Codify
BY AAPC

Health Information Compliance Alert

HIPAA: Can You Afford to Make These Data Security Mistakes?

Legal expert outlines lessons learned from lost hard drives

In the second major data security breach in which Health Net is involved, it announced on March 14, 2011 that some of its data drives were stolen or lost from its data center in Rancho Cordova, Calif.

In an exclusive interview given to **Eli**, **Kenneth N. Rashbaum, Esq**., of Rashbaum Associates, LLC, New York, NY, pointed out that: there are many legal implications of a data security breach such as this. "If the health IT providers are working with health care providers or health plans, such a loss could result in an investigation by the Office of Civil Rights of the U.S. Department of Health and Human Services, or a state attorney general if HHS declines to proceed, and that, in turn could result in the imposition of significant civil monetary penalties."

Get the word out immediately

Though the company discovered the breach in February, the matter was reported to the California Attorney General's office on March 4, 2011 by Health Net. The public was notified on March 14 via a press release.

"This investigation follows notification by IBM, Health Net's vendor responsible for managing Health Net's IT infrastructure, that it could not locate several server drives. After a forensic analysis, Health Net has determined that personal information of some former and current Health Net members, employees and health care providers is on the drives, and may include names, addresses, health information, Social Security numbers and/or financial information," the company's press release stated. However, the release does not mention how many people were actually affected or even how many servers were missing.

When one realizes that the nine missing server drives contained personal information for 1.9 million current and past enrollees nationwide, "including records for more than 622,000 enrollees in Health Net products regulated by the California Department of Managed Health Care (DMHC), more than 223,000 enrolled in California Department of Insurance products, and a number enrolled in Medicare," the issue takes on mammoth sized implications.

Prepare for an investigation

"The DMHC has opened an investigation into Health Net's security practices," DMHC spokesperson **Lynne Randolph** said in a press release after the DMHC swung into action following the announcement of the breach. She further assured people affected by the breach that "Health Net has agreed to provide two years of free credit monitoring services to its California enrollees, in addition to identity theft insurance, fraud resolution and restoration of credit files, if needed."

Health Net's press release about the breach incident came on Monday, March 14, 2011 after the Connecticut attorney general's office released a statement calling attention to its investigation of the breach. Connecticut Attorney General **George Jepsen** issued an alert stating that the breach could affect nearly 25,000 residents in Connecticut. California's Department of Insurance also announced their own investigations soon.

Loss of business reputation and credibility

When asked by Eli what the lessons learned by this loss are, Rashbaum responded by saying, "Entities accessing identifiable patient information ('Protected Health Information', or 'PHI') must prepare and implement policies and procedures to protect the data. This is required by HIPAA, the HITECH Act and the privacy laws of many states. The potential penalties for loss of this information are significant, and include loss of business reputation and credibility due to adverse publicity."

It is not clear whether the company has formed a breach site to answer breach victims' questions and to report on a status of the investigation. They have not mentioned it on the site announcing the breach. "To help protect the personal information of affected individuals, Health Net is offering them two years of free credit monitoring services, including fraud resolution and, if necessary, restoration of credit files, as well as identity theft insurance. These services will be provided through the Debix Identity Protection Network," the company's press release stated.

Show proof of security protocols

Covered entities need to have policies in place to physically and technically safeguard PHI as they remain liable for theft of their computers containing protected health information. According to Rashbaum, "If the covered entity has not taken appropriate precautions, by instituting protocols for physical, technical and administrative safeguards for PHI, the covered entity may face actions by OCR or, if OCR declines to proceed, state attorneys general, for civil monetary penalties, and may be exposed to civil law suits by affected patients under state privacy laws (there is no civil cause of action under HIPAA)."

So, what protections should covered entities have in place to avoid being held liable for a breach if computer hard drives are stolen? "Liability for penalties under HIPAA, or for damages in a state privacy law action, turns on many factors. However, the defense to such actions is best enhanced by implementation of policies and procedures for technical, physical and administrative safeguards for the protection of PHI, documented training of the work force on those safeguards, and regular monitoring of compliance," says Rashbaum.