Part B Insider (Multispecialty) Coding Alert

Physician Notes: Don't Forget Former Staff for HIPAA Compliance

You still have to worry about employees' laptops and portable devices when it comes to HIPAA even if they aren't employees anymore.

Case in point: A home burglary sparked a breach incident for St. Elizabeth's Medical Center in Brighton, Mass. Thieves stole a former employee's laptop and thumb drive that contained 595 patients' protected health information, according to attorney **Kathryn Sylvia** of Nixon Peabody. The laptop and thumb drive were not encrypted and contained patients' dates of birth, medical history, diagnoses, test results and medications.

The former employee was a physician at St. Elizabeth's. 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 in a blog post.

Takeaway: "This should be a lesson ... 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.

And it reinforces that PHI should be encrypted in any case, experts note.