Changes to HIPAA are on the Horizon

Is your email security strategy aligned with current and proposed HIPAA requirements?

IT leaders at healthcare organizations (HCOs) face many challenges. They need to ensure the IT systems that support patient care run continuously, without downtime. They need to focus on security, protecting networks and communication channels from cyberattackers. They also need to make sure their organizations are compliant with the hundreds of regulatory requirements that apply to HCOs.[1]

Not all HCO regulations have direct implications for IT and security. Of those that do, the one with the biggest impact on IT leaders is HIPAA. Changes to HIPAA, as well as the passage of related legislation and subsequent rulemaking (e.g., the HITECH Act (2009), the HIPAA Omnibus Rule (2012), the 21st Century Cures Act (2016), etc.) can make it difficult for HCOs to stay on top of cybersecurity compliance.

Proposed Changes to HIPAA Privacy Rule

In early 2021 Health & Human Services (HHS) proposed modifications to the HIPAA Privacy Rule "to increase permissible disclosures of personal health information (PHI) and to improve care coordination and case management."[2] The proposed changes include provisions to:

- Strengthen individuals' right to inspect their PHI
- Shorten the response time entities have to respond to requests for PHI from the current 30 days to 15 calendar days
- Clarify the form and format required for responding to individuals' request for their PHI
- Reduce the identity verification burden on individuals exercising their access rights
- Create a pathway for individuals to direct the sharing of PHI in an EHR among covered health care providers and health plans[3]

"The spirit behind the proposed changes is to be able to share information between entities more easily," said Fred Morton, Senior Security Strategist & Engineer, Mimecast. "At the same time, some of these changes may introduce additional risks to workflows."

For example, reducing the identity verification burden and shortening the required response time are both changes that could increase potential errors among employees already burdened by staff shortages and the challenges of dealing with the COVID-19 pandemic. "There's the potential for a threat actor to take advantage of the stressed attention span of those employees to create a situation where a vulnerability could be exploited, either within the workflow or within the technology that is sharing the information," Morton said.

When and if HHS will publish the final rule is unknown, although the expectation is that it will be published sometime in 2022. The final published rule may or may not include all of the changes contained in the proposed rule. Nevertheless, it's safe to expect HHS will continue to promote rules that support secure communications between patients and providers and between providers and other stakeholders.

The importance of email as a communication channel

The proposed rule acknowledges that HCOs share ePHI with patients and other providers using a variety of communication channels. Email, however, continues to be a mainstay of communication in the healthcare industry. "Not every patient opts into using the secure patient portal," said Lee Kim, Senior Principal, Cybersecurity and Privacy, HIMSS. "And providers and vendors often use different messaging systems as well. So it is quite common for providers to communicate with patients, other providers and business associates using email."

This [DMARC] has a downstream effect on an organization's other security controls, reducing the number of threats they need to prevent. Since email is the number one attack vector, it doesn't make sense to rely on endpoint solutions to mitigate those attacks. The more threats you can pull out further up the chain with an effective email filtering strategy, the better."

NEIL CLAUSON | Regional CISO | Mimecast

Unfortunately, the healthcare industry's reliance on email also makes it a prime target for cyberattackers. A HIMSS cybersecurity survey found that email was the initial point of compromise in 89% of significant security incidents occurring at HCOs.[4]

"HIPAA requires organizations to document they have implemented a cybersecurity program that is reasonable and commensurate with their risk," said Neil Clauson, Regional CISO, Mimecast. "Since email communication is known to be a vulnerable area, organizations have a duty of care to implement measures that address those risks."

Implementing a layered approach to email security to achieve HIPAA compliance

Email security is complex. "There is no silver bullet for defending against cyber threats, but because email is the entry point for the vast majority of attacks, applying the strongest possible protections to this communications channel should be a top priority," said Morton. "A layered approach is the best way to protect against multiple types of threats in a cost-effective manner."

To prepare for the proposed changes, Morton recommends HCOs conduct a gap analysis focused on the changing requirements. After IT leadership has identified what administrative and technical safeguards they need to implement to address those gaps, they can then present that information to hospital leadership.

The following layers of security should be considered when conducting a gap analysis. Clauson and Morton suggested that HCOs begin by evaluating their current email cybersecurity posture against these industry-standard practices:

1. **Block as many threats as possible at the email gateway**. A Secure Email Gateway (SEG) that protects against targeted threats, malicious code, dangerous attachments, and spam is one of the most effective defenses, as it helps prevent threats from ever reaching end-users.
2. **Implement Domain-based Message Authentication, Reporting & Conformance (DMARC)**. DMARC, an email authentication protocol, provides another layer of protection that complements the security provided by a SEG. According to Clauson, DMARC provides a tremendous amount of proactive protection. HCOs are just beginning to appreciate the value of DMARC as part of a comprehensive email security strategy. "DMARC's email rejection policy can prevent attacks that use email impersonations and spoofed internet domains," he said. "This has a downstream effect on an organization's other security controls, reducing the number of threats they need to prevent. Since email is the number one attack vector, it doesn't make sense to rely on endpoint solutions to mitigate those attacks. The more threats you can pull out further up the chain with an effective email filtering strategy, the better."
3. **Conduct security awareness training.** No approach to email security is 100% effective. Even with SEG and DMARC in place, some fraudulent emails may still reach end-users. That is why security awareness training is key. "Security awareness training should be engaging, brief, and frequent," said Morton. "Whenever possible, it should also use humor." Humor has been shown to boost retention of information presented in an educational context.[5] "It can also be very effective to inject brief user awareness training into end-users' email experience to reinforce best practices and alert them to potential threats," said Morton. For example, a solution might detect that a domain associated with an email has only been set up for a few days. The suspicious email could be tagged with the message, "This is a brand-new domain. You have never communicated with this person before. Are you sure you want to communicate with them?"
4. **Deploy business continuity and archiving solutions.** Email continuity and email archiving solutions enable further levels of protection for email communications. An email continuity strategy supports continued email communications in the event of unanticipated or planned downtime. "HIPAA's Security Rule does require covered entities, such as providers, to have contingency plans," said Kim. "If an organization loses a vital mode of communication such as email as the result of ransomware attack, you're stuck with old-school methods, such as the telephone or pen and paper. That slows down operations and influences things such as patient safety."

It's equally vital to have an archiving solution in place. "Many people use email as a kind of library or database," said Kim. "It's important to have an archive of those emails that preserves the integrity of those communications." An email archive can also be important for providing forensic analysis capabilities in the event of a legal request.

5. **Leverage the organization's ecosystem of controls**. "When you are talking about security, the sum is always greater than the parts," said Clauson. "That is why it is important to choose solutions that integrate with the organization's security ecosystem." In the same way that a patient leverages multiple experts as they move through a healthcare system, an HCO's security experts can leverage the threat intelligence derived from one platform (e.g., email) to inform other controls (e.g., endpoint controls, firewalls). "This strategy demonstrates to leadership that you are making the most of their cybersecurity investments, you're improving resilience across your ecosystem of controls, and you're focused on achieving the outcomes expected – protecting patients and the systems that deliver services to them," Clauson said.
6. **Consider managed services.** Managed services can be a good option for augmenting internal security teams, both for the additional manpower they provide and for access to resources and expertise. Some threat types — such as spoofing or brand impersonation — require tools and expertise that lie outside of an internal team's typical skill set. In addition, delegating management of specialized tools, such as DMARC, can free an organization's internal team to focus on the core mission: patient care.

A layered approach to email security is not only effective, but also adaptable. Using a multifaceted approach can help HCOs achieve compliance with current HIPAA regulations while also enabling the flexibility needed to make changes as HIPAA regulations evolve.

> **A layered approach to email security is not only effective, but also adaptable.**

It can also help HCOs fight against the evolving threat landscape. "Threat actors are pooling their resources to pull off more sophisticated attacks," said Morton. "Healthcare organizations are fighting asymmetrical warfare against these actors. They need to leverage the power of their ecosystems and vendor partners to help fight against that."

To learn more and see how Mimecast is a leading security solution in the healthcare industry, visit: Info.mimecast.com/healthcare.

References

1. American Hospital Association (AHA). 2017. Regulatory Overload: Assessing the regulatory burden on health systems, hospitals and post-acute care providers. https://www.aha.org/sites/default/files/regulatory-overload-report.pdf
2. Federal Register. January 21, 2021. Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement. 86 FR 6446. https://www.federalregister.gov/documents/2021/01/21/2020-27157/proposed-modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care
3. Federal Register. January 21, 2021. Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement. 86 FR 6446. https://www.federalregister.gov/documents/2021/01/21/2020-27157/proposed-modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care
4. HIMSS. 2020. Cybersecurity survey. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
5. Savage, Brandon M., Heidi L. Lujan, Raghavendar R. Thipparthi, and Stephen E. DiCarlo. 2017. Humor, laughter, learning, and health! A brief review. *Advances in Physiology Education 2017 41:3, 341-347. https://doi.org/10.1152/advan.00030.2017*

mimecast™

About Mimecast

Mimecast (NASDAQ: MIME) helps healthcare organizations reduce risk and increase resiliency by providing best-in-class protection for the top attack vector – email – and ensuring that email communications keep flowing no matter what. Simplified administration and easy integration with other security systems let you do more with less, while capabilities like end-user awareness training, world-class archiving, and brand protection allow you to deploy a more holistic security strategy. The bottom line? We take care of security so you can take care of your patients. Info.mimecast.com/healthcare