Briefings on HIPAA

Cyberattacks in healthcare: How to stay ahead of the threat

by Dom Nicastro

Cyberattacks, as you might expect, aren't going away. **Paige Hanson,** cofounder and head of communications and partnerships at SecureLabs Inc., summarizes the current landscape of cyberattacks and their impact on HIPAA compliance efforts.

"Over the past few years, authentication challenges have evolved due to the rise of sophisticated attacks like man-in-the-middle, credential stuffing, and password spraying," Hanson says. "Particularly concerning for HIPAA-compliant organizations are attacks that directly target healthcare personnel, leveraging tactics like phishing to gain unauthorized access."

Let's take a look at how industry and government officials are combating the continued cyberattacks, plus tips from Hanson for organizations trying to stay operational in the middle of it all.

Government doubles down on cybersecurity

The Advanced Research Projects Agency for Health (ARPA-H) has launched the Universal PatchinG and Remediation for Autonomous DEfense (UPGRADE) program, investing over $50 million to bolster cybersecurity in healthcare settings. UPGRADE aims to provide hospitals with advanced tools to secure their diverse and critical IT infrastructure against cyberthreats.

Healthcare facilities use a vast array of internet-connected devices, making traditional patching and security updates disruptive and challenging. In response, UPGRADE will create a software suite that allows for the rapid identification and automatic remediation of vulnerabilities in hospital IT systems without significant downtime. UPGRADE aims to reduce the time for deploying security fixes from months to days, enhancing the overall resilience of healthcare systems against cyberthreats.

The program will involve a collaborative effort among IT staff, medical device manufacturers, healthcare providers, and cybersecurity experts to develop and deploy security patches quickly and efficiently. UPGRADE also aligns with the broader efforts of the Department of Health and Human Services (HHS) to strengthen the cybersecurity posture of the healthcare sector.

ARPA-H's initiative is part of a larger strategy to secure digital health environments and mitigate the risks posed by the growing threat of cyberattacks in healthcare. The program's focus includes the development of high-fidelity digital models of hospital equipment to facilitate proactive security measures and automatic patch deployment.

Authentication best practices

Hanson provides compliance tips for managing authentication in healthcare settings. Implementing multifactor authentication (MFA) involves using a combination of something you know (password), something you have (smart card or token), and something you are (biometrics), Hanson explains.

MFA also entails:

- Ensuring any biometric data is stored securely and in compliance with privacy regulations
- Regularly updating and patching software to prevent the exploitation of known vulnerabilities
- Using adaptive or risk-based authentication, which evaluates the risk contextually and determines the level of authentication needed

"The future likely lies in biometric solutions and behavior-based authentication backed by AI," Hanson says. "Preparation involves piloting new technologies, ensuring compliance, and integrating them without compromising existing protocols."

Hanson stresses the importance of continually reassessing authentication strategies, staying updated on new threats, and proactively adapting to emerging technologies. The priority should always be the safety of electronic protected health information (ePHI) and patient trust.

"In our recommendations to healthcare practices or systems, we emphasize the importance of robust encryption practices," Hanson says. "This involves employing strong encryption protocols both during data transmission and while data is at rest. To ensure compliance with stringent privacy regulations, we advise conducting regular audits of these

storage solutions. These audits help verify that all security measures remain effective and fully compliant with current standards."

Phased approach to compliance

How do you balance the integration of a new technology with the maintenance of existing protocols? Hanson describes a methodical, phased approach:

1. **Compatibility assessments:** Begin with thorough compatibility assessments to ensure that the new technology integrates smoothly with current systems and protocols. This step helps identify potential challenges and areas where adjustments may be necessary.
2. **Documentation updates:** Revise and update all relevant documentation to reflect changes brought about by the new technology. This includes operational procedures, user manuals, and compliance documents.
3. **Staff training:** Conduct comprehensive training sessions for all affected staff. Training should not only cover how to use the new technology, but also explain how it fits into existing workflows and protocols.
4. **Gradual deployment:** Implement the new technology in phases. Start with a pilot phase involving a small group of users or a particular department. This allows you to collect feedback and make adjustments before a wider rollout.
5. **Feedback and adjustments:** Use the initial implementation phase to gather feedback from users. Feedback is crucial for making real-time adjustments and can help fine-tune both the technology and the training processes.
6. **Ongoing support and evaluation:** After full deployment, continue to provide support and periodically evaluate the technology's impact on operations. This ongoing evaluation helps ensure that the technology continues to meet needs and adapts to any changes in the operational environment or industry regulations.

Risk analysis and assessment

Organizations should conduct risk analyses at least annually or whenever significant changes to their IT environment occur. They should also keep careful records as they do. "It's extremely important that all risk assessment and gaps are documented. If it's not documented, in the eyes of the government, it's not happening," Hanson says.

Many healthcare organizations lack the staff or resources to conduct thorough risk assessments, so focusing on the highest-priority areas is a must. "The prioritization approach for risk analyses varies depending on several factors, including the size of the healthcare organization, the volume of patient records, and the existing security measures," she explains. "Our focus is primarily on areas where data is most sensitive and where disruptions would have the most critical impact. This method ensures that the most vulnerable and crucial aspects of healthcare operations receive the highest level of scrutiny and protection."

Remote access

Organizations can ensure secure remote access to ePHI by using virtual private networks (VPN) with strong encryption, deploying MFA for all remote logins, and employing endpoint security solutions on devices used for remote work. "Balancing security with usability is crucial for ensuring that healthcare personnel can perform their duties without unnecessary barriers," Hanson says.

"We recommend implementing user-friendly security solutions that maintain robust protection without impeding user experience," she says. "This includes seamless VPN connections that provide secure and efficient access to network resources, and single sign-on capabilities that reduce the cognitive load on users by minimizing the need for multiple passwords and login details."

Privileged access

Furthermore, Hanson recommends the use of privileged access management (PAM) solutions to monitor and manage privileged accounts to help strengthen security. This includes setting up just-in-time access, rotating passwords regularly, and logging all activities for audit purposes.

"We advocate for the implementation of time-based access controls," Hanson says. "These controls automatically revoke access rights to sensitive systems and data after a predefined period, such as the end of a shift or the completion of a specific task. This method ensures that access is strictly need-based, significantly reducing the risk of unauthorized long-term access."

Along similar lines, routinely changing passwords cuts down on the risk of compromised credentials. "Using a password manager is essential for securely managing and safeguarding credentials in healthcare settings," Hanson says. "We recommend integrating password managers that support regular password rotations and enforce robust password policies. These tools not only simplify the process of updating passwords but also ensure that each change is logged and fully auditable."

Finally, says Hanson, "we recommend implementing comprehensive logging systems that meticulously track all user

activities across systems. This approach provides a clear and detailed audit trail, crucial for thorough security audits and rigorous compliance checks.”

Phishing-resistant MFA

Examples of phishing-resistant MFA solutions in healthcare include hardware tokens and biometric solutions. Training can involve regular awareness sessions, simulated phishing tests, and immediate feedback on any test failures.

Hanson notes that organizations have adopted effective training approaches such as regular lunch-and-learns, inviting outside speakers, and introducing incentives for employees who report phishing attempts.

“These proactive steps have not only increased awareness but also significantly reduced the incidence of phishing attacks within their organizations,” Hanson says. “Feedback from these sessions consistently highlights enhanced understanding and vigilance among staff, contributing to a stronger security posture overall.”

HIPAA's flexibility

Organizations should prioritize core principles like confidentiality, integrity, and availability, and then evaluate new authentication technologies based on these principles. Pilot programs can also be useful before wide-scale implementation. When conducting pilot programs for new authentication technologies, start with a clearly defined scope and specific objectives.

“It's important to choose a representative sample of the user base and critical systems to ensure the pilot is comprehensive,” Hanson says. “Metrics to evaluate success should include user adoption rates, integration compatibility with existing systems, and improvement in security posture, such as reductions in unauthorized access incidents. Additionally, feedback from end users regarding ease of use and satisfaction is crucial to assessing the practical impact of the technology.”

Ongoing compliance

Continuous compliance can be ensured by periodic audits and deploying automated systems that can detect noncompliance or vulnerabilities. “We strongly recommend implementing an auditable process for your compliance program,” Hanson says.

Further, keeping up to date with regulatory changes is vital but can be challenging, especially for practices without a dedicated compliance officer.

Lessons from breaches

The healthcare sector is consistently the most targeted by cybercriminals, with breaches often resulting in substantial financial and reputational damage. These incidents underline the crucial need for robust security and compliance frameworks, adds Hanson.

“Common pitfalls include the use of weak or reused passwords and not implementing MFA,” Hanson says. “Avoid these by having strict password policies and ensuring MFA is mandatory. Many healthcare organizations have been fined for not following all of the HIPAA controls required to be fully compliant. It's important for healthcare organizations to document, document, document!”

“One key lesson we've learned is the absolute necessity of maintaining an auditable process for compliance management,” she continues. “Many breaches occur not just due to the lack of security measures, but also due to inadequate documentation and oversight of compliance practices. A comprehensive, auditable system helps ensure that all necessary precautions are documented and accessible for review and improvement.”

Additionally, by analyzing breaches in the industry, and by continuously educating and training on security protocols, organizations can significantly reduce the risk of successful attacks.

“Finally, collaboration between IT, security, and compliance teams within an organization is critical,” Hanson says. “Integrating these disciplines helps create a unified defense strategy against threats, making it harder for breaches to occur and easier to manage them if they do.”