Why the HIPAA Privacy Rules Would Not Adequately Protect Personal Health Records

September 2008

This brief explains why the HIPAA Privacy Rule, in its current format, would provide weak privacy protection for personal health records (PHRs) offered by employers and Internet companies. The brief argues for stronger protections regarding marketing and commercial uses of information in PHRs and advocates for the Federal Trade Commission (FTC) to be involved in developing and enforcing those protections.

- Personal health records (PHRs) hold great promise for improving health care quality and increasing consumer engagement in care. But many consumers are reluctant to use PHRs because of concerns about the privacy and security of the personal health information in those records.
- PHRs provided by entities covered by the HIPAA Privacy Rule (i.e., providers and health plans) are currently covered by the Rule. Further, covered entities must follow the Privacy Rule when transmitting personal health information to any consumer's PHR.
- PHRs are also being offered to consumers directly by employers, and they are being launched on the Internet, where there will likely be numerous options (from large brand providers like Google, Microsoft and Revolution Heath to dozens of others less publicly well known). PHRs offered by these entities are currently <u>not covered</u> under HIPAA, so the personal health information in them will not be covered by the Privacy Rule (unless the entity receives the medical information as a business associate of a covered health plan or provider).
- In an unregulated arena, consumer privacy is only protected by the PHR offeror's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information), and if those policies are

CENTER FOR DEMOCRACY & TECHNOLOGY Keeping the Internet Open, Innovative, and Free
1634 I St., NW, Suite 1100, Washington, DC 20006 • v. +1.202.637.9800. • f. +1.202.637.0968 • http://www.cdt.org

violated, the company may be subject to FTC action. The policies of PHR vendors range from very good to seriously deficient.[1]

- This emerging—and alarming—privacy "vacuum" is motivating some to suggest extending the Privacy Rule to cover all PHRs. However, CDT is concerned that the HIPAA Privacy Rule does not provide adequate protection for PHRs and may do more harm than good in its current scope.
- The HIPAA Privacy Rule was designed to protect information used by and exchanged among *traditional health care entities*. As a result:
  - personal health information is permitted to flow without patient authorization for certain purposes related to treatment and payment for care;
  - other uses are prohibited unless certain procedures and safeguards are in place (i.e., disclosure to researchers, law enforcement); and
  - a number of uses—such as to employers or for marketing and any uses not expressly mentioned in the Privacy Rule— require express, uncoerced patient authorization.
- Bringing third-party PHRs under the scope of HIPAA authorizes the disclosure of highly sensitive data outside of the health care system, with each such disclosure subject only to patient authorization.
- Total reliance on individual consent places people in an unfair and potentially dangerous situation, shifting the burden of protecting privacy solely to the individual and putting the bulk of the bargaining power on the side of the entity offering the PHR. A few of the most troubling problems are:
  - Research on consent on the Internet shows that most people do not read the details of consent forms before signing them, and those that do often do not understand the terms. Many wrongly assume that the existence of a privacy policy means that their personal information will not be shared, even when the policy and the accompanying consent form say just the opposite. And for free web-based products like PHRs, consent to the statement of uses and disclosures (a.k.a. the "privacy policy") will likely be required in order to use the service.
  - Applying the Privacy Rule to PHRs only gives individuals a right to authorize—or limit—certain marketing or commercial activities before they can take place.
  - A major business model to support third-party PHRs is advertising revenue and partnerships with third-party suppliers of health-related products and services. As a result, people using these tools will be more likely to be marketed to on the basis of health information in their PHI. They will likely be subjected to the tools that Internet companies typically use to gather information about consumer

[1] The HHS Office of the National Coordinator commissioned a study in 2007 of the policies of over 30 PHR vendors and found that none covered all of the typical criteria found in a privacy policy. For example, only two described what would happen to the data if the vendor were sold or sent out of business, and only one had a policy with respect to deactivated accounts.

preferences (such as cookies), so that the companies can target them with specific ads or product offers. Their data may be more likely to be sold to third parties (such as pharmaceutical companies and health insurers). They also will likely be solicited by the PHR's formal and informal business partners (for example, diabetes management programs sponsored by the diabetes meter companies, weight loss and fitness programs, etc.), who also will likely solicit individuals to share their data and may use that data for multiple business purposes (including selling it).

- For PHRs to flourish, CDT believes clear rules are needed regarding marketing and commercial uses of information that will better protect consumers by restricting PHR vendors from engaging in certain practices, or by providing individuals with certain rights—in other words, a much stronger and more comprehensive package of privacy and security safeguards than merely affording people the right to check a box acknowledging the uses and disclosures of their information. This may mean the application of certain provisions in HIPAA, but for the most part will require a different set of requirements.
- If the Privacy Rule is the best vehicle to strengthen or expand protections for consumers who use PHRs, CDT believes the Secretary of HHS should be tasked with promulgating rules specific to PHRs that respond to the unique issues raised by these tools. (For example, the rules permitting covered entities to use personal health information without express authorization for treatment, purposes, and "health care operations" should not be applied to PHRs.) CDT further recommends that Secretary consult with the Federal Trade Commission, which has experience in issues related to online privacy and consumer protection, in developing these rules.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact: Deven McGraw, (202) 637-9800 x 119, deven@cdt.org