

Avoiding a Medical Data Breach



By
Bruce Nelson

More than 30 healthcare networks have been victimized by identity thieves and data breaches, and more occurrences are expected in 2010. These events are extremely costly to the organization; in the short term, the reparations and notices to patients, along with the fines imposed by government entities are quite costly. However, the greater risk is the long-term negative impact on the hospital's credibility and reputation in the community.

Unfortunately, experts predict this trend to continue well beyond 2010 and hospitals need to mitigate their risk as well as protect their patients' medical information from a potential financial and public relations disaster.

Health care is well-suited for breaches

Most data breaches can be attributed to a disgruntled or departing employee. This is especially problematic for healthcare organizations. According to the Ponemon Institute, the industry experiences an annual turnover rate of 6.5% — almost double the national average of 3.6%.

The government responds with the HITECH Act

Proactive protection of health information is now mandated under the Health Information Technology for Economic and Clinical Health (HITECH) Act (and state laws in California and Missouri) — which requires healthcare institutions to develop notification and prebreach programs.

According to the Energy and Commerce, Ways and Means, and Science and Technology committees, the HITECH Act strengthens the enforcement of federal privacy and security laws by increasing penalties and providing greater resources for enforcement and oversight.

Among other mandates, the HITECH Act outlines how hospitals must notify their patients and community of a breach through the one of following notices:

- **Actual notice:** Affected individuals, guardians or next of kin must receive written notice at their last known mail or email address.
- **Substitute notice:** If contact information is not available, the health care network must provide substitute notice, usually in the form of a conspicuous posting on the network's website or other location and/or a media notice, as soon as reasonably possible.
- **Media notice:** For breaches affecting 500 or more residents of a single state or jurisdiction, the hospital is required to provide notice to prominent media outlets in that area.