

Change Healthcare Cyberattack Emphasizes Importance of Cybersecurity Readiness; Considerations for Hardening Your Cybersecurity Program

March 12, 2024

As the health care industry continues reeling from the recent Change Healthcare ransomware attack that crippled large portions of the U.S. health care system, health care providers are naturally reminded of the importance of their cybersecurity safeguards. The HIPAA Security Rule requires that regulated entities maintain reasonable and appropriate administrative, technical, and physical safeguards for electronic protected health information (ePHI), including:

- Ensuring the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
- Identifying and protecting against reasonably anticipated threats to the security or integrity of the information;
- Protecting against reasonably anticipated, impermissible uses or disclosures; and
- Ensuring compliance by their workforce.

These security measures require review and modification as threats change. Based on the Change

Healthcare attack, covered entities should consider:

1. **Taking a closer look at the [recent cybersecurity guidance](#)** prepared by the National Institute of Standards and Technology. The 122-page guide offers practical guidance and resources that regulated entities can use to better understand Security Rule requirements and safeguard ePHI. The first step in this process is a risk assessment to identify potential risks and vulnerabilities where ePHI can be improperly disclosed, modified, or made unavailable. The cybersecurity guide recommends the following steps:
 - a. **Understand** where ePHI is created, received, maintained, processed, and transmitted.
 - b. **Identify potential threat events, sources, and vulnerabilities** based on the operating environment and any knowledge acquired from analyzing where ePHI flows (e.g., ransomware, phishing, insider threats).
 - c. **Determine the level of risk** (e.g., low, moderate, or high) based on the likelihood that a reasonably anticipated threat will exploit a vulnerability and the impact that would result.
 - d. **Document** the results.
2. Based on this risk assessment, evaluate options for **implementing security measures and policies/procedures to reduce potential risks and vulnerabilities**. The cybersecurity guide provides a table of key activities to consider when implementing Security Rule requirements, including actionable steps to take and sample questions to consider when determining the adequacy of cybersecurity measures. Key activities may include technical safeguards, employee training, vendor audits, and data minimization.
3. **Preparing for the worst**. As [reported last month by the U.S. Department of Health and Human Services' Office for Civil Rights](#), there have been significant increases in HIPAA complaints and large breaches, and hacking/IT incidents continue to comprise the majority of reported breaches. With cyberattacks on the rise, and all eyes on the health care industry's cybersecurity, health care providers can expect an increased focus on their preparedness. For this reason, covered entities should consider:
 - a. **Refreshing their incident response and business continuity plans;**
 - b. Simulating their response to such events via a **tabletop exercise;** and
 - c. Reviewing **relevant contracts and insurance coverages** to ensure adequate protection.

Authored By



Patricia M. Carreiro



Olivia V. Dresevic



Lauren F. Gandle

Related Practices

[Cybersecurity and Privacy](#)
[Health Care](#)

Related Industries

[Health Care](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.