# New regs ramping up security on personal medical data

PROTECTION From Page 52

Targeted affiliates include companies with whom providers contract for specialty clinical services such as radiology and for non-medical services including computer repair, office cleaning and insurance. Barry referenced a hypothetical social worker who keeps electronic case notes, including drug information, on a client who may be schizophrenic.

"If that device is not encrypted, it's a violation," she said. "If it's stolen and that information gets out there, the penalties are stiff."

Penalties of up to $1.5 million already are being meted out, in addition to the damage bad publicity can cause. And the fines, averaging $1,500 per incident, will only grow as federal investigators enlarge the scope of their audits, according to Barry.

"They're emphasizing HIPAA security-risk analysis," she noted. "It's a prerequisite to HIPAA compliance."

Although the government has long sought the power to require vendors to secure data, the providers themselves have been responsible for security. Contractors didn't face audits, fines or risk – until now.

According to Marcy Dunn, senior vice president and chief information officer for Rockville Centre-based Catholic Health Services of Long Island, the effort is designed to ensure that third-party vendors "treat this information with the same care and diligence" as more and more data is moved around in electronic form.

"We haven't had as much data in the hands of third parties [in the past]," Dunn said. "Data's continuing to grow and so are the ways of managing data."

The sharing of responsibility between the healthcare providers and their third-party vendors has prompted some reworked agreements between various parties, noted Pat Darienzo, Catholic Health Services' chief information security officer.

"If we had a company doing our billing, we had to make sure they were following the proper steps," Darienzo said. "That was difficult. In the past, they could tell us this is what they're doing, but it was up to us to make certain they were. Now it's up to them ... and a lot of old business associate agreements needed to be rewritten."

MARCY DUNN: Handle data with care. *Photo by Bob Giglione*

The irony, Darienzo added, is the need to better protect data passing through third-party hands is at least partially caused by the growing demand to make personal healthcare information more readily available.

"On the one hand, they're saying, 'Make the data available to whoever needs it,'" she said. "But they also say, 'Make sure only the people who need it can look at it. You try to protect it from unauthorized people, but make it available to people who need it."

The new regulations mean more work for auditors who are being hired to test and verify the various protection protocols in place. They also mean higher data-protection expenses for healthcare providers and their associates, but that cost should prove minimal, according to Dunn.

"There is some cost added, but some is offset by the savings of having data electronically available," she said.

■ CLAUDE.SOLNIK@LIBN.COM



HEALTHCARE

# Feds taking fresh look at patient-data protection

## New rules, audits eye providers and third-party vendors

By CLAUDE SOLNIK

The federal government is imposing new rules and conducting fresh audits related to the protection of medical-record privacy.

The government's target: healthcare providers and a wide range of entities with access to the data.

The U.S. Department of Health and Human Services' Office of Civil Rights has completed a pilot program that reviewed how sensitive data is handled. It's now launching full-fledged audits of 1,200 entities – including providers and some 400 of their business associates – designed to make sure that organizations are complying with new, stricter compliance rules.

This is the latest addition to the Health Insurance Portability and Accountability Act, which was passed in 2006. The biggest change is that the government has increased the responsibility of "associates," companies that contract with hospitals and other providers, when it comes to safeguarding data.

"Business associates have to be able to prove that they protect any information they get from that client the same way a covered entity would," said Grace Barry, president of Melville IT services provider Barry Tech Consulting.

See PROTECTION, Page 58

GRACE BARRY: Risks are high, penalties are "stiff." *Photo by Bob Giglione*