#2006-03
February 2006

The Health Insurance Portability and Accountability Act Privacy Rule and Patient Access to Medical Records

by
Beth Tossell, Health Privacy Project
Emily Stewart, Health Privacy Project
Janlori Goldman, Health Privacy Project

The AARP Public Policy Institute, formed in 1985, is part of the Policy and Strategy Group at AARP. One of the missions of the Institute is to foster research and analysis on public policy issues of importance to mid-life and older Americans. This publication represents part of that effort.

The views expressed herein are for information, debate, and discussion, and do not necessarily represent official policies of AARP.

AARP, 601 E Street, NW., Washington, DC 20049
http://www.aarp.org/ppi

Foreword

Consumers must be engaged in their health care and have access to a full range of information, particularly their personal health information, if they are to make informed decisions. Patients indicate an interest in reading their medical records for a variety of reasons, including a general interest in seeing information about health issues, concerns about patient safety, and also because of an erosion in the trust relationship between patients and physicians.[1] Nevertheless, in spite of the fact that the Health Insurance Portability and Accountability Act (HIPAA) and its applicable regulations assure patients a federal right to access, inspect, and request amendments to their medical records, many consumers are unaware of these vital protections and many never request access to their medical records.

AARP's blueprint for the future, *Reimagining America*, recognizes the imperative of improving health care quality as a key challenge. Accordingly, the AARP Public Policy Institute is engaged in research and analyses to identify how to address this daunting challenge through public policies. It is clear, that consumers are increasingly being asked to bear greater responsibility for their health care. Studies indicate improved health outcomes when patients are activated and engaged in self-management and other proactive, "consumeristic" behaviors; such behaviors require useful and meaningful information. Since a primary source of information about one's health is contained in the clinical medical record, it is critical for consumers to know and understand their rights of access to this source of personal data. Greater access to such information will ultimately enhance patient involvement and, hence, improve care.

Thus, AARP commissioned this study from the Health Privacy Project to provide a comprehensive examination of the HIPAA protections afforded to patients to access their medical records. The study examines the rights and responsibilities of the parties who have or control access to an individual's medical record, reports on some obstacles to more widespread consumer access to medical records, and presents recommendations for improving the public's and clinicians' understanding of the regulatory requirements that could promote patient access to medical records.

Joyce Dubow
Associate Director
AARP Public Policy Institute
February 2006

[1] Fowles, J. B., Allan Kind, Cheryl Craft, Elizabeth Kind, Jeffrey Mandel Susan Adlis, " Patients' Interest in Reading Their Medical Record: Relation With Clinical and Sociodemographic Characteristics and Patients' Approach to Health Care," *Archives of Internal Medicine*, Vol. 164, April 12, 2004.

Table of Contents

Executive Summary

Background

The right to access information about oneself is essential to privacy. Control over personal information is central to the notion of privacy, and patients cannot have control over information they cannot access. Access to medical records can play a vital role in motivating consumers to become more active, informed agents in the delivery of health care services.

Health care providers keep detailed records on the medical histories, diagnoses, and treatments of each of their patients. But, until recently, patients had no federal right to see and copy their own medical records. The 1996 Health Insurance Portability and Accountability Act (HIPAA) changed that situation by instructing the Secretary of the Department of Health and Human Services (DHHS) to issue the HIPAA Privacy Rule in the event Congress failed to act within two years. As a result of congressional inaction, DHHS promulgated the Privacy Rule, which grants people new federal medical privacy rights, including the right to see and copy their own medical records.

Purpose of This Report

The goal of this report is to detail the provisions of the Privacy Rule, which grants patients access to their own medical records, and to provide an overview of the ability of health care providers and health plans to share patient information electronically.

Methodology

This report is based on a review of publications and on interviews with representatives of specified health care organizations.

Findings: Patient Access to Medical Records—Current Law and Practice

The Privacy Rule gives consumers the right to access, inspect, and request amendments to their medical records held by certain health care organizations, notably health care providers and plans.[2] The Privacy Rule establishes procedures for gaining access to personal health information, including limits on the number of days a provider has to respond to a request and the fees that may be charged.

[2] 45 C.F.R. § 160.103(3). Organizations covered by the Privacy Rule are referred to as "covered entities." The Privacy Rule defines covered entities as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with specified financial and administrative transactions.

In some circumstances, covered entities do have the right to deny access. For instance, when a licensed health care professional believes that access to the requested information is likely to endanger the life or physical safety of either the person requesting the information or another person, the covered entity is permitted to deny the request.[3] However, individuals also have the right to request a review of that denial. There are some circumstances in which a patient can be denied access without the right to request a review of the denial, such as access to psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[4] Some of these exceptions have caused concern among certain patient advocates, such as lawyers and Medicare and Medicaid advocates, who need access to protected health information to support their clients. For instance, there have been reports of covered entities denying the authorizations produced by patient advocates, and many have expressed concern that covered entities could potentially deny access to personal health information needed to pursue administrative appeals regarding Medicare or Medicaid benefit denials.

The Privacy Rule also gives patients the right to request that an amendment be added to the medical record.[5] Within 60 days of receiving the request, the covered entity must either accept or deny it.[6]

The Privacy Rule grants a health care consumer the right to know how his or her medical information has been disclosed outside the core health care arena (e.g., to employers). Upon request, covered entities must provide consumers with an accounting of disclosures during the previous six years. However, providers and plans do not have to keep an accounting of disclosures made to treat patients, pay for care, or conduct administrative activities related to treatment and payment.[7]

While the Privacy Rule grants Americans important rights, translating a legal right into practice can be difficult. Historically, patients have played a passive role in the delivery of their own care,

---

[3] C.F.R. § 164.524(a)(3)(i). Note that only "life or physical safety" is specified; possible harm to mental or emotional health is not a reason to deny access. The Preamble of the Privacy Rule clearly states that "covered entities may not deny access on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm."

[4] 45 C.F.R. § 164.524(a)(1-2). The proposed regulation stipulated that covered entities were permitted to "deny a request for access to personal health information compiled in reasonable anticipation of, or for use in, a *legal proceeding*." The Preamble of the Privacy Rule explains that the phrase "civil, criminal, and administrative actions or proceeding" was incorporated into the final Privacy Rule to clarify the scope of the term "legal proceeding." *See* 65 F.R. 82554.

[5] 45 C.F.R. § 164.526. Any amendment made to an individual medical record is technically a supplement to that record. In other words, no information is discarded in the amendment process; instead, information is added, identifying and amending the error in the medical record. This process was designed to ensure the integrity of the record and to protect the patient**.** *See* 45 C.F.R. § 164.526(c)(1).

[6] 45 C.F.R. § 164.526(b)(2).

[7] Activities related to health care treatment or the payment of health care services are referred to as "health care operations" in the HIPAA Privacy Rule. See C.F.R. § 164.528(a)(i).

and debate has often ensued over the concept of who owns medical records. In fact, some surveys have shown a reluctance on the part of physicians to give patients access to their own records, often because they found it costly and time-consuming.[8] Furthermore, the lack of any significant public education effort designed to inform consumers about their rights has had a damaging impact on the strength of the law.

Other concerns have emerged as well. For instance, although the Privacy Rule does not specify a format in which patients must request access to their records, some providers mistakenly insist that patients use the authorization form that the law requires for disclosures to others, such as to employers, who are otherwise prohibited from receiving protected health information from covered entities. As a result, some patients sign authorizations stipulating that they (the patients themselves) will not disclose their own information; however, patients have the discretion to disclose their information under the Privacy Rule.[9]

Furthermore, some patients have complained to DHHS' Office for Civil Rights (OCR), which oversees HIPAA implementation, about refusals of access, suggesting that some providers are not complying with the law or may not understand how to implement the patient access rules.

Findings: Improving Patient Access—The Promise of Electronic Communication

While the Privacy Rule allows for access to paper and electronic records, the increasing use of technology in the health care arena has the potential to streamline the process of granting patients access to their records. Americans support advancements in health information technology but also express serious concern about related privacy and security issues. In a 2003 survey, more than 70 percent of Americans reported that they believed their having the ability to access their personal health records online would improve the quality of their health care, and 75 percent of Americans reported that they would e-mail a doctor if they could keep their medical records

---

[8] A 2005 survey showed that physicians were significantly less likely than patients to expect certain benefits from patient-accessible medical records and significantly more likely to anticipate concerns. The survey showed that 63 percent of physicians thought that their "workload would increase substantially." See Stephen E. Ross, MD, et al., "Expectations of Patients and Physicians Regarding Patient-Accessible Medical Records," *Journal of Medical Internet Research* 7, no. 2 (2005): e13, www.jmir.org/2005/2/e13/ (accessed on 12/6/05). A 2004 survey showed that clinicians expressed concern about problems that could ensue over patient access, especially related to the clinicians' ability to be "frank in documenting patient problems and condition." See Andrea Hassol, MSPH, et al., "Patient Experiences and Attitudes about Access to a Patient Electronic Health Care Record and Linked Web Messaging," *Journal of the American Medical Informatics Association* 11, no. 6 (November/December 2004): http://www.pubmedcentral.gov/articlerender.fcgi?tool=pubmed&pubmedid=15299001 (accessed on 12/06/05). For a brief synopsis of physician concerns about patient electronic accessibility to records and costs, see Kelli M. Dugan, "Time Spent on E-mail Concerns Many Doctors," *Birmingham Business Journal*, November 8, 2004.

[9] Dan Rode, American Health Information Management Association, testimony before the National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality, November 19, 2003; transcript available at www.ncvhs.hhs.gov/031119tr.htm.

online.[10] A similar survey conducted in 2005 showed that 72 percent of Americans support the creation of a national electronic health information exchange network, and 60 percent of Americans support the establishment of personal health records (PHRs) that would enable consumers to refill prescriptions, e-mail their providers, access test results, and check their personal health information for errors.[11] At the same time, a 2005 Harris Interactive survey showed that 70 percent of Americans are concerned that weak security in an electronic medical record (EMR) system could expose their sensitive medical information, and 69 percent are concerned that an EMR system would lead to more personal health information being shared without patients' knowledge.[12] Furthermore, a 2005 California HealthCare Foundation survey showed that Americans think paper-based medical records are more secure than electronic medical records (66 percent of Americans think their paper medical records are secure versus 58 percent who think their medical records are secure when stored electronically, according to the survey).[13]

EMR systems could go a long way to addressing issues related to patient access to personal health information, such as cost and timeliness. But while the technology is certainly promising, the privacy risks are significant. The HIPAA Privacy and Security Rules provide a clear foundation for the development of EMR systems, but they are just that—a foundation. While both laws serve as a good starting point, neither fully anticipates or addresses issues associated with the development of a system in which personal health information is shared electronically across a spectrum of providers.

Conclusion and Recommendations

Generally, providers understand their responsibilities to grant patients access to their medical records under the HIPAA Privacy Rule. Nevertheless, some confusion remains among providers about the access provisions of the law.

Additionally, patients are ill-informed about the rights afforded them under the Privacy Rule. Overall, OCR needs to actively monitor, enforce, and educate the public and providers about the law. OCR should seek funding from Congress to launch an immediate, widespread public education campaign that encourages patients to assert their access rights under the law by

---

[10] Markle Foundation, Connecting for Health, "Americans Want Benefits of Personal Health Records," June 5, 2003, www.connectingforhealth.org/resources/phwg_survey_6.5.03.pdf (accessed on 12/06/05).
[11] Markle Foundation, Connecting for Health, "Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange," October 11, 2005, www.markle.org (accessed on 12/08/05).
[12] Harris Interactive Inc., "How the Public Sees Health Records and an EMR Program," conducted for Program on Information Technology, Health Records, and Privacy, Center for Social and Legal Research, February 2005.
[13] "Secure" combines "very secure" and "somewhat secure." *See* California HealthCare Foundation. "National Consumer Health Privacy Survey 2005," Executive Summary, November 2005. http://www.chcf.org/topics/view.cfm?itemID=115694 (accessed on 12/08/05).

offering them technical assistance, including written guidance and sample language to prepare written requests.

Access to personal health information is essential to strong privacy protections and quality health care. In the health care arena, access to personal medical records has been shown to encourage patient participation in care and adherence to treatment regimens. In addition, as found in a 2003 review of studies on patients' access to their medical records, access provides benefits such as enhanced doctor-patient communication.[14]

The implementation of the Privacy Rule was an important step towards ensuring that patients are afforded the necessary privacy protections. The related access provisions of the law are a vital component in meeting the needs of patients and the demands of an effective health care system. However, while the Privacy Rule was groundbreaking, the impact of the law has, so far, fallen short of its potential. Patients who are unaware of rights afforded them under the law are not exercising those rights—to the detriment of the quality of their own care, as well as the quality of the health care system. As the development and implementation of a national health information infrastructure continues, including EMRs, it is critical that providers are aware of their responsibilities and that patients are both knowledgeable about their rights and committed to asserting them.

[14] Stephen E. Ross, MD, and Chen-Tan Lin, MD, "The Effects of Promoting Patient Access to Medical Records: A Review," *Journal of American Medical Information Association* 10, no. 2 (March 2003): 129–138.

I. Introduction

Doctors keep detailed records on the condition and treatment of each of their patients. Medical records—often scrawled on a piece of paper, but increasingly entered into a computer system—are designed to facilitate health care by maintaining a history of a patient's health status and treatments. By offering a baseline against which to compare new conditions and by assisting in the maintenance of treatment continuity, medical records are fundamental to delivering the best possible care. Medical records are also used for purposes other than direct health care services, such as activities designed to measure quality of care, conduct research, and monitor the public's health. Thus, they are often accessed by professionals other than direct providers, such as quality improvement organizations, researchers, public health officials, and insurance companies.

Control over personal information is central to the notion of privacy, and patients cannot have any measure of control over health information if they cannot access their own medical records. In addition, access to medical records can play a vital role in motivating consumers to become more active, informed agents in the delivery of health care services; research has shown that people with access to their records are more likely to actively participate in their own care. Finally, access to medical records also affords consumers an important opportunity to ensure that their personal health information is complete and accurate—thereby promoting optimal health care.

Until recently, patients had no federal right to see or copy their medical records. Although most states had laws granting patients access to their medical records, such laws were not well known to patients or adequately enforced. In 1996, the process of creating a federal right began when Congress passed the Health Insurance Portability and Accountability Act (HIPAA). The federal medical privacy regulations issued pursuant to HIPAA—known as the Privacy Rule—gave patients new privacy rights, including the right to see and copy their own medical records. The Privacy Rule went into effect on April 14, 2001, and most providers and health plans were required to be in compliance with the law by April 14, 2003.

In the preamble to the Privacy Rule, the Department of Health and Human Services (DHHS) stated that a "major goal" of the law was "to protect and enhance the rights of consumers by providing them access to their health information."[15] Based on the principle of informed consent, the Privacy Rule acknowledges that to have meaningful control over personal health care decisions—including limitations on who can access information—individuals need to have access to their own health information.

Most patients want access to their medical records. A national survey showed that 68 percent of Americans believe that "giving people the right to see and make corrections to their own medical records" would be an effective way of promoting privacy and health care.[16] And, in 1999, before patients had a federal right of access, 45 percent of people reported that they had attempted to

[15] 65 F.R. 82463.

[16] California HealthCare Foundation, "Medical Privacy and Confidentiality Survey," Final Topline, January, 10, 1999, www.chcf.org/documents/ihealth/topline.pdf (accessed on 12/08/05).

access their medical records, most commonly because they changed doctors or had a personal concern about their health.[17]

While the Privacy Rule allows patient access to both paper and electronic records, the increasing use of technology in health care fosters the potential for streamlining the process of granting patients access to their records. Although there are significant concerns about privacy, cost, and feasibility, there is a strong, persistent push by government officials and private companies for the implementation of health information technology. Some providers and companies have already taken the leap—offering patients electronic access to their medical information. As long as strong privacy and security protections are in place, the ability of patients to access their personal health information electronically could have a positive impact on how they participate in their care.

The Privacy Rule was mandated under the Administrative Simplification section of HIPAA, in which Congress calls for the development of a "health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[18] One of the goals of HIPAA was to encourage a more productive exchange of health information. To this end, the HIPAA Privacy and Security Rules[19] provide a baseline of security and privacy protections that can be built on, ensuring that any move toward implementing new technologies does not endanger basic values of privacy and personal control.

However, translating a legal right into a practical one can be difficult. Historically, patients have often played a frustrated and passive role in the delivery of their own care, and debate has often ensued over the concept of who owns medical records. In fact, some surveys have shown a reluctance on the part of physicians to give patients access to their own records, often because they found it costly and time-consuming.[20] Furthermore, uncertainty about whether patients or providers own medical records—and providers' interest in maintaining ownership—also discouraged physicians from allowing patient access. As an outgrowth of these issues, there are still significant obstacles to overcome in the drive to create a health care system in which the majority of patients actually have a copy of their records. Above all, the Privacy Rule was a first

[17] Ibid.
[18] Health Insurance and Portability and Accountability Act of 1996, Pub. Law No. 104-191, 261, 110 Stat.1988 (1996).
[19] The HIPAA Security Rule (with an April 2005 compliance date) provides detailed provisions related to how covered entities must protect electronic health information.
[20] A 2005 survey showed that physicians were significantly less likely than patients to expect certain benefits for patient-accessible medical records and significantly more likely to anticipate problems. The survey showed that 63 percent of physicians thought that their "workload would increase substantially." *See* Ross et al., "Expectations of Patients and Physicians," 2005. A 2004 survey showed that clinicians expressed concern over problems that could ensue over patient access, especially related to the clinicians' ability to be "frank in documenting patient problems and condition." *See* Hassol et al., "Patient Experiences and Attitudes," 2004**.** For a brief synopsis of physician concerns about patient electronic accessibility to records and costs, *see* Dugan, "Time Spent on E-mail," 2004.

step toward this goal—guaranteeing that, at the very least, patients have a federal right to see and copy their personal health information.

Purpose of This Report

The goal of this report is to detail the provisions of the Privacy Rule, which grants patients access to their medical records, and to discuss the ability of health care providers and health plans to share patient information electronically. To that end, the following questions will be addressed:

- How does the HIPAA Privacy Rule—and, where applicable, the HIPAA Security Rule—address patient access to personal health information and electronic communication among providers, health plans, and patients?

- Are there misconceptions, sources of confusion, or other issues related to the Privacy Rule that currently inhibit patient access to information?

The Privacy Rule is an important step toward ensuring that patients will participate in their care, because it provides a floor of protection for personal health information and also guarantees access to medical records. However, there are many issues that impede patients' access to their heath information, including the ability to pay fees for copies, the ability to access the Internet, and the motivation and confidence to actively participate in their own care. These issues are significant and complex, and, although they are touched upon in this report, it is not intended to be a comprehensive account of the challenges associated with changing the role of patients in the health care system or the obstacles certain patients—such as low-income patients—face in accessing records.

Methodology

This report is based on a review of publications and interviews with representatives of several health care organizations.

Our activities focused on two major areas:

- Review of the Privacy and Security Rules and guidance provided by the DHHS Office for Civil Rights (OCR), the agency responsible for enforcing the Privacy Rule.

- Review of publications and interviews with representatives of health care organizations, including the American Health Information Management Association (AHIMA) and the National Committee on Vital and Health Statistics (NCVHS).

Appendix A contains the list of individuals interviewed and appendix B contains a bibliography of the materials reviewed.

II. Findings: Patient Access to Medical Records—Current Law and Practice

Why Patient Access to Medical Records Matters

The right to access information held about oneself is essential to privacy. Alan Westin's often-cited definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" serves as a solid foundation for this principle.[21] Individuals must be able to access information in order to control it. As George Annas of the Boston University School of Public Health[22] has emphasized, "it is considered a basic privacy principle that if anybody has personal information about you, you should have access to that information, too."[23] Without such access, privacy protections are hollow.

In the health care arena, access to one's own medical records has been shown to encourage participation in care and compliance with treatment. This finding is becoming widely recognized and reported in the news. For example, according to a May 11, 2004 *New York Times* article, a Minnesota patient

> "found that reviewing her own records gave her a starkly realistic view of how her weight had increased over the years and how her blood pressure and blood sugar numbers had "moved in the wrong direction." The revelation inspired her to lose 30 pounds."[24]

On a larger scale, a 2003 review of studies on patient access to medical records found that access provides certain benefits, such as enhanced doctor-patient communication.[25]

The 2003 review showed that "patients who in fact took receipt of their records were generally satisfied." Several of the studies reviewed showed that patients with access to their records improved their understanding of medical information, and one study showed that "smokers who received a copy of their most recent progress notes were significantly more likely to identify smoking as a problem" up to six months after their appointment. Studies also reported other benefits, such as a greater feeling of reassurance, a greater feeling of autonomy and self-efficacy, and improved doctor-patient communication.

The HIPAA Privacy Rule provides procedures for patients to request access to their records and for providers to grant access (or, under some circumstances, to deny it). More than two years after the Privacy Rule went into effect, understanding of the access provisions among providers

---

[21] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).
[22] George Annas is chair of the Department of Health Law, Bioethics and Human Rights at Boston University.
[23] Mary Duenwald, "How Patients Can Use the New Access to Their Medical Records," *New York Times*, May 11, 2004, F1.
[24] Ibid.
[25] Ross and Lin, "The Effects of Promoting Patient Access to Medical Records," 2003.

appears adequate—most providers clearly understand their responsibilities to grant patients access. However, unlike many other provisions of the Privacy Rule, meeting the full potential of the right to access medical records will require much more than providers understanding and following the law.

Discussion of Regulation

The Privacy Rule gives consumers rights with regard to certain health care organizations, called "covered entities." The Privacy Rule defines covered entities as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with specified financial and administrative transactions.[26]

Right of patient access
The Privacy Rule gives health care consumers "a right of access to inspect and obtain a copy of protected health information about the individual [held by a covered entity] in a designated record set."[27] The Privacy Rule defines *protected health information* (PHI) as any "individually identifiable health information," with the exception of some education and other records.[28] *Individually identifiable health information* is defined as "a subset of health information, including demographic information collected from an individual" that:

> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) 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; and
>
> (i) Identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[29]

Covered entities may "de-identify" PHI either by statistically determining that the risk of identifying the patient is very small or by removing certain specific identifiers, such as name, address, social security number, and ZIP code. If the information has been de-identified, it is no longer PHI and consumers no longer have a right to access it.[30]

---

[26] 45 C.F.R. § 160.103.
[27] 45 C.F.R. § 164.524(a)(1).
[28] 45 C.F.R. § 164.501.
[29] 45 C.F.R. § 160.103.
[30] 45 C.F.R. § 164.514(b). There are 18 individual identifiers that must be removed for health information to be considered de-identified. The Privacy Rule only regulates protected health information; therefore, information that is de-identified is not covered under the law.

Consumers only have a right to access PHI if, and for as long as, it is maintained in a *designated record set*, which the Rule defines as a "group of records maintained by or for a covered entity that is:

> (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
>
> (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
>
> (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals."[31]

Exceptions to the right of access

Although the Privacy Rule grants consumers the right of access in most situations, there are several specific situations in which covered entities are not required to give consumers access to their own PHI held in a designated record set. It should be noted that the Preamble of the Privacy Rule clearly articulates that exceptions to granting access should be implemented narrowly: "We intend to create narrow exceptions to the right of access and we expect covered entities to employ these exceptions rarely, if at all."[32] Under the Privacy Rule, individuals do not have the right to access the following information:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
- Information maintained by a covered entity that is subject to the Clinical Laboratory Improvements Amendments of 1988, to the extent that provision of access to the individual would be prohibited by law;
- Information maintained by a covered entity that is exempt from the Clinical Laboratory Improvements Amendments of 1988;
- Copies of their own medical records, if they are inmates at a correctional institution and granting them access would endanger the health, safety, security, custody, or rehabilitation of the individual or other inmates or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate;
- Information maintained by a health care provider in the course of research that includes treatment, while the research is in progress (as long as the individual has agreed to the denial of access when consenting to participate in the research);
- Information contained in records that are subject to the Privacy Act, if the denial of access meets the requirement of that law; and

[31] 45 C.F.R. § 164.501.
[32] 65 F.R. 82556.

- Information that was obtained from someone other than the health care provider under the promise of confidentiality and providing access would be reasonably likely to reveal the source of the information.[33]

In the above situations, a covered entity may deny an individual access without allowing the individual an opportunity to request a review of the denial. However, in some situations, covered entities have the right to deny access, but individuals also have the right to request a review of that denial. These situations occur when:

- A licensed health care professional believes, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;[34] or
- The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional believes, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.[35]

Procedure for patients' gaining access

To create a vehicle for informing patients about their rights under the law, the Privacy Rule requires covered entities to provide a *notice of privacy practices* to consumers. The notice must contain a statement of the individual's rights, including the right to inspect, copy, and amend PHI, as well as a brief description of how the individual may exercise these rights.[36]

The Privacy Rule outlines a process for individuals to seek access to their medical information and for covered entities to provide it in a timely manner. It stipulates that covered entities must allow individuals to request access to their own records and allows covered entities to require that requests be written if patients are informed of this requirement in advance.[37] Otherwise, patients may request access orally.

Within 30 days of the receipt of the request, the covered entity must act by providing the patient with access, providing a written denial of access, or informing the individual of the reason the covered entity needs additional time (but no more than 30 days) to complete the request. The one

[33] 45 C.F.R. § 164.524(a)(1-2).
[34] C.F.R. § 164.524(a)(3)(i); note that only "life or physical safety" is specified; possible harm to mental or emotional health is not a reason to deny access. The Preamble of the Privacy Rule clearly states that "covered entities may not deny access on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm." *See* 65 F.R. 82555.
[35] 45 C.F.R. § 164.524(a)(3).
[36] 45 C.F.R. § 164.520(a)-(b)(1)(iv).
[37] 45 C.F.R. § 164.524(b)(1).

exception is for information not maintained or accessible to the covered entity on-site; the covered entity may then take up to 60 days to take one of these actions.[38]

If the covered entity grants access, it must provide the individual with the information in the format requested, if possible, and otherwise in a readable hard copy or another format agreed upon by both the covered entity and the individual.[39] The covered entity may provide a summary of the health information if the individual agrees in advance to the summary *and* to any additional fees it would produce. The covered entity must arrange with the individual for "a convenient time and place to inspect or obtain a copy of the protected health information, or mail the copy of the protected health information at the individual's request" and may charge a "reasonable, cost-based fee" if the individual requests a copy of the record; however, the fee may only include costs for copying, postage, and the development of a summary if the individual agreed to one.[40]

If the covered entity denies access to a patient, it must deny access only to the specific information for which it has grounds to deny access. Within 30 days, it must provide the individual with a "timely, written denial" that is conveyed in plain language and contains the basis for the denial. A denial must include a statement of the individual's rights to a review of the denial (if applicable), a description of how the individual may exercise review rights, and a description (detailing pertinent names, titles, and contact information) of how the individual may file a complaint. Furthermore, if the covered entity does not maintain the PHI the individual requested but has knowledge of where it is stored, the law requires the covered entity to inform the individual about where to submit a request.[41]

If the individual requests a review of the covered entity's denial, the covered entity must ensure that the review is conducted by a licensed health care professional who was *not* directly involved in the denial. The covered entity must forward the request for a review in a timely manner to the reviewer, and the designated reviewing professional must determine "within a reasonable period of time" whether or not to deny access. Once a decision is made, the covered entity must promptly provide notice to the individual and take any necessary action.[42]

---

[38] 45 C.F.R. § 164.524(b).
[39] 45 C.F.R. § 164.524(c)(2)(i).
[40] 45 C.F.R. § 164.524(c). According to the Preamble to the Privacy Rule, 65 F.R. 82557, "If the individual requests a copy of protected health information, a covered entity may charge a reasonable, cost-based fee for the copying, including the labor and supply costs of copying. If hard copies are made, this would include the cost of paper. If electronic copies are made to a computer disk, this would include the cost of the computer disk. Covered entities may not charge any fees for retrieving or handling the information or for processing the request. If the individual requests the information to be mailed, the fee may include the cost of postage. Fees for copying and postage provided under state law, but not for other costs excluded under this rule, are presumed reasonable. If such per page costs include the cost of retrieving or handling the information, such costs are not acceptable under this rule." Available at http://aspe.hhs.gov/admnsimp/final/PvcPre02.htm.
[41] 45 C.F.R. § 164.524(d).
[42] 45 C.F.R. § 164.524(d)(4).

Procedure for patients requesting amendments to medical records

Catching an error or simply adding pertinent information about health status or history can have a significant impact on quality of care. When patients do access their medical records, there is a real possibility that they will find incorrect or missing information. For instance, a 2004 study showed that upon viewing their electronic health records, one-third of people felt that the information was incomplete and about 25 percent thought that their medical history was not accurate.[43]

The Privacy Rule recognizes the importance of allowing patients the right to amend inaccurate or incomplete medical records. Under the law, after an individual has reviewed his or her medical records, he or she may request that the covered entity amend the PHI in the designated record set.[44] However, to protect both the integrity of the record and the patient, the individual does not have the right to request that the covered entity delete any information from the record.[45]

The Privacy Rule allows covered entities to require that individuals make amendment requests in writing, as well as submit an accompanying explanation for the request, as long as individuals are notified in advance of any requirements. Within 60 days of receiving the request, the covered entity must either make the requested amendment or deny it.[46] However, just as with the other access provisions, the law does allow the covered entity one extension (of no more than 30 days), provided that it sends the individual a written statement explaining the delay and listing the expected completion date.[47]

If the covered entity accepts the amendment request, the Privacy Rule requires that, at a minimum, it must identify the records that are affected by the amendment and either attach the amendment or provide a link to the location of the amendment. The law also requires the covered entity to notify the individual that the record has been amended in a timely manner and secure the individual's agreement allowing the covered entity to inform other relevant persons. Also in a timely manner, the covered entity must make reasonable efforts to notify and provide the amendment to anyone whom the individual designates as having received PHI that needs to be amended. The covered entity must notify others, including business associates, who have the information and may have relied or could rely on the un-amended information to the detriment of the individual.[48]

---

[43] Hassol et al., "Patient Experiences and Attitudes," 2004.
[44] 45 C.F.R. § 164.526(a)(1).
[45] 45 C.F.R. § 164.526. Any amendment made to an individual medical record is technically a supplement to that record. In other words, no information is discarded in the amendment process; instead, information is added, identifying and amending the error in the medical record. This process was designed to ensure the integrity of the record and to protect the patient**.** *See* 45 C.F.R. § 164.526(c)(1).
[46] 45 C.F.R. § 164.526(a-b).
[47] 45 C.F.R. § 164.526(b)(2)(ii).
[48] 45 C.F.R. § 164.526(c).

If a covered entity denies the amendment request, it must still abide by several related requirements. For instance, using plain language, the covered entity must provide the individual with a "timely, written" denial that details both the basis for the denial and the individual's right (as well as how to exercise this right) to submit a written statement disagreeing with the denial. If the individual submits a statement of disagreement, the statement, the original request, the covered entity's denial, and any rebuttal must be appended to the designated record set and included in any future disclosures.[49] But even if the individual does not submit a statement of disagreement, he or she may request—and the covered entity must comply—that the covered entity include the request for amendment and the denial with any future disclosures of pertinent sections of the designated record set.[50] In addition, the covered entity is required to append or link to the appropriate section of the designated record set, as a recordkeeping function, the individual's amendment request, the denial of request, the statement of disagreement, and any rebuttal statement.[51]

Requirement to account for disclosures

Allowing individuals knowledge about how their personal health information is disclosed is central to ensuring strong privacy protections. Building on the concept of notifying patients about how their information *will be* shared, the Privacy Rule also grants patients the right to know how their personal health information *has been* shared. With exceptions, the Privacy Rule gives patients the right to see to whom covered entities have disclosed their personal health information for the six years before the date of request.[52]

Upon request, covered entities must provide consumers with a *written* accounting of disclosures during the previous six years, including the date of the disclosure, the name of the person who received the information, a brief description of the PHI disclosed, and a brief statement of the purpose of the disclosure. If a covered entity has made multiple disclosures to the same person for the same purpose, it may provide this information only for the first disclosure as long as it also provides the frequency of the disclosures and the date of the last disclosure.[53]

---

[49] 45 C.F.R. § 164.526(d); the Privacy Rule also allows covered entities to include in future disclosures—in lieu of including the actual request, denials, disagreement statements, and rebuttals—"an accurate summary of any such information." *See* 45 C.F.R. § 164.526(d)(4)-(5).

[50] 45 C.F.R. § 164.526(d); the Privacy Rule requires covered entities to inform individuals that if a disagreement statement is not submitted, the individual may request that the covered entity attach the request and denial to any future disclosures. *See* 45 C.F.R. § 164.526(d)(1)(iii). The Privacy Rule also allows covered entities to include in future disclosures—in lieu of including the actual request, denials, disagreement statements, and rebuttals—"an accurate summary of any such information." *See* 45 C.F.R. § 164.526(d)(4)-(5).

[51] 45 C.F.R. § 164.526(d)(4).

[52] 45 C.F.R. § 164.528(a).

[53] Additionally, if a covered entity has made PHI disclosures for research purposes for 50 or more people, the accounting of disclosures may (with respect to such disclosures for which the PHI of the individual may have been included) provide the following: the name of the protocol or research activity; a description of the activity in plain language, including purpose and criteria

Within 60 days of the request, a covered entity must provide the accounting or a written statement detailing a reason why it needs an extension of time (no more than 30 days).[54] The covered entity must provide an accounting of disclosures once a year without charge. However, if an individual requests an accounting more than once a year, a reasonable, cost-based fee may be imposed, provided that the individual was informed in advance of the fee and the covered entity also provides the individual with an opportunity to withdraw or modify the request to avoid the fee.[55]

Individuals do not have the right to accountings of certain disclosures, including disclosures

(i) To carry out treatment, payment, and health care operations;

(ii) To the individual requesting the accounting of disclosures of their own PHI;

(iii) For the facility's directory or to people involved in the individual's care or other notification purposes;

(iv) For national security or intelligence purposes;[56]

(v) To correctional institutions or law enforcement officials for certain purposes;[57]

(vi) As part of a limited data set; or[58]

---

for selecting records; a description of the type of PHI that was disclosed; when the disclosure occurred (date or period of time and date of the last disclosure); contact information (name, address, and telephone number) of the entity that sponsored the research and of the researcher to whom the PHI was disclosed; and a statement that the PHI of the individual may or may not have been disclosed. If it is reasonably likely that the PHI of the individual was disclosed, and at the request of the individual, a covered entity must assist in contacting the entity or the researcher. *See* 45 C.F.R. § 164.528(b).

[54] 45 C.F.R. § 164.528(c)(1)(ii). The covered entity is allowed only one 30-day extension.

[55] 45 C.F.R. § 164.528(c).

[56] This exception applies only to 45 C.F.R. § 164.512(k)(2), which stipulates that covered entities may provide PHI to authorized federal officials "for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401 et seq.) and implementing authority."

[57] This exception applies only to 45 C.F.R. § 164.512(k)(5), which stipulates that covered entities may provide PHI about an inmate or other individual to "a correctional institution or a law enforcement official having lawful custody of such inmate or other individual, if the correctional institution or law enforcement official represents that the PHI is necessary for" certain purposes (listed in the Privacy Rule), including for the provision of health care to such individuals, for the health and safety of the individual and other inmates, and for the health and safety of the officers or employees of or others at the correctional institution.

[58] Under the Privacy Rule, a limited data set is protected health information that excludes 16 specific direct identifiers of the individual or of relatives, employers, or household members,

(vii) That occurred before the compliance date for the covered entity.

Furthermore, a covered entity must temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official if the agency or official provides the covered entity with a written statement illustrating that such an accounting would be reasonably likely to impede the agency's activities. The written statement must also specify the time period for which such a suspension is required.[59]

Nonpreemption of more stringent state law

The HIPAA Privacy Rule generally preempts contradicting state law. However, when state laws are more stringent than the Privacy Rule, they remain in force.[60] Therefore, state laws that cap copying and postage fees for medical records or require additional accountings of disclosures remain in effect.

Access to information held by business associates

Covered entities may contract with business associates to perform some of the covered entity's functions. Business associates could be other covered entities or noncovered entities, such as accountants, attorneys, or data processors.[61] In the business associate contract, the business associates must agree to make PHI available for access, amendment, and accounting of disclosures.[62]

---

including name, postal address information, telephone numbers, and fax numbers. *See* 45 C.F.R. § 164.514(e)(2).

[59] 45 C.F.R. § 164.528.

[60] According to 45 C.F.R. § 160.202, "more stringent" (in relationship to access rights) means, in the context of a comparison of a provision of state law and a standard, requirement, or implementation specification, a state law that meets one or more of the following criteria: (2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; (3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information; (5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration; and (6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information**.** Note that these conditions of "more stringent" only include those that pertain to the access provisions of the law. For other conditions that qualify as "more stringent," *see* 45 C.F.R. § 160.202.

[61] 45 C.F.R. § 164.103.

[62] 45 C.F.R § 164.504(e)(2)(ii)(E-G).

Discussion: Patient Access and the Privacy Rule

The brightest marker for determining adequate implementation of the Privacy Rule highlights to what extent providers and patients understand and exercise respective rights and responsibilities under the law. Overall, providers appear to have an understanding of their responsibility to grant patients access to their personal health information in a designated record set.[63] This is not insignificant, given both the importance of the access provisions and the reality that many providers struggle with fully comprehending other aspects of the law. In this respect, the provisions granting patient access to medical records seem to have overcome one major hurdle to realizing the positive impact of the Privacy Rule. At the same time, however, patients continue to file complaints with DHHS's OCR about denial of access, and providers have expressed some concern with certain requirements related to granting patients access to their medical records.

Patients are still not adequately informed about their rights to access their own PHI under the Privacy Rule. In the absence of any strong government effort to educate Americans about their rights under the law, consumers often lack a clear understanding of their rights. For instance, despite the fact that surveys have established significant patient interest in accessing one's own medical records, the deluge of requests that some predicted would flood physicians' offices once the Privacy Rule was enforced has not occurred. In fact, in an informal survey of members of AHIMA,[64] most health information managers reported that their facilities had experienced only a modest increase in requests for access. While this may have eased providers into a HIPAA-compliant operation, it is also a certain signal that patients are not knowledgeable about their rights to access their records.

Complaints about refusal of patient access to medical records

[63] A 2005 American Health Information Management Association (AHIMA) survey showed that a majority of health care facilities are significantly compliant with the Privacy Rule and listed areas of concern that exclude issues regarding patient access. *See* AHIMA, "The State of HIPAA Privacy and Security Compliance," April 2005.

[64] In June 2004, on behalf of the Health Privacy Project, AHIMA surveyed members regarding their experiences with patient access to PHI under the HIPAA Privacy Rule. Approximately 50 AHIMA members responded to the following questions: (1) At your location, have patient requests for access or copies of their own personal health information increased since the implementation of the HIPAA privacy rules? (If possible, please provide a percentage reference.) (2) Have you noticed any misunderstandings with the HIPAA privacy provisions that provide patients with access to their own personal health information? If so, please describe. (3) At your location, please indicate your impression of the patients' experience with regard to accessing their own personal health information as permitted by HIPAA. (4) At your location, please describe your (the provider's) experience with providing patients with access to their own personal health information as required by HIPAA. (5) Do you think e-mail or other forms of electronic communication make it easier for you to provide patients with access to their personal health information? (If possible, please provide an example or two.)

By October 2005, OCR had received more than 16,118 complaints about possible violations of the Privacy Rule.[65] A significant portion of these complaints relate to patient access to medical records. In testimony before the NCVHS, OCR staff said "we continue to get complaints about [the] inability of individuals to access their information."[66] In fact, denial of an individual's access to his or her personal health information has been—and continues to be—one of the top five complaints raised with OCR.[67] Despite reports of broad compliance with the Privacy Rule, this signifies a need to ensure that providers fully understand the requirement to grant patients access to their records. And while some of these denials could fall under the covered entities' authority to deny access in certain situations, it is important to ensure that such denials are not a violation of patients' rights under the Privacy Rule.

Lack of patient knowledge

According to the Privacy Rule, covered entities must notify patients of their right to access their own medical records through a *Notice of Privacy Practices*. Each covered entity may develop its own notice, as long as certain requirements are met.[68] However, notices often take on the role of protecting providers against liability over providing patients with a consumer-friendly description of their rights. An informal review of *Notices of Privacy Practices* showed that information about how to request access is often buried at the end of a multipage document.[69]

A recent Harris Interactive survey showed that despite the flood of notices patients have received from a broad range of providers—and the fact that, presumably, every survey respondent had received at least one of these notices—32 percent of respondents said they had never received such a notice.[70] A possible explanation for this unexpectedly high response rate is that the survey question described the notice as a document that explains consumers' rights to access, amend, and control their personal health information as well as how providers will use and disclose PHI.[71] A 2005 California HealthCare Foundation survey had a related finding: while 59 percent of respondents recalled receiving a notice, only 27 percent of respondents thought they had new

---

[65] Astara March "National Health IT System Taking Off," United Press International, November 11, 2005. http://washingtontimes.com/upi/20051110-051125-3618r.htm (accessed on 12/08/05).

[66] Susan McAndrew, Office for Civil Rights, testimony before the National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality, March 5, 2004; transcript available at www.ncvhs.hhs.gov/040304t1.htm.

[67] Interview with Susan McAndrew, Office for Civil Rights, June 14, 2004.

[68] Required elements are listed at 45 C.F.R. § 164.520(b).

[69] The Health Privacy Project regularly collects *Notices of Privacy Practices* from providers, and the informal review is based on these notices.

[70] Harris Interactive, "How the Public Sees Health Records," 2005.

[71] The survey question described the notice as a "privacy notice explaining how the organization will collect and use the patient's information, how it will keep the information secure, how patients can get access to their own health records, correct any errors, and control most disclosures of their information to people outside of the health care system."

rights under the Privacy Rule.[72] The issue of inadequate notices for informing patients has been raised repeatedly by consumer advocates. In a report to the U.S. Senate Committee on Health, Education, Labor, and Pensions, the Government Accountability Office (GAO) cited the concern of consumer organizations (including the Health Privacy Project, AARP, and the National Health Law Program) that the notices of privacy practices do not currently serve the clear need to educate patients about their rights under the Privacy Rule. The report also illustrated that provider representatives, such as AHIMA, recognized that patients are unaware of their rights under the Privacy Rule.[73]

In practice, the privacy notice has fallen far short of the educational tool Congress intended it to be. Information about the right to access one's medical records is usually obscured among other information—often written in highly technical language—about PHI uses and disclosures. As a result, patients may not be sufficiently informed about their right to request access to their PHI. In light of the fact that there hasn't been any significant effort by DHHS to educate patients about the law, it is important that notices fulfill their original purpose as envisioned under the Privacy Rule.

At any rate, the consequence of this lack of public education is clear: Patients simply do not know their rights under the law. In fact, the 2004 GAO report illustrated that provider representatives, such as AHIMA, recognized that patients are unaware of these rights. Specifically, a recent AHIMA survey showed that providers estimate that only 3 percent of patients have complete understanding of their rights and providers' responsibilities under the Privacy Rule.[74]

Common patient misperceptions

In addition to the low level of patient awareness about the right to access one's own medical records, the informal survey of AHIMA members identified several areas of confusion for patients.[75] Some patients believe that they have rights that the HIPAA Privacy Rule does not permit, including the right to have information deleted[76] from their record, the right to access information not held in a designated record set, and the right to obtain the actual record rather than a copy of it.

---

[72] California HealthCare Foundation. "National Consumer Health Privacy Survey 2005," Executive Summary, November 2005. http://www.chcf.org/topics/view.cfm?itemID=115694 (accessed on 12/08/05).
[73] U.S. Government Accountability Office (GAO), "Health Information: First-Year Experiences under the Federal Privacy Rule," report to the chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate, GAO-04-965, September 2004.
[74] AHIMA, "The State of HIPAA Privacy and Security Compliance," 2005.
[75] In June 2004, on behalf of the Health Privacy Project, AHIMA surveyed members regarding their experiences with patient access to PHI under the HIPAA Privacy Rule. See footnote 60.
[76] Any amendment made to an individual medical record is technically a supplement to that record. Instead of any deletion, information is added to identify and amend information in the medical record.

Confusion among providers about the format of written requests for access

At a November 2003 meeting of the NCVHS, a representative of AHIMA raised a concern about the format for written requests of access to medical records. Section 524 of the Privacy Rule permits providers to require patients to submit requests for access in writing. That section does not, however, specify which elements the request must include. Without guidance, some providers have adopted the elements of authorizations under Section 508, which provides a process for individuals to authorize the release of their health information to others. Even though Section 508 stipulates that authorization requirements should be implemented "as applicable,"[77] some covered entities have included Section 508 authorization elements that are inappropriate in the context of a request for one's own records. According to AHIMA, some patients have been required to sign Section 508 authorizations in which they promise not to disclose their own information; in fact, patients have the right to disclose their medical information as they see fit.[78]

Many of the health information managers who responded to the informal AHIMA survey indicated that they believed that a specific "HIPAA-compliant" authorization was needed for patient access.[79] While individual covered entities are free to require authorizations before granting access, HIPAA does not require that they do so. In fact, HIPAA allows patients to request access orally.

Provider-imposed procedures not required by the Privacy Rule

Many respondents to the informal survey of AHIMA members indicated that their facility had implemented procedures, not required by the Privacy Rule, that have caused substantial frustration for patients.[80] These procedures include requiring patients to submit access requests in person, requiring them to submit access requests to a centralized office, and requiring that a doctor be present while patients review their records. These additional requirements could signal the need for better guidance for providers. In fact, another AHIMA survey showed that there is a consensus among covered entities regarding an ongoing need for retraining and education, especially as fewer institutional resources have been available for these activities since the HIPAA compliance deadline in 2003.[81] Often without a clear understanding of the Privacy Rule, covered entities err on the side of caution and impose restrictions that are not required by the Privacy Rule.

Inappropriate accountings for disclosure

The reporting of neglect or abuse is not listed as an exception to the *accounting of disclosures requirement* delineated in Section 528 of the Privacy Rule.[82] In a March 5, 2004 letter to Tommy

[77] 45 C.F.R. § 164.508(b)(1)(i).
[78] Dan Rode, testimony, 2003.
[79] In June 2004, on behalf of the Health Privacy Project, AHIMA surveyed members regarding their experiences with patient access to PHI under the HIPAA Privacy Rule. See footnote 63.
[80] Ibid.
[81] AHIMA, "The State of HIPAA Privacy and Security Compliance," 2005.
[82] 45 C.F.R. § 164.528(a)(1).

Thompson, then-secretary of DHHS, NCVHS noted that "with regard to accounting for disclosures, the reporting of suspected cases of abuse and neglect has been a particular concern of social service agencies." Although the agencies that receive reports of neglect or abuse are often prohibited from disclosing them, the covered entities that file the reports are required to disclose the reporting activity. NCVHS expressed concern that if "an abusing parent, acting as a child's personal representative, [obtains] an account of disclosures and learns of the [abuse] report," covered entities may be discouraged from filing reports of suspected abuse and neglect.

The belief among providers that accounting for disclosures may be overly burdensome

The 2005 AHIMA survey also clearly indicated that providers are concerned about the *accounting for disclosures requirement* of the Privacy Rule. Depending on the size and structure of the health care organization, the provision requiring covered entities to tell patients how their information *was* shared in certain circumstances can have a significant impact on the entities' administrative operation; some organizations cite the operational changes necessary to comply with the law as overly burdensome. For instance, if a large health care entity, such as a major hospital, stores PHI in separate departments, it would be more burdensome to account for all disclosures than it would be for a smaller entity.

In the 2005 AHIMA survey, responses from HIPAA Privacy Rule officers and similar employees in hospitals and health systems showed that 61 percent believed that the accounting requirements should be modified—up from 51 percent in 2004.[83] Although the same survey found that the majority—67 percent—of respondents reported having received no or only a few requests for accountings, the report pointed to the administrative costs of simply maintaining an accounting for disclosures operation.[84] In fact, a 2004 AHIMA survey showed that 55 percent of covered entities reported that they had to buy new software to facilitate accounting for disclosures. The 2004 survey reported that "many organizations spent considerable time addressing [accounting for disclosures] and changing processes, policies, and procedures to address such releases conservatively." Weighing the logistical demands of the accounting system against the lack of patient demand, AHIMA suggests that the accounting requirement, "be replaced in part by amending the notice of privacy practices to alert patients to disclosures required by law."[85]

Advocates acting on behalf of patients

Sometimes, patients want certain professionals or volunteers, such as lawyers or Medicare and Medicaid advocates, to act on their behalf in accessing their personal health information. Because they do not make health care decisions on behalf of the individual, these professionals or volunteers do not—and should not—qualify as personal representatives under the Privacy Rule.[86] Therefore, they must rely on the use of authorizations to seek the pertinent health

[83] AHIMA, "The State of HIPAA Privacy and Security Compliance," 2005.
[84] Ibid.
[85] Ibid.
[86] The Privacy Rule defines personal representatives as "under applicable law, a person [who] has authority to act on behalf of an individual who is an adult or an emancipated minor in

information on the individual they are assisting. However, there have been reports that some covered entities are not honoring some authorizations.[87] Furthermore, the Privacy Rule exception to granting access to PHI "in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding" could be problematic for advocates, lawyers, and their clients. While we do not know of any reports of covered entities denying access for this purpose, it is plausible that a covered entity could deny access to PHI that is needed by a patient to pursue an administrative appeal when Medicaid or Medicare eligibility is denied or payment is refused.[88]

III. Findings: Improving Patient Access—The Promise of Electronic Communication

Patients' ability to access their own personal health information quickly and efficiently could be significantly enhanced with the use of new technologies. From simple electronic communications, such as encrypted e-mail transactions, to complex electronic medical record (EMR) systems, technology could potentially simplify communication between providers and patients.

Americans support advancements in health information technology but also express serious concerns about related privacy and security issues. In a 2003 survey, more than 70 percent of Americans reported that they believed accessing their personal health records (PHRs) online would improve the quality of their health care, and 75 percent reported that they would e-mail a doctor if they could keep their medical records online.[89] A similar survey conducted in 2005 showed that 72 percent of Americans support the creation of a national electronic health information exchange network, and 60 percent of Americans support the establishment of personal health records (PHRs) that would enable consumers to refill prescriptions, e-mail their providers, access test results, and check their personal health information for errors.[90] At the same time, a 2005 Harris Interactive survey showed that 70 percent of Americans are concerned that an EMR system would lead to sensitive medical information being exposed because of weak security, and 69 percent are concerned that an EMR system would lead to more personal health information being shared without patients' knowledge.[91] That same survey showed that Americans were split on weighing the potential benefits of an EMR system against the privacy risks, with 48 percent of Americans believing that the benefits outweigh privacy risks and 47

---

making decisions related to health care." Covered entities must treat personal representatives as the individual. *See* 45 C.F.R. § 164.502(g)(2).

[87] Hilary Sohmer Dalin, "Advocacy in a Post-HIPAA World," *BIFOCAL, Bar Associations in Focus on Aging and the Law* 25, no. 2 (Winter 2004):1-9.

[88] Ibid.

[89] Markle Foundation, "Americans Want Benefits of Personal Health Records," 2003.

[90] Markle Foundation, Connecting for Health, "Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange," October 11, 2005, www.markle.org (accessed on 12/08/05).

[91] Harris Interactive, "How the Public Sees Health Records," 2005.

percent believing that the privacy risks outweigh any benefits.[92] Furthermore, a 2005 California HealthCare Foundation survey showed that Americans think paper-based medical records are more secure than electronic medical records (66 percent of Americans think their paper medical records are secure versus 58 percent who think their medical records are secure when stored electronically, according to the survey).[93]

Electronic communication tools could potentially help providers meet and even shorten the 30-day deadline for providing patients with access to records set by the Privacy Rule and consequently improve overall health care quality. But the benefits of easier access to health information are matched by significant risks. The primary concern for providers and patients alike is privacy. While the HIPAA Privacy and Security Rules provide a foundation for protecting health information in an electronic arena, they do not address the many regulatory issues that may arise. Before any health information technology product or system is conceived, it is essential that the significant privacy and security issues are carefully analyzed and confronted. Without strong protections in place, patients will simply not participate in in their health care.

Discussion: Regulatory Implications for e-Health

In many ways, HIPAA paved the way for e-health initiatives: The Administrative Simplification provisions of the law call for the development of electronic exchanges of health information while the HIPAA Privacy and Security Rules were designed to protect medical information, especially in the context of the increasing use of electronic communication between and among health providers. By specifically addressing and establishing the first-ever federal guidelines for medical privacy, the two sets of regulations have laid a foundation on which health care professionals and public officials can mold privacy protections around the unique structure of electronic medical systems. By guaranteeing patients access to their own health information, the Privacy Rule created a potentially important incentive for consumers to participate in e-health programs.

In response to concerns, DHHS has made it clear that the Privacy Rule does not impede the electronic communication of health information. In a May 17, 2004 letter to providers, OCR affirmed that "HIPAA is not anti-electronic." Now that the Privacy Rule is in effect, "doctors can continue to use e-mail…to communicate with patients, providers, and others using common sense, appropriate safeguards to protect patient privacy—just as many were doing before the Privacy Rule went into effect."[94]

---

[92] Ibid.

[93] "Secure" combines "very secure" and "somewhat secure." *See* California HealthCare Foundation. "National Consumer Health Privacy Survey 2005," Executive Summary, November 2005. http://www.chcf.org/topics/view.cfm?itemID=115694 (accessed on 12/08/05).

[94] Richard Campanelli, director, Office for Civil Rights, Department of Health and Human Services, Letter to Healthcare Providers, May 17, 2004, www.hhs.gov/ocr/Healthcare-Provider-letter.pdf (accessed 12/06/05).

Although the Privacy Rule simply requires covered entities to "have in place appropriate administrative, technical, and physical safeguards" to protect the privacy of electronic communication, the Security Rule goes into more detail.[95] Except for small health plans, which have an additional year to prepare, covered entities were required to be in compliance with the Security Rule in April 2005, The Security Rule instructs covered entities to "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[96] The regulation specifically instructs covered entities to implement security measures "to ensure that electronically protected health information is not improperly modified without detection until disposed of" and to implement "a mechanism to encrypt electronic protected health information whenever deemed appropriate."[97] Because many of the implementation specifications are "addressable," if a covered entity deems them inappropriate, it may implement alternative measures. However, covered entities may choose not to adopt addressable specifications as long as they (1) document why the specifications are not reasonable and appropriate, and (2) implement equivalent alternative measures, if reasonable and appropriate.[98]

E-mail and Patient Access

E-mail has become a popular method of communication among providers and between providers and health care consumers. According to recent surveys, providers are increasingly using e-mail to communicate with their colleagues. The American Medical Association (AMA) has reported that 96 percent of physicians send or receive e-mail,[99] and a Manhattan Research survey showed that 85 percent of physicians are currently using e-mail for professional reasons.[100] However, physicians do not communicate with patients via e-mail nearly as often. The AMA reported that only 25 percent of physicians who use e-mail communicate with their patients that way.[101] And while the Manhattan Research survey showed that nearly one-fifth of physicians communicate with patients via e-mail, that rate has not increased significantly in the past two years, leaving an unmet demand.[102] In fact, many Americans would like to communicate with their providers via e-mail. According to a 2002 Harris poll, approximately 90 percent of American adults with Internet access would like to communicate with their doctors by e-mail.[103] Many Americans (37

[95] 45 C.F.R. § 164.530(c)(1).
[96] 45 C.F.R. § 164.312(e)(1).
[97] 45 C.F.R. § 164.312(e)(2)(i-ii).
[98] 45 C.F.R. § 164.306(d)(3). In determining whether a specification is reasonable and appropriate, a covered entity may consider factors such as "the entity's risk analysis, risk mitigation strategy, security measures already in place, and the cost of implementation" (68 F.R. 8336).
[99] AHIMA, "Practice Brief: Provider-Patient E-mail Security (updated)," 2003. http://library.ahima.org/groups/public/documents/ahima/pub (accessed on 12/06/05).
[100] Manhattan Research, LLC, "The Connected Physician: E-mail, Communication, and Connectivity," June 2004.
[101] AHIMA, "Practice Brief: Provider-Patient E-mail Security," 2003.
[102] Manhattan Research, "The Connected Physician," 2004.
[103] Harris Interactive, Inc., "Patient/Physician Online Communication: Many Patients Want It, Would Pay for It, and It Would Influence Their Choice of Doctors and Health Plans," April 10,

percent) would be willing to pay out-of-pocket for the benefit of communicating with their doctors online.[104]

E-mail and Security

In addition to physician concerns about costs, providers and patients have significant concerns about confidentiality and security. In fact, according to the Manhattan Research survey, more than one-third of physicians listed security as one of the conditions that needed to be met in order for them to communicate with their patients via e-mail in the future.[105]

Although e-mail correspondence may create an illusion of security, without adequate safeguards, breaches of privacy may occur. Because e-mail is generally unencrypted, it can be intercepted with devastating results for a patient. In addition, e-mail can be changed, stored, and shared without notice or detection, and it is vulnerable to computer hackers. Human error is also common with e-mail correspondence and could have negative consequences. For instance, an e-mail address could be recorded incorrectly, an e-mail with sensitive information could be accidentally left on a computer desktop, or an e-mail could easily be used in an unauthorized manner. In many ways, the ease with which e-mail creates access reflects the ease with which it can allow for unauthorized disclosures of personal health information.

In an effort to address security and privacy concerns, as well as provide a mechanism for easy and efficient access to health information, many companies have developed "clinical messaging" services. Clinical messaging is touted as a safer alternative to e-mail, transferring encrypted messages over a secure Web server. The process includes patient registration (with an ID and password) and can be designed to accommodate EMR systems.[106]

However, it is important that, along with the development of any new health information technology, enforceable standards are in place to safeguard patients' information. The Security Rule is a step in the appropriate direction, but stronger protections are necessary. With appropriate safeguards, using e-mail to communicate sensitive health information could present a more efficient way to streamline health care operations, improve overall quality of care, and allow for easy access to important personal heath information. With privacy assurances in place, patients could be more likely to take advantage of accessing health care information through e-mail transactions.

2002, www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2002Vol2_Iss08.pdf (accessed on 12/08/05).

[104] Ibid.

[105] Manhattan Research, "The Connected Physician," 2004.

[106] Robert Lowes, "Phones Driving You Crazy? Try Clinical Messaging," *Medical Economics*, March 19, 2004. http://www.memag.com/memag/article/articleDetail.jsp?id=108571 (accessed on 12/08/05).

Electronic Medical Records and Patient Access

Health care information technology has become a much-debated topic in the public and political arenas. With policymakers calling for the development of EMRs, pressure is mounting on providers and public health authorities to develop these systems on both a small and large scale.[107] In April 2004, President Bush issued an Executive Order calling for the development of interoperable electronic health records within 10 years. The Executive Order also established the position of the national coordinator for health information technology. In July 2004, the first national coordinator issued a report examining the implementation of a strategic plan to guide the U.S. health care infrastructure toward building effective, interoperable health care information technology systems.

According to a Healthcare Information and Management Systems Society leadership survey, 79 percent of hospital respondents are already implementing or planning to implement an EMR system.[108] And of respondents not currently offering Web site appointment scheduling, 65 percent plan indicate they plan to do so in the next two years.[109] And patients appear interested in the new technology: A 2001 survey measuring potential patient use of EMRs showed that 68 percent of participants would recommend EMRs to friends.[110]

One potential tool that could help patients become more active, informed participants in their own care is the personal health record (PHR). Like EMRs, PHRs are Internet based and designed to provide access to important health-related information about patients. Unlike EMRs, however, PHRs would be used by the patient and would include additional information not found in the EMR Whereas EMRs generally contain information provided by health care professionals,

---

[107] The debate over EMRs foundered in the 1990s over concern that EMRs would necessarily require that patients be assigned a unique identifier. Privacy advocates worried that the unique patient identifiers would become as ubiquitous and vulnerable as the Social Security number. Although HIPAA required DHHS to develop a system of unique identifiers for linking personal health information, in response to public outcry, Congress barred DHHS from developing unique identifiers for patients. A 1999 California Health Care Foundation survey confirmed the public's privacy concerns regarding unique patient identifiers. According to the survey, even when people understood the huge health advantages that could result from linking their medical records through a national system of identifiers, a majority believed that the risks—of lost privacy and discrimination— outweighed the benefits. *See* California HealthCare Foundation, "Medical Privacy and Confidentiality Survey," 1999. Recent attempts to develop EMRs generally sidestep the issue of unique patient identifiers by relying on local medical records numbers or other less-centralized approaches.

[108] Douglas Page, "HIMSS Meeting Focuses on Security and Patient Safety," *Diagnostic Imaging*, May 1, 2004, page 79.
[109] Ibid.
[110] Ira C. Denton, "Will Patients Use Electronic Personal Health Records? Responses from a Real-life Experience." *Journal of Healthcare Information Management*, Fall 2001, pages 251-259.

PHRs would also include information provided by the patient, such as when a prescription was filled.

Because the individual patient is the primary user of his or her own PHR, he or she would make decisions about allowing access to the PHR to other individuals, such as doctors, employers, or family. Ideally, PHRs would function as information and communication hubs, through which patients could access and actively manage personal health information and e-mail doctors. Both the EMR and the PHR would benefit from information provided by the other and, together, these two tools could enhance access to personal health information.[111] A Markle Foundation report found that 70 percent of Americans believe that a PHR would improve quality of care.[112]

However, as with the development of any electronic form of health information, serious privacy and security issues must be addressed. Consumers have a keen awareness of the need to implement strong privacy protections: The Markle Foundation survey showed that 91 percent of respondents were very concerned about the privacy of their personal health information.[113] This concern is compounded by the reality that many of the companies now offering PHR services are not regulated by the Privacy Rule, because they do not meet the definition of a covered entity. This is problematic and serves as a critical reminder that strong laws and standards must be implemented to protect personal health information from inappropriate use or disclosure.

In the move toward EMR systems, the specific concerns of lower income patients are often ignored. A 2005 survey showed that low-income individuals have the same interest in the benefits of online access to their medical records as higher income individuals.[114] However, low-income individuals are not as likely to use the Internet. According to the survey, whereas approximately three-quarters of those with higher incomes use the Internet, only about one-half of those with lower incomes use the Internet.[115] To make any system of health information technology work best for the health care system, it needs to work for everyone. Addressing the needs of low-income and uninsured patients is essential to developing a successful EMR system.

EMR systems could go a long way to improving the quality of health care. But while the technology is certainly promising, the privacy risks are significant. The HIPAA Security Rule provides a clear foundation for the development of EMR systems, but it is just that: a foundation. Although both laws serve as a good starting point, neither the Privacy Rule nor the Security Rule fully anticipates or addresses issues associated with the development of a system in which personal health information is shared electronically across a spectrum of providers.

---

[111] Markle Foundation, Connecting for Health: A Public-Private Collaborative, "Personal Health Working Group Final Report," July 1, 2003, www.connectingforhealth.org/resources/final_phwg_report1.pdf (accessed on 12/08/05).
[112] Markle Foundation, Connecting for Health, "Personal Health Working Group Survey on Consumer Attitudes toward a Personal Health Record," June 2003.
[113] Ibid.
[114] Ross et al., "Expectations of Patients and Physicians," 2005.
[115] Ibid.

IV. Recommendations

The implementation of the Privacy Rule was an important step in ensuring that patients have necessary privacy protections. The related access provisions are a necessary component in meeting the needs of patients and the demands of an optimal health care system. By and large, providers seem to have an understanding of their responsibilities to grant patients access to their medical records under the HIPAA Privacy Rule. However, it is clear that some confusion remains among providers about the access provisions of the law.

Additionally, patients are ill-informed about their rights under the Privacy Rule, which not only has a deflating effect on the success of the law but impedes efforts to improve care. Other concerns related to patient access and the Privacy Rule have been raised as well, and the following recommendations are designed to address these issues:

Complaints about refusal of patient access

- OCR should analyze the complaints and make public (e.g., posted on a Web site) reports detailing trends in the denial of patients' access to their personal health information. On the basis of these reports, OCR should target its public education efforts to clarify problematic interpretations of the law. Related to this type of analysis, Congress should conduct annual oversight hearings, during which OCR should testify about complaints received, follow-up investigations, criminal referrals, public education, and enforcement. Congressional oversight will shed light on OCR's enforcement of the law and provide a public record of the implementation of the law. As we go forward, having information about how providers are implementing the law and how OCR is enforcing it will be critical to determining whether any changes are necessary to ensure that patients' rights under the Privacy Rule are being realized.

Lack of patient knowledge

- Consumers need to be actively informed and assertive about their rights if the Privacy Rule is going to meet its full potential. Educating the public about the Privacy Rule and the right to access personal health information is central to achieving a health care system that flourishes on adequate patient participation. It is important that patients are actually encouraged to access their medical records. Furthermore, in light of the strong push for the development of an EMR system, it is critical to address consumers' privacy fears by educating patients about their rights and providers about their responsibilities. If patients do not feel that their personal health information is being protected, they could well withdraw from their own care—to the detriment of themselves and their communities.

  DHHS should seek funding from Congress to launch an immediate, widespread public education campaign about the Privacy Rule. Encouraging patients to assert their rights, with a particular focus on the right to access personal health information, should be at the heart of any public education effort. As a part of this effort, OCR should encourage covered entities to highlight the right to access at the beginning of their *Notices of*

Privacy Practices. Furthermore, OCR should conduct a formal study of notices. The Privacy Rule stipulates that notices must be written in plain language.[116] Communicating their mutual rights and responsibilities to patients and providers through the notice is central to a better understanding of the law; and OCR should produce a report assessing notices to analyze trends and foster appropriate changes among covered entities.

Common patient misperceptions

- Patient misperceptions about the Privacy Rule additionally signal the need for a strong public education campaign. Any effort to inform and engage patients should include information that clarifies common misperceptions about the law.

Confusion among providers about the format of written requests for access

- OCR should clarify that the elements of the request are at the discretion of the provider and need not conform to Section 508 or even be in writing. In addition, for covered entities that do use Section 508 as guidance, OCR should clarify that the requirements in that section are to be implemented "as applicable."[117] Alternatively, OCR should consider issuing guidance that illustrates the recommended elements of a written request. As a part of this effort, OCR should produce and disseminate a sample form designed specifically for giving patients access to their own records.

Provider-imposed procedures not required by the Privacy Rule

- OCR should issue guidance on the specific steps that providers must take to comply with the access provisions of the Privacy Rule. While the Privacy Rule does not prohibit providers from implementing policies and procedures not required by the law, such policies should not impede patients' ability to access their personal health information. OCR should assess the prevalence of providers who are implementing procedures beyond those required by the Privacy Rule to determine whether any of these policies are actually discouraging patients from requesting records.

In appropriate accountings for disclosures

- As NCVHS suggested, OCR should create an exception to the accounting for disclosures requirement for reports of suspected abuse and neglect.[118] The accounting requirement should not affect how providers make these critical reports; doing so would undermine the spirit of the law, which is to protect patients.

Belief among providers that accounting for disclosures may be overly burdensome

---

[116] The Privacy Rule requires covered entities to "provide a notice that is written in plain language." *See* 45 C.F.R. § 164.520(b)(1).
[117] 45 C.F.R. § 164.506(b)(1)(i).
[118] NCVHS, "Recommendations on the Effect of the Privacy Rule," March 5, 2004, www.ncvhs.hhs.gov/040305l2.htm (accessed on 12/08/05).

- OCR should retain the accounting for disclosures requirement as it stands. The requirement is an important right for patients. It is a fundamental principle of privacy for patients to have information about who has accessed their sensitive health information. To eliminate this right would undermine the Privacy Rule.

Advocates acting on behalf of patients

- The Privacy Rule should not impede legitimate and authorized access to personal health information needed to advocate on behalf of a patient; for example, in a Medicare or Medicaid eligibility administrative appeal hearing. At the same time, a covered entity's authority to deny access to PHI, even with an authorization, to anyone other than the actual patient is an important element of the law. Some advocates have implemented other methods of accessing needed records, such as having patients request personal health information on their own behalf or in the company of the advocate.[119] At any rate, OCR should develop a sample authorization for these purposes that is compliant with the HIPAA Privacy Rule. Furthermore, as some advocates have suggested, the Privacy Rule should be modified to stipulate that the "administrative action or proceeding" exception does not apply when individuals need their personal health information to pursue administrative appeals on their own behalf.[120]

V. Conclusion

Being able to access personal health information is central to the right of medical privacy and a basic tenet of quality health care. Until 2003, the lack of a federal law guaranteeing Americans the right to inspect and amend their health information undermined the quality of health care in the United States. The implementation of the HIPAA Privacy Rule was an important move toward a more effective health care system, in which patients are active participants in their own care. By guaranteeing a federal floor of protection for sensitive health information and granting patients essential rights to accessing and amending their medical record, the Privacy Rule is groundbreaking.

However, the impact of the law has been stifled by inadequate education for providers and patients about responsibilities and rights. While providers appear to have a basic understanding of their responsibilities to grant access under the law, some confusion remains. At the same time, patients are uninformed about their rights under the Privacy Rule. It is critical that OCR immediately launch a public education campaign to ensure understanding and compliance with the law.

[119] Dalin, "Advocacy in a Post-HIPAA World," 2004.
[120] Health Assistance Partnership and National Health Law Program, Letter to Richard Campanelli, director, Office for Civil Rights, U.S. Department of Health and Human Services, August 7, 2003, www.healthassistancepartnership.org (accessed on 12/08/05).

As the health care industry adopts technologically savvy methods of record maintenance and patient communication, patients' access to their personal health information could potentially become easier and more cost-efficient. But as is the case with paper-based systems, whether consumers trust and cooperate with the new technologies will depend on how well their health information is protected.

Appendix A: Individuals Interviewed

Don Asmonga, Government Relations Manager, American Health Information Management Association, June 9, 2004.

Susan McAndrew, Senior Privacy Policy Advisor, U.S. Department of Health and Human Services, Office for Civil Rights, June 14, 2004.

Dan Rode, Vice President of Policy and Government Relations, American Health Information Management Association, June 3, 2004.

Appendix B: Materials Reviewed

American Health Information Management Association (AHIMA). "The State of HIPAA Privacy and Security Compliance," April 2004. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022739.pdf (accessed on 12/05/05).

American Health Information Management Association (AHIMA). "Practice Brief: Provider-Patient E-mail Security (updated)," 2003. http://library.ahima.org/groups/public/documents/ahima/pub (accessed on 12/05/05).

California HealthCare Foundation. "Medical Privacy and Confidentiality Survey," Final Topline, January, 10, 1999. www.chcf.org/documents/ihealth/topline.pdf (accessed on 12/06/05).

California HealthCare Foundation. "National Consumer Health Privacy Survey 2005," Executive Summary, November 2005. http://www.chcf.org/topics/view.cfm?itemID=115694 (accessed on 12/08/05).

Campanelli, Richard, director, Office for Civil Rights, Department of Health and Human Services, Letter to Healthcare Providers, May 17, 2004. www.hhs.gov/ocr/Healthcare-Provider-letter.pdf (accessed on 12/06/05).

Dalin, Hilary Sohmer "Advocacy in a Post-HIPAA World," *BIFOCAL, Bar Associations in Focus on Aging and the Law* 25, no. 2 (Winter 2004):ki1-9.

Denton, Ira C. "Will Patients Use Electronic Personal Health Records? Responses from a Real-life Experience." *Journal of Healthcare Information Management*, Fall 2001, pages 251-259.

Duenwald, Mary. "How Patients Can Use the New Access to Their Medical Records," *New York Times*, May 11, 2004, F1.

Dugan, Kelli M. "Time Spent on E-mail Concerns Many Doctors," *Birmingham Business Journal*, November 8, 2004.

Harris Interactive, Inc. "Patient/Physician Online Communication: Many Patients Want It, Would Pay for It, and It Would Influence Their Choice of Doctors and Health Plans," April 10, 2002. www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2002Vol2_Iss08.pdf (accessed on 12/06/05).

Harris Interactive Inc., "How the Public Sees Health Records and an EMR Program," conducted for Program on Information Technology, Health Records, and Privacy, Center for Social and Legal Research, February 2005.

Hassol, Andrea MSPH, et al., "Patient Experiences and Attitudes about Access to a Patient Electronic Health Care Record and Linked Web Messaging," *Journal of the American Medical Informatics Association* 11, no. 6 (November/December 2004): http://www.pubmedcentral.gov/articlerender.fcgi?tool=pubmed&pubmedid=15299001 (accessed on 12/06/05).

Health Assistance Partnership and National Health Law Program, Letter to Richard Campanelli, director, Office for Civil Rights, U.S. Department of Health and Human Services, August 7, 2003, www.healthassistancepartnership.org (accessed on 12/08/05).

Kolbasuk McGee, Marianne. "E-Visits Begin to Pay Off for Physicians: Some Health Plans and Insurers Will Reimburse Doctors for Online Consultations." *Information Week*, May 31, 2004, NEWS; E-Medicine; Pg. 34.

Lowes, Robert "Phones Driving You Crazy? Try Clinical Messaging," *Medical Economics*, March 19, 2004. http://www.memag.com/memag/article/articleDetail.jsp?id=108571 (accessed on 12/08/05).

Manhattan Research, LLC, "The Connected Physician: E-mail, Communication, and Connectivity," June 2004.

March, Astara "National Health IT System Taking Off," United Press International, November 11, 2005. http://washingtontimes.com/upi/20051110-051125-3618r.htm (accessed on 12/08/05).

Markle Foundation, Connecting for Health. "Americans Want Benefits of Personal Health Records," June 5, 2003. www.connectingforhealth.org/resources/phwg_survey_6.5.03.pdf (accessed on 12/06/05).

Markle Foundation, Connecting for Health, "Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange," October 11, 2005, www.markle.org (accessed on 12/08/05).

Markle Foundation, Connecting for Health: A Public-Private Collaborative, "Personal Health Working Group Final Report," July 1, 2003, www.connectingforhealth.org/resources/final_phwg_report1.pdf (accessed on 12/08/05).

McAndrew, Susan, Senior Privacy Policy Advisor, Office for Civil Rights, Department of Health and Human Services, testimony before the National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality, March 5, 2004; transcript available at www.ncvhs.hhs.gov/040304t1.htm (accessed on 12/06/05).

National Committee on Vital and Health Statistics (NCVHS). Subcommittee on Privacy and Confidentiality Hearing, March 5, 2004; transcript available at www.ncvhs.hhs.gov/040305t1.htm (accessed on 12/06/05).

National Committee on Vital and Health Statistics (NCVHS). "Recommendations on the Effect of the Privacy Rule," March 5, 2004. www.ncvhs.hhs.gov/040305l2.htm (accessed on 12/06/05).

Page, Douglas. "HIMSS Meeting Focuses on Security and Patient Safety." *Diagnostic Imaging*, May, 1, 2004, page 79**.**

Pierce, Bill, **[**HHS Deputy Assistant Secretary for Public Affairs**]**, Department of Health and Human Services. *All Things Considered*, National Public Radio, May 28, 2003; transcript available at www.medem.com/press/press_medeminthenews_detail.cfm?ExtranetPressNewsKey=153 (accessed 12/6/05).

Rode, Dan, Vice President of Policy and Government Relations, American Health Information Management Association, testimony before the National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality, November 19, 2003; transcript available at www.ncvhs.hhs.gov/031119tr.htm (accessed 12/06/05).

Ross, Stephen E., MD, and Chen-Tan Lin, MD. "The Effects of Promoting Patient Access to Medical Records: A Review." *Journal of American Medical Information Association* 10, no. 2 (March 2003): 129–38.

Ross, Stephen E., MD, et al., "Expectations of Patients and Physicians Regarding Patient-Accessible Medical Records," *Journal of Medical Internet Research* 7, no. 2 (2005): e13, www.jmir.org/2005/2/e13/ (accessed on 12/6/05).

U.S. Government Accountability Office (GAO). "Health Information: First-Year Experiences under the Federal Privacy Rule," report to the chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate, GAO-04-965, September 2004.

Westin, Alan. *Privacy and Freedom* (New York: Atheneum, 1967).