Part B Insider (Multispecialty) Coding Alert

Privacy: Make Sure Your Business Partners Don't Sabotage Your HIPAA Compliance

This stolen laptop led to headaches for one health entity.

How far do you want to go in policing your business partners' HIPAA information security practices? One Connecticut provider may wish it had gone further after a recent HIPAA violation.

VNA HealthCare in Hartford, Conn. and its parent Hartford Hospital learned that a contractor's employee doing hospital readmission data analysis had a laptop stolen from the employee's home, the VNA and hospital say in a release. The laptop contained unencrypted data on more than 7,400 VNA patients and 2,000 hospital patients, they reveal.

The data includes patients' names, addresses, dates of birth, marital status, Social Security numbers, Medicaid and Medicare numbers, medical record numbers, and certain diagnosis and treatment information. Having such unencrypted data on the employee's laptop was a violation of the contractor's policy, the VNA and hospital note in the release.

The HIPAA breach isn't technically the VNA's fault. The providers \"go to great lengths to ensure that data transmitted or transported by their employees are fully encrypted to prevent unintended disclosure,\" they note in the release.

But the VNA and hospital still are left holding the bag when it comes to dealing with the fallout from the breach. \"We profoundly regret this incident happened. Integrity and safety are two core values of both Hartford Hospital and VNA HealthCare,\" they say. \"We take very seriously our stewardship of this information, which is central to our roles as healers and caregivers.\"

In addition to apologizing, they are offering two years of free credit report monitoring for patients whose data was affected by the breach.

Think About HIPAA When Crafting Contracts

\"It might surprise you how often this happens,\" notes HIPAA expert Robert Markette Jr. with Benesch Friedlander Coplan & Aronoff in Indianapolis. \"Your business associates may not be as compliant as you think.\"

But how far do you want to go in policing your BAs? They already are subject to direct HIPAA penalties under the HITECH Act, Markette points out.

\"How do you verify no data has been placed on a contractor device?\" he asks. You can require that contractor employees don't take data home, but monitoring compliance would be a logistical challenge Procedures like random audits or programs that log data access and copying can be cumbersome.

Try this: Consider including penalty provisions in your associate contracts, Markette suggests. \"Instead of putting the BA on the hook for costs, have additional contractual penalties for breaches.\"