The Journal of Legal Medicine, 28:487–501

0194-7648/07 $12.00 + .00
DOI: 10.1080/01947640701732148

HEALTH PRIVACY IN THE ELECTRONIC AGE

Mark A. Rothstein, J.D.*

INTRODUCTION

Health care expenditure in the United States exceeds $2 trillion a year,[1] and on a per capita basis far exceeds the expenditure of any other country.[2] Much of this money is not well spent, as many studies have documented the inefficiency and waste in the public and private health care systems.[3] Furthermore, despite the high cost of American health care, key measures of the nation's health, such as infant mortality[4] and life expectancy,[5] lag well behind other developed countries.

One assumed method of increasing efficiency and improving outcomes is to expand and improve the use of health information technology, including the universal adoption of electronic health records (EHRs).[6] Supporters of EHRs assert that they avoid duplication of history taking and tests, promote coordination of care, reduce medical errors, ensure access to records from

---

* Herbert F. Boehl Chair of Law and Medicine and Director, Institute for Bioethics, Health Policy and Law, University of Louisville School of Medicine. This article is based on a speech given March 21, 2007 at Southern Illinois University School of Law as the John and Marsha Ryan Bioethicist-in-Residence. The author is Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, which is referenced in the article. The views expressed herein are solely those of the author.

[1] Christine Borger et al., *Health Spending Projections Through 2015: Changes on the Horizon*, 25 HEALTH AFFAIRS WEB EXCLUSIVE 2, w61 (Mar./Apr. 2006), *available at* http://content.healthaffairs.org/cgi/reprint/25/2/w61 (last accessed June 1, 2007) (estimating 2006 expenditures at $2.16 trillion).

[2] UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTH, UNITED STATES, 2006 WITH CHARTBOOK ON TRENDS IN THE HEALTH OF AMERICANS 373 (National Center for Health Statistics 2006).

[3] *See generally* DAVID M. CUTLER, YOUR MONEY OR YOUR LIFE: STRONG MEDICINE FOR AMERICA'S HEALTH CARE SYSTEM (2004); MAGGIE MAHAR, MONEY-DRIVEN MEDICINE: THE REAL REASON HEALTH CARE COSTS SO MUCH (2006).

[4] DEPARTMENT OF HEALTH AND HUMAN SERVICES, *supra* note 2, at 173 (ranking the United States twenty-eighth in infant mortality).

[5] *Id.* at 174 (ranking the United States twenty-sixth in life expectancy).

[6] *See* NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, INFORMATION FOR HEALTH: A STRATEGY FOR BUILDING THE NATIONAL HEALTH INFORMATION INFRASTRUCTURE (Nov. 2001), *available at* http://www.ncvhs.hhs.gov/nhilayo.pdf (last accessed June 2, 2007).

remote locations and in emergencies, permit better disease management, and facilitate electronic decision support.[7]

In 2004, President George W. Bush issued an executive order calling for the United States to develop a nationwide network of interconnected EHRs by 2014.[8] The United States Department of Health and Human Services (HHS) was charged with taking the lead in developing the framework for the Nationwide Health Information Network (NHIN), a system of interoperable, longitudinal, comprehensive EHRs.[9] Although the federal government is taking the lead in developing standardized formats and infrastructure, the private sector is actively developing health information technology (HIT), computer software and systems, and business relationships for the collection, storage, and use of EHRs.

After three years of organizing and developing technology, plans for the NHIN are proceeding apace, private vendors are investing large sums to position themselves as major economic forces in the anticipated HIT boom, and most large health care entities are already using or converting to EHRs.[10] Notwithstanding this activity, there has been very little action in policy development involving the numerous, significant privacy issues raised by a shift from a largely disconnected, paper-based health record system to one that is integrated and electronic.[11]

This article reviews the key privacy issues that must be resolved before widespread adoption of EHRs and the interoperable networks of the NHIN. It contains specific recommendations for each of the major privacy issues and concludes with a plea for expeditious action before health privacy is irretrievably lost in the electronic age.

I. BACKGROUND

The terms privacy, confidentiality, and security are often used interchangeably, thereby leading to confusion and imprecision. For the purposes of this article, the health-related definitions of these three terms are taken from the National Committee on Vital and Health Statistics (NCVHS)[12] report, *Privacy*

---

[7] *See* MARKLE FOUNDATION, CONNECTING AMERICANS TO THEIR HEALTH CARE: A COMMON FRAMEWORK FOR NETWORKED PERSONAL HEALTH INFORMATION (Dec. 2006), *available at* http:/www.connectingforhealth.org/commonframework/docs/p9_networkedphrs.pdf (last accessed June 2, 2007).

[8] Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator, Exec. Order No. 13335, 69 Fed. Reg. 24,059 (Apr. 30, 2004).

[9] *Id.*

[10] *See* MARKLE FOUNDATION, *supra* note 7, at 14-16.

[11] *See generally* UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, HEALTH INFORMATION TECHNOLOGY: EARLY EFFORTS INITIATED BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY, GAO-07-238 (Jan. 2007).

[12] The National Committee on Vital and Health Statistics is the statutory public advisory body to the Secretary of Health and Human Services on health information policy. *See* www.ncvhs.hhs.gov.

and Confidentiality in the Nationwide Health Information Network.[13] Privacy, in the context of health information, refers to the ability of an individual to prevent certain disclosures of personal health information to any other person or entity.[14] Confidentiality means the condition under which personal health information obtained or disclosed within a confidential relationship will not be redisclosed without the permission of the individual.[15] Security is defined as the personal and electronic measures that grant access to personal health information to persons or entities authorized to receive it and deny access to others.[16]

Numerous public opinion surveys have indicated the American public is greatly concerned about the possible loss of health "privacy" with the widespread adoption of EHRs. In reality, many of the public's concerns are more properly categorized as security issues. For example, according to a December of 2006 survey by the Markle Foundation, 80% of Americans responded they were very concerned about identity theft or fraud, and 77% said they were concerned about the possibility of their health information getting into the hands of marketers.[17] These are security issues. Snoops, hackers, and stolen or misplaced computer files are also security issues that are beyond the scope of this article.[18]

In today's mostly paper-based health records system, privacy is protected largely by fragmentation, inefficiency, illegibility, and general chaos. It would be virtually impossible for any adult to collect all of his or her health information maintained by numerous health care providers in different locations over years or decades. If a patient is unable to locate all of his or her health records, then third parties are also unable to do so. There is no question that fragmentation promotes health privacy, but it does so at a very high cost in terms of undermining coordination of care, efficiency, and health care quality.

As EHRs and the NHIN decrease fragmentation, what, if any, safeguards will be put into place to ensure privacy? At the present time, it is difficult to answer this question because the precise contours of the NHIN have yet to be

---

[13] NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, PRIVACY AND CONFIDENTIALITY IN THE NATIONWIDE HEALTH INFORMATION NETWORK (June 2006), *available at* www.ncvhs.hhs.gov/060622lt.htm (last accessed June 2, 2007).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] MARKLE FOUNDATION, CONNECTING FOR HEALTH, SURVEY FINDS AMERICANS WANT ELECTRONIC PERSONAL HEALTH INFORMATION TO IMPROVE OWN HEALTH 1 (Nov. 2006) *available at* http://www.markle.org/downloadable_assets/research_doc_120706.pdf (last accessed June 2, 2007).

[18] Conceptually, security issues are much easier to resolve than privacy and confidentiality issues. There is unanimity in the view that personal health information should be accessible only to people with authorization. By contrast, rules for privacy and confidentiality are much more contentious because they involve a difficult balancing of individual autonomy and dignitary interests with health care quality, public health, efficiency, and other valid interests.

determined. It is not clear what HIT model will be chosen for the component works of the NHIN, what governance structure will be established, how the identity of patients will be verified, how many paper records will be scanned or abstracted into electronic form, and what financing or business model will pay for the start-up and continuation costs.

Notwithstanding these and other unknown elements of the NHIN, it is essential that foundational privacy and confidentiality issues are determined in advance of the implementation of the NHIN. As described below, the essential privacy concerns are germane to any EHR network configuration, and the protections must be designed into the architecture of the system. It may be impossible or prohibitively expensive to add privacy-enhancing features once the NHIN has been established, and health record privacy must be in place at the start.

II. KEY PRIVACY ISSUES

A. Consent to Participate in the NHIN

Physicians have professional obligations in creating, and discretion in the manner of recording and maintaining, the individual health records of their patients. Thus, patient consent should not be required for a physician to change from paper records to EHRs.[19] The same cannot be said of the decision to include patient EHRs in a regional health information organization (RHIO), health information exchange (HIE), medical record bank (MRB), or other network. Any compilation of health records goes beyond the consent of the individual for treatment by a single provider and the expectation that personal health information will be recorded in the patient's chart by the physician. Moreover, the centralization of individual health records facilitates the aggregation and disclosure of health information for health care and other purposes.[20]

If individuals have a choice whether to participate in the NHIN, should it be via "opt in," "opt out," or some other method? An opt-in approach is consistent with the traditional model of patient permission in medical practice. Patients have to provide affirmative consent to undergo treatment,[21] participate

---

[19] *See* NATIONAL COMMITTEE, *supra* note 13.

[20] Under HIPAA Privacy Rules, individual consent or authorization is not required for disclosures for treatment, payment, or health care operations (TPO). 45 C.F.R. § 164.506 (2006). Although it could be argued the purpose of the network, ultimately, is to enhance TPO, the immediate purpose of the disclosure is not for TPO. Even if it were, an argument could be made that this provision of the Privacy Rule is insufficiently protective of patient privacy.

[21] *See generally* Baruch A. Brody, *Informed Consent and Refusal, in* MEDICAL ETHICS: ANALYSIS OF THE ISSUES RAISED BY THE CODES, OPINIONS, AND STATEMENTS 421 (Baruch A. Brody et al. eds., 2001).

in research,[22] or authorize the disclosure of their information to third parties.[23] Those who favor an opt-out approach argue that an opt-in approach would result in fewer participants in the NHIN and be more burdensome on health care providers.[24] On reflection, however, as discussed below, it may not matter which approach is used.[25]

Our experience under the HIPAA Privacy Rule is instructive. When the initial final Privacy Rule was promulgated by the Clinton Administration in 2000, it required patient consent for treatment, payment, and health care operations (TPO).[26] When the Privacy Rule was amended by the Bush Administration in 2002, consent was no longer required for TPO.[27] Covered entities were merely required to provide a notice of privacy practices (NPP),[28] and covered entities with a direct treatment relationship were required to make a good faith effort to obtain the patient's written acknowledgment of receipt of the NPP.[29] In practice, few patients read the NPP before signing the acknowledgment, and it is common for the clerical staff of health care providers to ask new patients to sign an acknowledgment without even providing the NPP.

As long as a patient's signing of a written privacy document remains a *pro forma* exercise, it really does not matter what the instrument is called. To be a meaningful and knowing expression of patient preference, there must be a conscientious program of public education, health care staff training, and the time to discuss the implications of the document. A hospital admissions desk or a physician's sign-in window are not the best places for patients to contemplate the implications of health privacy policy. The lack of attention to these matters under the HIPAA Privacy Rule will, no doubt, cloud any efforts to make patient election of EHR and NHIN disclosures an exercise in knowing and informed decision making.[30]

---

[22] *See, e.g.*, Baruch A. Brody, *Research Ethics*, *in* MEDICAL ETHICS, *supra* note 21, at 791.

[23] 45 C.F.R. § 164.508 (2006).

[24] If substantial numbers of people do not want to participate in the NHIN, then the answer is to make the benefits of participation outweigh the risks, rather than coercing participation or enrolling individuals without their knowledge or consent.

[25] A related issue is whether patients will be able to elect to opt into the NHIN on a one-time basis. For example, a patient may decline to participate in the NHIN, but be perfectly willing to allow the transmittal of his or her EHR to another physician for treatment purposes. In such an event, the physician probably would obtain one-time consent for transmittal. It remains to be seen whether this "single token" model of the NHIN will become popular with patients who have concerns about the privacy, confidentiality, and security of NHIN entities, but who want to take advantage of the benefits of electronic exchange of health information.

[26] Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462 & 82,810 (Dec. 28, 2000) (codified at 45 C.F.R. Parts 160 & 164); 45 C.F.R. § 164.506 (2000).

[27] Standards for Privacy of Individually Identifiable Health Information, as amended, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. Parts 160 & 164); 45 C.F.R. § 164.506 (2002).

[28] 45 C.F.R. § 164.520 (2006).

[29] *Id.* § 164.520(c)(2)(ii).

[30] *See* National Committee on Vital and Health Statistics, Letter to Secretary Tommy G. Thompson (Sept. 27, 2002), *available at* http://www.ncvhs.hhs.gov/020927lt.htm (last accessed June 3, 2007).

The real problem with the Privacy Rule is not the consent-versus-notice approach at the outset, but the substantive provisions that apply under the rule. Patients have no opportunity to limit disclosures in the broadly defined categories of TPO.[31] In addition, the Privacy Rule permits the disclosure of protected health information (PHI) without patient permission under numerous exceptions, including disclosures to a covered entity's "business associates" and the associates of those associates, disclosures to law enforcement officials without a showing of probable cause, and disclosures for "health education" and "disease management" purposes that often blur into marketing.[32] If the substantive provisions of the NHIN are not more stringent than those in effect under HIPAA, many patients might exercise a right under the NHIN that they currently lack under HIPAA—to opt out of the system.

B. Patients' Control of the Contents of Their Health Records

The development of longitudinal, comprehensive EHRs will greatly increase the volume and scope of health information readily accessible in individual health records. Some of the health information will be highly sensitive and of little or no clinical utility. Potentially embarrassing information, currently lost to fragmentation and neglect, may become accessible to a wide range of viewers. Should patients have the right to delete, block, or otherwise exclude this information from their EHR and the NHIN? Two examples of the types of health information at issue may help to make these issues more vivid and concrete.

1. A 25-year-old woman presented to the emergency department with bruises and minor lacerations as a result of domestic abuse by her boyfriend. She was treated and released. There were no internal injuries and no loss of consciousness or other medical signs and symptoms with potentially long-term consequences. She promptly ended her relationship with the abusive boyfriend. Now, 20 years later, she is happily married to another man, with two healthy children. Does the report of abuse at the hands of her old boyfriend need to remain in her record indefinitely?

2. A 25-year-old male graduate student celebrated the end of exams with an evening of excessive drinking and carousing, culminating with a liaison with a commercial sex worker. The following week, concerned about the health implications of this adventure, he asked his personal physician to run a comprehensive battery of tests for all sexually transmitted diseases (STDs). All of the tests were negative,

---

[31] 45 C.F.R. § 164.506 (2006).

[32] *Id.* § 164.501 (definition of "marketing" excludes communications about products used in case management).

> and the nocturnal indiscretion was not repeated. Does the record of STD testing, and the reason for it, need to remain in his record indefinitely?

The American Medical Association (AMA) Code of Ethics specifically addresses the issue of retention of medical records. "Physicians have an obligation to retain patient records which may reasonably be of value to a patient . . . . Medical considerations are the primary basis for deciding how long to retain medical records."[33] This provision declares the purpose of a medical record is to aid the treatment of the patient, and it recognizes that all records need not be retained indefinitely. The same section also provides: "In deciding whether to keep certain parts of the record, an appropriate criterion is whether a physician would want the information if he or she were seeing the patient for the first time."[34]

In the two hypothetical examples above, it is clear the old health records do not provide information of value to a physician seeing a new patient. Furthermore, the information is unlikely to be volunteered or disclosed by the patient to a new physician. It should also be noted that the decision regarding the disclosing or maintaining of sensitive information has important public health implications. The nation's health record system should not discourage individuals who are victims of domestic violence, those concerned about possible STDs, or other individuals with substance abuse, mental illness, or other potentially stigmatizing conditions from seeking prompt medical care.

If patients are given some control over the contents of their medical records, such as by permitting them to redact certain information, the question arises as to how much control they should be given. Those who assert that patients should have unlimited control argue it is a matter of autonomy and patients should have the right to establish the conditions under which they are being treated. They further point out that many current health records contain numerous errors and omissions, and health care quality is unlikely to be compromised by greater patient control. On the other hand, patients may not realize the medical significance of information they would choose to redact or may want to alter the contents of their health records for nonmedical purposes (for example, for personal, economic, or legal reasons). In addition, if clinicians cannot trust the accuracy and completeness of health records edited by patients, they will feel compelled to repeat histories and physicals, diagnostic tests, and other procedures—undermining one of the express purposes of interoperable and comprehensive EHRs. In effect, EHRs will become personal health records (PHRs), the patient-compiled records of

---

[33] AMERICAN MEDICAL ASSOCIATION CODE OF MEDICAL ETHICS § 7.05—Retention of Medical Records (2006).
[34] *Id.*

medications, tests, and symptoms being developed to help patients monitor their own health and health care.

Deciding on the degree of patient control and the method chosen to enable patient control is undoubtedly the most complicated and contentious issue facing EHR and NHIN designers.[35] It is an issue facing all of the countries establishing EHR networks. Approaches that have already been adopted or are being considered include masking, sealing, blocking, and locking certain information fields.[36] Even after committing to use such measures and deciding to which information they apply, other issues will still remain. For example, policymakers still need to consider when, if ever, an override function is permissible (for instance, in emergencies) and whether electronic decision support can still review blocked information to alert clinicians about, for example, the risk of possible adverse medication interactions.

C. Special Types of Information

A related issue is whether special protections should be developed for certain classes of sensitive information, such as mental health, substance abuse, STDs, and genetic test results. According to one study, respondents ranked the top areas in which they believed special health privacy protections are needed as follows: abortion history (68.6%); mental health history (60.1%); HIV/AIDS (54.0%); genetic test results (46.5%); drug and alcohol history (44.4%); and STDs (44.0%).[37]

The only separate treatment of a subclass of health information under HIPAA involves psychotherapy notes. Under the HIPAA Privacy Rule, a special provision excludes psychotherapy notes from the definition of PHI. Psychotherapy notes are defined as: "[N]otes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the individual's medical record."[38]

The quoted provision seeks to exclude sensitive narrative information about an individual's most intimate thoughts, fears, and emotions from disclosure outside of the therapeutic setting. The exclusion does not apply to mental health diagnoses, progress reports, prescriptions, or other similar matters. The limited HIPAA exemption may be criticized as being underinclusive because

---

[35] *See* NATIONAL COMMITTEE, *supra* note 13.

[36] *See* JOY PRITTS & KATHLEEN CONNOR, THE IMPLEMENTATION OF E-CONSENT MECHANISMS IN THREE COUNTRIES: CANADA, ENGLAND, AND THE NETHERLANDS (THE ABILITY TO MASK OR LIMIT ACCESS TO DATA), A REPORT TO THE SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION 5-6 (2007), *available at* http://ihcrp.georgetown.edu/pdfs/prittse-consent.pdf (last accessed June 3, 2007).

[37] Laura Plantinga et al., *Disclosure, Confidentiality, and Families: Experiences and Attitudes of Those with Genetic Versus Nongenetic Medical Conditions*, 119 AM. J. MED. GENETICS PART C 51, 55 (2003).

[38] 45 C.F.R. § 164.501 (2006).

it only applies to notes recorded by a mental health professional and kept separate from other medical records. In fact, a substantial amount of mental health counseling and therapy is either provided by primary care physicians and recorded in the regular health records of their patients or provided by a mental health professional and not kept in a separate file.[39]

Another source of special protection for health information involves substance abuse treatment information. Under the Public Health Service Act and its implementing regulations, strict confidentiality rules are applied to patient records maintained in connection with any federally assisted substance abuse treatment program.[40] Without such additional disclosure safeguards, many individuals would be reluctant to undergo drug treatment for fear their records would be available to law enforcement personnel and result in their being prosecuted for drug-related offenses.

Federal legislation to prohibit discrimination based on genetic information has been pending in Congress since the mid-1990s, and there is an increased likelihood of passage in the current Congress.[41] Numerous states have enacted comparable laws in an attempt to prohibit genetic discrimination in health insurance, employment, and other matters.[42] The substantive shortcomings of these laws and proposals are beyond the scope of this article.[43]

Of relevance to this discussion, though, is that segregating sensitive health information could increase the stigma of mental illness and other traditionally disfavored conditions. Thus, even though certain types of health information undoubtedly may be more sensitive, concerns about disclosure must be balanced against the considerable risk that maintaining separate records will increase stigma and discrimination and thereby become a self-fulfilling prophesy.[44]

---

[39] Other sensitive health information may be recorded by social workers, marriage counselors, or other professionals who are not covered entities under HIPAA because, for example, they do not submit claims for their services in electronic format.

[40] Public Health Service Act, 42 U.S.C. § 290dd-2 (2006); 42 C.F.R. Pt. 2 (2006).

[41] Genetic Information and Nondiscrimination Act of 2007, H.R. 493, 110th, Cong. 1st Sess. (2007).

[42] The state laws are compiled by the National Conference of State Legislatures and are available at www.ncsl.org/programs/health/genetics (last accessed June 3, 2007).

[43] *But see, e.g.*, Mark A. Rothstein, *Genetic Privacy and Confidentiality: Why They Are So Hard to Protect*, 26 J.L. MED. & ETHICS 198 (1998).

[44] *See, e.g.*, Thomas H. Murray, *Genetic Exceptionalism and "Future Diaries": Is Genetic Information Different from Other Medical Information?*, *in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA (Mark A. Rothstein, ed. 1997); Deborah Hellman, *What Makes Genetic Discrimination Exceptional?*, 29 AM. J.L. & MED. 77 (2003); Mark A. Rothstein, *Genetic Exceptionalism and Legislative Pragmatism*, 35 HASTINGS CENTER REP. NO. 4, at 27 (2005); Sonia M. Suter, *The Allure and Peril of Genetic Exceptionalism*, 79 WASH. U.L.Q. 669 (2001); Susan M. Wolf, *Beyond "Genetic Discrimination": Toward the Broader Harm of Geneticism*, 23 J.L. MED. & ETHICS 23 (1995).

D. Role-Based and Context-Based Restrictions

Health care, especially in hospital settings, is provided by a large number of individuals with different training, expertise, and responsibilities. Although many health care providers may need access to an individual's health record to perform treatment-related functions, not all individuals need the same level of access. For example, billing clerks, dieticians, phlebotomists, and surgeons need quite different information to perform their respective jobs properly. As a general principle, health care providers and support staff should have access only to the minimum necessary health information about individual patients. EHRs facilitate such role-based access through various means of system entry, encryption, pass codes, audit trails, and electronic field segregation. Numerous large institutions have successfully used these systems for many years. As the NHIN is developed, the capacity of role-based access restrictions needs to be a functional requirement and regulatory standard.

Although health records are designed to be used in health care settings, health information may be lawfully obtained and used by a wide range of third parties. In reality, any entity with an interest in an individual's current or future health status might have an interest in having access to the individual's health records. With few exceptions, such entities may lawfully require that the individual execute an authorization for the disclosure of all his or her health records.[45] In a very recent study, my colleague Meghan Talbott and I estimate that each year there are 25 million compelled authorizations in the United States.[46] The main contexts of the authorizations are employment entrance examinations, individual health insurance applications, individual life insurance applications, individual long-term care insurance applications, individual and group disability insurance claims, automobile insurance personal injury claims, Social Security Disability Insurance applications, workers' compensation claims, veterans' disability claims, and personal injury lawsuits.[47]

For the vast majority of these authorizations, there are no limits placed on the scope of the information disclosed. For example, under section 102(d)(3) of the Americans with Disabilities Act,[48] after a conditional offer of employment, the employer may require a preplacement medical examination and as part of the examination the individual may be required to disclose all of his or her health records.[49] Even if a party requesting health information submits a more focused request for information, with paper-based health records it

---

[45] Mark A. Rothstein & Meghan K. Talbott, *Compelled Disclosure of Health Information: Protecting Against the Greatest Potential Threat to Privacy*, 295 J.A.M.A. 2882 (2006).

[46] Mark A. Rothstein & Meghan K. Talbott, *Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications*, 7 AM. J. BIOETHICS 38 (2007).

[47] *Id.*

[48] 42 U.S.C. § 12112(d)(3) (2000).

[49] *See* EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, ENFORCEMENT GUIDANCE ON PREEMPLOYMENT INQUIRIES UNDER THE AMERICANS WITH DISABILITIES ACT (1994).

is virtually impossible and cost-prohibitive to glean an entire file and submit only the information deemed relevant to the request. Consequently, it is common for custodians to send a copy of the entire record, which might contain not only irrelevant material, but highly sensitive material as well.

The development of the NHIN increases the amount of information that can be easily disclosed to third-party requestors. Significantly, however, EHRs create the opportunity to tailor the disclosure to relevant information. Contextual access criteria are electronic algorithms permitting the isolation of health information in response to a particular request. For example, contextual access criteria could be developed to respond to a request from a life insurance company by identifying and aggregating only the information relevant to mortality risk.

It will be a time- and labor-intensive undertaking to develop the substantive criteria for each of the more limited disclosures, but the result would be a substantial increase in privacy. The use of contextual access criteria is consistent with the AMA Code of Ethics provision on the use of electronic medical records, which reads: "Release of confidential information from the data base should be confined to the specific purpose for which the information is requested and limited to the specific time frame requested . . . ."[50] Unfortunately, despite a recommendation from the NCVHS to undertake research and development on contextual access criteria,[51] there have been no efforts made in either the public or private sectors.

E. Expanded Coverage

When the HIPAA Privacy Rule took effect in April of 2003, it marked the first time federal privacy standards were applied to a large segment of the health care enterprise. The complexity of the rule and the lack of public outreach and professional education by HHS[52] contributed to a general lack of understanding of both the substance and scope of the Privacy Rule. Although new demands were placed on covered entities, the Privacy Rule is not—and never was intended to be—a comprehensive health privacy rule with universal applicability.

During the early 1990s, rising health care costs caused some health insurers and health plans to engage in individual medical underwriting in the group market. Consequently, individuals with chronic health conditions and employer-based coverage faced "job lock"—being forced to continue working at a particular employer because of an inability to obtain comparable health coverage at a new employer. Such a restriction on labor mobility was not only

---

[50] AMERICAN MEDICAL ASSOCIATION, CODE OF MEDICAL ETHICS § 5.07(4) (2006).
[51] *See* NATIONAL COMMITTEE, *supra* note 13, at Recommendations R-9 to R-11.
[52] *See* 2002 NCVHS Letter, *supra* note 30.

personally damaging to affected individuals, but constituted an inefficient and wasteful utilization of human resources.

The proposed solution was the bipartisan Kassebaum-Kennedy bill (later enacted as HIPAA), which proposed granting employees with group health coverage the ability to move to another employer offering group health coverage without the individual's new health plan excluding coverage for any preexisting conditions or imposing a waiting period before the health coverage went into effect. The bill also proposed to permit individuals to convert from group health plans to an individual health insurance policy if they became self-employed or went to work for an employer that did not offer health benefits.

The health insurance industry recognized the legislation would result in additional costs to the industry by prohibiting the rejection of new high-risk employees and dependents. Its response was to renew efforts to obtain legislation mandating uniform standards for the electronic submission of health claims.[53] In theory, any losses caused by portability would be more than offset by savings from using industry-wide, standardized electronic billing procedures. Thus, the "Administrative Simplification" title of the bill was proposed as an amendment.[54]

At the same time, it also became clear to Congress that the public would not tolerate electronic processing of health information and electronic claims submission without legal protection for the privacy and security of personal health information. To address these concerns, Congress included a provision in the bill committing to the enactment of privacy and security rules within three years from the enactment of the original legislation and, if it failed to enact such legislation by that date, the Secretary of the Department of Health and Human Services (HHS) was directed to promulgate regulations with the same effect.[55] When, to nobody's surprise, Congress failed to act within the allotted time, the task of drafting privacy and security regulations fell to HHS.

Because the privacy and security provisions arose from and were intended to safeguard the claims submission process, there were only three classes of "covered entities" under HIPAA and its Privacy Rule: health care providers, health clearinghouses, and health plans.[56] Furthermore, to be a covered health care provider, the entity must submit claims for payment in standard electronic formats.[57]

---

[53] *See* Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,469 (Dec. 28, 2000).
[54] *Id.*
[55] 42 U.S.C. § 1320d-2 (2000).
[56] *Id.* § 1320d-1(a).
[57] *Id.* § 1320d-1(a)(3).

Virtually every large hospital and health care institution, every physician submitting claims to Medicare and Medicaid, every large employer-sponsored health plan, and every commercial health insurance company is a covered entity. Thus, it would be easy to reach the erroneous conclusion that all health care providers, plans, and entities are covered by the Privacy Rule. An unknown number, but undoubtedly tens or even hundreds of thousands, of health care providers and providers of health-related services are not covered entities under HIPAA. These include all health care providers who perform their services on a cash-only basis, such as services not normally covered by health insurance or health plans, Some examples include "concierge" physicians, cosmetic surgeons, massage therapists, acupuncturists, nutritional counselors, and some urgent care facilities. Other categories of uncovered health care providers include athletic trainers, employer health clinics, school health clinics, health and fitness clubs, home testing clinical laboratories, and mental health and substance abuse counselors working for social service agencies.

In addition to health care providers, numerous other entities obtain individual health records for legitimate purposes. These include employers, life insurers, disability insurers, long-term care insurers, financial institutions, and educational institutions. In some instances, there are separate privacy provisions under other federal laws that may overlap or conflict with the HIPAA Privacy Rule. For example, school records, including health information in school records, are subject to the Family and Educational Rights and Privacy Act.[58]

As the health information system becomes an integrated network of longitudinal, comprehensive health records, the HIPAA paradigm of regulating only entities in the payment chain is untenable. Comprehensive privacy legislation is essential to regulate the access, use, storage, and disclosure of health information in any form and by any entity. Without such protections, the essential trust underlying the patient-physician relationship will be seriously eroded and patients may limit disclosures to their health care providers. A foreseeable result would be a decrease in the quality of individual health care and even threats to public health.

There are two ways to enact comprehensive legislation. First, Congress could enact a completely new health privacy statute. Alternatively, Congress could amend HIPAA to extend its coverage. In light of the inability of Congress to enact health privacy legislation in the late 1990s, amending HIPAA may be the more practical alternative.[59]

---

[58] 20 U.S.C. § 1232g (2000); 34 C.F.R. Pt. 99 (2006).

[59] There is precedent for Congress to add new covered entities to HIPAA. When it enacted the Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Pub. L. No. 108-173 (2003), Congress added prescription drug card sponsors to the list of HIPAA covered entities. 42 U.S.C. § 1395w-141(h)(6)(A) (West 2004).

F. Enforcement

Even if the NHIN is perfectly designed to include privacy-enhancing features, and even if comprehensive health information privacy legislation is enacted, it is still essential that the public have confidence in the rules governing the system and the people overseeing it. In particular, the public must be convinced the federal government will vigorously enforce the privacy law as a deterrent to unlawful activity.

As of March 2007, the Office for Civil Rights (OCR), the DHHS office in charge of enforcing the HIPAA Privacy Rule, had received approximately 26,000 complaints.[60] Although OCR proudly claims a high percentage of closed cases and relief obtained through conciliation, it has not brought a single action to enforce civil monetary penalties against unlawful conduct. A handful of criminal cases have been brought under HIPAA by the Department of Justice,[61] but none of these were based on the more than 350 referrals from OCR. The lack of enforcement by OCR sends the wrong signal to individuals, covered entities, and potential lawbreakers that violations of health privacy law are not taken seriously. For the NHIN to be successful, there needs to be a complete change in enforcement strategy.[62]

Although the specifics are beyond the scope of this article, it is also important to note that a variety of important issues will need to be addressed related to regulation and enforcement. For example, the contours of fair information practices in the system need to be developed and implemented. These include the right of individuals to access their own health records, the right to learn who has accessed their records, the right to amend their record, the right to notice of a security breach, and the right to compensation for harms caused by the wrongful release of health information.[63]

CONCLUSION

In 2004, when President Bush announced the goal of establishing a national, interoperable network of EHRs by 2014, it appeared to some people there was ample time to develop plans for system design, regulatory oversight, and privacy protection. Nearly a third of the time for reaching the goal has elapsed. In some ways, it appears that the effort is on schedule, or even ahead of schedule. This is particularly the case with private sector initiatives to

---

[60] United States Department of Health and Human Services, Office for Civil Rights, HIPAA Privacy Rule Compliance Summary, *available at* http://www.hhs.gov/ocr/privacy/enforcement/ (follow "Privacy Rule Enforcement Highlights" hyperlink) (last accessed June 7, 2007) (as of Mar. 31, 2007, there were 26, 408 complaints).

[61] *Id.* (384 referrals to the Department of Justice).

[62] *See* NATIONAL COMMITTEE, *supra* note 13, Recommendation R-17.

[63] *Id.* Recommendation R-15.

develop PHRs and state and local efforts to establish RHIOs and HIEs. With regard to privacy, however, there has been little, if any, meaningful progress.

In 2007, a Government Accountability Office report on health information technology concluded: "HHS is in the early stages of identifying solutions for protecting personal health information and has not yet defined an overall approach for integrating its various privacy-related initiatives and for addressing key privacy principles."[64] Not only have HHS privacy efforts fallen behind its technology-development efforts, but they are being overwhelmed by HIT system creation and implementation in the private sector. Unless effective privacy policies are promptly established, there will be a tremendous increase in individual health information carried by new electronic networks with little or no regulation of its many potential uses.

[64] GOVERNMENT ACCOUNTABILITY OFFICE, *supra* note 11, at 14.