Two Little Mistakes Will Cost Chicago and Connecticut Home Care Agencies Thousands in HIPAA Reparations

It can no longer be said that major HIPAA disasters happen to other people, people in the news, not "good agencies like ours." They did happen to people you know, people just like you, just last month. If it could happen to Northwestern Memorial Hospital Hospice in Chicago and Hartford Hospital and VNA HealthCare in Connecticut, good healthcare providers just like you, it could happen to you, unless you are extraordinarily vigilent.

Chicago

This time it was not a nurse or therapist leaving a laptop PC on the front seat of a car or in a coffee shop; it was the IT department's fumble. On June 11, burglars broke into Northwestern Memorial Hospital's Home Hospice office in Chicago and made off with six laptops and tablets.

The laptops and tablets had been brought in from the field by clinicians for a software upgrade. They run a home care and hospice application that cannot be upgraded remotely. During the process, technicians turned off the units' security protections, which is standard procedure when updating this software, but did not complete all upgrades in one day. The burglars happened to choose that particular night to break in.

The hospital released a statement saying that personal information on the stolen devices could include patient demographics, name, address, date of birth and social security numbers, plus detailed medical treatment and medication information for current hospice services and any previous home health services. The hospital regrets the incident and will now take "decisive measures" to prevent future breaches.

Regarding the Chicago incident

Ask your point-of-care software vendor why software upgrades must be installed in-person on every field computer by bringing them into the office for technicians to apply the upgrade manually. These PCs are able to synchronize remotely to exchange visit and other data with the office every day. Could software upgrades not also be accomplished via that connection?

1. Ask your technicians, if encryption and other security systems must be disabled in order to install a software upgrade, does HIPAA protocol not automatically mean that those exposed laptop PCs and tablets, assuming they still have patient data stored on them, will not be left alone until the upgrade is completed and security is reinstalled?

2. Ask your software vendor why it is necessary for field computers to store information of hundreds, even thousands, of patients. Is it not possible for their software application to store not more than each user's current caseload and to download additional patient data only if needed?

Hartford
On June 26, Hartford Hospital and VNA HealthCare learned that an unencrypted laptop computer containing personal information on 7,461 home care patients and 2,097 hospital patients was stolen from an employee of an outside contractor hired to do data analysis. The data included names, addresses, dates of birth, marital status, Social Security numbers, Medicaid and Medicare numbers, medical record numbers and certain diagnosis and treatment information.

The contractor, Greenplum, a subsidiary of hospital vendor EMC Corp., stated that the unnamed employee was in violation of company policy. It is not clear from reports whether that policy concerned having unencrypted patient data on a company laptop or taking that laptop home.

Regarding the Connecticut incident

1. Examine the wording of the Business Associate agreement with the outside contractor. Does it state that the VNA will accept responsibility for the costs of a security breach if a VNA employee is found to be at fault and that the contractor will absorb the expenses if one of its own employees causes the breach? Does the BA agreement include the contractor's written policy for its own employees about removing patient data from the contractor's office?
2. As this is a familiar type of breach – a contractor employee taking a laptop home and losing it to a thief has happened – perhaps it is time for HIPAA covered entities to insist that outside contractors do their work on the entity's premises, not the contractor's office.
3. When trusting an outside contractor with protected patient information for the purposes of data analysis, determine whether de-identified data will serve the desired purpose as well as data with patient names and personal information will. If so, forbid identifiable patient data from being copied from your central database to any outside, especially mobile, computers.

No measures are ever 100% foolproof but remember that demonstrating that reasonable prevention efforts were in place goes a long way when defending oneself, both in the press and before the Office of Civil Rights.