Codify
BY AAPC

Health Information Compliance Alert

Compliance: Plot Out Your Organization's Security Incident Response Plan

Follow 7 expert-recommended steps to evaluate, document, and report breaches.

With the increase in data breach incidents as well as the rise in HIPAA breach penalties it's more important than ever before for covered entities (CEs) and business associates (BAs) to develop a thorough incident response plan. Here's what you need to do right now to protect your organization from a devastating fallout from a mishandled breach response.

Form an Incident Response Team

Payoff: "Being prepared on an organizational level can mitigate the risk of both extensive data loss and negative press," says **Diana Maier**, an employment and privacy law attorney of the **Law Offices of Diana Maier** based in San Francisco.

"Before a breach takes place, a response team should be formed with key personnel, such as executives and privacy, legal, IT, and public relations staff," Maier advises. "This team should inform the organization on the protocol to expect following a breach. When a breach does happen, the team should be responsible for implementing the response plan."

Also, keep in mind that you may need to have more than one plan, depending on the kind of data involved in the incident, Maier notes.

Follow 3 Steps to Address Security Incidents

There are three phases of security incident management, which you should carry out in succession as needed, according to **Jim Sheldon-Dean**, principal and director of compliances services for **Lewis Creek Systems LLC** based in Charlotte, VT. The three major phases are:

1. Assess the security incident. First, you need to assess the incident to determine what happened and what you need to do to avoid the problem in the future, Sheldon-Dean says. "Part of this assessment includes a determination of whether or not the incident includes information that may qualify the incident as a reportable breach under state or federal laws."

This determination will help you to determine your next steps. If the information is not covered under breach notification laws, you would document the incident and consider it at a future periodic incident review meeting, Sheldon-Dean advises.

2. Evaluate potentially reportable breaches. But if the information is covered under breach notification laws, then you need to review the incident, Sheldon-Dean says. In this second phase, review the incident in the context of the applicable breach notification laws to determine if the breach is reportable under those laws.

3. Report the breach as necessary. If you determine that the incident is a reportable breach, this would trigger the reporting process, according to Sheldon-Dean. You would then need to report (and document your reporting) to the affected individuals, HHS, the press, and various state agencies as the law requires.

The basics: According to Maier, your incident response plan should vary depending on the kinds of data involved but all plans should include the following steps after discovering a breach:

1. Secure the area or network involved in the cause of the breach;
2. Ensure the breach has stopped or stop it;
3. Preserve evidence (for example, secure the metadata) and document all aspects of the incident;
4. Notify those whose information has been breached and, as necessary, the media and any relevant authorities like the **HHS Office for Civil Rights** (OCR); and
5. Work with forensics firms, law enforcement, OCR, etc. as needed.

Break it Down: 7 Steps to Evaluate & Report Breaches

Essential: The HIPAA Breach Notification rule (§164.400 et seq.) requires you to take specific actions when faced with a breach incident. Sheldon-Dean outlines the following steps you need to take to evaluate and report breaches, as well as to properly document compliance incidents:

1. Report all breaches promptly to the individual, unless:

a. The disclosure is one of the three exceptions to HHS' definition of a breach at www.hhs.gov/hipaa/for-professionals/breach-notification/index.html; OR
b. The PHI is encrypted using processes meeting the requirements of HHS guidance; OR
c. A risk assessment determines that there is a low probability of protected health information (PHI) disclosure.

2. Determine whether there is a low probability of disclosure using a HIPAA breach risk assessment that considers four factors:

1) The nature of the information (how detailed, how much identifying information, sensitivity, including the potential for "adverse impact" to the individual?);
2) To whom the information was released (was it another healthcare provider?);
3) Whether the information was actually accessed, used, or disclosed (was it discarded without reading?); and
4) How you mitigated the incident (are there assurances that the information disclosed cannot be further used, disclosed, or retained?).

3. Report breaches of PHI involving more than 500 individuals to HHS at the same time you report the breach to the affected individuals. If the breach involves fewer than 500 individuals, you must report it to HHS within 60 days of the end of the calendar year in which it occurred.

4. Report breaches of PHI to individuals, HHS, and the public according to the applicable regulation (see www.hhs.gov/hipaa/for-professionals/breach-notification/index.html for details).

5. Involve your organization's counsel and senior management in any breaches that may be reportable under law, to ensure that you follow federal and state laws correctly when providing various notices and reports to agencies. Keep in mind that breaches of an individual's information may also be subject to the state laws where the individual resides, and not just the state where your organization is located.

6. Document all privacy and security incidents, breaches, and HIPAA breach risk assessments performed to determine whether an incident is a reportable breach. Include documentation of incidents in any compliance evaluation procedures or usage audit and activity review procedures, as appropriate.

7. Develop and preserve information gathered in your investigation of security incidents to the greatest extent possible as potential evidence admissible in court, in case it's needed in legal proceedings. Whenever possible, identify any individuals or entities that may be liable for harm caused by the incident.

Put These Policies & Procedures in Place

You must have procedures for reporting, processing, and responding to suspected or known information security incidents, Sheldon-Dean stresses. These procedures are essential for investigating, mitigating, and documenting security incidents, so that you can appropriately report and promptly handle security violations and breaches.

According to Sheldon-Dean, your procedures should identify:

- How to determine what qualifies as an "incident;"
- How to report incidents (including designating a person to whom incidents and alerts must be reported on 24/7 basis);
- The steps to take in investigating;
- The roles and responsibilities of the response team;
- The steps to take and information to include when documenting incidents;
- The steps to take to mitigate the effects of incidents (where possible and/or allowed by law);
- The steps to take to provide business recovery and continuity, including the use of adequate backup procedures;
- Who may release information about the incident and the procedures for doing so;
- To which entities incidents involving breaches must be reported;
- Who is authorized to release a system following an investigation; and
- How you should perform a follow-up analysis and who should participate.

Bottom line: A security incident is bad enough, and you need to know when not to panic versus when you need to launch a response. But if you drop the ball on your duties following a data breach, the risks for bad press and costly penalties are higher than ever before. Make sure you have a solid incident response plan in place to make a bad situation much more bearable.