Health Insurance Carrier Data Breaches—How to Respond

Any company is a potential target for cyber criminals, and insurance carriers are no exception. A cyber data breach occurs when protected information is viewed or stolen by unauthorized individuals, often through a criminal hacking into a company's network.

Compromised data may include private or personally identifiable information, such as names, addresses, phone numbers, email addresses, birthdates, Social Security numbers, medical records, health history, and bank account and credit card numbers.

When an insurance carrier suffers a data breach, many people are affected, and the stolen information may trigger various responsibilities under the Health Insurance Portability and Accountability Act (HIPAA). If a carrier or third-party administrator (TPA) that you work with is attacked by hackers, you need to understand your responsibilities and develop best practices for communicating with your employees as well as complying with any legal obligations.

HIPAA Notification Requirements

Notification requirements apply to HIPAA-covered entities and business associates in the event of a breach of unsecured protected health information (PHI). The responsibility for issuing appropriate notifications to affected individuals will likely **depend on whether the employer's plan is fully insured or self-funded.**

For a fully insured plan, the carrier will generally be the HIPAA-covered entity responsible for notifications. A self-insured plan sponsor acting on behalf of the plan is responsible for notifications, although this may be addressed in an administrative services agreement with a carrier or TPA.

Several notifications may be required after a data breach. Specific notification requirements will depend on the scope of the breach and other factors.

The following are three ways in which notification may be required:

- **Individual Notice** – A notice of a data breach must be provided by the covered entity to affected individuals. Generally, this notice will be in written form delivered via first-class mail (or email if the individual has agreed to receive such notices electronically). Notification must take place without unreasonable delay and no later than 60 days from the breach discovery.

  A toll-free phone number must be provided for individuals to use to learn whether their information was involved in the breach. This number must be active for at least 90 days.

  A notice may have to be placed on the covered entity's website or a similar location if more than 10 affected individuals cannot be reached due to insufficient or out-of-date contact information.

- **Media Notice** – A covered entity that experiences a breach affecting more than 500 residents of a state or jurisdiction must notify prominent media outlets that serve that state or jurisdiction. Notification is generally in the form of a press release to these media outlets and will include the same information as the individual notice. The notice to the media must be provided without unreasonable delay and no later than 60 days after the breach is discovered.

1501 Fourth Ave, Suite 2400
Seattle, WA 98101

DiMartino Associates
EMPLOYEE BENEFITS CONSULTING

Phone: 206-623-2400
Fax: 206-682-8027

- **Notice to the Secretary** – Breaches of protected health information must be reported to the Secretary of Health and Human Services (HHS) via the HHS website. Breaches that affect 500 or more individuals must be reported without delay and no later than 60 days after the breach discovery; breaches affecting fewer than 500 people must be reported on an annual basis.

Further details regarding notification requirements are available at: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule.

Employee Communication

Communication with employees is important, especially when they may be anxious about a data breach that personally affects them. This is the case regardless of any legal requirements that may apply.

Below are a few points to consider as you develop best practices for communication following a carrier data breach:

- Let employees know what's going on. After a breach occurs, employees may hear about it on the news or from friends and family. Make sure you give them the facts and inform them of how it affects them as soon as you have information from your insurance carrier. Depending on your contracted relationship, you may be responsible for complying with federal or state notification rules, as discussed above.
- Reassure employees of your security measures. As their employer, you possess a lot of personally identifiable and financial information, so make sure they know that the information you store is properly secured.
- Warn employees about the potential for scams, especially ones that are already known. Following large data breaches, phishing scams and other criminal attempts at soliciting personal information proliferate quickly. Scammers will often pose as the affected company and contact individuals under the pretense of helping them in order to gain sensitive information.
- Take this opportunity to remind employees of the importance of protecting personal and company data. Reminders about passwords and other data security measures may be heeded more strongly following a breach of employees' personal information.

Whether or not you are legally obligated to provide breach notifications to your employees, you still need to have a strategy in place to communicate with them because affected employees will have questions and concerns.

Contact DiMartino Associates for more information on responding to carrier data breaches.