



# New Rules Challenge Health-Care Services

## *Modifications to HIPAA's Privacy and Security Rules may alter regulations for ISOs and MSPs*

By Julie Ritzer Ross

Besides stimulating the economy, the new American Recovery and Reinvestment Act aims to modify the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For ISOs and MSPs in the health-care market, that could mean new levels of risk and responsibility.

The issue of whether an ISO or MSP qualifies as a "covered entity" under HIPAA, and is therefore required to comply is not entirely clear-cut, says Mary Dees Griffith, president and COO of Preferred Health Technology in Carrollton, Texas. Griffith, whose company provides electronic payment, processing, and ancillary services to health-care entities, notes that while "a financial institution or payment processor may not be technically exempt from HIPAA, it also may not necessarily fall into the covered entity category in accordance with Administrative Simplification Standards adopted by Health and Human Services (HHS) under HIPAA."

According to the standards, a company is a covered entity if it is:

- a health-care provider that conducts certain transactions in electronic form, such as a physician, hospital, physical therapist, occupational therapist, or laboratory.
- a health-care "clearinghouse" that provides electronic health-care processing, such as insurance eligibility verification, claims adjudication, claim status messaging, pre-certification messaging, and electronic data interchange of claims data, as well as other types of health-care related data processing.
- a health plan, including an insurer, a third-party administrator or payer, a preferred provider organization (PPO), a health maintenance organization (HMO), or other type of health coverage plan.

In general, an ISO or MSP does not fit the definition of a "covered entity" unless it performs some other service in addition to payment processing that involves

contact with information that identifies the patient, includes details of a particular visit to a health-care provider, or reveals the specifics of services. Generally, health-care providers also must sign a HIPAA business associate addendum with any service provider whose relationship with them involves the use or disclosure of protected health information (PHI).

### More breach notification rules

All data breach requirements for the payment industry are managed by state law, Griffith explains. However, "the new requirement just enacted in the federal legislation puts the exposure of PHI of a certain magnitude by any company within the scope of breach notification requirements at a federal level. A breach of payment data of a certain number of consumers' payment information, that also included PHI, would need to meet a federal notification requirement based on this law, not only state law requirements," she says. For large breaches involving more than 500 residents in a particular area, HHS and a prominent media outlet must be contacted.

While the original version of HIPAA did not mandate a covered entity or business associate take "significant" notification action in all instances of data breaches, now they would need to notify each affected individual via U.S. mail, or, if previously specified, e-mail.

Not surprisingly, new breach provisions also specify the actual type and breadth of information that must be collected and provided to individuals, HHS, and media outlets, including a brief description of the incident, the date it happened, the date it was discovered, and the steps to be taken to prevent further potential harm. A covered entity also must disclose its investigation of the breach and how it plans to mitigate losses and protect against any further breaches.

### Stiffer penalties

For the first time, business associates now

must directly comply with many of HIPAA's Security Rules, including appointing a security official, developing written policies and procedures, and training workforces on how to protect PHI. And they must follow HIPAA's Security Rules relating to physical safeguards (locking computers that contain PHI), technical safeguards (encrypting e-mails), and adopting written policies and procedures. Failure to comply means civil monetary and criminal penalties for each notification.

In addition, state attorneys general can now take action against a covered entity or business associate that violates data security regulations.

"Covered entities" also face higher civil monetary penalties for privacy and security violations; for example, \$1,000 per violation if due to "reasonable cause and not to willful neglect," with a maximum penalty of \$100,000. Each violation that stems from willful neglect and is subsequently corrected brings a penalty of \$10,000, with a maximum of \$250,000. A penalty of \$50,000 is collected for each violation that is not corrected properly, with a maximum penalty of \$1.5 million per calendar year. Within the next three years, HHS will establish a regulation enabling individuals affected by a HIPAA violation to receive a percentage of any civil monetary penalty or settlement collected in line with that offense.

"Clearly, from audits, to penalties, to new notification requirements, to modifications, HIPAA's Privacy and Security Rules will create new levels of risk and responsibility for covered entities and businesses associates," says John Barlament, a partner at Michael Best & Friederich, a Milwaukee-based law firm that specializes in health care. "Covered entities in the payment industry are no exception" and should prepare for the challenges ahead. **TT**

*Julie Ritzer Ross is a contributing writer for Transaction Trends. Reach her at [jritzerross@gmail.com](mailto:jritzerross@gmail.com).*