also require that each authorization be signed and dated by the data subject.[227] The regulations, however, do not instruct covered entities to alert data subjects that a risk of unauthorized disclosure will exist no matter what security measures are implemented. Because awareness of the risk could be essential to individuals' decision making and provision of meaningful consent, we recommend that the regulatory notice provision be amended to require that covered entities include a statement in their patient consent forms such as, "despite our efforts to safeguard your privacy, a risk remains that your electronically stored PHI will be disclosed without authorization because of an unan-

---

[223] *See infra* notes 233–235 and accompanying text (discussing means of contacting HHS).

[224] 45 C.F.R. § 164.502 (2006).

[225] *Id.* §§ 164.502(a), .512.

[226] *Id.* § 164.520(b).

[227] *Id.* § 164.508(c)(1)(vi).

ticipated security failure."[228] Individuals who sign an authorization containing this statement will be empowered to conduct their own risk analysis and to make a more educated decision about consent.

The expanded prohibition will adversely affect marketing[229] and data mining operations, but it will not eradicate them. Covered entities that wish to sell PHI would have to obtain consent from those whose data is disclosed,[230] but this may willingly be given if the request is carefully worded. For example, many individuals might provide authorization if they are told that their information "will be used to identify products that will better fit your needs." Data miners that garner information from sources other than the person to which it relates would likewise need to obtain consent for every sale of their lists. To simplify matters, a "do not market list," similar to the "national do not call list" that relates to phone solicitations, could be constructed.

The Privacy Rule details numerous exceptions to the use and disclosure prohibition, all of which would apply to the newly covered entities.[231] These exemptions include, among others, uses and disclosures without consent that are: (1) required by law; (2) necessary for public health activities; (3) related to victims of abuse, neglect, or domestic violence; (4) required for purposes of health oversight activities; (5) necessary for judicial and administrative proceedings; (6) required for law enforcement purposes; (7) necessary to avert a serious threat to health or safety; or (8) needed for specialized government functions.[232]

---

[228] Unfortunately, covered entities will not be able to quantify the risk, such as by stating that the risk is one in a hundred or a thousand.

[229] *See* 45 C.F.R. § 164.508(a)(3) (establishing that covered entities must obtain consent for any use or disclosure of PHI for marketing purposes with very limited exceptions).

[230] *Cf.* Parliament and Council Directive 2002/58/EC, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37, 41–42 (stating that "[i]f the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained" and that "[w]hen electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage").

[231] *See* 45 C.F.R. §§ 164.502, .512 (2006) (detailing currently permitted uses and disclosures).

[232] *Id.* § 164.512. By comparison, the E.U. Privacy Directive, which applies to all entities processing numerous categories of data, allows the processing of private information under the following circumstances: (1) the data subject has consented to the processing; (2) processing is necessary for purposes of employment law; (3) the data subject is unable to provide authorization and processing is necessary to protect the vital interests of the individual in question or a third party; (4) processing is done by a foundation, association, or other nonprofit-seeking body for its own purposes, and no data is disclosed to third parties without consent; (5) the data is made public by its subject or is necessary for purposes of a legal

It is possible that the expansion of the "covered entities" definition will necessitate other unanticipated exceptions. These may be identified through public input provided during the notice and comment period that would follow the proposal of the amendments delineated in this Article.[233]

In addition, the HHS website establishes an avenue for communicating with the agency concerning comments and questions.[234] Specifically, it provides:

> [Y]ou may submit an e-mail by clicking on the mailbox (OCRPrivacy@hhs.gov). Individual responses will not be provided, however, we will address concerns of general interest through development of new FAQs or other guidance for inclusion on our web site. As an alternative, you may call the HIPAA toll-free number at (866) 627–7748.[235]

Thus, inquiries could be submitted to HHS concerning the permissibility of particular uses and disclosures, whether certain data constitutes "health information," and other matters requiring clarification.

4. Alternatives to Revising the Privacy Rule

An alternative approach to modifying the HIPAA Privacy Rule would be to amend individually a large number of laws that govern actors who might pose a threat to medical privacy. For example, the Americans with Disabilities Act places boundaries upon the timing, content, and use of employer-conducted medical inquiries and examinations.[236] It does not, however, address the permissibility of acquiring medical data from third parties or the security measures that must be applied to any health records possessed by employers.[237] This

---

claim; or (6) processing is required for medical reasons. E.U. Privacy Directive, *supra* note 99, art. 8, 1995 O.J. (L 281) at 40; *see also* Andrew Charlesworth, *Implementing the European Union Data Protection Directive 1995 in UK Law: The Data Protection Act 1998*, 16 GOV'T INFO. Q. 203, 215–18 (1999) (discussing the United Kingdom Data Protection Act of 1998 and the uses and disclosures permitted by the law); Theo Hooghiemstra, *The Implementation of Directive 95/46/EC in the Netherlands, with Special Regard to Medical Data*, 9 EUR. J. HEALTH L. 219, 219–21 (2002) (discussing the Netherlands's Personal Data Protection Act and its exceptions).

[233] *See* 5 U.S.C. § 553(b)–(c) (2000) (establishing notice and comment requirements for proposed administrative rules).

[234] U.S. Dep't of Health & Human Servs., Office for Civil Rights, http://www.hhs.gov/ocr/contact.html (last visited Feb. 23, 2007).

[235] *Id.*

[236] 42 U.S.C. § 12112(d) (2000).

[237] *Id.*

provision could be revised to indicate explicitly that it is impermissible for employers to use health information obtained from external sources without the informed consent of the individuals in question and to address the security of electronic medical data. As a second example, the Gramm-Leach-Bliley Act requires financial institutions to safeguard the confidentiality of their customers' nonpublic personal information but allows for its disclosure in a variety of circumstances.[238] This law too could be tightened to establish a more rigid prohibition of PHI disclosure and to instruct financial institutions to employ appropriate security safeguards for computerized PHI.

Nevertheless, a piecemeal approach to enhancing PHI protection is undesirable. First, from a practical standpoint, legislatures are unlikely to revisit numerous statutes in order to address PHI issues. Second, the process of revising multiple laws to include detailed security mandates would be extremely cumbersome. Finally, a statute-by-statute approach is likely to lead to inconsistencies in levels of protection furnished by different laws and to the introduction of new ambiguities in statutory language that will require judicial interpretation. By contrast, a revision of the HIPAA Privacy Rule will comprehensively repair the law. Broadening the definitions of "covered entity" and "health information" will significantly augment the efficacy of the HIPAA Security Rule in particular and the Privacy Rule in general and will address many additional threats to health information privacy.

B. *Allowing for Meaningful Inquiry Regarding the Origins and Uses of PHI*

As explained above, the HIPAA privacy regulations allow patients to inspect and obtain copies of their PHI from covered entities.[239] So long as the only entities covered by HIPAA are health plans, health care clearinghouses, and health care providers, the origins and uses of the documents generally should be obvious from the documents themselves and the party from which they were obtained. However, if the privacy regulations are expanded, as we recommend, to cover any person who knowingly stores or transmits individually identifiable health information in electronic form for any business purpose related to the substance of such information, it will become important for individuals

---

[238] 15 U.S.C. §§ 6801–6802 (2000). For example, the statute permits disclosure "to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services . . . ." *Id.* § 6802(b)(2).

[239] 45 C.F.R. § 164.524(a)(1) (2006).

to be able not only to have access to PHI that is possessed by others, but also to establish the provenance of the data and the manner in which it has been used. This evidence will be vital for determining both the extent of the injury to the individual and the existence of Privacy Rule breaches by data sources.

The requirement of informed consent for the use or dissemination of PHI should allow individuals to remain educated concerning the movement of their PHI in most cases.[240] A party that wishes to transmit PHI would need to obtain authorization from the affected individuals. The right of inquiry described above, however, will provide an added information resource in cases in which data is obtained accidentally, through the black market, or by other unlawful means.

The right of inquiry also will serve as a deterrent to malfeasance. If a covered entity obtains PHI from a dubious source and then seeks authorization to use it, the data subject is likely to be surprised by the request for consent and to inquire about the origins of the data. An unsatisfactory response likely would lead the data subject to refuse to authorize data use and thus, the purchaser will have wasted its effort and money in obtaining the PHI. Furthermore, the data subject may file a complaint with the government and/or initiate litigation against the source that distributed the PHI in violation of the regulations. The expanded right of inquiry should, consequently, incentivize covered entities to engage in due diligence to determine the legitimacy of PHI suppliers. Because it provides data subjects with an inexpensive means of conducting preliminary investigations concerning potentially inappropriate PHI disclosures, this mechanism should also deter regulatory violations.

The privacy regulations allow covered entities to charge a "reasonable, cost-based fee" for the copying, postage, and labor costs associated with providing individuals access to their PHI.[241] Additional payments could be required for processing of inquiries about the provenance and use of PHI. These charges should prevent frivolous inquiries and harassment of covered entities by the public.[242]

The process of inquiry should not be excessively burdensome for covered entities and could be easily automated. Those processing PHI should establish websites to which individuals can submit queries concerning whether the entity possesses their PHI, and, if so, where it origi-

---

[240] *See id.* § 164.508(a) (discussing the requirement that covered entities obtain authorization for the use and disclosure of PHI); *supra* notes 224–235 and accompanying text.

[241] *See* 45 C.F.R. § 164.524(c)(4).

[242] *See id.*

nated and how it has been used. Generally, respondents will be able to develop boilerplate answers to diminish the need for individually designed narratives. For example, common responses might be "obtained from Hippo Direct list"[243] and "used for marketing purposes."

C. *Enhancing Compliance Guidelines*

The Security Rule provides a dearth of specific instructions for regulatory compliance, preferring to assume good judgment on the part of covered entities.[244] This approach leaves a vacuum of guidance for health care providers with no technological expertise.[245] It also could encourage malfeasance by prosperous covered entities that could invest significant resources in ensuring the security of electronic PHI, but that instead choose to take minimal precautions.[246] We recommend that a number of steps be taken to provide more specific guidance to covered entities.

1. Augmenting the Implementation Specifications

The HIPAA Security Rule offers skeletal and vague implementation specifications that leave many substantial gaps and loopholes. Consequently, a more robust scheme of standards and implementation specifications would significantly advance the goal of improved security protection for PHI.[247]

First, a clarification should be made to the phrase "criticality of potential risks" in the Security Rule's "flexibility of approach" provisions[248] and the "risk analysis" requirement in the administrative safeguards' implementation specifications.[249] It should be clarified to indicate that

---

[243] *See* Hippo Direct, *supra* note 134.

[244] *See* 45 C.F.R. § 164.306(b)(1) (stating that "[c]overed entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart"); *supra* notes 141–157 and accompanying text. Covered entities are instructed to consider several factors in making their implementation decisions, including their size, complexity, capabilities, and technical infrastructure; the costs of the security measures; and the nature of the potential threats to the PHI they maintain, but they are given no assistance in making specific implementation decisions. 45 C.F.R. § 164.306(b)(2).

[245] *See* 45 C.F.R. § 164.306(b)(1) (2006).

[246] *See id.*

[247] *See supra* notes 141–157 and accompanying text (critiquing the Security Rule's flexible approach and vague guidance).

[248] 45 C.F.R. § 164.306(b)(2)(iv).

[249] *Id.* § 164.308(a)(1)(ii)(A); *see supra* notes 148–150 and accompanying text (critiquing these provisions of the Security Rule).

the risks to be considered are the risks to all stakeholders, including data subjects, covered entities, and business associates.

Second, because effective risk analysis is crucial to a covered entity's ability to choose appropriate security measures, the Rule must provide further guidance as to how risk analysis should be conducted.[250] A simple way to do so would be to require covered entities to follow the NIST *Risk Management Guide for Information Technology Systems*.[251] HHS cited the NIST document as authority in its response to comments provided during the proposed Security Rule's public comment period,[252] but the Security Rule itself has no reference to it. We recommend that the regulations' risk analysis provision[253] be amended to require that covered entities' risk analyses be consistent with all relevant guidelines established in the NIST *Risk Management Guide for Information Technology Systems*. If HHS determines at a later time that a better document exists because the NIST guidance has become outdated or a superior document is issued by a different organization, the regulatory provision would need to be changed again to refer to the new source.[254]

Covered entities that cannot implement this guidance themselves for lack of expertise or resources could hire vendors to conduct the risk analysis for them or provide them with a simplified form of the risk analysis procedure that is tailored to their type of entity. Vendors that specialize in electronic PHI security will be able to adapt the NIST guidance to particular categories of businesses that they service and may be able to accomplish the task by asking clients to fill out a relatively short questionnaire that will provide all necessary information. The use of vendors for HIPAA compliance purposes is discussed in the next subsection of this Article.[255]

---

[250] *See* 45 C.F.R. § 164.306(b)(1) (allowing covered entities discretion to choose appropriate security measures).

[251] *See generally* GARY STONEBURNER ET AL., NAT'L INST. OF STANDARDS & TECH., RISK MANAGEMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS (2002), *available at* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[252] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8346 (Feb. 20, 2003).

[253] 45 C.F.R. § 164.308(a)(1)(ii)(A) (2006).

[254] A draft international standard, *ISO/DIS 27799*, entitled "Health Informatics—Security Management in Health Using ISO/IEC 17799," contains a thorough discussion of threats to the security of health information. *See* Int'l Org. for Standardization, ISO/DIS 27799, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41298&scopelist=PROGRAMME (last visited Feb. 23, 2007). If this standard is passed and the risk assessment section remains intact, the regulations may need to make reference to *ISO 27799* as well, because, unlike the NIST guidance, it is specific to the health information context.

[255] *See infra* notes 269–292 and accompanying text.

Third, the Security Rule must induce covered entities to implement the best current practices of the health informatics and computer security communities.[256] To that end, the "general requirements" section[257] should include an additional element, placed before the current fourth requirement, worded as follows: "Make reasonable efforts to identify and employ best practices relating to security measures, software development, validation, maintenance, and software system administration that are either commonly used by similarly situated business entities and governmental institutions or can be clearly demonstrated to be superior to best common practices."[258] The best current practices requirement would apply to all standards and implementation specifications. Thus, if a covered entity determined that it would not be "reasonable and appropriate" to implement an addressable implementation specification, it would need to document why implementing the specification would not constitute best current practices under the circumstances.[259]

The best current practices standard is essential to making the Security Rule meaningful in light of the dynamic nature of the computer security field. The text of the Security Rule must maintain a level of generality and cannot dictate that covered entities adopt specific technologies because these could easily become outdated even before the regulations are enacted. A "best practices" standard is an effective way to provide some guidance while maintaining sensitivity to the computer technology environment. This approach is not unprecedented, given that "best practices" standards are found elsewhere in U.S. law. For example, a provision of the Sentencing Guidelines that requires the establishment of effective compliance and ethics programs allows small organizations to model their programs partly on the "best practices of other similar organizations."[260] Likewise, an Environmental Protection Agency regulation relating to hazardous air pollutants instructs covered entities to design startup, shutdown, and malfunction plans that "reflect the best practices now in use by the industry to minimize emissions."[261]

As discussed below, many if not most covered entities are expected to utilize vendors to serve their HIPAA Security Rule compliance

---

[256] *See supra* notes 153–154 and accompanying text.

[257] *See* 45 C.F.R. § 164.306(a).

[258] *See id.*

[259] *See* 45 C.F.R. § 164.306(d)(3)(i), (d)(3)(ii)(B)(1) (2006).

[260] U.S. SENTENCING GUIDELINES MANUAL § 8B2.1, cmt. n.2(C)(iii) (2005).

[261] 40 C.F.R. § 63.2852.

needs,[262] and thus, they will not themselves need to engage in the work of determining industry standards. Moreover, a plethora of information about security standards and industry practices is readily available through the Internet and in print, published by reputable organizations such as ISO, CERT, NIST, and NIAP, as well as software vendors.[263] Both vendors and covered entities should easily be able to access these sources, from which best current practices can be ascertained. Although covered entities can rely on a reading of industry literature to determine best practices, they should not depend upon one single source, given that no comprehensive guidance has been produced to cover all aspects of HIPAA Security Rule compliance. Different documents will be relevant to risk analysis, security vulnerabilities, software engineering, system administration, and so on.[264]

Fourth, the Security Rule, which currently fails to address software engineering, should include language that explicitly focuses on this essential security component. The best practices provision described above, which would require covered entities to make reasonable efforts to identify and employ best practices relating to software development, validation, maintenance, and systems administration, is one step in the right direction.[265] Furthermore, the risk analysis provision should incorporate an additional statement that the risks to be considered include those associated with software development, operation, and maintenance.[266] Similarly, the risk management provision should be elucidated to state that the risks and vulnerabilities at issue include those linked to software development, operation, and maintenance.[267]

2. Security Product Vendors and Certification

The previous subsection recommended a "best current practices" standard as a general Security Rule requirement.[268] The question to which we now turn is how "best practices" should be identified and implemented by covered entities.

One option is for CMS, in its oversight capacity, to create a centralized repository of information. CMS could maintain a website in which it describes the security measures and technology needed by different

---

[262] *See infra* notes 269–292 and accompanying text.
[263] *See infra* notes 293–318 and accompanying text.
[264] *See infra* notes 293–318 and accompanying text.
[265] *See supra* notes 256–261 and accompanying text.
[266] *See* 45 C.F.R. § 164.308(a)(ii)(A) (2006).
[267] *See id.* § 164.308(a)(ii)(B).
[268] *See supra* notes 256–261 and accompanying text.

entities for compliance purposes, provides a current list of known security vulnerabilities in health information systems and the computing platforms they rely upon, and designates the updates and fixes that are sufficient to address these problems.

This approach, however, may run afoul of the notice and comment requirements established by the Administrative Procedure Act.[269] A binding set of technical requirements could be interpreted to constitute rule making, which would trigger public notice and comment requirements.[270] These, in turn, would generate significant delays and render it impossible for CMS to respond to rapidly changing technology and emerging security threats in a timely fashion. The Act establishes an exception for cases in which an "agency for good cause finds (and incorporates the finding and a brief statement of reasons therefore in the rules issued) that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest."[271] It is possible but not certain that this exception would apply to the above-described website.

Several other problems are inherent in the centralized repository approach. CMS would require significant additional funding and personnel resources to produce and continuously update a comprehensive set of materials for the website, and it would need to develop technical expertise that it does not currently have. Furthermore, relying on a single source of information means that any mistakes or flaws in the information could affect all covered entities. Finally, if the government retains power to designate best current practices, covered entities' security obligations might vacillate significantly with changes in the political environment. Thus, some administrations might articulate very demanding standards and others very lax ones.

A superior alternative would be to allow best current practices to emerge through the free market. Presumably, members of the computer security industry would compete to produce the best possible products at a reasonable cost. As a check against market flaws that generate low standards within private industry, covered entities also would be instructed to research, as part of their best practices analysis, the computer security measures that are adopted by the government.[272]

---

[269] *See* 5 U.S.C. § 553(b)–(c) (2000) (establishing notice and comment requirements for proposed administrative rules).

[270] *See id.*

[271] *Id.* § 553(b)(3)(B).

[272] *See supra* notes 256–261 and accompanying text (explaining that best practices are those commonly used by industry and governmental institutions).

Many covered entities will lack the technical knowledge and resources to identify best current practices and achieve Security Rule compliance and will require the services of computer security professionals. To that end, it would be useful for CMS to maintain on its website a list of approved vendors that can be retained by covered entities for purposes of achieving Security Rule compliance. The vendors would provide both products and technical assistance and would need to have not only technical expertise but also thorough familiarity with the HIPAA Security Rule. The vendors would be certified based on proof that their technology is state-of-the-art and Security Rule compliant, that they have not been negligently responsible for any Security Rule breaches, and that they are able to address critical new security threats through timely user advisories, software improvements, and automatic installation of software updates.[273] Vendors would also have to be certified for entities of particular sizes and types, because different business environments require different services.

Covered entities that retain the certified vendors would be presumed to have complied with the Security Rule's requirements, though the presumption could be rebutted by evidence that they failed to follow the vendor's instructions or refused to accept the vendor's recommendations. It also could be rebutted with evidence that the covered entity knew or should have known that the vendor was not actually providing products and services that were Security Rule compliant.[274] This would occur in instances in which a vendor had been exposed by a whistleblower or the media as engaging in quackery or the sale of ineffective products. The rebuttable presumption would provide protection against under-scrutiny by the government during the certification process and against vendors that might act in bad faith after they are certified in order to under-sell competitors or enjoy greater profits.

Where appropriate, the vendors should provide clients with alternatives from which they can select, depending on their resources and capabilities. For example, covered entities that are experiencing financial difficulties could be given the option of de-identifying all of their

---

[273] The government licenses and recertifies individuals and entities in other contexts. For example, attorneys must pass the bar in order to practice law and, in many states, must earn a certain amount of CLE credit each year to retain their licenses. Similarly, nursing homes are certified and periodically surveyed for purposes of recertification. *See* Senator Charles Grassley, *The Resurrection of Nursing Home Reform: A Historical Account of the Recent Revival of the Quality of Care Standards for Long-Term Care Facilities Established in the Omnibus Reconciliation Act of 1987*, 7 ELDER L.J. 267, 271–72 (1999).

[274] *See supra* note 273 and accompanying text.

electronic PHI. This would entail associating a new, automatically generated identifier, such as a random number, with a patient's electronic health record. A list mapping these identifiers to patients' names and/or Social Security numbers would be maintained only in paper form. This approach would constitute an inexpensive and simple alternative to implementing sophisticated, technological security measures.

Furthermore, to achieve Security Rule compliance, covered entities should have ongoing relationships with vendors so that vendors can provide software updates as the need arises and reassess entities every year or two to ensure that they continue to employ current and appropriate security practices.[275] Covered entities that do not hire one of the approved vendors will be responsible for developing their own implementation measures, which must be at least as effective as those provided by certified vendors.

Proposals for certification by CMS were discussed in the comments to the proposed Security Rule.[276] CMS asserted that it did not intend to establish certification criteria for covered entities because it did not "have the resources to address the large number of different business environments."[277] Similarly, CMS refused to "assume the task of certifying software and off-the-shelf products" for lack of resources and expertise.[278] Instead, CMS believed that compliance assessment instruments should be developed and implemented by the private marketplace.[279]

Certification of vendors, rather than covered entities or products, was not discussed in the comments.[280] This type of certification may be less burdensome for CMS, because there should be fewer vendors than covered entities or products. It is likely, however, that CMS still would argue that it lacks sufficient resources and expertise to certify even vendors alone.

Nevertheless, CMS should reconsider its unwillingness to provide some form of certification for compliance purposes. Several comments to the proposed Security Rule emphasized the need for a list of federally approved security products and for certification procedures.[281] This need is acute for small covered entities that do not have the funds, per-

---

[275] The reassessment might be easily achieved through a well-tailored questionnaire.

[276] *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8352 (Feb. 20, 2003).

[277] *Id.*

[278] *Id.*

[279] *Id.*

[280] *Id.* at 8351–52.

[281] *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8352.

sonnel, and computer proficiency to assess their Security Rule compliance or to determine which commercially available security products they should purchase in order to fulfill regulatory requirements. With vendor certification, resource-poor covered entities would have an accessible and reliable mechanism to achieve compliance.

CMS acknowledged that other governmental entities are adopting the certification approach.[282] For example, NIST and the National Security Agency (the "NSA") have established the National Information Assurance Partnership, whose goal is to help information technology producers and consumers meet their security testing and assessment needs.[283] To that end, the NSA has established the TEMPEST[284] Endorsement Program, through which it provides lists of TEMPEST telecommunications equipment, TEMPEST test services facilities, and Commercial Off-the-Shelf telecommunications equipment that it has endorsed.[285] Germany has embraced certification to a much larger extent. Its Federal Office of Information Security (the "BSI") provides certification services through which information technology products and systems are tested and certified.[286]

In the comments to the proposed Security Rule, HHS stated that it encourages professional associations to undertake assessment and implementation activities with respect to HIPAA security requirements.[287] Assuming that the demand for certified products grows dramatically with the expansion of the "covered entity" definition, it is likely that some organizations would become interested in providing certification services for a fee.

If CMS cannot certify the vendors themselves, at the very least it should certify entities that provide certification services. There is precedent for this practice as well. Germany's BSI not only certifies in-

---

[282] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8352 (Feb. 20, 2003) (stating that HHS has "noted with interest that other Government agencies such as the National Institute of Standards and Technology (NIST) are working towards that end").

[283] *See* Nat'l Sec. Agency Cent. Sec. Serv., National Information Assurance Partnership, http://www.nsa.gov/ia/industry/niap.cfm (last visited Feb. 23, 2007).

[284] TEMPEST INC., http://www.tempest-inc.com/home.htm (last visited Feb. 23, 2007). TEMPEST INC. "offers TEMPEST/EMSEC and Electromagnetic Compatibility testing and design services in accordance with current Military, FCC, Australian & European Community Requirements." *Id.*

[285] Nat'l Sec. Agency Cent. Sec. Serv., Tempest Endorsement Program, http://www.nsa.gov/ia/industry/tempest.cfm?MenuID=10.2.1.3 (last visited Feb. 23, 2007).

[286] Bundesamt für Sicherheit in der Informationstechnik, Department 3: Certification, Approval and Conformity Testing, New Technologies, http://www.bsi.de/english/department3.htm (last visited Feb. 23, 2007).

[287] Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8352.

formation technology security products, but also accredits and licenses evaluation facilities so that they can assess information technology products and systems.[288] ISO, a well-respected nongovernmental global federation established in 1946 to promote "the international exchange of goods and services" through the creation of uniform standards,[289] has issued several standards that provide best practices guidance to those operating certification systems.[290] One of these, *ISO Guide 65*, has been adopted by the U.S. Department of Agriculture, and is applied to companies operating product certification standards for livestock, meat, seed, and other agricultural products.[291] CMS also could adopt appropriate ISO certification guidelines so that it would not have to wholly invent its own criteria. The certification bodies that are accredited by CMS would in turn certify vendors, and use of the certified vendors' products would create a rebuttable presumption of HIPAA security compliance, as described above.[292] The certifying bodies would have to be recertified by CMS periodically to ensure their continued competence. Furthermore, the CMS website would list the certifying bodies, which would then direct covered entities to the vendors they have approved.

3. Existing Tools and Emerging Technologies

Ultimately, the electronic PHI security business could develop into a sophisticated international industry.[293] Some tools that will facilitate regulatory compliance and certification already exist. These tools can be used to determine best current practices in various areas covered by the Security Rule.

ISO and the International Engineering Council ("IEC") have published a variety of standards describing sound information security prac-

---

[288] Bundesamt für Sicherheit in der Informationstechnik, *supra* note 286.

[289] Paulette L. Stenzel, *Can the ISO 14000 Series Environmental Management Standards Provide a Viable Alternative to Government Regulation?*, 37 Am. Bus. L.J. 237, 240 (2000).

[290] ISO, Combined Search Result for "Certification," http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=certification (last visited Feb. 23, 2007).

[291] *See* U.S. Dep't of Agric., USDA ISO Guide 65 Program, http://www.ams.usda.gov/lsg/arc/iso65.htm (last visited Feb. 23, 2007).

[292] *See supra* note 274 and accompanying text.

[293] *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 Berkeley Tech. L.J. 1553, 1610–11 (2005) (noting that "[w]ith cybercrimes skyrocketing and an ever-increasing amount of sensitive information being exchanged on the internet, the development of robust and trustworthy computer systems is a necessity" and urging that "[m]ore security-conscious network architects, software designers, and website developers are the solution").

tices. The *ISO/IEC 17799:2005*, entitled "Information Technology—Security Techniques—Code of Practice for Information Security Management," establishes guidelines and "general principles for initiating, implementing, maintaining, and improving information security management in an organization" by describing best practices in these areas.[294] *ISO/IEC 27001:2005* specifies the requirements for initiating, operating, and monitoring an information security management system in light of the organization's overall business risks.[295] *ISO/IEC 15408*, known as the *Common Criteria*, establishes an international standard for computer security specifications and evaluations.[296] Finally, *ISO 27799*, entitled "Health Informatics—Security Management in Health Using *ISO/IEC 17799*," will apply specifically to health information security, if approved.[297] We reviewed a current draft of *ISO 27799* and found it to be promising, and to provide more thorough and relevant guidance than currently exists in other documents.

ISO, IEC, and the Institute for Electrical and Electronics Engineering ("IEEE") have also developed a large number of standards and guidelines for various aspects of software engineering. Notable examples include *ISO/IEC 90003:2004*, entitled "Software Engineering—Guidelines for the Application of ISO 9001:2000 to Computer Software,"[298] which provides guidance for organizations concerning the acquisition, supply, development, operation, and maintenance of computer software and related support services, and *ISO/IEC 12207*, entitled "Information Technology—Software Life-Cycle Processes,"[299] which establishes a system for software life-cycle processes.

In addition, at least one national organization is already devoted to research and development concerning Internet security. CERT is a federally funded center of computer security expertise, operated out of Carnegie Mellon University's Software Engineering Institute.[300] It stud-

---

[294] ISO, ISO/IEC 17799:2005, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3= (last visited Feb. 23, 2007).

[295] ISO, ISO/IEC 27001:2005, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40&ICS3= (last visited Feb. 23, 2007).

[296] *See generally* COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION: USER GUIDE (1999), *available at* http://www.commoncriteriaportal.org/public/files/ccusersguide.pdf.

[297] ISO/DIS 27799, *supra* note 254.

[298] ISO, ISO/IEC 90003:2004, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35867&ICS1=35&ICS2=80&ICS3= (last visited Feb. 23, 2007).

[299] ISO, ISO/IEC 12207:1995, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21208&ICS1=35&ICS2=80&ICS3= (last visited Feb. 23, 2007).

[300] *See* Carnegie Mellon Univ., Software Eng'g Inst., CERT Coordination Center, http://www.cert.org (last visited Feb. 23, 2007).

ies Internet security vulnerabilities and long-term changes in networked systems and develops information and training to promote improved security.[301] Among its other features, CERT's website offers security alerts and solutions.[302] Certification bodies could require vendors to follow CERT's recommendations in order to attain certification, and covered entities not utilizing vendors could also rely on these for guidance.

The NIST, discussed above,[303] has produced not only important guidance concerning risk analysis,[304] but also a website entitled "National Vulnerability Database."[305] The website states that the database is "a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources."[306]

The list of standards and resources provided above is not meant to be exclusive, and, because of the ever-changing nature of technology and security threats, it would be impractical to attempt to develop a comprehensive list that would endure over time. Certification bodies should be expected to remain updated concerning guidelines and resources that are relevant to PHI security and should distribute pertinent information to their certified vendors. Similarly, under the "best current practices" standard discussed above, covered entities that do not take advantage of certified vendors would be expected to follow applicable industry standards and guidelines for HIPAA compliance purposes. As an additional aid, CMS should maintain on its website an updated, nonexclusive list of documents and Internet sources that it recommends to covered entities.

It should also be noted that in the comments concerning the proposed Security Rule, HHS acknowledged that it is required to adopt industry standards developed by standards-developing organizations that are accredited by the American National Standards Institute ("ANSI"),[307]

---

[301] *Id.*

[302] *Id.*

[303] *See supra* notes 154, 263 and accompanying text.

[304] *See supra* text accompanying notes 251–254.

[305] National Vulnerability Database, http://nvd.nist.gov (last visited Feb. 23, 2007). Although it is produced by NIST, the database is sponsored by the Department of Homeland Security's National Cyber Security Division. *Id.*

[306] *Id.* As of February 23, 2007, the database contained 22,653 vulnerabilities. *Id.*

[307] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8345 (Feb. 20, 2003). However, 42 U.S.C. § 1320d-1(c)(2)(B) (2000) provides that "[i]f no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt," the Secretary may create his own standard.

the U.S. representative of ISO and IEC.[308] In 2003, HHS concluded that the available security standards were not technology-neutral, were inconsistent with HIPAA, and were too narrow to be adopted in the final Rule.[309] The advent of *ISO 27799*, which will specifically address health information security,[310] should cause HHS to reevaluate its conclusion and may require revision of the Security Rule to include the new standard's adoption.

It is reasonable to expect that implementation of the proposed changes to the HIPAA Privacy Rule will influence vendors to provide relatively low-cost "turnkey" systems for processing and maintaining PHI that will be affordable even for small businesses.[311] We anticipate that all but the largest covered entities will lack the expertise and resources to achieve Security Rule compliance without the assistance of an intermediary, and thus, the development of a market for HIPAA compliance aids is essential.

A Google search for HIPAA security turnkey solutions reveals a number of organizations already purporting to provide such solutions for compliance with the HIPAA Security Rule.[312] Some offer comprehensive practice management solutions that combine scheduling, recordkeeping, intraoffice communication, and billing in a single application, thereby centralizing all HIPAA-related electronic data.[313] Other products offer tutorials, templates, documents, and aids aimed at enabling an entity to achieve HIPAA compliance.[314] Still other applications

---

[308] ANSI, About ANSI—A Historical Overview, http://www.ansi.org/about_ansi/introduction/history.aspx?menuid=1 (last visited Feb. 23, 2007).

[309] Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8345.

[310] *See supra* text accompanying note 297.

[311] Turnkey systems are "built, supplied, or installed complete and ready to operate." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1274 (10th ed. 1996).

[312] Google Search for HIPAA Security Turnkey Solutions, http://www.google.com (last visited Mar. 7, 2007).

[313] *See, e.g.*, AdvancedMD, http://www.advancedmd.com (last visited Feb. 23, 2007); LeonardoMD Online Medicine, http://www.leonardomd.com (last visited Feb. 23, 2007). There are two versions of the LeonardoMD product: standard and professional. LeonardoMD Online Medicine, *supra*. The standard package provides "entry-level practice management with registration, scheduling, and messaging," and its cost starts at $150 per month with a one-time $1250 setup charge. *Id.* The professional package is advertised as providing "comprehensive practice management with scheduling, charge capture, billing, and integrated chart documentation." *Id.* Its cost starts at $300 per month, with a $2500 setup charge. *Id.*

[314] *See, e.g.*, HipaaManager, http://www.hipaamanager.com/hm/online_hcat.cfm (last visited Feb. 23, 2007); NewGovernance HIPAA Privacy Accelerator (HPA)—Product Overview (v2.2), http://www.newgovernance.com/hpa.html (last visited Feb. 23, 2007). The standard version of HipaaManager costs $199, the professional version costs $699, and the institutional version is priced at $2999. HipaaManager, *supra*.

are designed for more complex organizations with more sophisticated technology. Symantec BindView[315] is a compliance management application that analyzes an organization's current security profile, suggests modifications based on best practices, and monitors and reports compliance-related data (for example, who is accessing files containing PHI).[316] SecureInfo RMS[317] claims to cut costs, create a standardized compliance and accreditation program, and provide packages for regular auditing.[318] It is likely that increasingly sophisticated and cost-effective tools will continue to be developed in response to marketplace demands for security technology.

D. *Bolstering Enforcement Through a Private Cause of Action*

The HIPAA Privacy Rule's lack of a private cause of action diminishes its deterrent and remedial powers.[319] We recommend that the privacy regulations adopt the approach of many of the other U.S. privacy laws and the E.U. Privacy Directive, and establish a private cause of action.[320]

The HIPAA Privacy Rule's administrative penalties[321] should be retained alongside the private right of litigation. This approach will allow governmental intervention even when no individuals suffer injury, such as in cases in which electronic security is inadequately maintained but no information is actually obtained by unauthorized third parties. It will also introduce the threat of private enforcement in cases that would not be prioritized by the government for political reasons or that the government does not have the resources to pursue, which may be

---

[315] Symantec, Regulation Solutions, HIPAA, http://www.bindview.com/solutions/regulations/hipaa.cfm (last visited Feb. 23, 2007).

[316] *Id.*

[317] SecureInfo RMS, http://www.secureinfo.com/solutions/certification-accreditation/ (last visited Mar. 7, 2007).

[318] *Id.*

[319] *See supra* notes 159–193 and accompanying text.

[320] *See supra* notes 159–193 and accompanying text. It is well-established that defendants can be subjected to both criminal penalties and punitive damages for the same wrong. *See* United States v. Bajakajian, 524 U.S. 321, 331 (1998) (holding that the Double Jeopardy Clause does not prohibit the institution of both a criminal prosecution and a later civil in rem forfeiture action); Tuttle v. Raymond, 494 A.2d 1353, 1357–58 (Me. 1985) (holding that double jeopardy is not implicated when a defendant is both criminally prosecuted and required to pay punitive damages for the same misconduct because the latter is imposed in a private civil suit rather than a criminal action).

[321] 42 U.S.C. §§ 1320d-5 to -6 (2000).

the vast majority of cases.[322] Without a private cause of action, covered entities may have incentive to conduct a cost-benefit analysis from which they conclude that because the cost of compliance is great and the risk of being penalized for a violation is very small, they should not aggressively invest in PHI security measures.[323]

The dual enforcement approach of a private cause of action and administrative penalties is adopted by several other U.S. privacy laws.[324] Borrowing from the private cause of action provisions found in other privacy legislation, we recommend that the HIPAA statute include the following language[325]:

> (a) Any person aggrieved by any act of a covered entity in violation of this section may bring a civil action in a United States District Court.[326]
>
> (b) The court may award—
>
> (1) actual damages, but not less than liquidated damages in the amount of $2500;
>
> (2) punitive damages upon proof of willful or reckless disregard of the law;
>
> (3) reasonable attorney's fees and other litigation costs reasonably incurred; and
>
> (4) such other preliminary and equitable relief as the court determines to be appropriate.[327]

---

[322] *See supra* notes 171–172 and accompanying text; *see also* Stein, *supra* note 178 (quoting an HHS administrator as acknowledging that the agency has "challenges with our resources investigating complaints").

[323] *See* Choi et al., *supra* note 2, at 62 (predicting that health care providers will need to expend billions of dollars to comply with the HIPAA Privacy Rule).

[324] *See* Privacy Act of 1974, 5 U.S.C. § 552a(g), (h)(i)(1) (2000) (establishing private cause of action and criminal penalties); Electronic Communications Privacy Act, 18 U.S.C. §§ 2520, 2522(c) (2000) (establishing private cause of action and civil penalties); Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2723–2724 (2000) (establishing criminal penalties and a civil cause of action).

[325] The private cause of action should be added to both the administrative regulations and the federal statute, given that the means of enforcement are authorized under the statute itself. *See* 42 U.S.C. §§ 1320d-5 to 1320d-6 (2000).

[326] *See* Privacy Act of 1974, 5 U.S.C. § 552a(g)(1)(D) (providing for a cause of action whenever an agency "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual"); Cable Communications Policy Act, 47 U.S.C. § 551(f)(1) (2000) (providing that "[a]ny person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States District Court").

[327] *See* Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2724 (providing identical language).

In the future, Congress might consider requiring aggrieved parties to exhaust administrative remedies before filing lawsuits in court.[328] Presumably, such a system would filter out many of the weakest cases because lawyers and potential litigants would be discouraged by negative administrative agency findings and would not burden the courts with frivolous cases. Effective administrative review, however, is dependent upon a strong network of agency offices that are adequately staffed to process a large volume of claims. HHS's anemic HIPAA enforcement record indicates that it does not currently have such resources.[329]

Some cases brought by private litigants may be complex and large, with far-reaching impacts. If vendors or certifying bodies are suspected of being responsible for Security Rule breaches, they could be joined as defendants[330] under theories of negligence or fraud,[331] or be brought in by covered entities as third party defendants.[332] In addition, cases involving Security Rule breaches that injure numerous individuals could generate class actions with hundreds, thousands, or even millions of plaintiffs.[333]

Conclusion

An abundance of evidence confirms that the confidentiality of our private health information faces grave threats from a large number of sources. The danger of privacy violations will only intensify in the future with increased computerization and centralization of health re-

---

[328] This mechanism has been embraced by several employment discrimination laws, which establish that potential plaintiffs first must file charges of discrimination with the Equal Employment Opportunity Commission and receive a determination and/or a right to sue before filing a lawsuit in court. *See* Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e-5(b), (f)(1) (2000) (describing the Equal Employment Opportunity Commission's (the "EEOC's") charge filing process); Americans with Disabilities Act, 42 U.S.C. § 12117(a) (2000) (adopting Title VII's enforcement provisions for the ADA); Age Discrimination in Employment Act of 1967, 29 U.S.C. § 626(d) (2000) (establishing that civil actions may not be commenced prior to the filing of a charge of discrimination with the EEOC).

[329] *See supra* notes 177–182 and accompanying text (criticizing HHS's enforcement of HIPAA and reporting that as of June of 2006, the agency imposed no civil penalties on covered entities).

[330] *See* Fed. R. Civ. P. 20 (discussing permissive joinder of parties).

[331] *See* 28 U.S.C. § 1367(a) (2000) (discussing supplemental jurisdiction, which allows tort claims to be joined to related federal statutory claims in some circumstances); Fed. R. Civ. P. 18 (discussing permissive joinder of claims).

[332] *See* 28 U.S.C. § 1367(a) (discussing supplemental jurisdiction in federal court cases asserting a federal statutory claim); Fed. R. Civ. P. 14 (discussing third party practice).

[333] *See* Fed. R. Civ. P. 23 (discussing class action requirements).

cords.[334] The U.S. government, which has aggressively promoted the use of electronic health records,[335] has responded to concerns about privacy by enacting HIPAA and its privacy regulations. The legislation and regulations are, however, significantly flawed from both legal and technical perspectives. Focusing on the HIPAA Security Rule, this Article presents recommendations to rectify some of its considerable weaknesses.

The new requirements outlined in this Article would need to be phased in gradually. Just as existing covered entities were given several years to prepare for compliance with the HIPAA Privacy Rule, new covered entities should be given the same courtesy. Moreover, time will pass before a sufficiently advanced health information security industry develops to make effective and affordable products readily available for covered entities. The HHS Secretary should determine a reasonable compliance deadline for the newly introduced provisions.

A public education campaign would have to be initiated to educate the public about its rights under the revised regulations and to educate newly covered entities about their obligations. Similar efforts were made when the original privacy regulations were enacted.[336]

The HIPAA Privacy Rule represents a significant regulatory effort on the part of the U.S. government and has generated emotional and often negative responses from the American public.[337] The recommen-

---

[334] Stein, *supra* note 178 (stating that "[p]rivacy advocates say large, centralized electronic databases will be especially vulnerable to invasions, making it even more crucial that existing safeguards be enforced").

[335] Mark A. Rothstein & Meghan Talbott, *Compelled Disclosure of Health Information: Protecting Against the Greatest Potential Threat to Privacy*, 295 JAMA 2882, 2882 (2006) (discussing the creation of the Nationwide Health Information Network pursuant to President Bush's call for the promotion of interconnected electronic health records); Terry & Francis, *supra* note 1, at 1 (noting that in April of 2004, President Bush announced a plan to ensure that Americans' health records are computerized within ten years); Office of the Nat'l Coordinator for Health Info. Tech., Goals of Strategic Framework, http://www.hhs.gov/healthit/goals.html (last visited Feb. 23, 2007) (discussing the goal of computerizing health records to promote "workflow efficiencies" and improved patient care).

[336] *See, e.g.*, *HIPAA Compliance Program Offered to Local Companies*, DAILY RECORD (Rochester), Dec. 26, 2003, at 1 (reporting that "[t]he Alliance for HIPAA Compliance, a diverse and well-integrated team of healthcare attorneys, consultants and administrators who are experts in HIPAA issues, offer a program to assist companies in becoming HIPAA compliant"); Jonna Lorenz, *Summit Explains New Health Care Rules*, TOPEKA CAPITAL-J., Jan. 15, 2002, at 7A (reporting that "[a]bout 300 people gathered at the Kansas Expocentre . . . to learn about the Health Insurance Portability and Accountability Act and what they should do to get their health care organizations into compliance with that legislation").

[337] Although the HIPAA statute was passed in 1996, the privacy regulations took years to develop and did not become effective until 2003. 45 C.F.R. § 164.534 (2006). When it first published its proposed Rule, HHS received 2350 public comments about it. Health

dations detailed in this Article should render the HIPAA Security Rule in particular and the HIPAA Privacy Rule in general far more meaningful. They should benefit both patients, whose privacy and autonomy are at stake, and organizations seeking guidance concerning compliance requirements. It is only with rethinking some of HIPAA's statutory and regulatory provisions that electronic PHI will truly constitute protected health information.

Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003). The Rule's enforcement provisions were not finalized until 2006. HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8390, 8390 (Feb. 16, 2006); *see also* SOLOVE *supra* note 13, at 70 (discussing the controversial nature of the HIPAA regulations).