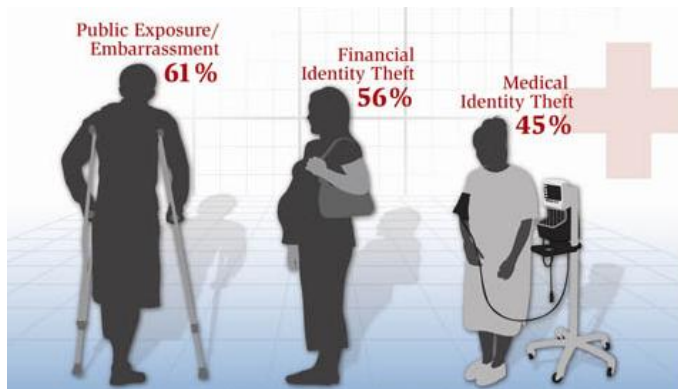


June 2011

STAFF NEWSLETTER

©by Vianna Zimbel Consulting

WHEN PATIENT DATA IS BREACHED



4.9 million patients had their personal health information (PHI) compromised between 2009 and 2010.

Factors causing data access, acquisition, loss, or disclosure of personal information are typically unintentional employee action, such as a delivery vehicle is stolen along with customer forms, papers fly out a truck window as a Tech is driving down the road; or, worse yet, a clinician or manager's laptop is stolen.

What do you do?

First, determine how many patients are affected, and what kind of information was lost, revealed or stolen.

Notice to Affected Individuals. In most instances you must provide notification of a breach to each individual whose unsecured PHI has been involved in the breach. This notice must be provided without delay and in no later than 60 calendar days after the date the breach was discovered. The notice must be provided in writing to the individual by first-class mail and must include certain information, such as a brief description of the breach incident and the types of unsecured PHI involved (e.g., full name, social security number, etc.).

Notice to Health & Human Services (HHS). If more than 500 individuals are affected by a breach, you must notify HHS concurrently with notification to the affected individuals as specified on their website: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>. With breaches that affect fewer than 500 individuals, the notification may occur later.

Notice to Media. In cases where a breach of unsecured PHI involves more than 500 residents of a state, you must provide notification of the breach to prominent media outlets serving your state no later than 60 calendar days after discovery of the breach. This notice must include the same information that is required for the notice to affected individuals. A breach is generally considered "discovered" as of the first day the breach is known.

Encrypt for Safe Harbor

If the stolen desktop or laptop has an encrypted disk, the "safe harbor" provision of the HITECH Act says that the theft does not have to be reported. Today, disk encryption is an inexpensive way to avoid the more onerous and punitive parts of HITECH.



Safeguarding our patients' PHI is not rocket science. In fact, the best advice sounds a lot like what our mothers would tell us: Don't go where you're not supposed to go. Treat other people's things (PHI) just like you want your own things to be treated. And when you're finished, clean up after yourself and put everything safely away.