Privacy and Medical Information on the Internet

Steven B Nelson MSc RRT CPFT FAARC

Health-care consumers are beginning to realize the presence and value of health-care information available on the Internet, but they need to be aware of risks that may be involved. In addition to delivering information, some Web sites collect information. Though not all of the information might be classified as protected health information, consumers need to realize what is collected and how it might be used. Consumers should know a Web site's privacy policy before divulging any personal information. Health-care providers have a responsibility to know what information they are collecting and why. Web servers may collect large amounts of visitor information by default, and they should be modified to limit data collection to only what is necessary. Providers need to be cognizant of the many regulations concerning collection and disclosure of information obtained from consumers. Providers should also provide an easily understood privacy policy for users. *Key words: privacy, Health Information Portability and Accountability Act, consumer rights, Internet.* [Respir Care 2006;51(2):183–187. © 2006 Daedalus Enterprises]

Introduction

Nearly every week there is another news story about a breach of computer security that affects hundreds to hundreds of thousands of consumers. Responsibility for protecting information has, of necessity, been pushed back toward the consumer. People using the Internet need to be aware of practices to protect themselves and their information as much as possible.

There are countless regulations that can be used to punish offenders who disclose information, from national regulations such as the Health Insurance Portability and Accountability Act (HIPAA) to state laws such as California Senate Bill 1386. Unfortunately, these regulations cannot undo disclosures. A few precautionary steps can help a Web user prevent herself from becoming the next victim.

Consumer Protection

One of the first steps a consumer should take before providing any information to a Web site is to verify that the Web site you see on your monitor is actually the intended site. The easiest way to confirm that is to type in the name of the Universal Record Locator (URL), or name, of the site, rather than following a link from another source. It is simple to redirect a seemingly correct link to an unintended location. When in doubt, type it out.

Many reputable Web sites have a privacy policy link, easily found on each page. Interpreting the information, however, may be difficult. The privacy policy for Disney Online services is 5,244 words long.[1] For comparison, the entirety of the United States Constitution is slightly more

Steven B Nelson MSc RRT CPFT FAARC, a Certified Information Systems Security Professional (CISSP), is affiliated with Pulmonary Industrial Testing Associates, Overland Park, Kansas, and with Sun Microsystems, Santa Clara, California.

Correspondence: Steven B Nelson MSc RRT CPFT FAARC, Pulmonary Industrial Testing Associates, 8314 W 128th Street, Overland Park KS 66213. E-mail: sbn_kc@mac.com.

than 4,500 words. The Cleveland Clinic has a succinct, clear policy of only 353 words.[2]

The privacy policy, at a minimum, should clearly explain what data are collected, why they are needed, to whom they are disclosed, and how they are protected from inadvertent disclosure. There should be a clear statement about the method to opt in or out of collecting and sharing the user's information.

The policy might also include information about "cookies" and their use. Cookies are small files, stored on the user's computer, that can be used to track pages visited. They may contain many other bits of information that control the view that the users get when they return to the site.

Online discussion forums provide a means to find other people with similar issues and conditions. People with a particular condition can discuss issues that they are experiencing and may benefit from the support of others who have had the same experience. One common use is virtual support groups for smoking cessation (eg, QuitNet.com). A user may be able to log in at any hour to talk about immediate difficulties. This method provides feedback that might otherwise not be available. Generally, forums are unregulated and open to public view. Each user must consider how much information disclosure is appropriate. Some users may provide great detail, while others are reluctant to do so. Remember that anything shared in a forum is available for public viewing. Even forums that require members to register do little to verify the identity or veracity of participants. In some cases, people with vested interests can be found participating in forums, without disclosing their potential biases or conflicts of interest.

Rather than reading through an entire privacy policy, one can allow the Web browser to review the site policy and quickly show the results. The Platform for Privacy Preferences specification (P3P) establishes a machine-readable format that uses Extensible Markup Language (XML), a programming language for Web pages. The user indicates in the browser preferences what information they want shared, how, and with whom. The choices may be graphically displayed to show whether cookies are set, whether health or medical information is shared or sold to third parties, and other policy questions. P3P is currently available for the Microsoft Internet Explorer 6 browser and Mozilla Firefox browser. Microsoft Internet Explorer 5 for Windows users can get an add-on program called Privacy Bird (PrivacyBird.com), developed by AT&T, that provides the same type of function. Unfortunately, fewer than 500 sites are currently listed as compliant with P3P since the standard was published in 1999.[3]

One of the advantages of an automated privacy review is that it can monitor the Web site for inappropriate activity as you use it. For example, in the frequently-asked questions (FAQ) area of an online discussion forum at HealthDigest.org, it is stated, among other things, that the site does not place cookies on your computer.[4] However, unless you have a program actively monitoring the placement and use of cookies on your computer, you might not realize that the Web site actually does use cookies. Perhaps its privacy FAQ was not updated to reflect a change in the policy.

Table 1. Information Classified as Protected Health Information by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Name
Geographic subdivisions smaller than a state
Dates, including date of birth, admission, discharge, death
Telephone number
Fax number
E-mail address
Social Security number
Medical record number
Health-plan beneficiary number
Account number
Certificate/license number
Vehicle identification, including license plate
Device identifiers and serial numbers
Web-site addresses, uniform resource locators (URLs)
Internet Protocol (IP) addresses
Biometric identifiers, including voice and finger prints
Full-face photos and comparable images
Any other unique identifying number or characteristic

HIPAA designates 18 items that are considered privileged information (Table 1).[5] These range from the obvious, such as Social Security and medical record numbers, to the unusual, such as vehicle license plate number and voice print, and conclude with the inevitable, "Any other unique identifying number, characteristic, or code." Any entity that asks for or acquires such information should clearly state how it would be used and protected. Web sites that ask for any of this information should provide a secure link to protect it in transit. The user can verify that transmissions to and from a given Web site are secure. If the Web site address starts with "https://" (stands for "hypertext transfer protocol secure") a secure form is being displayed. Also, most Web browsers show a secured padlock icon if the site is secure, even if the "https://" designation is absent.

As a safety precaution, never enter personal medical information on a public-access computer, such as those found in libraries, even into secure-transmission Web forms. A Web browser keeps information in a "cache" file that can be read by anyone who uses the computer later. Even though it is possible to flush out cache files, they can still be easily recovered and the information disclosed.

As an example, the Web site YourHealthRecord.com seems to provide a temporarily free "personal health record

on the Internet." The user can create an account and record any of his or her medical information, such as medications, allergies, peak flow measurements, and medical history. The data can then be accessed and updated anywhere the patient wants to see it, or conveniently printed out prior to a physician visit. A close look at the site shows that the company may share your e-mail address with their parent entity. The site is hosted in Australia, which means that a United States user's assumptions, based on United States law, about privacy of information might not be justified; the privacy rules that apply to that Web site might be different than expected, or even absent. The site's assurance that it has agreements with third-party suppliers does not ensure that all suppliers have similar agreements with their suppliers.

A recent incident at a California hospital illustrates this problem. The hospital contracted with a Florida company to transcribe dictation. The Florida company subcontracted to a Texas company that further subcontracted to a woman in Pakistan, who became frustrated by slow payment for her work. The woman tried to blackmail the hospital by threatening exposure of patient records if she was not paid immediately.[6] Data paths and control can be difficult to follow in an era of international out-sourcing.

Similar to consumer credit bureaus, there is an agency that collects and sells consumers' medical information: the Medical Information Bureau Inc (MIB.com). Like a credit-reporting agency, the Medical Information Bureau Inc provides a free annual disclosure of any information it has collected. Information is typically retained for a period of 7 years, and there is a process to dispute erroneous entries.

Protecting personal medical information is important, but equally important is being certain that the publicly available information about health care found on the Web is reputable. The most widely recognized validation system for Web sites that provide health information is the Health On the Net Foundation's Code of Conduct.[7] The Health On the Net Foundation publishes guidelines to ensure that health information on Web sites is provided by medically qualified professionals, is scientifically sound, maintains confidentiality of user data, and clearly discloses authorship and sponsorship. Sites that meet the Code of Conduct can display the HONcode symbol (Fig. 1) and provide a direct link to the HON Foundation Web site for quick verification.

Fig. 1. The Health On the Net Foundation's Code of Conduct "HONcode" symbol and verification link.

Provider Considerations

Providers that offer Web sites, discussion forums, e-mail contact lists, or obtain personal medical information from any source are, obviously, regulated by HIPAA. But there are additional requirements that may need to be considered, even for something as innocuous as an intradepartmental Web site.

Data collection for medically related Web sites can take on insidious characteristics. Simple log files typically kept by Web servers to collect visit information might now contain personal medical information. Securing these seemingly random bits of information is not just a good idea; it's now a requirement.

As a starting point, providers can apply to their own Web sites the above-discussed information for consumers. Display obvious links to a privacy policy. Before any data are collected, verify that collecting the data is necessary and that the data can be protected. Use third-party validation for content accuracy. Use secure transactions for collecting information.

Privacy policy templates can be obtained from several sources.[8,9] A Google search will turn up many more options. Once the privacy policy has been written, verify that it is reasonable, then make sure that everyone is aware of and understands it. One recent security breach that exposed information on over 300,000 people[10] was caused not by clever hackers bypassing a security system. Rather, critical system information was inadvertently disclosed to thieves by company personnel. In another incident in San Jose, California, a medical-group manager stole computers with information on about 185,000 patients.[11] These 2 cases illustrate the fact that an estimated 80% of exposures are due to internal breakdowns in people and policies, not hackers.

When computers or storage media—such as disk drives, floppy disks, and CDs—are replaced, the data on them must be destroyed. In a recent case, a plastic surgeon set out an unused computer for trash pick-up. He thought that by removing the memory chips from the computer he had effectively deleted the data, which included images of many

patients. Someone subsequently picked up the computer before the trash company could, put a new memory chip in, and was able to see all of the patient records and images.[12] If there is any question about deletion of data, the device should be physically destroyed.

Sites that collect patient data should indicate to users that privacy and security are important by using a third party, such as TRUST-e (TrustE.org) or VeriSign (VeriSign.com). These companies perform audits that verify adherence to good data practices. They provide a level of trust for consumers, similar to the Good Housekeeping Seal. Users can quickly verify that a site adheres to the policies by simply clicking the verification link on the Web page.

Teaching institutions not only fall under HIPAA requirements, they must be cognizant of the Family Educational Rights and Privacy Act,[13] which allows release of student information under a number of conditions, unless a student specifically opts out of the disclosure. Although it is unlikely on medically oriented Web sites, there are also regulations about young visitors. The Children's Online Privacy Protection Act[14] requires compliance by general-audience Web sites that might collect individually identifiable information from children under 13 years of age.

Technology Creeps Forward

Perhaps the clearest indication that health care is slow to adapt to and adopt new technology can be seen in a study published in 1997.[15] In 1995, before HIPAA had been enacted, the National Library of Medicine and several other bodies convened a committee to identify threats to health-care information, adequacy of privacy and security measures, and barriers to adoption. They were overly optimistic in their view of the future, but correctly identified information-security issues that plague health-care organizations. The committee advocated a strong, industry-wide security policy, yet today security is still seemingly ad hoc. They made numerous recommendations regarding privacy of medical records, yet today an application for homeowner's insurance can be dependent on release of medical information. They proposed audit trails and strong access controls, yet today heterogeneous systems are still unable to use centralized identity management. They recommended a universal patient identifier, similar to the secure "smart cards" used by several Canadian provinces, yet today we still carry Social Security, Medicare, Medicaid, and insurance provider cards. Finally, adoption has been much slower than they predicted. As recently as 2003, only 5% of the nation's hospitals had adopted computerized physician-order-entry, even though it has been shown to pay for itself in reduced errors and shorter length of stay.[16]

Consolidation of data is still an issue, with the ability of large data warehouses to assimilate disparate facts from many sources. The United States government recognized the potential for insidious loss of control over personal information. In 1977, the Privacy Protection Study Commission issued the following warning: "The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."[17]

Summary

Health-care consumers are becoming more involved in their own care by using the many publicly accessible resources on the Internet. Consumers need to realize that some Web sites collect information, overtly or surreptitiously, as the user explores the various pages on a site. They also need to decide whether they want to disclose personal information on public forums, which can be read by anyone who visits the site.

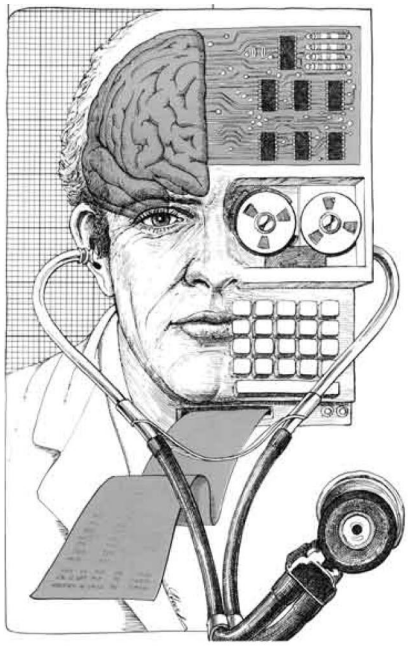
Health-information providers on the Internet are held to a higher standard than other Web sites, since they might acquire protected health information. There are numerous national and state laws that mandate what information can be disclosed, and these laws provide heavy penalties for unauthorized information disclosure. Providers should consider subscribing to the principles of the Health On the Net Code of Conduct to ensure that they are providing accurate, unbiased information.

Finally, and again, before any data are entered into or collected on a web site, know what is being collected, why it is being collected, how it will be disclosed, and who will have responsibility for it.

REFERENCES

1. Disney Online Services. http://disney.go.com/corporate/privacy/pp_wdig.html. Accessed December 9, 2005.
2. The Cleveland Clinic privacy policy. http://cms.clevelandclinic.org/body.cfm?id=20. Accessed December 9, 2005.
3. Sites using P3P. http://www.w3.org/P3P/compliant_sites. Accessed December 9, 2005.
4. Frequently asked questions. http://www.healthdigest.org/faqs.html. Accessed April 26, 2005.
5. Standards for privacy of individually identifiable health information. US Department of Health and Human Services, Office of Civil Rights. 45 CFR §164.514(b)(2)(i) December 28, 2000. Amended April 17, 2003.
6. Henry P. View from the top: medical data theft. http://www.sciencedaily.com/upi/index.php?feed=Science&article=UPI-1–20050805–15441200-bc-viewfromtop-henry.xml. Accessed December 9, 2005.
7. HON code of conduct. http://www.hon.ch/HONcode. Accessed December 9. 2005.

8. EPIC online guide to practical privacy tools. Electronic Privacy Information Center. http://www.epic.org/privacy/tools.html. Accessed December 12, 2005.
9. Template: privacy policy. WorkZ. http://www.workz.com/content/view_content.html?section_id=543&content_id=6438. Accessed December 12. 2005.
10. LexisNexis acknowledges more ID theft. http://money.cnn.com/2005/04/12/technology/personaltech/lexis/?cnn=yes. Accessed December 9, 2005.
11. Manager at San Jose Medical Group charged with stealing patient data. San Francisco Chronicle, May 14, 2005. http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/05/14/state/n122402D59.DTL. Accessed December 9, 2005.
12. Margolies D. Privacy, news right clash. Kansas City Star. http://www.kansascity.com/mld/kansascity/business/11925354.htm. Accessed December 10, 2005.
13. Family Educational Rights and Privacy Act (FERPA). http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Accessed December 9, 2005.
14. Children's Online Privacy Protection Act of 1998. http://www.ftc.gov/ogc/coppa1.htm. Accessed December 9, 2005.
15. Committee on maintaining privacy and security in health care applications of the national information infrastructure. For the record: protecting electronic health information. Washington DC: National Academy Press; 1997.
16. Pennsylvania Health Care Cost Containment Council. PHC4 FYI–prescription drug safety. http://www.phc4.org/reports/FYI/fyi25.htm. Accessed December 9, 2005.
17. Privacy Protection Study Commission. Personal privacy in an information society. Washington DC: US Government Printing Office; July 1977:53.



Artificial Intelligence (Brochure, US Government Printing Office, 1980).
Courtesy National Library of Medicine