EXPERIAN® DATA BREACH RESOLUTION

Prepare. Respond. Recover.

Experian℠

Are you prepared to respond to a breach and recover with your patient loyalty and reputation intact? Use these steps as a guide to help you **AVOID LOSS**:

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.

To learn more about data breach resolution, contact Bob Krenek at bob.krenek@experianinteractive.com or call 1 770 619 1778.

Visit us online at Experian.com/DataBreach.

Conducting a HITECH Risk Assessment

SINAIKO
HEALTHCARE CONSULTING, INC.
An Altegra Health Company

The risk assessment process varies according to an organization's particular business needs and available skills. However, at its core, the most basic risk assessment process must answer the questions: What is at risk? What can go wrong? What is the probability that it would go wrong? What are the consequences if it does go wrong?

Risk assessment processes require the definition and inventory of systems and the business processes they support; an assessment of potential vulnerability and threat; a decision to act or not; evaluation of the effectiveness of the action; and communication about decisions made. Once these steps are completed, the process should be repeated on a regular basis to ensure that the decisions made and controls implemented remain effective in reducing risk and meeting business needs and goals.

Risk Assessment Phases

Phase I: Inventory of Systems and Processes

- Identify the technologies, processes and people that interact with protected health information (PHI)
- Align assessment with organization's business objectives and/or mission

Phase II: Threat and Vulnerability Assessment

- Methodically consider accidental breaches, destruction or alteration of data, and unauthorized disclosures
- Determine likelihood of risk occurrence
- Identify possible accidental vs. intentional vulnerabilities/exploits
- Identify possible internal vs. external vulnerabilities/exploits
- Identify reasonably anticipated harm
- Define risk ranking (likelihood and cost of each identified vulnerability/exploit)

Phase III: Evaluation of Controls

- A perfect control reduces a threat/vulnerability to zero
- Establish a control that reduces (or eliminates) the risk for each actionable vulnerability/exploit (from Phase II)
- Each control should be measurable in terms of effectiveness

Phase IV: Decision

- Decide how to manage the identified and ranked risks
  - Accept the risk (do nothing)
  - Mitigate the risk (implement identified controls)
  - Transfer the risk (e.g., buy insurance)

Phase V: Communication and Monitoring

- Ongoing communication and regular monitoring are the best ways to ensure ongoing program success
  - Develop policies and procedures that match what you do (avoid saying one thing, but doing it differently)
  - Find ways to communicate regularly to business-process owners about risk and what it means to them
  - Create an annual risk assessment program calendar that allows for monitoring and review of action plans; policies and procedures; and contemplation of the program's ability to reduce risk
  - On an annual basis, adjust the risk program to reflect any new risks that need to be addressed, or past risks that can be retired

For more information about revenue cycle services or HITECH risk assessments, contact Derek Woo at derek.woo@sinaiko.com or call 510-913-2534.

Visit us online at www.sinaiko.com.