# Solutions and Best Practices for Addressing a Healthcare Data Breach


June 2010

Businesses are impacted by data breaches in many ways, including potential loss of business or negative effects to their brand equity. According to the 2009 Javelin Strategy and Research study, "Using Triage to Ease the Pain of Customers At Risk", 50% of consumers who have been severely injured by a data breach switched their business to a competitor.

Recently more than 40 healthcare networks of all sizes have been victimized by medical data breaches and more are expected throughout 2010[1]. These events are extremely costly to hospitals and healthcare organizations. In the short term, the reparations and notices to patients and 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. Hospitals need to mitigate their risk as well as protect their patients' medical information and their network from this potential financial and public relations disaster.

Most recorded data breaches can be attributed to employee theft or mismanaged data practices, often initiated by disgruntled or departing staff. Healthcare organizations experience a high annual churn rate of employees of 6.5 percent which is almost double the national cross-industry average turnover rate of 3.6 percent, according to the Ponemon Institute[2]. With more employees entering and exiting hospital payrolls, the risk of data breaches increases. Unfortunately, the potential consequences of a data breach can be severe for healthcare companies, clients and/or employees.

Additionally, the current economic environment has made healthcare costs rise sharply. With more individuals out of work or underinsured, the market for health information is more profitable, which draws even more attention from identity thieves.

Proactive protection of health information is now mandated under the Health Information Technology for Economic and Clinical Health (HITECH) Act and requires healthcare institutions to develop notification and pre-breach programs[3]. This 2009 legislation expands current federal privacy and security protections of health information. Given these guidelines and penalties, a hospital's best choice is to proactively curb medical data breaches before they occur.

Deterring and detecting data breach threats does not happen by chance. Leading healthcare companies are taking advantage of new processes and proven solutions used in other industries, namely financial and credit card markets, to prevent breaches from occurring.

**Leading best practices include:**

**Appoint a responsible party:** Hospitals should make data breach avoidance part of an individual's or a team's job description. Appointing an accountable resource will initiate process improvements, provide a central contact to direct noncompliance inquiries to, define a point of contact who would perform any investigations, and would assign leadership for all legal and notification efforts in the event of a breach.

**Expand compliance training:** A variety of individuals require access to patient health information to perform their job. Hospitals need a process to ensure that all employees participate in annual compliance training.

**Build a compliance culture:** The entire hospital community should value the privacy of patients' data as part of the organization's mission. This includes offering trusted avenues to report noncompliance activities. All individuals — staff, contractors and partners

1 Identity Theft Resource Center 2009
2 The Ponemon Institute Annual Study, "U.S, Cost of a Data Breach." February 2008
3 Javelin Strategy and Research, "New Federal Personal Health Information Breach Notification Law HITECH ACT - A Tsunami of Opportunity." April 2009.

— must be diligent in their compliance and alert the responsible party to processes and/or individuals who may be operating outside of privacy policies.

**Monitor information:** Automated monitoring of employee and patient information will alert hospitals of possible data breaches, often before they impact hundreds of individuals. Used by thousands of corporations across the United States, third-party products and services are available to monitor credit reporting agencies and proactively alert organizations of fraudulent events.

**There are several strategies a firm can implement for immediate breach response planning, customer notification, protecting vulnerable customers, and supporting long term breach preparation:**

**Respond to a breach:** Immediate and swift response is highly recommended. Consider consulting with a data breach resolution agency. There are a number of data breach resolution providers, offering a range of services including: notification services, call center support, forensic analysis, credit monitoring, fraud alerts and protection, and fraud resolution services. Additionally, completing an investigation and assessment of the data accessed, the individuals affected, and the potential cause of the breach is recommended.

**Notify affected consumers:** Breach notification should occur in a timely, thorough and clear manner following company awareness of the breach and across many channels. Customer communication should address who, what, where and why the data was breached. Communication should be transparent and reinforce the message that the consumer is being protected from potential financial damages as a result of the breached personal health information (PHI).

**Protect most vulnerable consumers:** In order to mitigate the risk of new account fraud from occurring among consumers with exposed PHI, offer complimentary subscriptions for identity theft detection, protection and fraud resolution products.

**Empathize with consumers:** After a breach, consumer confidence in the breached company can lag. As such, it is critical that the breached company take measures to reassure consumers. Maintaining open communication and providing assurance that the situation is being addressed through a robust data breach resolution program, can help to reduce potential consumer fallout for a company.

**Prepare a long-term plan:** Develop a formalized plan that is flexible enough to address changing threats and legal requirements. Create a breach response team to manage communication with those affected.

Data breaches are problematic for healthcare organizations. Progressive healthcare professionals are looking at new means to protect themselves, and they are finding their answers from colleagues in other industries. To provide maximized results, it's recommended that hospitals advance their culture, training and systems to encourage compliance in every activity and have a plan in place to immediately address a medical data breach should one occur.

Unfortunately, medical data breaches do occur despite the best practices put in place by conscientious companies. As a matter of fact, an institution's response to a security breach may ultimately worsen or salvage any potential reputation damage generated by a data loss incident[4]. Managing a breach of personal health information (PHI) can be an overwhelming task, especially if the breach occurs suddenly and a company does not have a plan in place.

To learn more about data breach resolution, visit www.experian.com/databreach, or contact Experian® at databreachinfo@experian.com or 1 866 751 1323.

For more information on SearchAmerica, a part of Experian, and our SaaS financial clearing solutions for the healthcare industry, visit www.searchamerica.com.

4 Javelin Strategy and Research, "Data Breach Response Best Practices; Prepared for Experian." May 2009