Long-Term Care Survey Alert

Patient Privacy: Don't Let Terminated Employees Sneak Out With Patients' PHI

Yet another HIPAA breach reinforces all the crucial reasons why you should encrypt all mobile devices and portable data storage, as well as why you must keep a close watch over what employees and former employees take home with them.

A home burglary sparked a breach incident for **St. Elizabeth's Medical Center** in Brighton, Mass., after thieves stole a former employee's laptop and USB thumb drive that both contained 595 patients' protected health information (PHI), according to an Aug. 29 blog posting for the law firm **Nixon Peabody LLP** by attorney **Kathryn Sylvia**. The laptop and thumb drive were not encrypted and contained patients' dates of birth, medical history, diagnoses, test results and medications.

The patients received treatment at **St. Elizabeth's Center for Breast Care** or the hospital's hematology/oncology department sometime from May 14, 2011 through Jan. 31, 2014. The former employee was a physician at St. Elizabeth's.

St. Elizabeth's does not allow storage of unencrypted PHI. Although St. Elizabeth's has reported the theft to affected patients and officials do not believe that the thieves have misused the PHI, local police are still investigating the incident, Sylvia noted.

Takeaway: "This should be a lesson for health care facilities and hospitals to ensure that, upon termination, all employees return electronic patient data and all hard drives or USB thumb drives are wiped clean to avoid situations like this," Sylvia stressed.