

Best Practices for a Healthcare Data Breach: What You Don't Know Will Cost You



STROZ FRIEDBERG

By:
Emilio Cividanes, Venable LLP
Partner and Co-Chair Regulatory Practice Group

Paul Luehr, Stroz Friedberg
Managing Director & Chief Privacy Officer

Bob Krenek, Experian® Data Breach Resolution
Senior Director

May 2011

In the healthcare industry, data breaches are common and costly. There is a lot at stake for companies that aren't prepared.

When your company discovers a data breach, will you a) panic or b) put your data breach response plan into action? If your only option at the moment is to panic, then you need to consider putting a response plan in place. Notice that the question doesn't begin with, "If your company discovers a data breach." That's because data breach experts are no longer talking in terms of "if." Today, data breaches are so common, everyone is talking in terms of "when."

In the healthcare industry, data breaches are common and costly. There is a lot at stake for companies that aren't prepared. Customer turnover is one of the driving costs. If you're watching the numbers, they're going from bad to worse:

- Data breaches cost hospitals alone \$6 billion per year, according to a 2010 study.¹
- The total economic impact of medical identity theft is \$30.9 billion annually, up from \$28.6 billion in 2010.²
- Healthcare firms spend about \$1 million per year, per firm, on data breaches.³

A data breach response plan helps to counteract all of these negative effects. Today, all facilities that maintain medical data or personal data need to have an incident response plan in place.

Challenges Unique to Healthcare

There's no doubt that the healthcare industry is under a great deal of scrutiny when it comes to data breaches. So much so that an organization may find it difficult to determine which legislation and regulations govern a particular data breach at a particular time.

Healthcare organizations must balance state and federal laws, such as HIPAA and HITECH, in formulating a data breach response. Different states or different laws may define protected information differently. For example, some states only cover consumer information, such as credit card data and Social Security numbers, but Arkansas, California, Delaware and Missouri include medical information in their state data breach laws. A single, widespread data breach may call into play the regulations of multiple states, depending on where the affected individuals reside.

Clearly it is confusing territory. Proposed legislation may not make it any easier. One proposed bill would surpass HIPAA in its treatment of consumer data related to medical conditions. Other bills directed at all industries would require notification of regulators within just 48 hours of a breach.

Making compliance even more daunting, the federal Department of Health and Human Services (HHS) is now only one of the watchdogs flexing its muscle over healthcare data security. State health and insurance commissioners have imposed their own tight timelines on reporting a breach. In addition, the Federal Trade Commission has issued a rule similar to state laws governing breach notification. It applies to establishments serving in at least one of these roles: vendor of personal health records, related entity and/or third party service provider to either of the aforementioned. Note that a company or healthcare institution can play a "dual role." Should an organization like this suffer a data breach, its main role at the time of the incident ultimately determines agency jurisdiction.

¹ Ponemon Institute, "Benchmark Study on Patient Privacy and Data Security." (2010)

² Ponemon Institute, "Second Annual Survey on Medical Identity Theft." (2011)

³ Ponemon Institute, "Benchmark Study on Patient Privacy and Data Security." (2010)

Incident Response Plans

The legal framework of data breach response is a changing landscape. But that doesn't give your organization a free pass to put off creating a response plan. While each organization needs an incident response plan unique to its business operations, in general, every plan should include:

- **Designated incident team leader and back-up.** This is typically someone from an internal or external legal department or a Chief Privacy Officer who will coordinate response efforts among all groups.
- **Emergency contacts.** These will include your outside experts as well as your internal C-level executives, legal, HR, IT, PR/Marketing and customer service. Know in advance whom you will call for specialty services such as digital forensic investigations or identity theft protection and resolution.
- **Internal reporting system.** Your response plan should outline a structure of internal reporting to ensure everyone on the data breach response team is notified and taking appropriate action in a timely manner.
- **Regulatory and law enforcement contacts.** If you believe the data breach may have involved illegal activities, notify law enforcement, which could involve the U.S. Secret Service or Federal Bureau of Investigation. During an ongoing investigation, law enforcement may ask you to *delay* notification to consumers. Regardless, be sure to document all conversations, instructions and steps followed.

- **Action items to assess and respond to the scope of a breach.** Clearly defined steps, timelines and checklists are critical to keep everyone focused during the stress of handling a data breach.

The First 72 Hours of a Data Breach

After confirming a data breach has occurred, quickly mobilize your plan and teams. How you react in the first 72 hours can be critical to the outcome. Thus, an immediate and flawless investigation is imperative; one early misstep can destroy crucial evidence, delay an effective response and trigger government penalties or class-action lawsuits.

The three key steps during the first 72 hours are:

1. **Preserve data and digital evidence.** Secure the premises and take an inventory of missing items. Review keycard and surveillance data for unusual activity, and work with law enforcement or private security experts to conduct on-site investigations. First and foremost, though, avoid poking around on the machines before seeking the guidance of digital forensic experts. Instead, leave affected computers powered ON, but promptly disconnect them from the network. This will help isolate the affected system, prevent further possible data loss and preserve vital evidence.

How you react in the first 72 hours can be critical to the outcome.

Once a breach is identified, the clock starts ticking and you must act swiftly to identify affected individuals and comply with notification regulations.

2. Identify the compromised data.

Coordinate with IT, HR, legal and forensic experts to interview key custodians and analyze pertinent data. Determine what data was taken, how it was taken and what the consequential risks are. When doing so, focus on compromised protected health information (PHI) and personally identifiable information (PII). To identify the full extent of data loss, call on digital forensic investigators to help. These highly skilled professionals can uncover substantial latent evidence that most IT teams do not have the ability to access and can also help delete hacker tools.

3. Communicate and track progress.

Your data breach response team, C-level executives, regulators, employees, shareholders, patients and/or customers are your key stakeholders and should be frequently informed of your progress and resolution efforts. Document your work at all times and take note of conversations with law enforcement and pertinent individuals. Additionally, record your reasoning behind every action taken along the way. This is a “best practice” and can prove to be valuable documentation to have on hand if “second guessed” by internal personnel and/or by regulators.

Data Breach Notification

The “discovery” of a breach refers to the first day any employee, officer or agent of the company knows about the breach or reasonably should have known about it. Once a breach is identified, the clock starts ticking and you must act swiftly to identify affected individuals and comply with notification regulations.

Given the nature of the breach, you may need to notify the HHS, other government authorities, the credit bureaus, card holder associations, insurance carriers and other parties. Notification can become complicated if both federal and state laws are involved because although these laws sometimes complement each other, at different times they can conflict. Savvy outside counsel can offer beneficial insight to navigate the legal lay of the land.

Be especially aware of HITECH requirements for timetables, content and method of notification. You'll likely need to notify affected individuals within 60 days of a breach discovery; however, some states, such as Florida and Ohio, may actually require notification within 45 days. Bottom line, it is in your best interest to send notifications out within the allotted time in order to avoid fines and to retain the confidence of your patients and/or customers.

Best Practices for a Healthcare Data Breach: What You Don't Know Will Cost You

Keep in mind that state and federal laws may dictate the actual content of your notifications. In general, notifications must include:

- Plain language
- Description of the data breach and how you're responding to it
- Dates of breach and discovery
- Description of the types of information involved
- Steps individuals should take to help protect themselves
- Details on protection products that a company may offer victims
- Contact information for affected individuals that have questions

Working with a data breach solutions provider can help keep your notification on track. These providers can handle the entire notification process and offer your patients or customers an identity theft monitoring and protection product.

Looking Ahead – Post-Breach Review

Hackers, untrustworthy employees and careless vendors continue to create a volatile cyber environment across all industries, but healthcare establishments may face the most difficult challenge in light of the multitude of strict regulations governing the sector. If you don't have a data breach response plan in place now, make it a top priority. The latest high-profile data breaches should be reason enough for you to develop a plan. More importantly, being prepared for a data breach puts you in the best position to respond quickly and reduce risks.

If you do experience a data breach, the aftermath affords the chance to assess and improve the effectiveness of your response plan, processes and people. It can also shed light on opportunities to strengthen physical and electronic security. In the end, you want to be sure to walk away from the unfortunate event more knowledgeable and prepared than ever.

In the end, you want to be sure to walk away from the unfortunate event more knowledgeable and prepared than ever.

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