E-health: What's Outside the Privacy Rule's Jurisdiction?

by Angela Choy, Joy Pritts, and Janlori Goldman

E-health—from basic health information Web sites to online consultations—is flourishing. And though the government is trying to protect consumers under the HIPAA privacy rule, many Web sites aren't covered. In this article, privacy experts explain which Web sites are covered and why—and where consumers are taking risks.

E-health is touted as the future of healthcare, promising to transform the way healthcare entities conduct business and change the way patients relate to their healthcare providers. However, while the Internet can be a powerful tool in the delivery of healthcare, it enables the collection and distribution of highly sensitive information in new ways by online services. It can also leave such information vulnerable to security breaches.

Individuals share a great deal of personal and sensitive health information in the course of obtaining healthcare, yet there is little legal protection for health information—online or offline. A substantial barrier to improving the quality of 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, and discrimination.

Congress recognized the importance of protecting people's medical records when it passed HIPAA. The administrative simplification portion of the rule is 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, the Department of Health and Human Services (HHS) would be required to issue health privacy regulations. HHS issued a landmark federal health privacy regulation in December 2000 and most healthcare entities have until April 2003 to implement the new rule.

Our analysis of the privacy regulation's impact on e-health, 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 and individuals may assume that their health information is protected when it is not.

What Does the Privacy Rule Protect?

Unlike financial records, credit reports, and even video rental records, there is no comprehensive federal law that protects the privacy of medical records. While the privacy rule is an important step toward boosting the public trust and confidence in our nation's healthcare system, its application is limited. HIPAA imposed constraints on HHS' rulemaking authority, restricting the scope of the rule. The rule does not apply to all persons or entities that have access to personal health information. It only directly covers three kinds of healthcare entities:

- **providers**, such as doctors, hospitals, and pharmacists, who electronically transmit health claims related information in "standard format"[1,2]
- **health plans**, such as traditional insurers and HMOs
- **clearinghouses**, which are entities that process health claims information in a uniform format for providers and insurers, such as WebMD Office[3]

A person or organization that falls within one of these categories is considered a covered entity (CE).[4]

Many health Web sites, however, are not owned or operated by one of these three entities. Therefore, while online healthcareactivities that are already conducted offline by a "covered" healthcare 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.

The result is that the same activities conducted at different Web sites will be subject to different legal treatment. Specific activities, such as ordering a prescription, getting a 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 CEs engage in diverse activities, many of which are not covered by HIPAA. On these sites it will be difficult to determine what activities are covered by HIPAA.

Covered Web Sites: Providers and Insurers

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

It should be fairly easy to determine if a health plan is a CE. The term "health plan" is broadly defined in the regulation and covers just about anyone that provides or pays the cost of medical care, including 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.

It's more difficult to tell whether any given provider is subject to the regulation, because not all healthcare providers fall under the CE definition. To determine whether a person or organization is a covered provider under the privacy rule, consider the following key questions:

- Is the person or organization a healthcare provider as defined by the rule?
- Does the person or organization transmit health information in connection with one of the financial or administrative standard transactions listed in HIPAA?
- Does the person or organization transmit that information electronically in the required standard format?[5]

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 "healthcare provider" covers most of the people and organizations that consumers traditionally think of as providers. It includes any person who furnishes, bills, or is paid for healthcare in the normal course of business. Thus doctors, counselors, clinics, hospitals, nurses, and similar persons and organizations are considered to be healthcare 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.[6] Under this requirement, a pharmacist, such as CVS, is a healthcare provider, while a Web site that sells books and tapes on losing weight, such as eDiets.com, is not.[7] Similarly, a pharmaceutical company is not a healthcare provider since it does not sell or dispense drugs pursuant to a prescription.

If a person or an organization is a healthcare 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. Because 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 healthcare payment and remittance advice
- receiving referral certification and authorization

All of these transactions are related to health insurance-type transactions.

Finally, 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. That is, the provider must include certain information and use specified codes for diagnosis and treatment. Currently, providers do not have to use standard formats until October 2002. They can get a one-year extension of that deadline if they submit a

compliance extension plan to HHS before October 15, 2002. HHS has taken the position that only providers who actually use the required format are covered by the privacy rule.

Once a provider meets all three of the required criteria, it becomes a CE, and the information collected at its site would be protected by the regulation.

Partially and Indirectly Covered Web Sites

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 CE, 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 covered by the privacy regulation.

For example, drugstore.com sells both prescription drugs and over-the-counter products.[8] 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 "healthcare." This term does not include selling or distributing non-prescription healthcare items.

Business Associates

Health plans and providers routinely hire other companies and consultants, known as business associates, to perform a variety of functions, such as legal, financial, and administrative services. They receive health information on behalf of or from a CE. In general, business associates are not directly covered by the privacy regulation.

The regulation establishes specific conditions on when and how covered entities may share information with business associates. 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.[9] It is the CE, however, that is liable if the business associate violates the contract, and then only if it had actual knowledge of the breach yet did nothing to remedy it.[10]

Web Sites Not Covered

General Health Information Sites

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 "healthcare," as it is defined in the federal regulation.

Some sites offer additional services that require users to provide personal information to the site, such as 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—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.[11] HealthStatus.com's disclaimer makes clear its belief that the site does "not provide medical advice or treatment."[12] HHS may not necessarily agree with this assertion, but because HealthStatus.com does not accept any insurance it will not be covered by the privacy rule.

Health-related Product Sites

The press has been filled with stories about rogue Web sites selling drugs without a legitimate prescription.[13] Many of these pharmacists only conduct business online and specialize in drugs that treat sensitive or embarrassing conditions that a patient may not discuss with a doctor.[14, 15] There also are sites that provide online prescriptions for products that are not always easy to obtain, like the "morning-after" pill.[16]

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

Web sites that sell only non-prescription health products, such as healthandbeautydepot.com, also fall outside the scope of the privacy regulation, because the sale of non-prescription health products is not considered healthcare, 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.

Healthcare "Treatment" Sites

Some Web sites provide healthcare but still are not covered by the regulation, because they do not accept health insurance. Only providers that process health claims electronically in a standard format are covered by the regulation. Hence, simple activities like filling a prescription online may not be covered by the regulation.

Another example is online counseling. Some Web sites allow users to participate in an online therapy session. These sites also tend to only accept credit cards. For example, at Cyberanalysis.com, patients can make arrangements to communicate with participating doctors by cyber chat, e-mail, videophone, or telephone.[17] 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 CE. Because 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.

Another type of online health service that consumers may consider healthcare is clinical trial recruitment. At ClinicalTrials.com, 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.[18] ClinicalTrials.com falls outside the scope of the privacy regulation—it is neither a CE nor a business associate.

Patient-driven Sites

Many hope that online healthcare 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 unprotected when they take information from their doctor and give it to a Web site. For example, sites where the patient acts as the intermediary between providers may not be covered.

Consider online medical records. PersonalMD.com, for example, enables patients to manage all of their medical information on one site, which the patient can access from anywhere in the world.[19] The site is storing this information on behalf of the patients, not their doctors.[20] 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, because it is not a provider, health plan, or clearinghouse. Patients who use these sites essentially are relying on the site's own privacy policy for protection.

Patients may 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. The privacy regulation recognizes that this can occur and requires that forms authorizing the disclosure of health information include a statement that the information released pursuant to the authorization may no longer be protected by the privacy rule.

PersonalMD.com has strict policies against sharing personally identifiable information without an individual's permission, but privacy policies are not required by law and they are subject to change at any time.[21] Furthermore, PersonalMD.com advertisers or Web sites that have links on the site may collect personally identifiable information about individuals, but these third-party sites are not required to comply with PersonalMD.com's privacy policy.

A False Sense of Security

Health-related information is being collected and shared about individuals more than ever, and until the release of the privacy rule, there were almost no federal legal limits on how this information could be used and disclosed. However, due to the wide range of activities on the Internet and the relatively narrow scope of the regulation, it's likely that a great deal of health information collected on the Web will not be covered by the regulation.[22] Unfortunately, many consumers may already be operating under a false sense of security when they engage in online health activities.

Portions of this article are excerpted from a recent Health Privacy Project report, Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users*, with the permission of the Pew Internet & American Life Project. The authors are grateful to the Pew Project for funding the original research and publication of the full report, which is available at the Health Privacy Project Web site at www.healthprivacy.org.*

Notes

1. Some of the electronic transactions that trigger a provider's classification as a CE include health claims or equivalent encounter information, enrollment or disenrollment in a health plan, determining eligibility for a health plan, healthcare payment and remittance advice, and referral certification and authorization. All of these transactions are related to health insurance-type transactions. See HIPAA, Section 1173.

2. Healthcare providers and health plans currently use many different formats to conduct administrative and financial healthcare transactions electronically. To reduce healthcare 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 healthcare data interchange. For more information about the transaction standards, see the Transactions and Code Sets Frequently Asked Questions at the HHS Administrative Simplification Web site at http://aspe.hhs.gov/admnsimp/ bannertx.htm.

3. WebMD Office is available at http://professional-content.webmd.com/Article.asp?article=article://3834.1081&AuthLevel=2.

4. Healthcare clearinghouses are CEs under the regulation. However, 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.

5. Although the language of the statute and the regulation can be read to cover any provider who transmits information in electronic format (whether it is in standard format or not), HHS has taken the public position that the rule will apply only to those providers who engage in transactions in standard format. There are a number of places in the preamble to the regulation that HHS indicates that this is its position.

6. The privacy rule applies to providers of healthcare. The rule defines "healthcare" as including the sale or dispensing of a drug, device, or other equipment, or item in accordance with a prescription. "Healthcare" therefore does not include over-the-counter drugs.

7. eDiets.com Web site available at www.ediets.com.

8. Drugstore.com Web site available at www.drugstore.com.

9. On March 21, 2002, HHS proposed modifications to the privacy regulation. HHS' proposal includes model business associate contract provisions and gives some covered entities up to one year beyond the April 14, 2003, compliance date to change their existing contracts. The proposed modifications are available at www.hhs.gov/ocr/hipaa/whatsnew.html.

10. Healthcare clearinghouses are directly covered by the privacy regulation. While in many cases they will be business associates of a provider or insurer, they will be directly liable for violations of the business associate contract and thus

violations of the regulation.

11. Information about HealthStatus.com's health risk assessments is available at www.healthstatus.com/ assessments.html.

12. HealthStatus.com's disclaimer is available at www.healthstatus.com/disclaimer.html.

13. See Fawcett, A. "Online Rx." *Atlanta Journal and Constitution* (August 7, 2001); Ignelzi, R. J. "Risky Prescription: Online Drug Buyers Gamble With More Than Their Credit Cards." The *San Diego Union-Tribune* (August 6, 2001); Wheelwright, G. "Inevitable Marketplace For Lifestyle Drug: Online Viagra Sales," *Financial Times* (February 21, 2001); Coburn, S. "A Web Bazaar Turns Into a Pharmaceutical Free-for-All." *New York Times* (October 25, 2000); Karash, J. A. "More Prescriptions are Being Filled on the Net." *Kansas City Star* (October 22, 2000).

14. See www.at-home-viagra.com.

15. See www.propeciapharmacy.com.

16. See www.virtualmedicalgroup.com.

17. See www.cyberanalysis.com.

18. See www.clinicaltrials.com.

19. See www.personalmd.com.

20. In contrast, some sites store and manage health information on behalf of doctors. These sites are treated differently under the regulation.

21. See the PersonalMD privacy policy at www.personalmd.com/privacypolicy.shtml.

22. 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 healthcare arena.

References

"Health Insurance Portability and Accountability Act of 1996." Public Law 104-191. August 21, 1996. Available at http://aspe.hhs.gov/admnsimp/.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 65, no. 250 (December 28, 2000). Available at http://aspe.hhs.gov/admnsimp/.

Acknowledgment

The authors wish to thank their research associate, Stacey Spivey, for her assistance on this paper.

Angela Choy *(awc@georgetown.edu),* ***Joy Pritts*** *(jlp@georgetown.edu), and* ***Janlori Goldman*** *(goldmajl@georgetown.edu) are field director, senior counsel, and director, respectively, of the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy in Washington, DC. The Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve healthcare access and quality, both on an individual and a community level.*

Article citation:
Choy, Angela, et al. "E-health: What's Outside the Privacy Rule's Jurisdiction?" *Journal of AHIMA* 73, no.5 (2002): 34-39.