Improving the Cybersecurity Posture of Healthcare in 2022

February 28, 2022 | *By: Lisa Pino (/blog/authors/lisa-j-pino), Director for Office for Civil Rights (OCR)*

Summary: Encourages HIPAA covered entities and business associates to strengthen their cyber posture in 2022.

As the Director of the Office for Civil Rights at the U.S. Department of Health and Human Services (OCR), prioritizing cyber security and patient privacy is of the utmost concern. From my years in government service, I understand cyberattacks all too well from my role at the U.S. Department of Homeland Security where I drove the agency's response to the 2015 U.S. cyber breach mitigation of 4 million federal personnel and 22 million surrogate profiles, which at the time was the largest hack in federal history. Now as the OCR Director, I am continuing this important work leading HHS's enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules.

Cyberattacks grabbed headlines throughout 2021 as hacking and IT incidents affected government agencies, major companies, and even supply chains for essential goods, like gasoline. For healthcare, this year was even more turbulent as cybercriminals took advantage of hospitals and healthcare systems responding to the Covid-19 pandemic. More than one health care provider was forced to cancel surgeries, radiology exams, and other services, because their systems, software, and/or networks had been disabled. And at the end of December, a critical vulnerability in a widely used Java-based software known as "Log4j" grabbed headlines with warnings about the potential risks this security flaw could pose for organizations of all sizes. Such unpatched vulnerabilities give hackers easy access to an organization's computer server, and possible entry into other parts of a network. These reports underscore why it is so important for health care to be vigilant in their approach to cybersecurity. With these risks in mind, I would like to call on covered entities and business associates to strengthen your organization's cyber posture in 2022.

All too often, we see that risk analyses only cover the electronic health record. I cannot underscore enough the importance of enterprise-wide risk analysis. Risk management strategies need to be comprehensive in scope. You should fully understand where all electronic protected health information (ePHI) exists across your organization – from software, to connected devices, legacy systems, and elsewhere across your network.

If you haven't looked at your risk management policies and procedures recently to prevent or mitigate these concerns, now is the time to do so. Some best practices include:

- Maintaining offline, encrypted backups of data and regularly test your backups;
- Conducting regular scans to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface;
- Regular patches and updates of software and Operating Systems; and
- Training your employees regarding phishing and other common IT attacks.

Good cyber hygiene habits help keep your network healthy and protect the ePHI on your systems. OCR is here to help with guidance and resources:

- Ransomware: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf - PDF (/sites/default/files/RansomwareFactSheet.pdf)
- Cybersecurity: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html (/hipaa/for-professionals/security/guidance/cybersecurity/index.html)
- Risk Analysis: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf - PDF (/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf)
- HHS Security Risk Assessment Tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool (https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool) .

As part of the whole-of- government response to help public and private organizations defend against the rise in ransomware cases, the Cybersecurity and Infrastructure Security Agency (CISA) launched StopRansomware.gov (https://www.cisa.gov/stopransomware) with resources designed to help organizations understand the threat of ransomware, mitigate risk, and in the event of an attack, know what steps to take next.

Finally, our office has issued the 2020 Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance - PDF (/sites/default/files/compliance-report-to-congress-2020.pdf), and 2020 Annual Report to Congress on Breaches of Unsecured Protected Health Information - PDF (/sites/default/files/breach-report-to-congress-

2020.pdf). These reports highlight the continued need for regulated entities to improve compliance with the HIPAA Security Rule standards, in particular the implementation specifications of risk analysis and risk management, information system activity review, audit controls, security awareness and training, and authentication. All of these compliance concerns were identified as areas needing improvement in 2020 OCR breach investigations.

We owe it to our patients, and industry, to improve our cybersecurity posture in 2022 so that health information is private and secure.

Best,
Lisa J. Pino, Director, Office for Civil Rights, U.S. Department of Health and Human Services

Posted In: HIPAA (/blog/categories/hipaa)

Tagged: HIPAA (/blog/tags/hipaa)

Sign Up for Email Updates

Receive the latest updates from the Secretary, Blogs, and News Releases

Sign Up (https://cloud.connect.hhs.gov/subscriptioncenter)

HHS Headquarters

U.S. Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
Toll Free Call Center: 1-877-696-6775