COMPLIANCE BULLETIN

HHS Issues HIPAA Cyber Attack Response Checklist

HIGHLIGHTS

- Group health plan sponsors must have procedures to prevent and mitigate the effects of cyber security breaches involving PHI.
- A cyber security incident must be reported to affected individuals and to the OCR if PHI is accessed, acquired, used or disclosed.
- Cyber security crimes should also be reported to law enforcement.

IMPORTANT DATES

60 Days After Security Breach

A breach must be reported to all affected individuals as soon as possible, but **no later than 60 days** after it is discovered.

In some cases, a cyber security breach must also be reported to the OCR within 60 days after discovery.

Provided By:
Deutsch & Associates, LLC

OVERVIEW

Under the Health Insurance Portability and Accountability Act (HIPAA), a covered entity that experiences a ransomware attack or other cyber-related security incident must take immediate steps to prevent or mitigate any impermissible release of protected health information (PHI).

The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) has issued a checklist to help HIPAA-covered entities determine the specific steps they must take in the event of a data breach.

This document outlines those steps and provides general information regarding which entities are subject to HIPAA and the type of data that must be protected under the law.

ACTION STEPS

Employers that are subject to HIPAA should become familiar with the OCR's checklist and other guidance for preventing and responding to cyber security breaches involving PHI. These employers should also ensure that they have procedures and contingency plans in place for responding to and mitigating the effects of any potential breach.

OCR Quick-response Checklist

Deutsch & Associates LLC

Has your entity just experienced a ransomware attack or other cyber-related security incident, and you are wondering what to do now? The guide issued by OCR explains, in brief, the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident.

In the event of a cyber attack or similar emergency, a covered entity:

- **Must execute its response and mitigation procedures and contingency plans**. For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible PHI disclosure. These steps may be performed by the entity's own information technology staff, or by an outside entity brought in to help (which would be a business associate, if it has access to PHI for that purpose).

- **Should report the crime to appropriate law enforcement agencies**. These agencies may include state or local law enforcement, the FBI or the Secret Service. Reports to these agencies should not include PHI unless otherwise permitted under HIPAA. If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach for the time the law enforcement official requests in writing or for 30 days if the request is made orally.

- **Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs).** These organizations may include the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Reports to these organizations should not include PHI. The OCR does not receive these reports from its federal or HHS partners.

- **Must report the breach to affected individuals and to the OCR as soon as possible**.
    - If a breach affects 500 or more individuals, the covered entity must notify the affected individuals, the OCR and the media **no later than 60 days** after discovering the breach, unless a law enforcement official has requested a delay in the reporting.
    - If a breach affects fewer than 500 individuals, the entity must notify the affected individuals without unreasonable delay, but **no later than 60 days** after discovery of the breach, and notify the OCR within **60 days after the end of the calendar year** in which the breach was discovered.

Continue reading for more information on various aspects of the HIPAA Security Rule, which was provided by OCR along with the checklist.

HIPAA Covered Entities

HIPAA is a federal law designed in part to protect the privacy of certain health care information known as PHI. In general, the HIPAA privacy and security rules apply to all health plans that provide or pay for the cost of medical care. These include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. However, a group health plan with less than 50 participants is not a covered entity if it is administered solely by the employer that established and maintains the plan.

The HIPAA privacy and security rules also apply to business associates of HIPAA-covered entities. A business associate is any vendor that creates, receives, maintains or transmits PHI for or on behalf of a covered entity. This includes vendors that have access to PHI in order to provide information technology-related services to a covered entity. Other activities a business associate may perform on behalf of a covered entity include claims processing, data analysis, utilization review and billing.

Protected Health Information

PHI includes all individually identifiable health information held by covered entities. Information is "individually identifiable" if it identifies, or if there is a reasonable basis to believe it can be used to identify, an individual. This information is PHI if it relates to:

- The individual's past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present or future payment for the provision of health care to the individual.

For example, PHI includes:

- ✓ Treatment information
- ✓ Billing information
- ✓ Insurance information
- ✓ Contact information
- ✓ Social Security

PHI does not include:

- Employment records
- Records covered by the Family Educational Rights and Privacy Act (FERPA)
- Information about individuals who have been deceased for more than 50 years

HIPAA Security Rule

Under HIPAA's Security Rule, a "security incident" is defined as the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with system operations in an information system. The Security Rule requires covered entities to:

- ✓ Identify and respond to suspected or known security incidents;
- ✓ Mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity;
- ✓ Document security incidents and their outcomes; and

- ✓ Establish and implement contingency plans, including data backup plans, disaster recovery plans and emergency mode operation plans.

Reportable Incidents and Indicators

HIPAA regulations also require covered entities to report certain cyber-related security incidents to affected individuals, the OCR and other agencies. In general, a reportable breach occurs anytime PHI was accessed, acquired, used or disclosed.

Certain "cyber threat indicators" may be reportable under the Cybersecurity Information Sharing Act (CISA) as well. CISA describes cyber threat indicators as information that is necessary to describe or identify any of the following:

- ✓ Malicious reconnaissance;
- ✓ Methods of defeating a security control or exploitation of a security vulnerability;
- ✓ A security vulnerability;
- ✓ Methods of causing a user with legitimate access to defeat a security control or exploitation of a security vulnerability;
- ✓ Malicious cyber command and control;
- ✓ A description of actual or potential harm caused by an incident; or
- ✓ Any other attribute of a cyber security threat, if disclosure of such attribute is not prohibited by law.

*A security incident may **not** be reportable if the affected covered entity:*

- *Encrypted the information at the time of the incident; or*
- *Determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach.*

Enforcement and Liability

Under HIPAA's Enforcement Rule, the OCR may assess civil money penalties of up to $1,677,299 per violation, per year, against a covered entity that fails to properly protect PHI. In determining the amount of an applicable penalty, the OCR may consider all mitigation efforts taken by a covered entity during any particular cyber security breach investigation. A covered entity's mitigation efforts may include voluntary sharing of breach-related information with law enforcement agencies and other federal and analysis organizations.

In addition, the CISA provides liability protection to entities that monitor information systems or share or receive indicators or defensive measures in a manner consistent with the HHS sharing process.

Therefore, covered entities should ensure that their procedures for protecting PHI meet HIPAA standards and should take the steps outlined in the above OCR checklist in the event of a cyber security incident involving PHI.