Pew Internet & American Life PROJECT

HEALTH PRIVACY PROJECT
INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users

Report of the Pew Internet & American Life Project

November 2001

Prepared by:

Angela Choy, Zoe Hudson, Joy Pritts and Janlori Goldman
Health Privacy Project
Institute for Health Care Research and Policy
Georgetown University
http://www.healthprivacy.org

For more information, please contact:
Janlori Goldman, Director, Health Privacy Project, (202) 687-0880
Susannah Fox, Director of Research, Pew Internet & American Life Project, (202) 296-0019

About the Pew Internet & American Life Project

The Pew Internet & American Life Project is a non-profit initiative fully funded by The Pew Charitable Trusts. The Project creates original research that explores the impact of the Internet on children, families, communities, health care, schools, the work place, and civic/political life. The Pew Internet & American Life Project aims to be an authoritative source for timely information on the Internet's growth and societal impact, through research that strives to be impartial. For more information, please visit our Web site: http://www.pewinternet.org/.

About the Health Privacy Project

The Health Privacy Project is a part of the Institute for Health Care Research and Policy at Georgetown University. The Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. It is funded primarily by the Open Society Institute, the W.K. Kellogg Foundation, the California HealthCare Foundation, the Trellis Fund, the Pew Internet & American Life Project, the Robert Wood Johnson Foundation and the Deer Creek Foundation.

For additional background information on health privacy, please visit the Health Privacy Project's Web site: http://www.healthprivacy.org. Among the resources available:

Virtually Exposed: Privacy and E-Health, *Health Affairs*, November/December 2000.

Health Privacy Principles for Protecting Victims of Domestic Violence, October 2000; *produced by the Family Violence Prevention Fund.*

Health Insurance Purchasing and Privacy Online for Individuals and Small Groups, June 2000; *prepared for the California HealthCare Foundation.*

Privacy: Report on the Privacy Policies and Practices of Health Web Sites, February 2000; *prepared for the California HealthCare Foundation.*

Exposed: A Health Privacy Primer for Consumers, December 1999; w*ith support from the Open Society Institute's Program on Medicine as a Profession.*

Best Principles for Health Privacy, a report of the Health Privacy Working Group, July 1999; *funded by the Robert Wood Johnson Foundation*.

The State of Health Privacy: An Uneven Terrain, a practical, comprehensive guide to state health privacy laws, July 1999; *funded by the Robert Wood Johnson Foundation.*

Promoting Health/Protecting Privacy, a guide to health privacy with an emphasis on California law and practice, January 1999; *funded by the California HealthCare Foundation.*

TABLE OF CONTENTS

Disclaimer

This report is intended to give a general overview of how the federal health privacy regulation may or may not apply to health Web sites. It is provided with the understanding that the authors and publishers are not engaged in rendering legal or other professional services. Such services can only be conducted based on a complete understanding of specific factual circumstances. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The authors, Georgetown University, the Institute for Health Care Research and Policy, and the Pew Internet & American Life Project specifically disclaim any personal liability, loss or risk incurred as a consequence of the use and the application, either directly or indirectly, of any information presented herein.

References to particular health Web sites are made to illustrate the potential application and shortcomings of the federal health privacy regulation in anticipation of the April 2003 compliance date. They are neither criticisms nor legal judgments of policies and practices of specific sites. The report refers to health Web sites as they existed during September 2001. Given the ever-changing nature of the Internet, it is possible that the organization or practices of these sites have changed since that time.

KEY FINDINGS

The new federal health privacy regulation does not apply to most health Web sites.

As part of the Health Insurance Portability and Accountability Act of 1996, Congress included provisions, known as Administrative Simplification, that are intended to facilitate the development of a uniform, computer-based health information system. Recognizing that privacy is an essential component of that system, Congress included a requirement that if it failed to enact health privacy legislation by a legislative deadline, then the Department of Health and Human Services would be required to issue health privacy regulations. However, it imposed constraints on the Department's rulemaking authority, so the federal regulation only applies to three health care entities: health care providers, health plans and health care clearinghouses. Many health Web sites are not owned or operated by one of these three entities. Therefore, while online health care activities that are already conducted offline by a "covered" health care provider or plan will likely be covered by the privacy rule, many other types of health Web sites will fall outside the scope of the rule.

Different rules may apply to different Web sites offering the same services.

Because only Web sites that fit within the definition of a "covered entity" are required to comply with the privacy regulation, specific activities like filling a prescription, receiving e-mail alerts or getting a second opinion may be covered by the new regulation at one site and unregulated at another.

Even at Web sites that are owned or operated by organizations covered by the privacy regulation, it is ambiguous which activities at those sites are subject to the privacy rule.

Many Web sites provide a variety of services, some of which are not considered "health care" functions under the regulation. It is not clear in many cases what activities, even at "covered" sites, may fall outside the scope of the regulation. Consumers may engage in online health activities with the expectation that the personal information they provide to specific health Web sites is protected when, in fact, there are no privacy protections afforded by the federal regulation. The burden will be on consumers and Web site operators to determine which Web sites must comply with the regulation.

OVERVIEW

Individuals share a great deal of personal and sensitive health information in the course of obtaining health care, yet there is little legal protection for health information – online or offline. A substantial barrier to improving the quality of care and access to care is the lack of enforceable privacy rules. In the absence of federal health privacy laws, people have suffered job loss, loss of dignity, discrimination, and stigma. To shield themselves from what they consider harmful and intrusive uses of their health information, individuals have engaged in privacy-protective behaviors, such as providing incomplete information, thereby putting themselves at risk from undiagnosed, untreated conditions. The lack of complete and accurate health information on patients impacts the community as well. Health care information used for important research and public health initiatives downstream becomes unreliable and incomplete.

Congress recognized the importance of protecting people's medical records when it passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA requires the Secretary of the U.S. Department of Health and Human Services (HHS) to issue regulations if Congress failed to enact comprehensive privacy legislation. HHS issued a landmark federal health privacy regulation in December 2000. Health care entities have until April 2003 to implement the new rule. While this regulation is an important step toward boosting the public trust and confidence in our nation's health care system, its application is limited. Due to constraints on the Department's rulemaking authority, the regulation does not cover a significant portion of the health-related activities that take place online.

eHealth is touted as the future of health care, promising to transform the way health care entities conduct business and change the way patients relate to their health care providers. More than sixty-five million American Internet users have sought health and medical information online, and a study last fall by the Pew Internet & American Life Project showed that a significant number of them use this information to make important decisions about medical care for themselves and loved ones.[1] The Internet allows for online communication, and the collection, storage and transfer of consumer health information. These are important features particularly during national emergencies, such as the recent terrorist attacks in New York City and Washington, D.C., when physicians require immediate access to medical information. However, while the Internet can be a powerful tool in the delivery of health care, it enables the collection and distribution of highly sensitive information in new ways by online services. It also can leave such information vulnerable to security breaches.

The HIPAA privacy regulation makes no distinctions between health care online and offline. Hence, some Web sites will be covered by the regulation, and consumers will benefit from the new privacy protections required of these sites. Under the first-ever federal privacy regulation, consumers have a right to inspect and copy their own health information (a right that currently exists only in about half of the states). Consumers will

[1] *The Online Health Care Revolution: How the Web helps Americans take better care of themselves*, Pew Internet & American Life Project (November 2000).

receive notice about how their personal health information will be used and shared with others and what options they have to restrict disclosures. They will have the right to limit disclosures in many circumstances. Furthermore, the regulation creates a new "duty of care" with respect to health information, so in addition to the penalties that can be imposed by HHS, it is possible that violations of the regulation may be grounds for state tort actions.

Our analysis of the HIPAA regulation's impact on eHealth, however, shows that many who engage in online health activities will fall outside the scope of the regulation. We believe that the application of the regulation on the Internet will be greatly uneven. Individuals may assume that their health information is protected when it is not. Continued diligence will be required of those online consumers who value their privacy. Consumers will need to be educated about the limits of the new regulation and empowered to safeguard their most sensitive health information online.

This report is intended to help consumers, health professionals, and policy makers understand how the new federal regulation covers – and does not cover – consumer-oriented health Web sites and Internet-based health care. This report also comments on what new standards will be required for those sites covered by the regulation. The examples used in this report will highlight particular aspects of online health care activities; however, it is important to note that many health Web sites perform numerous functions and therefore do not fit neatly into specific categories.

THE TERRAIN

Health care providers maintain and share a vast amount of sensitive patient information for a variety of reasons. Such records are kept and shared for diagnosis and treatment of the patient, payment of health care services rendered, public health reporting, research, and even for marketing and use by the media. Until recently, most of that information was in paper records.

While a paper-based system has vulnerabilities, it also places some natural limits on the ability of information collectors to share and disseminate information. It is sometimes a challenge to locate paper records, and in order to disseminate the information someone must physically remove it from the premises – either by carrying, mailing or faxing it. These limitations constitute a double-edged sword. They offer some protection from improper dissemination of health information, but also may obstruct the flow of the information when it is being shared for legitimate, health care-related purposes.

The difficulties and expense of transmitting health information in a paper-based system have motivated the health care industry to migrate toward electronic collection, storage and transmission of information, such as via the Internet. Health data can be easily located, collated and organized. With the click of a mouse, sensitive and personal information can be sent to any number of places thousands of miles away.

The new information technologies benefit not only the traditional bricks and mortar health care entities but also consumers. A health care provider's ability to access quickly a patient's entire medical record, assembled from various sources, can facilitate diagnosis and eliminate medical errors, such as prescribing incompatible medications. In fact, electronic health information on the Internet can be easily accessible to many different people, including the patient herself. The electronic medium also facilitates communication between consumers and health care businesses. A wide range of health care activities and services, from general health information to online support groups and personal health management tools, are offered online. Consumers can "surf" the Web for information about symptoms, remedies and health insurance rates. They can obtain health care services, such as second opinions and medical consultations, and products, such as prescription drugs, online.[2] They also can interact with doctors and other users in chat rooms and by e-mail.

Since HIPAA's passage in 1996, there has been an explosion of health-related activity on the Internet. There are thousands of health-related Web sites,[3] and they are

---

[2] *See, e.g.*, David Schwab, "Merck sells $1B Worth of drug online," *The Star-Ledger*, Oct. 16, 2001 (Merck-Medco, which manages prescriptions for sixty-five million Americans sold $1 billion worth of prescription drugs since its Internet pharmacy started three years ago. It expects to sell $750 million worth of prescription drugs online this year).

[3] T.R. Eng, *The eHealth Landscape: A Terrain Map of Emerging Information and Communication Technologies in Health and Health Care*, The Robert Wood Johnson Foundation (2001).

proving popular.[4] In the past two years, it is estimated that the number of people accessing health information online has doubled. As of September 2001, an estimated 61% of Internet users or sixty-five million people in the United States have gone online in search of health information.[5]

However, while the Internet offers unique advantages to both patients and the health care industry, some consumers are afraid to take advantage of the benefits because of privacy and confidentiality concerns. More than 75% of people are concerned about Web sites sharing information without their permission and this impacts their willingness to use the Internet for health-related activities.[6]

I. Public Opinion

Consumers are increasingly worried about the loss of their privacy, and have heightened concerns when it comes to their health information. They worry that their health information may be used or disclosed inappropriately and leave them vulnerable to unwanted exposure, stigma, discrimination and serious economic losses. They fear that their personal information will be used to deny them health insurance, employment, credit and housing. As a result, consumers sometimes take drastic steps to keep their health information private. According to a 1999 survey, almost one out of six U.S. adults have taken extraordinary steps to maintain the privacy of their medical information.[7] They withhold information from their doctors, provide inaccurate or incomplete information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by their insurance, and even avoid care altogether.[8]

Consumers engage in privacy-protective behaviors both online and offline. A study released by the Pew Internet & American Life Project last fall found that:

- An overwhelming majority of Internet users who seek health information online are worried that others will find out about their activities: 89% of "health seekers" are worried that Internet companies might sell or give away information, and 85% fear that insurance companies might change their coverage after finding out what online information they accessed.

[4] A few are ranked in the top 500 most visited Web sites by Media Metrix, a service provided by Jupiter Media Metrix, which measures user activity and site traffic. Jupiter Media Metrix also compiles a top 10 health Web sites list.
[5] Pew Internet & American Life Project survey (August-September 2001).
[6] *Ethics Survey of Consumer Attitudes about Health Web Sites*, conducted by Cyber Dialogue and the Institute for the Future for the California HealthCare Foundation and the Internet Healthcare Coalition (January 2000).
[7] *Confidentiality of Medical Records: National Survey*, conducted by the Princeton Survey Research Associates for the California HealthCare Foundation (January 1999).
[8] *Id*.

- 63% of Internet health seekers and 60% of all Internet users oppose the idea of keeping medical records online, even at a secure, password-protected site, because they fear other people will see those records.

- 80% of health seekers say it is important to them that they can get information anonymously. For the most part, users have not shared personal information at health Web sites: only 21% have provided their e-mail address; only 17% have provided their name or other identifying information; and only 9% have participated in an online support group about a health condition. (Note that 54% of all Internet users have shared personal information at other kinds of Web sites.)

- 81% of Internet health seekers want the right to sue a Web company if it violates its own privacy policy.[9]

The public's concerns are real. A report by the Health Privacy Project in 1999 documented that major health Web sites lack adequate privacy policies, and their practices are often in conflict with their existing privacy statements.[10] For example, third parties may collect personally identifiable information through banner advertisements without host sites disclosing this practice to the user. A subsequent Federal Trade Commission (FTC) investigation of several of these health Web sites found that the sites made changes to their policies in response to the findings of the report. Moreover, many sites do not have adequate security in place to protect consumer information. In recent years, there have been breaches of privacy and security at Web sites of major academic institutions.[11]

II. The New Federal Health Privacy Regulation

Until the release of the federal health privacy regulation, there was little legal protection for health information – online or offline. Unlike financial records, credit reports and even video rental records, there is no comprehensive federal law that protects the privacy of medical records. For online activities, the FTC has the authority to prosecute Web sites that engage in unfair or deceptive practices, such as noncompliance

[9] *The Online Health Care Revolution: How the Web Helps Americans Take Better Care of Themselves*, *supra* note 1.
[10] Janlori Goldman, Zoe Hudson, and Richard M. Smith, *Report on the Privacy Policies and Practices of Health Web Sites*, sponsored by the California HealthCare Foundation (January 2000).
[11] *See* discussion of horror stories *infra* Part VI.

with their own privacy policies.[12] It remains to be seen whether the FTC will take action to challenge sites that say nothing or post poorly drafted privacy policies.[13]

HIPAA required HHS to issue health privacy regulations because Congress failed to enact such legislation by a legislative deadline. After substantial public comment, the Department released the final regulation on December 20, 2000. The privacy regulation was originally scheduled to go into effect on February 26, 2001, but was delayed due to an administrative oversight.[14] On April 14, the Bush Administration allowed the regulation to go into effect but stated that future modifications were likely. The compliance deadline is April 2003 for most of those covered by the regulation.

A. Who and What Are Covered

The privacy regulation is part of a package of regulations mandated by HIPAA that covers privacy, security and electronic transaction standards. Taken together, these regulations are designed to facilitate the development of a uniform computer-based health information system. HIPAA, however, imposed constraints on HHS' rulemaking authority, limiting the scope of the privacy regulation. The regulation does not apply to all persons or entities that have access to personal health information. It only directly covers three different kinds of health care entities:

- Providers, such as doctors, hospitals and pharmacists, who electronically transmit health claims related information[15] in "standard format;"[16]

---

[12] The FTC found in its May 2000 study that about 40 percent of commercial Web sites do not have privacy policies or post poorly drafted privacy policies. *Privacy Online: Fair Information Practices in the Electronic Marketplace*, Federal Trade Commission Report to Congress (May 2000); health Web sites are more likely than non-health related sites to post privacy policies, and indeed many health Web sites do have privacy policies. *See* Goldman et al., *supra* note 10.

[13] FTC Chairman Timothy J. Muris recently stated that the FTC plans to abandon pursuit of online privacy bills but will increase funds for agency enforcement by 50% in the next year. *See* John Schwartz, "F.T.C. Plans to Abandon New Bills on Privacy," *N.Y. Times*, Oct. 3, 2001, at C5; Edmund Sanders, "FTC to Drop Push for More Privacy Laws," *L.A. Times*, Oct. 2, 2001, at C1.

[14] Before major regulations can take effect, they must be formally submitted to Congress for review, which is usually done at the same time that the regulation is published in the Federal Register. The privacy regulation, however, was not sent to Congress until February 13, about six weeks after the regulation was published, so the effective date was postponed until April. *See* Robert Pear, "Health Secretary Delays Medical Records Protections," *N.Y. Times*, Feb. 27, 2001, at A18.

[15] Some of the electronic transactions that trigger a provider's classification as a covered entity include: health claims or equivalent encounter information, enrollment or disenrollment in a health plan; determining eligibility for a health plan; health care payment and remittance advice; and referral certification and authorization. HIPAA, Public Law 104-191, Section 1173, available at http://aspe.hhs.gov/admnsimp/pl104191.htm. All of these transactions are related to health insurance-type transactions.

[16] Health care providers and health plans currently use many different formats to conduct administrative and financial health care transactions electronically. To reduce health care costs and administrative burdens on providers and plans, HIPAA requires HHS to adopt national standards for such transactions. "Standard format" is used throughout this report to refer to the national formats for electronic health care data interchange, which health plans, health care clearinghouses and certain health care providers will be required to comply with by October 2002. For more information about the transaction standards, visit the HHS Administrative Simplification Web site at http://aspe.hhs.gov/admnsimp/bannertx.htm.

- Health plans, such as traditional insurers and HMOs; and

- "Clearinghouses," entities that process health claims information in a uniform format for providers and insurers, such as WebMD Office.[17]

A person or organization that falls within one of these categories is considered to be a "covered entity."[18]

This is a critical factor in determining whether health information is protected under the regulation. Only individually identifiable health information[19] that is transmitted or maintained by a covered entity is protected by the regulation (*i.e.*, "protected health information"). This is true regardless of the format of the information – electronic, paper or oral.

Most health Web sites are pitched publicly as tools that give consumers greater control over their lives and their health care. However, many sites require users to provide a great deal of sensitive health information, and they also may collect information on users without the users' knowledge or consent.

The central issue addressed by this report is whether such activities are covered by HIPAA or not. Our finding is that a significant portion of activities at health-related Web sites are not covered for several reasons. The major reason is that a great many Web sites are run by organizations that are not "covered entities."

In effect, the most popular Web sites, such as eDiets.com[20] and drkoop.com,[21] will remain uncovered by the privacy rule because they are not run by health plans (such as health insurers or HMOs) or covered health care providers.

The result is that the same activities conducted at different Web sites will be subject to different legal treatment. Specific activities – ordering a prescription, getting a

---

[17] http://professional-content.webmd.com/Article.asp?article=article://3834.1081&AuthLevel=2.

[18] *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") § 160.103. The Privacy Rule has been codified at Title 45 of the Code of Federal Regulations. It is available at http://www.hhs.gov/ocr/regtext.html.

[19] Individually identifiable health information as defined in the privacy rule is information that is a subset of health information, including demographic information collected from an individual, and:

(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) that 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.

Privacy Rule, § 164.501, available at http://www.hhs.gov/ocr/regtext.html.

[20] http://www.ediets.com.

[21] http://www.drkoop.com

second opinion, consulting with a doctor, or even maintaining a medical record – may be covered by the new regulation at one Web site and unregulated at another.

Additionally, even Web sites that are run by covered entities engage in diverse activities, many of which are not covered by HIPAA. On these sites it will be difficult for consumers to know what activities are covered by HIPAA and what activities are not.

B. New Requirements

The federal health privacy rule creates new rights for individuals. These rights translate into new responsibilities for some health Web sites that are required to comply with the rule.

1. Access

The privacy regulation gives individuals a new federal legal right to see, copy and correct their own health information. People will also have a right to an accounting of disclosures that have been made to others. Covered entities will be required to respond to an individual's request for access or amendment by a specific deadline (generally 30 days). If the entity denies an individual's requests, there are procedures for reviewing the denial. Because of this new right, online consumers may notice changes in a covered health Web site's privacy policy since these sites may need to develop new policies and procedures for handling requests.

2. Notice

The privacy regulation gives individuals a right to receive notice from covered Web sites as to how their health information is going to be used and shared. Such notices will allow people to make informed, meaningful choices about the uses and disclosures of the health information they provide to Web sites. Under the regulation, consumers must be informed of their rights with respect to their health information and how they may exercise these rights. The notice must include information on anticipated uses and disclosures of personal health information without the individual's written permission as well as the legal duties of the covered entity. Individuals also must be given the name of a contact person at the Web site who will answer queries and provide information on how they can file complaints with the covered entity and HHS.

Because individuals must be given notice of their rights and the new privacy protections, some Web sites will likely have to change their current privacy policies to satisfy federal requirements. A 1999 study of twenty-one leading health-related Web sites had found that the policies and practices of many of the sites did not meet minimum fair information practices.[22] Following the release of the report, several members of Congress requested the FTC to immediately initiate an investigation of whether certain

[22] Goldman et al., *supra* note 10.

health Web sites may be engaged in "unfair or deceptive acts or practices."[23] Nine months later, the FTC closed its investigation, concluding that the sites had made a number of improvements in their privacy policies, although further steps could be taken to develop meaningful privacy protections for consumers.[24] Some of the sites mentioned in the 1999 report, such as drugstore.com,[25] will be required to comply with the notice requirements of the privacy rule by April 2003.

3. Administrative Requirements

Consumers also benefit from the new regulation's administrative requirements. Under the privacy rule, a covered entity will be required to designate a privacy official to develop and implement the entity's policies and procedures;[26] train its employees; implement administrative, technical and physical safeguards;[27] develop a method for handling complaints; and develop sanctions for members of its workforce who fail to comply with its privacy policies or procedures or with the requirements of the rule. The regulation imposes such requirements to ensure that the appropriate members of the covered entity are familiar with and comply with the privacy rule, and that covered entities will be held accountable for the actions of their employees.

C. Restrictions on Use and Disclosure

The new regulation places restrictions on how a covered entity can use and share personal health information with others. In general, the rule prohibits a covered entity from using or sharing a patient's health information unless the covered entity either has the patient's written permission or the regulation specifically allows the use or disclosure.[28]

---

[23] Letter from members of Congress to the Honorable Robert Pitofsky, Chairman of the FTC (Feb. 2, 2000), available at http://www.house.gov/commerce_democrats/press/106ltr84.htm.

[24] *See* letter from C. Lee Peeler, Associate Director, FTC, to Benham Dayanim, Esq., Paul, Hastings, Janofsky & Walker LLP, regarding investigation of HealthCentral.com (Nov. 17, 2000); letter from C. Lee Peeler, Associate Director, FTC, to Sharis A. Pozen, Esq., Hogan & Hartson LLP, regarding the investigation of Healtheon/WebMD (Nov. 17, 2000); letter from C. Lee Peeler, Associate Director, FTC, to Sharis A. Pozen, Esq., Hogan & Hartson LLP, regarding the investigation of OnHealth Network Company (Nov. 17, 2000); letter from C. Lee Peeler, Associate Director, FTC, to Sharis A. Pozen, Esq., Hogan & Hartson LLP, regarding the investigation of WellMed, Inc. (Nov. 17, 2000); letter from C. Lee Peeler, Associate Director, FTC, to Mary Ellen Callahan, Esq., Hogan & Hartson LLP, regarding the investigation of iVillage, Inc. (allHealth.com) (Nov. 17, 2000); and letter from C. Lee Peeler, Associate Director, FTC, to Susan P. Crawford, Esq., Wilmer, Cutler & Pickering, regarding the investigation of Yahoo! Inc. (Nov. 17, 2000). The letters are available on the FTC Web site at http://www.ftc.gov/os/closings/staff/index.htm.

[25] http://www.drugstore.com.

[26] Privacy Rule, § 164.530(a), available at http://www.hhs.gov/ocr/regtext.html.

[27] For example, to protect identifiable information maintained at a Web site, a covered entity might develop a secure password system and encrypt data to protect the information transmitted from one computer to another or through a network.

[28] The regulation provides for two distinct types of patient permission – "consent" and "authorization." A health care *provider* (such as a doctor, hospital or pharmacist) *must* obtain a patient's *consent* before using or disclosing her health information for treatment, payment or health care operations. A provider may condition providing treatment on a patient's signing the consent form. In contrast, any covered entity must obtain a patient's authorization (a more detailed, specific permission form) to use or disclose health

1. Treatment, Payment and Health Care Operations

One of the most significant restrictions on covered health care providers, whether bricks and mortar or Internet-based, is the requirement that they obtain patients' written permission to use or disclose their health information for treatment, payment, or health care operations. For example, both the local bricks and mortar CVS drug store and CVS.com[29] will be required to obtain written permission to use an individual's information to fill her prescription. In contrast, an online pharmacy that fills the same prescription but is not covered by the regulation, such as ABeeWell Pharmacy,[30] would not be required to obtain the patient's written permission since it does not accept insurance.[31]

2. Business Associates

Health plans and providers routinely hire other companies and consultants to perform a wide variety of functions for them, such as legal, financial and administrative services (the privacy rule refers to these as "business associates"). They receive health information on behalf of or from a covered entity. In general, they are not directly covered by the privacy regulation.

To ensure that privacy protections follow the data, the privacy rule requires that covered entities enter into contracts with business associates that require the recipients of health information not to use or disclose the information other than as permitted or required by the contract or as required by law, and to implement appropriate safeguards to prevent inappropriate uses and disclosures. The regulation establishes specific conditions on when and how covered entities may share information with business associates.[32] However, the business associate is not directly subject to the privacy rule. Rather, it is the covered entity that is liable for violations of the contract, and then only if it had actual knowledge of the breach yet did nothing to remedy it.[33]

3. Marketing

One of the more controversial aspects of the privacy rule is that it permits the use

---

information for a purpose other than treatment, payment, and health care operations that is not otherwise specifically permitted by the privacy rule. For instance, a provider would need a patient's authorization to disclose health information to a life insurer. *See* Privacy Rule, §§ 164.506 and 164.508, available at http://www.hhs.gov/ocr/regtext.html.

[29] http://www.cvs.com.

[30] http://www.abeewell.com.

[31] Because these online pharmacies do not accept any insurance, it is unlikely that they engage in the type of HIPAA standard transaction that would trigger application of the privacy regulation to its online activities. *See* discussion on covered Web sites *infra* Part III.

[32] Privacy Rule, § 164.504(e)(2), available at http://www.hhs.gov/ocr/regtext.html.

[33] While health care clearinghouses are *directly* covered by the privacy regulation, in many cases they will be acting on behalf of a provider or insurer, and therefore would be considered business associates of that provider or insurer as well. However, they will be directly liable for violations of the business associate contract and thus violations of the regulation.

of health information for marketing purposes without the patient's affirmative, informed permission.[34] Once a patient has given written permission to use her health information for "treatment, payment and health care operations" purposes, a provider (such as an online pharmacist) can then use her health information to market its own products and services as well as those of third parties. There is no requirement that this consent form notify the patient that by signing the form she is giving permission to use her information for marketing purposes. Furthermore, the provider may condition the provision of treatment, such as filling a prescription, on the patient's signing this form. In its initial marketing contact, the provider must give the patient the opportunity to opt out of receiving such materials in the future. This scheme essentially gives providers "one free shot" at marketing without a patient's informed permission.

For example, CVS or CVS.com could compile a list of Prozac consumers and send them marketing information about an alternative anti-depressant on behalf of a pharmaceutical company, so long as the initial marketing information told patients that they could decline future marketing materials.[35] The privacy rule draws the line, however, at sharing information with *others* for marketing purposes. It does not permit covered entities to share customer information with other parties for marketing unless the patient has signed another, detailed form stating that she gives permission for her information to be shared in this manner. For instance, CVS could not *sell* its list of Prozac users to the pharmaceutical company or to a telemarketer without all of the patients' specific permission to use and share their information for marketing. In contrast, an online pharmacy that is not covered by the regulation can compile and sell patient lists, subject only to the restrictions of its own privacy policy.

D. Enforcement and Penalties

HIPAA establishes civil and criminal penalties for violations of the privacy regulation. Civil penalties range from $100 to a maximum of $25,000 per year for each standard that is violated. Criminal penalties are imposed for certain wrongful disclosures of health information with a maximum of 10 years imprisonment and/or a $250,000 penalty, depending on the offense committed.

There is no federal statutory right for a patient to sue under the regulation but it does create a new federal "duty of care" with respect to health information. That means violations of the privacy rule may be grounds for state tort actions.

---

[34] "Marketing" is a communication about a product or service that is intended to encourage recipients of the communication to purchase or use the product or service. The definition generally excludes communications that are part of the normal treatment activities of a health care provider. Marketing generally *excludes* communications that are made to individuals to describe health plans or health benefits. It also excludes communications that are made within the context of treating the individual for the purpose of treatment or for directing or recommending to the individual alternative treatments, providers or settings. However, if such a communication is in writing and the provider receives remuneration it is considered to be a marketing activity. Privacy Rule, § 164.501, available at http://www.hhs.gov/ocr/regtext.html.

[35] There are also other requirements, such as the communication must identify the source of the marketing material. Privacy Rule, § 164.514(e), available at http://www.hhs.gov/ocr/regtext.html.

Any person who believes a covered entity is not complying with the privacy rule also may file a complaint with the Secretary of HHS. Covered Web sites will be required to cooperate with HHS and to provide records and compliance reports to the Department. The Office for Civil Rights at HHS has been given the authority to enforce the regulation.

III. Covered Web Sites

A. Providers and Insurers[36]

The privacy rule covers health plans and health care providers that transmit health information electronically in a standard format. Once an entity is a "covered entity," it is subject to the new regulation whether it is conducting business on or offline.

It should be fairly easy to tell whether a health plan is a covered entity. The term "health plan" is broadly defined in the regulation and covers just about anyone that provides or pays the cost of medical care. It covers fee-for-service insurers, HMOs, Medicare and Medicaid programs, issuers of long-term care policies, group health plans and others. Given this broad definition, it is fairly likely that a Web site hosted by a health insurer or HMO will be a covered health plan under the regulation.

Aetna U.S. Healthcare, for example, is a covered health plan with a Web site[37] that allows members to view their personal health information, check the status of a claim, make changes in primary care physicians, and seek replacements of ID cards. The information collected and maintained by the site would be covered by the regulation.

It will be more difficult for consumers to tell whether any given provider is subject to the regulation, since not all health care providers fall under the definition of "covered entity." To determine whether a person or organization is a covered provider under the privacy rule, a consumer would need to answer three key questions:

1. Is the person or organization a health care provider as defined by the rule?
2. Do they transmit health information in connection with one of the financial or administrative "standard transactions" listed in HIPAA?
3. Do they transmit that information electronically in the required "standard format"?

A provider is only covered by the privacy rule if the answer to *all* of these questions is "yes." Answering even the simplest of these questions, however, may not be as easy as it appears.

As defined in the privacy rule, the term "health care provider" covers most of the

[36] Health care clearinghouses are covered entities under the regulation. However, as a practical matter, whether a clearinghouse is a covered entity would be irrelevant to most consumers, since they do not generally have direct contact with them. *See* discussion on business associates *infra* Part IV.B.
[37] http://www.aetna.com/members/index.html.

people and organizations that consumers traditionally think of as providers. It includes any person who furnishes, bills or is paid for health care in the normal course of business. Thus doctors, counselors, clinics, hospitals, nurses and similar persons and organizations are, not surprisingly, considered to be health care providers under the regulation.

As for those who furnish health-related supplies, the rule applies *only* to those who sell or dispense these items pursuant to a *prescription*.[38] Under this requirement, a pharmacist, such as CVS, is a health care provider, while a Web site that sells books and tapes on losing weight, such as eDiets.com, is not. Similarly, a pharmaceutical company is not a health care provider since it does not sell or dispense drugs pursuant to a prescription.

If a person or an organization is a "health care provider" under the regulation, the next question to ask is whether it engages in the type of "standard transactions" that will bring it within the scope of the privacy rule. Since the intent of the administrative simplification provisions of HIPAA (including the privacy rule) is to simplify the processing of health insurance claims, the privacy rule applies only to providers who conduct insurance related transactions. Some of the electronic transactions that trigger application of HIPAA to a provider include: submitting health claims or equivalent information related to physician-patient interactions; determining eligibility for a health plan; receiving health care payment and remittance advice; and receiving referral certification and authorization. All of these transactions are related to health insurance-type transactions.

In a very general sense, this question can be boiled down to: "Does the provider accept health insurance (including Medicaid) or participate in an HMO?" If the answer to this question is yes, it is likely that the provider will engage in the type of standard transactions necessary to bring her within the scope of the privacy rule.

Even if a provider does engage in standard transactions, that still leaves the last, and perhaps the most difficult, question to answer: "Does the health care provider transmit information in relation to these standard transactions electronically in the required standard format?" If a provider transmits health information electronically in relation to any of these standard transactions, such as verifying insurance coverage or filing a health claim, HIPAA requires the provider to use a standard electronic format (*i.e.*, the provider must include certain information and use specified codes for diagnosis and treatment).[39] Currently, October 2002 is the deadline for compliance with the requirement for adopting the standard format. HHS has taken the position that only providers who actually use the required format are covered by the privacy rule.

If a provider has an online presence and accepts insurance, it probably will be safe

---

[38] The privacy rule applies to providers of health care. The rule defines "health care" as including the sale or dispensing of a drug, device or other equipment, or item in accordance with a prescription. Privacy Rule, § 160.103, available at http://www.hhs.gov/ocr/regtext.html. "Health care" therefore does not include over-the-counter drugs.

[39] *See supra* note 16.

to assume that she transmits the required type of information electronically. But how a consumer is to determine whether a provider uses the standard format is problematic.

It becomes apparent how difficult it is to know whether a provider is covered when the test is applied to an actual site – for example, PatientSite,[40] a Web site created by CareGroup HealthCare System, a network of six hospitals in Massachusetts. PatientSite allows patients to communicate with their physicians through the Web. These electronic communications become part of the patient's medical record. In addition, the site allows patients to check insurance benefits, refill prescriptions, request referrals, review lab results and make appointments. Notably, these are online health care activities that the provider already conducts offline. But is PatientSite run by a health care provider covered by the privacy regulation?

The answer is "maybe." PatientSite appears to be directly operated by a network of hospitals that clearly would be health care providers under the regulation. Additionally, the providers accept insurance. Its status as a covered entity, however, is not definitive – it is not clear from the Web site if or when CareGroup will use the standard format that is required in order to be covered by the privacy rule. Currently, providers do not have to use the standard format until October 2002, and there has been extensive lobbying to extend that date. It is only once a provider meets all three of the required criteria that it becomes a covered entity, and the information collected at its site would be protected by the regulation.

IV. Partially Covered and Indirectly Covered Web Sites

A. Sites with Multiple Activities

As covered entities establish an online presence, their online collection and transmission of personal health information will be regulated by the privacy rule. Even if a company is a covered entity, however, it is not obvious whether all information collected by the entity at its Web site is covered. Most health-related Web sites engage in a number of different activities, from providing general educational health information to allowing patients to review test results online. Only some of these activities will be protected by the privacy regulation. For example, drugstore.com sells both drugs pursuant to a prescription and over-the-counter products. While information related to the prescription drug will be covered by the privacy regulation, information related to the over-the-counter product will not. The privacy rule covers only identifiable information related to "health care." This term does not include selling or distributing non-prescription health care items.

This scenario could pose serious concerns for some online patients. Consumers often use the Internet to purchase health items with the belief that their purchase will be

[40] http://patientsite.caregroup.org/default.asp.

anonymous.[41] Drugstore.com, for example, sells sexual enhancement items that a customer would find difficult to locate in a bricks and mortar pharmacy.[42] Yet, information related to these over-the-counter items is not protected by the privacy rule. For instance, an HIV/AIDS patient can purchase AZT and condoms at Drugstore.com in one transaction and have them both shipped at the same time. Yet only information related to the AZT purchase will be protected by the privacy regulation.

The posting of a notice of privacy practices at the Web site, as required by the federal privacy rule, may compound the problem. A customer may read the notice and believe that it applies to the entire Web site, as opposed to just certain activities.

The issue becomes even more ambiguous when a site operated by a covered entity offers general health information for "educational" purposes. For example, Cleveland Clinic has a Web site,[43] a small portion of which functions as an extension of its offline health care activities. Patients can request an appointment online, for instance. Assuming that Cleveland Clinic will be a covered provider under the regulation, these activities would be covered by the privacy rule. However, a significant component of the site[44] is information-based and furnishes information on a wide spectrum of health conditions. Individuals can sign up at the "health information" component of the site to receive e-mail alerts on specific health topics of interest, including sensitive medical conditions such as AIDS, alcoholism and incontinence. Is the fact that a person has registered to receive this type of health information from a covered provider protected by the privacy rule?

It is not clear. The question centers on whether the personal data provided in registering to receive information on a specific health topic would be considered "individually identifiable health information" under the privacy rule, since this is the only type of information that is protected. To be protected, identifiable information must relate either to the health or condition of a person or to the provision of health care to a person.[45] The Cleveland Clinic takes the position that it does not provide health care by furnishing health information via e-mail.[46] And it is unclear when a person merely asks for information on a health topic whether they are relating health information about themselves.

Why would signing up to receive health information on a medical topic, however,

---

[41] *See e.g.*, C. Frey, "Online Shopper; When Privacy Matters; If buying condoms or adult diapers embarrasses you, try a Web drugstore," *L.A. Times*, June 14, 2001, at T-4, which actually encourages consumers to shop for embarrassing products on the Web.

[42] *See* the Specialty Shops at http://www.drugstore.com.

[43] http://www.clevelandclinic.org.

[44] http://www.clevelandclinic.org/health.

[45] The information also must be created or received by a covered entity.

[46] The privacy policy at the health information portion of Cleveland Clinic's Web site states in part: "please remember that medical information provided by The Cleveland Clinic Foundation, in the absence of a visit with a health care professional, must be considered as an educational service only. The information sent through e-mail should not be relied upon as a medical consultation." Available at http://www.clevelandclinic.org/health/popupprivacy.htm.

be any different from a trip to the library to obtain information on a specific disorder? The privacy rule itself is ambiguous, and HHS has not issued any guidance on this topic.

In short, a health care consumer should not assume that all information that she provides at a Web site run by a covered entity will be protected by the privacy rule.

B. Business Associates

Health plans and providers routinely hire business associates. Business associates receive health information on behalf of or from a covered entity, but they are not directly covered by the privacy rule. Rather, the burden is on the covered entity to ensure through contracts that the business associates protect the health information that they receive.

Some of the most promoted and publicized Web sites, such as MedicaLogic,[47] which recently merged with Medscape, may be considered "business associates" by the new regulation. MedicaLogic allows physicians to create online medical records. MedicaLogic would be a business associate of covered health care providers that use its online services. And information stored at MedicaLogic's site would only be indirectly protected by the privacy rule.

As a general matter, health information collected by a business associate should receive some indirect protection under the privacy rule. If the business associate does anything improper with the health information, the covered entity would be expected to cancel its contract, if possible. However, HHS does not have the ability to impose any civil or criminal fines directly against a business associate. The business associate contract should provide adequate protection, but what happens when a Web-based business associate files for bankruptcy and its only valuable asset is the information that it has collected on patients?[48]

V. Web Sites Not Covered

Every day people go online to get information about a medical condition or symptom, fill a prescription, get an insurance quote, participate in a chat room, or fill out a health assessment. All of these activities involve the exchange of information with or without the consent of the individual, and with or without their knowledge. For users

---

[47] http://www.medicalogic.com/.

[48] There is no definitive answer to this question, since the issue of selling customer data lists when a company goes bankrupt has only been addressed outside of the courtroom. For example, when Toysmart.com, an online toy seller, went bankrupt, the company advertised an asset auction that included its customer database as an auction item, even though its privacy policy had promised not to disclose customers' data to outside parties. The Federal Trade Commission filed a lawsuit against Toysmart, and ultimately Walt Disney, a major investor in Toysmart, agreed to buy and destroy the information. Similarly, when the online furniture seller Living.com went bankrupt, the Texas Attorney General sued the company to prevent it from selling customer data. On the same day, Living.com agreed to destroy all customers' financial records. Kim Peterson, "Don't count on privacy if you're on the Internet," *San Diego Union Trib.*, Jan. 13, 2001, at A1.

concerned about protecting their privacy, *where* they go (*i.e.*, what sites they visit) will determine whether there are enforceable rules about how their health information is protected. More often than not, however, users will be getting health information and services from Web sites that are not covered at all by the new federal health privacy regulation. Here are some examples of Web sites that are not covered.

A. Sites Providing General Health Information

Some of the most popular health Web sites are information-based. In other words, they provide people with information about general fitness and nutrition (*e.g.*, www.foodfit.com), medical conditions (*e.g.*, www.drkoop.com), and treatment options (*e.g.*, www.medigenesis.com). Some offer a broad range of information, while others specialize in a certain drug or medical condition. They do not have an offline existence where they engage in covered activities like treating patients. They only furnish health information – they do not provide "health care," as it is defined in the federal regulation.[49]

Some sites offer additional services that require users to provide personal information to the site. Many Web sites offer a "health assessment" feature where users may enter all sorts of information from height and weight to drug and alcohol use. The personal health information that consumers provide to many of these sites (*e.g.*, through self-screening questionnaires or registration for e-mail reminders) will not be protected by the privacy regulation. For example, HealthStatus.com offers free general health assessments as well as disease specific assessments to determine an individual's risk for some of the leading causes of death.[50] Does this constitute health care? HealthStatus.com's disclaimer makes clear its belief that the site does "not provide medical advice or treatment."[51] It is not so clear that HHS would agree with this assertion. However, because HealthStatus.com does not accept any insurance it will not be covered by the privacy rule.

Prozac.com, a Web site owned by the drug company Eli Lilly and Co., provides information about depression. Until recently, individuals could sign up for an Internet service that would send them e-mail reminders about taking their medication. Eli Lilly and Co. is not a covered entity so health information consumers provide to prozac.com is not protected by the privacy regulation.[52] The key is that the e-mail reminder originates from someone who is not covered by the privacy rule. If, in contrast, a covered physician sent a patient an e-mail reminder that it was time for her annual mammogram, the e-mail would be covered by the privacy rule.

---

[49] Privacy Rule, § 160.103, available at http://www.hhs.gov/ocr/regtext.html.
[50] http://www.healthstatus.com/assessments.html.
[51] http://www.healthstatus.com/disclaimer.html.
[52] Because pharmaceutical companies do not sell or distribute drugs pursuant to prescription (unlike drug stores) they do not provide health care and are not covered by the privacy rule. *See* Privacy Rule, § 160.103 (defining "health care"), available at http://www.hhs.gov/ocr/regtext.html.

Users also may give Web sites personal information when they provide an e-mail address to obtain more information about a certain health topic. For example, users can receive free diet and nutrition-related information from eDiets.com by entering their e-mail address at the site. This information would not be covered by the privacy rule.

A user might participate in a chat room where her e-mail address is used as well. Or, a site may have banner advertisers that collect information without users ever knowing. Many of these sites track users through cookies.[53] Cookie files allow a Web site to know when a user has visited a site and each page the user visits to create online user profiles. User profiles help sites determine what information, products and services are used by the visitors. They also allow sites to deliver specific content to users based on their previous online activities. Although cookies are only numbers assigned by a site to each user, personal data can be linked to the number when an individual provides identifiable information to the site (*e.g.*, completing health assessments). A 1999 study of health-related Web sites found, however, that profiling is not generally disclosed or explained to visitors of a site.[54] The end result is that the Web site owner – and possibly third parties – has a great deal of health-related information that can be attached to a particular person without the person's knowledge or consent. But the sites are bound by nothing more than their own privacy policies.

B. Sites for Purchasing Health-related Products

The press has been filled with stories about rogue Web sites selling drugs without a legitimate prescription.[55] Many of these "pharmacists" only do business online. They specialize in drugs that treat sensitive or embarrassing conditions – like Viagra for impotence[56] and Propecia for hair-loss[57] – that a patient may not ask for from his doctor. There also are sites that provide online prescriptions for products that are not always easy to obtain, like the "morning after" pill.[58] The recent public scare of biological warfare prompted by the September 11 attacks has popularized Web sites that offer Cipro, an antibiotic used to treat bacterial infections, including anthrax.[59]

The sites allow people to purchase a drug if they fill out a health assessment. The transaction may include a fee for an online "consultation" with a doctor. Most importantly, however, the sites require payment for the entire transaction via credit card.

---

[53] Cookies are small text files a Web site places on a computer's hard drive so the site can collect information about a person's visit.

[54] Goldman et al., *supra* note 10.

[55] *See e.g.*, A. Fawcett, "Online Rx," *Atlanta J. & Const.*, Aug. 7, 2001, at 1C; R.J. Ignelzi, "Risky prescription; Online drug buyers gamble with more than their credit cards," *The San Diego Union-Trib.*, Aug. 6, 2001, at E1; G. Wheelwright, "Inevitable marketplace for lifestyle drug: Online Viagra Sales," *Fin. Times*, Feb. 21, 2001, at 11. S. Coburn, "A Web Bazaar Turns Into a Pharmaceutical Free-for-All," *N.Y. Times*, Oct. 25, 2000, at H20; J.A. Karash, "More prescriptions are being filled on the Net. It's buyer beware when getting medications online," *Kan. City Star*, Oct. 22, 2000, at G1.

[56] *See, e.g.*,http://www.at-home-viagra.com.

[57] *See, e.g.*, http://www.propeciapharmacy.com.

[58] *See, e.g.*, http://www.virtualmedicalgroup.com.

[59] *See, e.g.*, http://www.2-buy-cipro-online-4-anthrax-bacteria-resistance.com; s*ee* Julie Appleby, "Web sites market antibiotic to treat anthrax," *USA Today*, Oct. 11, 2001, at 1B.

They do not accept health insurance. It is important to note that the distinguishing factor here is not that the information is being obtained online, but that the pharmacist never processes health claims information in standard format, and therefore, is not a "covered entity" under the regulation. By refusing insurance, these sites remain outside the scope of the federal privacy regulation.

The vigilant patient might better protect her privacy by filling her prescription at a site that takes insurance – such as CVS.com or drugstore.com. Here, even if a person pays out-of-pocket, her information will be protected by the regulation.

Web sites that sell only non-prescription health products, such as healthandbeautydepot.com, also fall outside the scope of the privacy regulation – they are not covered entities. The sale of non-prescription health products is not considered "health care," whether it takes place online or at a local drugstore. Hence, identifiable health information disclosed when purchasing over-the-counter allergy medicine, for example, is not protected health information.

C. Sites Providing Health Care "Treatment"

Some Web sites provide health care but *still* are not covered by the regulation. Why? They do not accept health insurance. Only providers that process health claims electronically in a standard format are covered by the regulation. What does this mean for consumers? Simple activities like filling a prescription online may not be covered by the regulation.

Another example is online counseling. Some Web sites now allow users to participate in a therapy session online. These sites also tend to be "credit card only." Here2listen.com[60] and cyberanalysis.com[61] are examples of Web sites that offer online consultations.

At here2listen.com, individuals can select a participating therapist from the here2listen.com database to conduct sessions online based on the counselor's education, geographic location or fee level. The site accepts credit cards as payment for the counseling service. Insurance is not accepted through the Web site. This site appears to be acting as a referral service for the counselors. For some counselors, it appears that the online counseling is an extension of their offline practice. Although the counselors on this site are clearly "health care providers," it is unclear whether they are required to comply with the regulation. A health care provider must meet specific criteria to be covered by HIPAA. Do they ever accept health insurance (such as in their offline practice)? If so, do they process claims information electronically? Is the information transmitted in the required standard format? If the counselors transmit health claims type data electronically in standard format, they are covered entities and the privacy regulation would apply to their online counseling activities. The Web site itself would be a business associate, since it receives health information on behalf of the covered providers.

[60] http://www.here2listen.com.
[61] http://www.cyberanalysis.com.

Cyberanalysis.com presents a slightly different format for online counseling services. At cyberanalysis.com, patients can make arrangements to communicate with participating doctors by cyber chat, e-mail, videophone or telephone. An important point about this Web site is that it is *not* a referral service but is actually a virtual counseling center that has analysts on staff. Thus, the critical question here is whether the Web site itself is a covered entity. Since it does not accept health insurance, the site and the counseling that takes place on the site, would not be covered by the privacy rule.

In both of these instances, a person's desire for anonymity may ironically leave her more vulnerable to exposure. It is important to note that while consumers often lie, withhold information, or mask their identity on the Web to maintain anonymity, in these examples, they may be forced to identify themselves. To get the service, an individual will be required to provide her name, credit card number and a mailing address.

Another type of online health service that consumers may consider health care is clinical trial recruitment. At ClinicalTrials.com,[62] individuals can register for e-mail updates about clinical trials and learn about current trials by providing their name and address and selecting the medical condition(s) of interest. ClinicalTrials.com falls outside the scope of the privacy regulation – it is neither a covered entity nor a business associate.

AmericasDoctor[63] engages in slightly different activities – it offers information about clinical trials and recruits patients for its own investigative sites as well as non-AmericasDoctor trial sites. AmericasDoctor is not a covered entity because it is not engaged in providing health care so the health information collected on its Web site would not be protected by the regulation. It is not obvious from the site, however, whether or not AmericasDoctor might be considered a business associate when it assists non-AmericasDoctor study sites with patient recruitment. If the Web site is recruiting patients for a covered entity engaged in clinical research, it might be a business associate and, therefore, identifiable health information collected by the site with respect to that trial would be protected by the regulation under a business associate contract. If the physicians or hospitals are not covered entities, then the privacy regulation's restrictions on use and disclosure will not apply to AmericasDoctor.

D. Patient-driven Sites

Many hope that online health care puts patients in the driver's seat by giving them access to more information, and indeed many Web sites do give patients more information. Some even offer health management tools like online medical records. But sites that are *exclusively* controlled by patients are not covered by the new privacy regulation. Individuals may unknowingly make "protected health information" *un*protected when they take information from their doctor and give it to a Web site. For

[62] http://www.clinicaltrials.com.
[63] http://www.americasdoctor.com.

example, sites where the patient acts as the intermediary between providers may not be covered.

Consider the following two examples: online second opinions and online medical records. Online second opinions allow patients to obtain expert medical advice in the comfort of their homes. Cancer patients, for example, can release their medical records to MDExpert.com,[64] which has a network of over 200 cancer experts who offer second opinions after reviewing the medical records. The expert dictates or e-mails her opinion to MDExpert, where it is reviewed by MDExpert's medical director and a consulting physician. The opinion is then compiled into a report with clinical trials information, reference information and patient education materials and is sent to the primary physician for review and discussion with his or her patient. A second opinion from MDExpert.com is payable only by credit card, which suggests that the site is not a covered entity, and therefore that its online activities do not fall within the scope of the privacy regulation.

There are also sites that allow consumers to create their own medical records online. For example, PersonalMD.com[65] enables patients to manage all of their medical information on one site, which the patient can access from anywhere in the world. The site is storing this information on behalf of the patients, not their doctor.[66] Personal files can include records of visits to the doctor or hospital, lab reports, medications, allergies, family history and immunizations. The information is provided by the patient in a variety of ways (such as via fax and direct entry). The site, however, is not covered by the privacy rule – it is not a provider, a health plan or a health care clearinghouse. Patients who use these sites essentially are relying on the site's own privacy policy for protection.

Patients may also authorize their doctor to send health information directly to PersonalMD.com for inclusion in their online medical record. The fact that the information is transmitted to the site by the doctor does not change the situation—it loses its protection under the privacy regulation once it leaves the doctor's office.[67] In fact, the privacy regulation recognizes that this can occur and requires that authorization forms include a statement that health information released pursuant to the authorization may no longer be protected by the privacy rule.[68] PersonalMD.com has strict policies against the sharing of personally identifiable information without an individual's permission,[69] but privacy policies are not required by law and they are subject to change at any time. Furthermore, PersonalMD.com advertisers or Web sites that have links on

---

[64] http://www.mdexpert.com.
[65] http://www.personalmd.com.
[66] In contrast, some sites store and manage health information on behalf of doctors. These sites are treated differently under the regulation. *See* discussion under "Business Associates," *supra* Part IV.B.
[67] *See* Privacy Rule, § 164.508(c), available at http://www.hhs.gov/ocr/regtext.html.
[68] *See id.*
[69] The PersonalMD privacy policy states, "As a general rule, PersonalMD will not disclose any of your personally identifiable information without your permission. The exception shall be under special circumstances, such as when we believe in good faith that the law requires it or under the circumstances described below…. PersonalMD will never rent or sell your health-related information. This site has security measures in place to protect the loss, misuse and alteration of the information under our control." Available at http://www.personalmd.com/privacypolicy.shtml.

PersonalMD.com may collect personally identifiable information about individuals, but these third party sites are not required to comply with PersonalMD.com's privacy policy.

VI. Putting It All Together

A. "Horror Stories"

News stories have highlighted various types of privacy violations related to health information. The new federal privacy regulation will address only some violations of privacy that can occur online. The following examples are violations previously reported by the press. None of them are covered by the privacy regulation since compliance with the regulation is not required until April 14, 2003. They are used to illustrate how the regulation would cover and not cover similar violations after the compliance date.

> A hacker downloaded medical records, health information and Social Security numbers on more than 5,000 patients at the University of Washington Medical Center. The hacker claimed to be motivated by a desire to expose the vulnerability of electronic medical records.[70]

After April 14, 2003, a penalty could be imposed on a covered medical center in similar circumstances if the Secretary of HHS determines that the covered entity failed to comply with the requirements of the privacy regulation. The regulation requires covered entities to put in place administrative, technical and physical safeguards to protect the privacy of protected health information, and reasonably safeguard such information from intentional or unintentional use or disclosure. In addition, HIPAA mandates the Secretary of HHS to adopt security standards to protect the confidentiality and integrity of individual health information. These standards are expected to be issued in final form in 2001.

> Global Health Trax sells over-the-counter health and nutrition supplements online. It inadvertently revealed customer names, home phone numbers, and bank account and credit card information of thousands of its customers on its Web site.[71]

A company like Global Health Trax in all likelihood would not be considered a covered entity or a business associate of a covered entity. Therefore, the privacy regulation would not apply to any information collected by that company.

---

[70] This incident is an example of an external security breach. R. O'Harrow, "Hacker Accesses Patients Records," *Wash. Post*, December 9, 2000, at E1; a year earlier, at the University of Michigan Medical Center, several thousand patient records inadvertently lingered on public Internet sites for two months – example of an internal security violation. "Black Eye at the Med Center," *Wash. Post*, February 22, 1999, at F5; similarly, detailed psychological records concerning visits and diagnoses of at least sixty-two children and teenagers were accidentally posted on the University of Montana Web site for eight days. C. Piller, "Web Mishap: Kids' Psychological Files Posted," *L.A. Times*, November 7, 2001, at A1.

[71] B. Sullivan, "Bank Information Exposed Online," MSNBC, January 19, 2000.

> SelectQuote Insurance Services exposed some of its customers' personal information, including health information, on its Web site. Information that was submitted by users to obtain life insurance quotes was not "cleared," and thus remained on the site and could be viewed by subsequent users.[72]

Life insurance brokers, like SelectQuote Insurance Services, are not covered entities, so they fall outside the scope of the privacy regulation. Their customers' health-related information, therefore, would not be protected by the privacy rule.

> Eli Lilly and Co. inadvertently revealed 600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac. In the past, the e-mail messages were addressed to individuals. The message announcing the end of the reminder service, however, was addressed to all of the participants.[73]

A pharmaceutical company, like Eli Lilly and Co., is not a covered entity. Therefore, a breach of confidentiality would not be covered by the privacy regulation.

> The hospital records and photograph of an Illinois woman were posted on the Internet without her knowledge or consent a few days after she was treated at St. Elizabeth's Medical Center in Granite City following complications from an abortion at the Hope Clinic for Women. The woman has sued the hospital, alleging St. Elizabeth's released her records without her consent.[74]

Many hospitals will eventually engage in the type of standard transactions that would bring them within the scope of the federal privacy regulation. A covered hospital that makes unauthorized disclosures would be in violation of the privacy rule and thus may be subject to penalties under the regulation. Similarly, it would be a violation of the privacy rule if the covered hospital had lax procedures for storing medical records that facilitated this information's being improperly disclosed.

Civil fines under HIPAA are $100 per standard violated with a maximum of $25,000 per year.[75] Furthermore, a person who knowingly discloses individually identifiable health information in violation of HIPAA could be fined as much as $50,000, imprisoned not more than one year, or both. If HHS determines that the offense was committed with the intent to transfer the information for malicious harm, then greater penalties may be imposed.

---

[72] M. Bunker, "Insurance Site Exposes Personal Data," MSNBC, March 22, 2000.
[73] R. O'Harrow, "Prozac Maker Reveals Patient E-Mail Addresses," *Wash. Post,* July 4, 2001, at E1.
[74] T. Hillig and J. Mannies, "Woman Sues Over Posting of Abortion Details," *St. Louis Post-Dispatch*, July 3, 2001, at A1.
[75] For example, if a hospital erroneously disclosed the records of 1000 patients in a single incident, it potentially could be fined $25,000.

VII. Conclusion

More health-related information is being collected and shared about individuals than ever, and until the release of the federal health privacy regulation in December 2000, there were almost no federal legal limits on how this information could be used and disclosed. By focusing on electronic transactions, the privacy regulation required by HIPAA aimed to give consumers confidence that as the health information system moved to a networked, electronic, computer-based system, their most sensitive health information will be protected. However, the HIPAA rule only applies to health plans, health care providers and health care clearinghouses, so it may create an illusion of legal protection that may lull consumers into a false sense of security when they engage in online health activities. Consumers may believe that the personal information they provide to health Web sites is protected by the new regulation when in fact many Web sites will remain unregulated.

The extent to which the new federal health privacy regulation will impact eHealth will depend largely on whether or not a Web site or Internet service is affiliated with or controlled by a covered entity and whether that site or service collects identifiable health information. Web sites not associated with a provider, plan or clearinghouse and not acting on behalf of these entities will fall outside the scope of the regulation. Personal health information collected and maintained by these sites, therefore, will be left unprotected by the federal regulation.[76] Given the wide range of activities on the Internet and the relatively narrow scope of the regulation, it is likely that a great deal of health information collected on health Web sites will *not* be covered by the new regulation.

Some sites have responded to the public's concern regarding privacy and security on the Internet through self-regulation. To head off possible federal Internet privacy legislation, several professional organizations and trade associations have developed or are developing standards and seal programs to address privacy, security and quality on the Internet.[77] However, compliance is voluntary and there are few, if any, enforcement

---

[76] State laws do not offer adequate protection of information collected by health Web sites either. Protection varies greatly from state to state, and in general only applies to some of the core players in the health care arena.

[77] Standards and seal programs that are in development or have been developed include: Association of American Health Plans, *AAHP Principles for Consumer Information In an E-Health Environment*, http://www.aahp.org; American Health Information Management Association, *Recommendations to Ensure Privacy and Quality of Personal Health Information on the Internet*, http://www.ahima.org/infocenter/guidelines/tenets.html; Health On the Net Foundation, *HON Code of Conduct*, http://www.hon.ch/HONcode/Conduct.html; Hi-Ethics, *Ethical Principles For Offering Internet Health Services to Consumers*, http://www.hiethics.org; International Society for Mental Health Online, *Suggested Principles for the Online Provision of Mental Health Services*, http://www.ismho.org/suggestions.html; Internet Healthcare Coalition, eHealth Ethics Initiative, *eHealth Code of Ethics*, http://www.ihealthcoalition.org/ethics/ethics.html; National Association of Boards of Pharmacy, Verified Internet Pharmacy Practice Sites program, http://www.nabp.net; National Board for Certified Counselors, *Standards for the Ethical Practice of WebCounseling*, http://www.nbcc.org/ethics/webethics.htm; TRUSTe and Hi-Ethics, E-Health Seal Program, http://www.truste.org/programs/pub_ehealth.html; URAC and Hi-Ethics, Health Web Site Accreditation, http://www.urac.org/programs/technologyhws.htm; and M.A. Winker et al., *Guidelines for Medical and Health Information Sites on the Internet American Medical Association*, 283 JAMA 1600 (2000).

mechanisms. Furthermore, a survey conducted by Cyber Dialogue and the Institute for the Future shows that the presence of a seal of approval from an Internet trade group, such as TRUSTe, does not have an impact – positive or negative – on consumer willingness to submit health information online,[78] although an accreditation seal would increase consumer trust in health Web sites.[79]

People often believe they are invisible and anonymous online, but they are often exposing their most sensitive health information to online health care sites that are not required by law to protect the information or keep it confidential. The potential for abuse is enormous.

[78] *Ethics Survey of Consumer Attitudes about Health Web Sites*, *supra* note 6; however, a seal of approval for the quality of the content of a Web site is important to consumers. URAC released a study in May 2001 showing that 78% of consumers said a quality seal on a health Web site was extremely important or very important to them and 74% prefer that a private, nonprofit organization administer a health Web site accreditation program.

[79] *Survey of Consumers' Attitudes Towards Health Web Sites and Accreditation*, conducted by Harris Interactive for URAC (May 2001).