NATIONAL ASSOCIATION OF Community Health Centers®

Cyber Insurance & HIPAA Breaches—

TIP SHEET

As cyberattacks increase, the health care industry is a prime target for such attacks, given the amount and types of information maintained (including patient, employee, payment and other business records); the urgent, constant need for the information (to provide care to patients, to pay employees, to process payments and to conduct business); and the dependence on technology (including electronic health record systems, payroll systems, and processing systems). A cyberattack on a health care provider's electronic health records system can interrupt patient care, jeopardize patient safety, and impact claims submission. To help protect against such outcomes, many health care providers purchase cyber insurance coverage.

A cyberattack may impact one or all of the types of information maintained by a health care provider and cyber insurance policies including a variety of coverage (including business interruption, system failure, and contingent business interruption). This Tip Sheet specifically addresses how cyber insurance coverage can support health centers in meeting their obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to respond to security incidents and to report breaches.[1] This Tip Sheet provides a review of the following HIPAA requirements:

- Security Incidents and Incident Response
- Breach Determination
- Breach Reporting
- Responding to Investigations, Compliance Reviews and Lawsuits

Each section also includes suggested "key terms" to be included in a cybersecurity insurance policy and "key questions" what to ask your insurance carrier or broker.

HIPAA Overview

HIPAA establishes standards for the privacy and security of individually identifiable health information known as "protected health information" or "PHI." The U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") enforces the following HIPAA Rules:

- Privacy Rule: Provides federal protection to protect the privacy of individuals' medical records and other individually identifiable The Privacy Rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures without an individual's authorization.
- Security Rule: Establishes national standards to protect electronic PHI ("ePHI") that is created, received, used, or maintained by covered entities and business associates. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.
- Breach Notification Rule: Requires HIPAA covered entities to notify affected individuals, OCR and, in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates are also required to notify covered entities following the discovery of a breach.

1 Health centers should review state law which may provide additional or different requirements related to responding to security incidents and reporting breaches.

Security Incidents and Incident Response

The HIPAA Security Rule defines a security incident as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system" (45 CFR 164.304). The HIPAA Security Rule requires covered entities to "[i]dentify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes" (45 CFR 164.308(a)(6)). Covered entities are required to implement policies and procedures to address security incidents.

In guidance on responding to ransomware attacks, OCR advises that security incident procedures should include processes to:

- Detect and conduct an initial analysis of the ransomware;
- Contain the impact and propagation of the ransomware;
- Eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- Recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations;
- Conduct post-incident activities to determine if the entity has any regulatory, contractual or other obligations as a result of the incident and to incorporate any lessons learned into the overall security management process of the entity.[2]

KEY TERMS:

- Types of incidents: The policy should describe and define the types of security incidents covered. For example, the policy may cover network security and privacy wrongful acts, technology services wrongful acts, network extortions, social engineering fraud, telecommunications fraud, and funds transfer fraud.
- Reporting requirements: The policy or other written documents should detail how the health center is to report security incidents, including deadlines.
- Scope of coverage: The policy should cover costs incurred by the insured or on the insured's behalf to engage with an external security consultant to identify the source and scope of the cyber event; obtain initial advice to remediate the impact of the cyber event; conduct a forensic investigation of impacted system; contain and remove any malware discovered on impacted systems; and engage with an IT security consultant to provide expert witness testimony at any trial or hearing arising from the cyber event.

2 *See* Office for Civil Rights, "FACT SHEET: Ransomware and HIPAA" available at **https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents//RansomwareFactSheet.pdf.**

KEY QUESTIONS:

- How do we report security incidents? What information will be needed during initial reporting?
- What forensic firms does the insurer work with? Will we be able to talk with several firms and pick one or does the insurer determine the firm to be used?
- How quickly can we expect a security consult to be engaged to respond to a reported security incident?

Breach Determination

The HIPAA Breach Notification Rule defines a breach 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 the PHI" (45 CFR 164.402). An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

Determining whether there has been a data breach involves an understanding of both the security incident, including the systems and information impacted, and the reporting requirements under all applicable laws and regulations.

KEY TERMS:

- Coverage for legal and regulatory costs: The policy should cover legal costs related to obtaining legal advice to determine the correct course of action, including determining whether there has been a breach and identifying notification requirements (see below section on Breach Reporting).

KEY QUESTIONS:

- What law firms does the insurer work with? Will we be able to talk with several firms and pick one or does the insurer determine the firm to be used? Can we engage our own legal counsel, with the insurer paying all or part of the costs?
- How quickly can we expect legal counsel to be engaged to lead an investigation of a reported security incident?

Breach Reporting

The HIPAA Breach Notification Rule requires covered entities to notify:

1. Affected individuals (45 CFR 164.404): Without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of unsecured PHI, a covered entity must provide affected individuals with a written notice that includes:

    a. A brief description of the breach (including the date of breach and date of discovery);

    b. A description of the types of unsecure PHI involved;

    c. Any steps individuals should take to protect themselves from potential harm;

    d. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals and to protect against further breaches; and

    e. 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.

If a covered entity does not have current contact information for all affected individuals, substitute notice may be used.

2. Media (45 CFR 164.406): Without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of unsecured PHI, a covered entity must report breaches involving more than 500 residents of a state or jurisdiction to prominent media outlets serving the state or jurisdiction.

3. OCR (45 CFR 164.408): For breaches of unsecured PHI involving 500 or more individuals, a covered entity must notify OCR at the same time affected individuals are notified (without unreasonable delay and in no case later than 60 calendar days after discovery of the breach). For breaches of unsecured PHI involving less than 500 individuals, a covered entity must notify OCR no later than 60 days after the end of the calendar year in which the breach was discovered.

KEY TERMS:

Coverage for breach notifications: The policy should include coverage for the required notifications, including costs related to:

- Legal fees related to drafting notification letters, substitute notices, website notices or email notification templates, as well as notifications to regulatory bodies;
- Print and posting appropriate notices for affected individuals or for sending email notices or issuing substitute notices;
- Providing credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals;
- Setting up a call center to manage inbound and outbound calls in direct relation to the cyber event;
- Providing translation services to manage communications with affected individuals; and
- Public relations costs related to drafting media notifications and responding to media inquiries.

KEY QUESTIONS:

- Does the insurer maintain lists of preferred vendors of mail houses, call centers and translation services? Can we select from among those vendors or does the insurer select? Can we use our own vendor for such services, with the insurer paying all or part of the costs?

Responding to Investigations, Compliance Reviews and Lawsuits

OCR conducts a compliance review for every breach affecting 500 or more individuals. Covered entities and business associates are required to cooperate with OCR investigations and compliance reviews, including providing access to their facilities, books, records, accounts and other sources of information (including PHI) relevant to determining compliance (45 CFR 160.310). During a compliance review OCR sends the covered entity a data request, which may be followed by additional document requests, interviews or a site visit. OCR may require the covered entity to pay a settlement amount and enter a Corrective Action Plan. If a voluntary agreement is not reached, OCR may refer a case to the Justice Department for litigation.

In addition to government enforcement, many covered entities face class action lawsuits related to breaches. HIPAA does not provide affected individuals with a private right of action to sue a covered entity. Instead, affected individuals may file lawsuits against covered entities under state laws, bringing claims such as negligence, invasion of privacy, breach of third-party beneficiary contract, breach of confidence and breach of confidentiality and privacy.

KEY TERMS:

- Coverage for regulatory or law enforcement investigations and reviews. The policy should cover costs related to responding to any regulatory or law enforcement investigation or action.
- Coverage for settlement amounts. The policy should cover costs for the payment of settlement amounts related to regulatory or law enforcement investigations or actions, as well as settlements related to any legal actions brought by affected individuals.
- Coverage for breach remediation activities. The policy should cover costs to respond to the security incident and prevent similar events in the future. Such coverage might include coverage for conducting an information security risk assessment; conducting an information security gap analysis; developing an information security document set; and delivering an information security awareness training session.

This Tip Sheet was supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $6,625,000 with 0 percentage financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov.

This Tip Sheet was written for NACHC by: Dianne K. Pledgie (lead author), Feldesman Tucker Leifer Fidell LLP, Washington, D.C. Phone: 202-466-8960

For information about this Tip Sheet, contact: Andy Gulati, Email: agulati@nachc.org or trainings@nachc.org Phone: 301-347-0400