**DATA BREACHES: HOW TO RESPOND AND WHAT TO EXPECT**

**By: Erin Fleming Dunlap, Esq. and Abby Bonjean, Esq.**

**February 17, 2017**

Reports of a potential data breach can be devastating to any organization. Often times, IT departments are under-staffed or ill-equipped to jump into “incident response” mode and take immediate steps that are necessary to identify, correct and contain the problem. Further, compliance departments do not always have a formal process in place to address the problem quickly from a regulatory and operational perspective, so organizations are scrambling to figure out what to do and when to do it. While we always advise our clients to put in the time and effort to create an incident response team and prepare a formal incident response plan that is tailored to the specific organization (and blessed by senior leadership), this white paper provides a quick overview and some practical tips on how to respond and what to expect following a data breach.

**I. Reporting/Investigation/Mitigation**

Data breaches and security incidents are triggered in many ways (*e.g.*, phishing attacks, malware, ransomware attacks and system errors). It is critical that employees know how to identify and report a potential data breach. Some organizations have a well-publicized help-desk line or reporting hotline. Employees should know who to call, and they should be instructed not to delay reporting – even if it is only a suspected issue. The quicker the organization learns about an incident, the sooner they can start their incident response process.

When an organization learns of a potential data breach, it should take immediate steps to identify, correct and/or contain the issue. This may require shutting down systems or terminating workforce members’ access to the system. The organization will then need to determine the scope of the breach, including what data is involved and how many individuals have been affected. This may require interviews with workforce members, a thorough review of systems or the use of an outside vendor. Some IT departments are limited in the type or depth of the forensic analysis they can perform. If the issue is big enough, it may be worth spending the money on an outside analyst to take a deeper dive into the system or the data.

Once the issue is corrected and contained, the organization should consider what it can do to mitigate harm to the affected individuals. For example, an organization may choose to contact patients immediately if there is a real risk of identity theft (*e.g.*, credit card information was stolen). The organization should also consider whether to contact law enforcement and whether it has insurance to cover the data breach. If it has insurance, review the scope of coverage and provide proper notice to the carrier.

The organization then needs to consider taking additional mitigation steps – both short term and long term – to minimize the chance of the same type of incident from occurring in the future. These steps can range from sanctioning an employee who acted improperly or negligently to sending organization-wide emails about security/cyber risks to retraining the workforce to reviewing and revising applicable policies and procedures to updating the organization’s risk analysis and risk management plan.

**PRACTICAL TIP:** If the data breach affected more than 500 individuals, your organization will likely be subject to a compliance review by the Office for Civil Rights (OCR), so be sure to maintain thorough documentation of both your internal investigation into the incident and any subsequent mitigation steps. We have found that creating a timeline of the events is helpful and can serve well in preparing a response to OCR’s data request about the incident.

**II. Breach Analysis/Reporting Under HIPAA**

Once you get through the initial phase of identifying the issue and taking steps to mitigate the harm, you must consider your other legal obligations. Assuming your organization meets the definition of a “Covered Entity” or a “Business Associate” under the Health Insurance Portability and Accountability Act and its implementing regulations (“HIPAA”), you must comply with the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414.[[1]](#footnote-1) Under the HIPAA Breach Notification Rule, a Covered Entity is required to provide notification following a Breach of Unsecured Protected Health Information (“PHI”).[[2]](#footnote-2)

A Breach is defined as the “***acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of such information.***” There are three exceptions to the definition of Breach, but they are limited and rarely apply in the context of a large data breach or cyber-attack.[[3]](#footnote-3)

Assuming your organization has had an impermissible acquisition, access, use or disclosure of PHI that does not meet one of the Breach exceptions, the incident is ***presumed*** to be a Breach requiring notification unless you can demonstrate through a written risk assessment that there is a “low probability that the PHI has been compromised”based on the following four factors:

* 1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
	2. The unauthorized person who used the PHI or to whom the disclosure was made;
	3. Whether the PHI was actually acquired or viewed; and
	4. The extent to which the risk to the PHI has been mitigated.

A Covered Entity or Business Associate may consider other factors (as appropriate), but the risk assessment must be documented, thorough, completed in good faith and the conclusions reached must be reasonable.

**PRACTICAL TIP:** We have had clients conclude through a written risk assessment that there is a low probability that PHI has been compromised following an impermissible disclosure – often because the type of data exposed posed minimal risk of identity theft or re-identification, but entities should be careful about performing a risk assessment on a large data breach. OCR has issued a fair amount of guidance on the four factors set forth above. Entities should ensure they are staying within that guidance and making reasonable conclusions.[[4]](#footnote-4)

If your organization cannot conclude through a written risk assessment that there is a low probability that the PHI was compromised – you must find that there was a Breach of Unsecured PHI and provide notification of the Breach to: (i) each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such Breach; (ii) the Secretary of HHS; and (iii) in certain circumstances, the media.

 (i) Notice to Affected Individual(s)

A Covered Entity must provide notice to the affected individuals in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. ***Individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a Breach*** and must include, to the extent possible, a description of the Breach, a description of the types of information that were involved in the Breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the Covered Entity is doing to investigate the Breach, mitigate the harm, and prevent further Breaches, as well as contact information for the Covered Entity.

If the Covered Entity has insufficient or out-of-date contact information for fewer than 10 individuals, the Covered Entity may provide substitute notice by an alternative form of written, telephone, or other means. If the Covered Entity has insufficient or out-of-date contact information for 10 or more individuals, the Covered Entity must provide substitute individual notice by ***either*** posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If a Covered Entity chooses to provide substitute notice on its web site, it may provide all the information described at § 164.404(c) directly on its home page (“home page” includes the home page for visitors to the covered entity’s web site and the landing page or login page for existing account holders) or may provide a prominent hyperlink on its home page to the notice containing such information.Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the Covered Entity to determine if their PHI was involved in the Breach.

(ii) Notice to Secretary

In addition to notifying the affected individuals, a Covered Entity must notify the Secretary of HHS of a Breach of Unsecured PHI. A Covered Entity must notify the Secretary by visiting the HHS web site and filling out and electronically submitting a Breach report form: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>. If a Breach affects fewer than 500 individuals, the Covered Entity may notify the Secretary on an annual basis – but no later than 60 days after the end of the calendar year in which the Breach occurred. ***If a Breach affects 500 or more individuals, the Covered Entity must notify the Secretary without unreasonable delay and in no case later than 60 days following the discovery of a Breach***.

(iii) Notice to Media

A Covered Entity that experiences a Breach affecting more than 500 Individuals of a State or jurisdiction is also required to provide notice to prominent media outlets serving the State or jurisdiction. Covered Entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. The media notification obligation is met when notice to the media is provided; it does not matter whether or not the media outlet chooses to report on the notification. ***The media notification, if required, must be provided without unreasonable delay and in no case later than 60 days following the discovery of a Breach and must include the same information required for the individual notice. Notices to the media should be provided contemporaneously with those to the affected individuals.***

**PRACTICAL TIP:** As soon as you have determined the discovery date, make a timeline for your incident response team and determine as soon as possible if substitute notice or media notice is required. If you decide to use an outside vendor to handle the notification process, build in sufficient time to engage the vendor and get the patient list and documentation in final form (*e.g.*, several vendors require 3-5 business days after the patient list is uploaded and the breach template letters are finalized to send the notifications).

**III. Preparing for OCR Compliance Review**

After you report a Breach, OCR may perform a compliance review. Due to a new intake process at OCR, it could be handled by any regional office.

For each Breach report involving 500 or more affected individuals, OCR automatically opens a compliance review. In August 2016, OCR announced that it was also going to begin investigating breaches affecting under 500 individuals (“Under 500 Breaches”). As part of this new initiative, we understand that each of OCR’s regional offices has been instructed to investigate a certain number of Under 500 Breaches, and it appears those investigations have begun.  Over the past few months, some of our clients have received data requests about Under 500 Breaches they reported in 2015, and OCR seems to be using these investigations to perform “compliance checks” – delving into HIPAA compliance areas unrelated to the areas/issues that caused or relate to the Under 500 Breaches that triggered the review.  According to OCR, when determining whether to investigate Under 500 Breaches, it may consider the number of individuals affected by the breach; the amount and type of PHI involved; breaches caused by theft or improper disposal of PHI; hacking incidents; or entities that have filed numerous Under 500 Breaches involving the same types of issues.  Thus, we believe any entity that reported Under 500 Breaches that fit or highlight these focus areas should be prepared for an OCR compliance review. An OCR compliance review may also be opened after receiving a complaint from an affected patient or another third-party, such as the media.

Once a compliance review is opened, a Covered Entity or Business Associate (specifically, the individual identified on the OCR breach report) usually receives an initial call from an OCR investigator within two weeks (or, in some cases, within a day or two) of submitting the report.  The purpose of this call is to ensure that the information submitted in the initial report is accurate.  Following the call, OCR will send the entity a letter and document request list to initiate the formal investigation. The timing may vary, but OCR tends to send the letter and document request list within two weeks of the initial call.  The investigator on the initial call may offer specific information as to when an entity can expect the formal investigation letter and document request.

Although OCR’s document requests vary depending on the type of incident at issue, be prepared to submit the following:

* Position statement regarding the incident
* Risk analysis
* Risk management plan
* Evidence of implemented security measures (*e.g.*, configuration settings, invoices, screenshots, etc.)
* Evidence of training (*e.g.*, copies of training materials and attendance records)
* Relevant policies and procedures (*e.g.*, sanction, security incident, facility access controls, device and media controls, access control, breach notification, etc.)
* Evidence of sanctions imposed on the responsible employee(s), if applicable
* Security incident report
* Copies of notices to individuals and the media
* Business Associate Agreements, if applicable

**PRACTICAL TIP:** Organizations facing a compliance review should also review the “corrective action obligations” in the Corrective Action Plans (that correspond to the Resolution Agreements) on OCR’s website: <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>. These can serve as great “roadmaps” for what types of corrective action OCR expects an entity to take following a breach or security incident.

**IV. Potential Penalties/Resolution Agreement**

If an entity is found to have violated HIPAA, OCR and States’ Attorneys General may impose sanctions, including civil monetary penalties (“CMPs”) ranging from $100 to $50,000 per HIPAA violation – but the maximum CMPs that can be applied for additional violations of the same regulation in any one year are within a range of $25,000 to $1,500,000. HHS is required to impose a CMP if a violation is found to constitute willful neglect of the law. The chart below shows the tiered penalties based on the entity’s culpability:

|  |  |  |
| --- | --- | --- |
| **Violation Category** | **Each Violation** | **All Such Violations of an Identical provision in Calendar Year** |
| Did Not Know | $100-$50,000 | $1.5 million |
| Reasonable Cause | $1,000-$50,000 | $1.5 million |
| Willful Neglect, Corrected within 30 Days | $10,000-$50,000 | $1.5 million |
| Willful Neglect, Not Corrected within 30 Days | $50,000 | $1.5 million |

HHS will not impose the maximum penalty amount in all cases, but will instead determine the penalty based on: (i) the nature and extent of the violation; (ii) the resulting harm (e.g., the number of individuals affected, reputational harm, etc.); (iii) the entity’s history of prior offenses or compliance; (iv) the financial condition of the entity; and (v) any other factor that justice may require be considered. HHS also retains the ability to waive a CMP, in whole or in part, and to settle any issue or case or to compromise the amount of a CMP.

However, a ***large majority*** of OCR compliance reviews do not end with the imposition of CMPs. Rather, OCR may close the matter with suggested action items for the entity or, in more egregious cases, OCR will enter into a Resolution Agreement, in which the entity agrees to pay a settlement amount and enter into a corrective action plan. The latter type of OCR enforcement continues to increase.  In 2016, OCR announced that it had entered into 12 settlements and imposed 1 CMP – the most enforcement actions in a given calendar year.  Those settlements included the first involving a Business Associate as well as the largest settlement to date, which totaled $5.5 million. We are seeing similar enforcement activity in 2017. As of the date of this publication, OCR has entered into 3 Resolution Agreements and imposed a CMP of $3.2 million.

**V. Conclusion**

Data breaches are a scary subject for most organizations. In our experience, however, the more an organization does at the front end – the less likely it is to make missteps and the better it fairs in a subsequent government investigation. Preparation, education and documentation are essential. If your organization has not prepared an incident response plan, it should. Consider adding “incident response plan” to the next compliance committee meeting agenda. If your employees have not been educated about the current cyber threats and security risks, they should be **–** through multiple communication channels. Finally, if you are not documenting all of your efforts, then you will have a hard time showing the government that you took the necessary and appropriate steps to address the problem. Now is the time.

1. Separate from the HIPAA Breach Notification Rule, almost every state has a breach notification law. Those laws should be reviewed in short order, as some of those laws are more stringent that the HIPAA Breach Notification Rule. [↑](#footnote-ref-1)
2. “Unsecured PHI” is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance (*e.g.,* PHI that has not been encrypted). [↑](#footnote-ref-2)
3. The three exceptions to the definition of a Breach are: (i) any unintentional acquisition, access, or use of PHI by a workforce member or person acting 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 use or disclosure in a manner not permitted under the HIPAA Privacy Rule; (ii) any inadvertent disclosure by a person who is 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 a manner not permitted under the HIPAA Privacy Rule; and (iii) 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. [↑](#footnote-ref-3)
4. If the incident involved a ransomware attack, OCR has issued guidance suggesting that entities should consider the following in determining whether there is a low probability that the PHI was compromised: (i) the exact type and variant of malware discovered; (ii) the algorithmic steps undertaken by that type of malware; and (iii) whether there were communications, including exfiltration attempts between the malware propagated to other systems, potentially affecting additional sources of ePHI. According to OCR, by understanding what a particular strain of malware is programmed to do can help determine how or if a particular malware variant may laterally propagate throughout an entity’s enterprise, what types of data the malware is searching for, whether or not the malware may attempt to exfiltrate data, or whether or not the malware deposits hidden malicious software or exploits vulnerabilities to provide future unauthorized access. OCR also suggests that entities should consider: (i) whether there is a high risk of data unavailability or a high risk to data integrity; (ii) whether the ransomware deletes the original data and leaves only the data in encrypted form; (iii) whether or not the data has been exfiltrated. [↑](#footnote-ref-4)