Codify
BY AAPC

Health Information Compliance Alert

Case Study: Take These 4 Actions Before (Not After) A Breach Incident Occurs

Beware: An additional state AG has healthcare data breaches in its crosshairs.

Yet another HIPAA breach case has involved the misdeeds of a healthcare provider's business associate (BA), giving you one more reason to refine your BA agreements (BAAs) and ensure that your vendors aren't putting your patients' protected health information (PHI) at risk for exposure.

State AGs are Cracking Down on HIPAA Breaches

Background: A hospital and its BA are paying out $90,000 and instituting extensive correctional measures to resolve a breach arising from the 2012 theft of a laptop containing unencrypted patient information, according to a Nov. 6 announcement by the Connecticut Attorney General's (AG's) office.

Hartford Hospital contracted with **EMC Corporation** to assist with a quality improvement project on hospital readmissions. An employee received a laptop from a company that EMC had previously acquired, and the device contained the unencrypted PHI of 8,883 hospital patients. In June 2012, the laptop was stolen from the employee's home.

"While the laptop has not been recovered, the hospital maintains that there is no evidence that the information has been misused," the AG's statement said. Nevertheless, both the hospital and EMC entered into an agreement with the AG to pay the monetary penalty and implement new training requirements and other policies.

Pay attention: Covered entities' (CEs') and BAs' responsibilities for safeguarding PHI under HIPAA and state law are clear, Connecticut AG **George Jepsen** said in the announcement. "All healthcare providers and any contractors who work with healthcare providers should pay close attention to these responsibilities and review their internal controls and policies to ensure that they're doing all they possibly can to comply with the law and to keep this information safe."

Lessons Learned: Check Off These Tasks Now

In addition to making a $90,000 payment to be deposited in the state's General Fund, the agreement with the AG requires EMC and the hospital to:

1. Tighten up BAAs. Following the breach, the hospital instituted a variety of corrective measures to ensure that contractual agreements BAAs in particular are properly executed with vendors, and that the hospital implements minimum privacy and security controls when it will share PHI with a vendor. The hospital created new contract templates for their BAAs that incorporate applicable HIPAA provisions.

2. Enhance HIPAA compliance training. Under EMC's agreement with the AG, the company must provide training to employees who are responsible for handling or using PHI. Also, the hospital electively enhanced its annual mandatory compliance training and developed new training for business managers regarding their HIPAA obligations.

3. Use multi-layered encryption methods. In addition to complying with the privacy provisions and standards under HIPAA, the AG agreement requires the hospital to use a combination of hardware and software to encrypt files or data

containing PHI prior to its transmission or transfer, whenever applicable. The AG is requiring the hospital to submit a report in one year to demonstrate its implementation of the corrective measures.

4. Create ultra-specific compliance policies. Under the AG agreement, EMC must maintain reasonable policies requiring the encryption of all PHI stored on laptops or other portable devices and transmitted across wireless or public networks. EMC must maintain reasonable policies for employees relating to the storage, access and transfer of PHI outside of EMC premises, as well as policies for responding to events involving unauthorized acquisition, access, use or disclosure of PHI.