

HEALTHCARE WEBSITES: THE OTHER PRIVACY ISSUE

by David Rabinowitz, Esq

This article originally appeared in the May 1st issue of iHealthcare Weekly

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the proposed privacy regulations of the Department of Health and Human Services (HHS) are well-known in the health care community. The regulations, in whatever form they are ultimately adopted, will protect patients' rights to the privacy of their medical records in the Internet age. The rules that HHS promulgates will shape the medical community's Internet infrastructure and the electronic infrastructure connected to the Internet.

Less well known in the health care community is another separate and entirely independent body of privacy law that will further constrain the health care community's Internet websites and its collection and use of data coming out of those websites. A body of privacy law is about to be fashioned that will apply to the whole Internet, not just health care, and health care websites will not be excepted by reason of HIPAA.

I speak in the future tense because, legally speaking, we are in the twilight of the Wild West era of Internet privacy. Putting aside pieties, with the exception of children's information and specialized industry rules, practically any non-deceptive privacy policy is perfectly fine, at least in New York. As long as no pledge of privacy or secrecy to website visitors is violated, website operators can collect information about their visitors and use or sell that information for commercial purposes.

The cases in which the Federal Trade Commission has taken an interest, such as the Doubleclick case, are deception cases. Doubleclick is a leading provider of Internet advertising. Doubleclick monitors the behavior of visitors to participating websites, accumulating data valuable in targeting ads to receptive audiences. In the Doubleclick case, Doubleclick had collected information from website visitors while promising, in its privacy notice, that it would maintain their anonymity. When it merged with another company, Abacus Direct, which was in the individually identifiable information business, it proposed to start correlating its information with that of the newly acquired business.

It was that step that resulted in the filing of a complaint with the FTC by the Electronic Privacy Information Center (EPIC). The correlation of the anonymous data with the individuals' identities (shades of HIPAA) amounted, in EPIC's view, to a breach of faith with previous website visitors. Abacus Direct had been able to operate without interference because it had not promised the anonymity that Doubleclick did.

So where are we going? That may be shaped by the imagination of one or more of the Congress, the federal regulatory agencies, the states, or the Internet industry itself.

The Congress and state legislatures are studying a menu of proposed Internet privacy laws. They run the gamut from prohibiting certain uses of information, to prohibiting the deposit of cookies on users' computers without their express consent, to requiring websites to have people actively opt in before their information can be used, to more laissez faire laws that would simply require notice to website visitors of all the uses to which their information was going to be put, and to whom it would be sold.

The FTC has promulgated regulations under the 1998 federal Children's On-line Privacy Protection Act and has proposed regulations under the 1999 federal law on financial information privacy. In a 1998 report to Congress, the FTC identified five core elements of what it considered fair information practice: notice (to the individual), choice (about whether to reveal information), access (to information previously gathered), security (of the collected information) and enforcement (of privacy standards). The report concluded that industry self-regulation would be the best regulation, but concluded ominously that no effective industry self-regulation had yet emerged.

The Internet industry has been trying to ward off government action by self-regulation. Companies have sprung up selling their services as private guardians of Internet virtue, by auditing their member Internet companies (which can include any organization that operates a web site) and certifying that they behave according to a certain code. As with Hollywood and the Hays office of the 1930s and 1940s, the theory is that the vaccination of self-regulation is better than the disease of government supervision. However, critics of these certification

companies have charged them with lax oversight in failing to hold the certified websites to their own policies.

All in all, it now seems likely that self-regulation will not deter government action, and that the health care industry has to monitor the progress both of the HIPAA regulations and of public on-line privacy law.

MOSES & SINGER LLP

Disclaimer

Viewing this document or contacting Moses & Singer LLP does not create an attorney-client relationship.

This document is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This document contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.

Copyright © 2009 Moses & Singer LLP
All Rights Reserved