Davis Wright Tremaine LLP

Incidental Exposure to Health Information May Lead to Substantial HIPAA Exposure for ISPs

06.29.11
By Adam H. Greene and Michael C. Sloan

Whether telecommunications carriers or Internet service providers (ISPs) know it or not, they may be subject to the privacy, security, and breach notification requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules. HIPAA's expansive reach may extend to ISPs that maintain individually identifiable health information on their systems. Penalties for violating the HIPAA rules can reach the millions of dollars, even for unknowing violations.

Thus, carriers and ISPs would be well served to:

- Evaluate the likelihood that they are maintaining health information on behalf of health care providers or health plans, such as through the provision of e-mail accounts, web hosting services, and other on-line offerings;
- Determine whether they are covered by HIPAA as business associates; and
- Consider creating a HIPAA compliance program to conform existing privacy and security safeguards to HIPAA.

HIPAA and business associates

HIPAA's Privacy, Security, and Breach Notification Rules require certain health care entities and their "business associates" to maintain the privacy and security of certain individually identifiable health information, called protected health information. Under the statute, HIPAA only applied to three types of "covered entities": (1) health plans; (2) health care clearinghouses; and (3) health care providers that electronically conduct certain transactions (such as the submission of health care claims). The HIPAA Privacy and Security Rules extended, through contract, many of HIPAA's requirements to business associates of a covered entity. A "business associate" includes any person who performs a function or activity involving the use or disclosure of protected health information on the covered entity's behalf.

Patient information generally constitutes "protected health information" under HIPAA if it identifies or reasonably could lead to the identification of an individual. Information is health information if it relates to an individual's health, receipt of health care, or payment for health care, including any information indicating that an individual received services from a particular health care provider.

The Department of Health and Human Services (HHS) has provided an exception from the business associate requirements for entities that act as "conduits." To the extent that an ISP is transporting protected health information on behalf of a covered entity and does not access the information other than on a random or infrequent basis as necessary for transport or as required by law, the ISP is a "conduit," not a business associate of the covered entity. Thus, a telecommunications carrier whose activities are limited to transmitting information "between or among points specified by the user … without change in the form or content of the information as sent and received" will usually be considered a conduit, and not subject to HIPAA in the course of providing telecommunications services. *See* 47 U.S.C. §§ 153(50, 51 & 53)) (defining "telecommunications," "telecommunications carrier," and "telecommunications service," respectively).

HHS also has indicated that document storage companies are not business associates to the extent that they transfer and maintain protected health information in "closed and sealed containers" and do not otherwise access the information. Thus, to the extent that an ISP maintains information in the electronic equivalent of a "closed and sealed container" (i.e., encrypted data), it can be argued that the ISP is not acting as a business associate.

However, to the extent a telecommunications carrier stores protected health information by offering Internet access and related data services, it potentially faces obligations under HIPAA as a business associate. For example, an ISP may provide a limited number of e-mail accounts to all customers. If a small health care provider maintains unencrypted protected health information on an e-mail account where the emails are stored on an ISP's servers, then this may take the ISP outside of the conduit exception and the ISP may become a business associate of the covered

entity.

The HITECH act's expansion of HIPAA

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, substantially expanded HIPAA in a number of ways. Importantly for ISPs who may qualify as business associates, the HITECH Act creates new breach notification requirements, makes business associates directly liable under HIPAA for the first time, exponentially increases HIPAA's penalties, and takes away the affirmative defense for an entity that did not know it was violating HIPAA.

Under the interim Breach Notification Rule (HHS has not yet issued the final rule), business associates must notify covered entities of breaches of unsecured protected health information without unreasonable delay, but no later than 60 days from the date of discovery (or the date the breach reasonably should have been discovered).

The HITECH Act makes business associates directly subject to the Breach Notification Rule, the Security Rule, and parts of the Privacy Rule for the first time. Accordingly, business associates are subject to civil and criminal enforcement actions, as well as ongoing contractual liability.

The HITECH Act also greatly increased the penalties under HIPAA and eliminated the innocent violation defense. Previously, a violation was punishable up to $100 per day, with continuing violations of a single requirement subject to penalties of up to $25,000 per calendar year (continuing violations of multiple requirements could reach hundreds of thousands). The HITECH Act increased these penalties to a range of $100 to $50,000 or more per violation, with continuing violations of a single requirement capped at $1.5 million per calendar year (continuing violations of multiple requirements could potentially reach tens of millions of dollars). This range of penalties applies even if an entity did not know, and by exercising reasonable diligence would not have known, of a violation.

Next steps for ISPs

ISPs would be well served to examine whether, in any of their lines of business, they may be acting as a business associate of a covered entity by storing or handling patient information. ISPs that are business associates should begin appropriate HIPAA compliance efforts, if they have not already done so. ISPs also may wish to consider to what extent, if any, it would be appropriate to enter into business associate contracts with customers (since covered entity customers are required to have such contracts in place with the ISP to the extent the ISP is acting as a business associate).

If an ISP experiences a security breach, it should consider whether there is the potential that some of the breached information includes protected health information that was being maintained on behalf of a covered entity. The practical reality is that ISPs will seldom know the content of the information they maintain and the identity of all their customers, so they should consider whether to treat all information as potentially subject to HIPAA.

Complying with the HIPAA Security Rule, which requires documentation of a variety of administrative, physical, and technical safeguards, does not happen overnight. Accordingly, if ISPs believe that they may have some exposure to HIPAA, they promptly should begin the process of conforming their existing security framework into a HIPAA-compliant program.

Finally, if ISPs use or share information for purposes other than storing or transmitting information, including sharing information with law enforcement, they should consider whether there is the potential that protected health information is being shared in a manner that would violate the Privacy Rule.

We recommend staying abreast of the changes in law that will occur as the HIPAA and HITECH rulemakings proceed, and DWT will provide updates from time to time.

Disclaimer