Healthcare Data Breach Preparedness

Improving security continues to be a top concern for the industry.

It has been 14 years since the enactment of HIPAA. Yet it is only recently that we are beginning to understand the impact and intent of what has become a wave of regulatory focus on privacy and security, especially as it pertains to an individual's protected health information (PHI). With the latest HITECH Act mandates, the healthcare industry is finding that, yes, HIPAA is here to stay. Not only that, but now covered entities and business associates need to prove that they're actually doing what their policies and procedures state.[1]

A recent survey[2] of healthcare organizations indicates that the industry is aware of the urgent need to improve technology and training in order to protect PHI but still has a long way to go. The survey also found that:

- Only 4% of healthcare organizations are highly confident in the security measures of business associates and their subcontractors
- 43% rank their own ability to counter external and internal security threats as failing, poor or in need of improvements
- The two top security priorities for the upcoming fiscal year are improving regulatory compliance efforts and internal awareness of security issues

With so much uncertainty regarding security and privacy, the healthcare industry is likely to continue experiencing data breaches until – and even after – today's key security challenges are addressed. Organizations have to keep in mind that the technological aspects of data security are always changing. And, you can never completely eliminate human error.

So while organizations focus on training their staff and improving their technology to help protect data, a third goal also needs to be addressed. That is preparing for a data breach. Preparing for a data breach means outlining exactly what steps you would take to bring things under control if one occurs.

There's a lot to lose if your organization experiences a breach of PHI. If the breach catches you off guard, you may face severe fines and reputation damage for mishandling it. Fifty-four percent of companies believe it can take 10 months to more than two years to restore a company's reputation following a breach of customer data.[3]

Fifty-four percent of companies believe it can take 10 months to more than two years to restore a company's reputation following a breach of customer data.[4]

[1] Risk Assessment in HITECH, Experian® Data Breach Resolution and Sinaiko Healthcare Consulting, Inc. (2010)
[2] Healthcare Information Security Today Survey by Information Security Media Group, co-sponsored by Experian® Data Breach Resolution (2011)
[3] Reputation Impact of a Data Breach, Ponemon Institute (2011)
[4] Reputation Impact of a Data Breach, Ponemon Institute (2011)

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

Experian® Data Breach Resolution

Experian℠

AVOID LOSS

These steps can help your organization prepare for and minimize the loss associated with a data breach:

Appoint a responsible party: Every organization needs a dedicated resource to handle privacy and security issues. This person or team should implement process improvements, review noncompliance issues, initiate any investigations and assign leadership for all legal and notification efforts in the event of a breach.

Vet your compliance training: Healthcare organizations need to make annual compliance training a priority. A variety of individuals require access to PHI to perform their jobs, and everyone needs to be aware of the risks associated with mishandling PHI. The more informed everyone in your office is, the stronger your compliance efforts are.

Observe information: Automated monitoring of employee and patient information will alert organizations to possible data breaches, often before they spiral out of control.

Instill a compliance culture: All individuals — staff, contractors and partners — must be diligent and alert the responsible party to processes and/or individuals who may be operating outside of privacy policies.

Design a long-term plan: Develop a formalized security strategy that is flexible enough to address changing threats and legal requirements. Update it as needed.

Leverage response efforts: If a data breach occurs, know in advance whom you'd call for a forensic analysis of the breach as well as data breach resolution services, including consumer notification, call center support, identity theft protection and fraud resolution services for affected individuals.

Organize notifications: Various state and federal laws mandate notification timelines and standards. Breach notification should occur in a timely, thorough and clear manner following company awareness of the breach. Engage a data breach resolution provider to keep your notification efforts compliant and on track.

Secure affected individuals: In order to mitigate the risk of new account fraud from occurring among consumers with exposed PHI, offer complimentary subscriptions for an identity theft detection, protection and fraud resolution product.

Sympathize with consumers: Maintain open communication with and provide assurance to affected individuals that the situation is being professionally addressed through a robust data breach resolution program. How you handle or mishandle data breach response can help to either reduce or increase potential consumer fallout.

Data security is sure to remain an important initiative and challenge for healthcare organizations. Be sure you're prepared if your security measures are compromised and a data breach occurs.

Healthcare Information Security Today Survey: View the full report at www.Experian.com/HealthcareInfoSurvey

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

Experian® Data Breach Resolution

Experian℠