OCR's HIPAA breach "wall of shame" breaks 2,000

Emily A. Johnson, James J. Giszczak, Dominic A. Paluzzi | Thursday, August 24, 2017

The list of reported Health Insurance Portability and Accountability Act (HIPAA) breaches has broken a new record. More than 2,000 breaches affecting 500 or more individuals have now been reported to the Department of Health and Human Services Office for Civil Rights (OCR) since 2009. It took nearly five years for the "wall of shame" to reach 1,000 breaches affecting 500 or more individuals and reporting has since increased due in part to OCR's ramped up enforcement efforts, which seek to hold covered entities responsible for failure to report a breach within 60 days of discovery.

With the increase of sophisticated hacking and ransomware incidents in recent years, it is anticipated that the number of reported breaches will continue to rise at an accelerated rate. In 2017 it is anticipated that OCR will receive the most breach reports to date within a single calendar year.

In addition to the recent milestone, the "wall of shame" underwent a significant makeover in July which now enables users to view breaches currently under investigation that were reported within the previous 24 months, all breaches reported more than 24 months ago, and all breaches since 2009 for which OCR investigations have concluded. There is also a research report function that provides the total number of breaches reported to OCR, regardless of whether they are still under investigation or when they were reported.

In light of this, it is critical that covered entities and business associates assess their compliance with HIPAA privacy and security rules and continuously educate staff on HIPAA compliance. Analyzing a security incident and determining that a breach occurred can be a complex analysis that significantly eats into the 60-day notification window. In the event of a breach, a strong understanding of the HIPAA breach notification rule is imperative so that notifications are timely filed with the required notification elements.

HIPAA breach reporting 101

In the event of a breach involving protected health information (PHI), a covered entity should immediately contact its cyber liability insurance carrier to put the carrier on notice of the incident. Once the carrier has been notified, the covered entity should notify its legal counsel regarding next steps and notification

obligations. Often, cyber liability insurance carriers have preferred legal counsel they advise covered entities to engage. Once legal counsel is properly engaged, it is important to determine whether a breach in fact occurred. If yes, it is critical to then determine what are the covered entity's notification and reporting obligations. Below is a summary of such obligations.

WHAT IS A DATA BREACH BREACH?

Under the HIPAA Final Rrule, a breach is defined as the acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of the PHI. Excluded from the definition of breach are:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person action under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further impermissible use or disclosure.
2. Any inadvertent disclosure by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in an impermissible manner.
3. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

45 C.F.R.§164.402

Under the Final Rule, there is a presumption of a breach unless the covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

1. Nature and extent of PHI involved.
2. Unauthorized person who used the PHI or to whom the disclosure was made.
3. Whether the PHI was actually acquired or viewed.
4. Extent to which the risk to the PHI has been mitigated.

WHO MUST BE NOTIFIED OF A DATA BREACH INVOLVING PHI?

After determining that a breach occurred, the individual(s) who are the subject of the impermissibly acquired, accessed, used, or disclosed PHI must be notified. Such notification must be made within 60 days of the date the breach is discovered. The notification must include the following information:

1. Brief description of what happened, including date of breach and date of discovery, if known.
2. Description of types of unsecured PHI involved.
3. Steps individuals should take to protect themselves from potential harm resulting from the breach.
4. Brief description of what the covered entity is doing to investigate the breach, mitigate harm to individuals, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.

HOW TO NOTIFY PATIENTS?

The written notice described above must be sent via first-class mail to the affected individual at the last known address of the individual, or, if the individual agrees to electronic notice, by email.

If the affected individual is known to be deceased and the covered entity has the address of the individual's next of kin or personal representative, the covered entity must send the breach notification letter via first-class mail to either the next of kin or personal representative of the individual.

If the covered entity has insufficient or out-of-date contact information that precludes written notification, a substitute notice reasonably calculated to reach the individual shall be provided. Substitute notice is not required when the affected individual is deceased, but the covered entity has sufficient or out-of-date contact information for the next of kin or personal representative of the individual.

WHO ELSE MUST BE NOTIFIED?

- **OCR**

For breaches affecting less than 500 individuals, the Secretary of the U.S. Department of Health and Human Services (HHS) must be notified no later than 60 days after the end of the calendar year in which the breach was discovered. For breaches affecting 500 or more individuals, covered entities must notify the secretary without unreasonable delay and in no event later than 60 days following discovery of a breach.

To notify the secretary in either case, covered entities must submit an electronic breach report form through the HHS website. When submitting a breach report, covered entities will be asked to provide the following information:

1. Whether the breach affects less than 500 or 500 or more individuals.
2. Whether the report is an initial report or amendment to an existing report.
3. Who is filing the report (i.e., covered entity on behalf of itself, covered entity on behalf of business associate, or business associate on behalf of covered entity).
4. Name and type of covered entity.
5. Contact information (address, name of contact person, email, and phone number).
6. Breach start and end dates.
7. Discovery start and end dates.
8. Approximate number of individuals affected by the breach.
9. Location of breach (e.g., server).
10. Type of PHI involved.
11. Brief description of the breach.
12. Safeguards in place prior to breach.

13. Date individual notice was provided.
14. Whether substitute notice or media notice was provided.
15. Actions taken in response to the breach.

- **MEDIA**

  If a breach affects more than 500 residents of a state or jurisdiction, the covered entity is required to notify prominent media outlets serving the state or jurisdiction. This is typically done in the form of a press release to local media outlets servicing the affected area. Similar to individual notices and notices to the secretary, media notification must be provided without unreasonable delay and in no event later than 60 days following discovery of the breach. Such notice must include the same elements required for individual notice described above.

- **STATE NOTIFICATION OBLIGATIONS**

  Certain states require notification to the attorney general in the event of a breach of personal information. More and more states are including medical information in their definition of “personal information.” Therefore, in the event of a breach of PHI, covered entities must also carefully consider reporting obligations under applicable state law. Several state reporting obligations shorten the time period for reporting to a much shorter notification window.

Emily A. Johnson

James J. Giszczak

OCR's HIPAA breach "wall of shame" breaks 2,000

Dominic A. Paluzzi