Briefings on HIPAA

Best of the best HIPAA Q&A from the past year

by Dom Nicastro

We've compiled the most popular questions and answers from the past year in the area of HIPAA compliance and healthcare data security. Below are the top five questions and answers, featuring insights from experts **Rebecca Herold, CDPSE, FIP, CISSP, CIPM, CIPP/US, CIPT, CISM, CISA, FLMI,** CEO of Privacy & Security Brainiacs SaaS services, and **Julia Huddleston, CIPP/US, CIPM, CCSFP,** a principal from Apgar & Associates.

Q: How can healthcare organizations ensure the security of electronic protected health information (ePHI) during telehealth sessions, especially with a growing number of patients and providers adopting virtual care?

A: During the COVID-19 public health emergency (PHE), the Office for Civil Rights (OCR) waived certain HIPAA requirements that otherwise apply to the use of telehealth. During the period of the PHE, OCR allowed the use of non-public-facing communication products to provide patients with telehealth services and disregarded many parts of the HIPAA Privacy and Security rules that were required in order to facilitate safe and timely patient care.

The PHE ended on May 11, 2023, and the period of OCR enforcement discretion finished 90 days later. In 2022, OCR provided information about the expectations for covered entities (CE) using telehealth services after the period of enforcement discretion ended.

OCR wants you to remember that telehealth presents security concerns. The HIPAA Security Rule applies unless the CE delivers telehealth via a landline. OCR also stated that telehealth should be an identified asset in your security risk analysis and vetted accordingly.

What does this mean for your telehealth management?

- You should be imposing access controls over the use of telehealth. Providers and staff should be formally authorized to use telehealth applications. Use of these applications should be logged and monitored like other applications used to provide care. Termination procedures should be implemented to ensure that provider and employee access to telehealth applications is terminated in a timely manner. Telehealth applications should only be accessible using organizational credentials and not personal email addresses.
- You should define and implement procedures to safeguard telehealth session recordings. Do you include these recordings as part of your designated record set? Are there limitations on who can record a session? Can sessions be downloaded to places besides the organizational environment? If so, how do you control usage and access? Are the recordings encrypted? (They should be!)
- You should draw up a business associate agreement (BAA) with your telehealth supplier. The BAA legally requires the supplier to implement the standards and specifications of the HIPAA Security Rule. That helps to provide security for your organization and your patients.

If you think that providers are accessing internet-based telehealth services that are not what the organization is standardly using, don’t turn a blind eye to it. If a provider who represents your organization breaches a patient’s PHI using a free service that they prefer, the argument that “you told them not to do that” won’t hold a lot of water with anyone. So, blacklist the telehealth applications that you think they might use in the same way that you blacklist non-approved applications.

— Answered by Julia Huddleston

Q: What are the most common challenges organizations face in achieving and maintaining HIPAA privacy compliance?

A: There are many common challenges. They vary depending upon the size, type, location, and complexity of each organization. Businesses with one person to a few employees in a single location have significant challenges that are different from the huge, corporate entities with many locations, which provide a wide range of services.

Here, in no particular order, are five significant common challenges to all organizations, taking into consideration the vast range of differences among them:

- **Keeping systems, applications, and networks updated with the latest versions and applying patches**

to newly discovered vulnerabilities. Cybercriminals know the newest vulnerabilities, and they have tools to find and attack any organization that is online, or sometimes online, through any of their endpoints, to exploit those vulnerabilities. Size and location do not matter.

- **Keeping personnel awareness of HIPAA compliance requirements high.** This is why providing regular training (active and formal), in addition to ongoing awareness messages and activities (passive and informal), are critically important for all employees and contractors who have access to any protected health information (PHI) and possess any associated devices, systems, networks, and applications.
- **Performing ongoing risk management activities.** One such activity that is rarely performed in any size or type of HIPAA CE, and almost never performed in any type of HIPAA business associate (BA), is maintaining awareness of, and documentation for, all data, devices, and applications used within the organization. Why is this policy important? Because a lack of this type of policy leads to HIPAA violations, security incidents, and privacy violations. Examples of potential HIPAA hazards of this type include:
    - Personally owned devices, unknown to the organization, being used to support CE activities that have not been secured per the CE's security and privacy policies.
    - Tracking technologies (such as Meta Pixels and other types of web beacons) being implemented by IT, individuals, and BAs who did not clear taking such actions with the security and privacy compliance team. These types of unauthorized implementations have resulted in many incidents of improper PHI collection and dissemination, violating many Privacy and Security Rule requirements.
    - Other new technologies (e.g., smart internet of things products, AI tools) being used within the overall organization's digital ecosystem in ways that create risks, and also violate technical, administrative, and physical Privacy and Security rule requirements.
- **Maintaining ongoing oversight of BAs.** A significant portion of large CEs, most of the mid-sized CEs, and virtually all small CEs do nothing for BA oversight beyond having BAs sign an agreement. All CEs need to understand that part of their risk management activities require taking reasonable actions to ensure their BAs are, at the very least, applying the same security and privacy practices to all environments where PHI is located. The responsibility for the security and privacy protections follow the PHI to the BAs, and CEs will be held responsible for HIPAA violations, privacy breaches, and security incidents that originated within their BAs.
- **Protecting against ransomware.** This is a problem for all organizations and members of the general public; however, hospital systems and all other types of healthcare providers, insurers, clearinghouses, and BAs are targets because cybercriminals know that healthcare organizations do not invest enough into budgets, personnel, or attention to security and privacy protections. Additionally, healthcare data is also the most valuable type of data to cybercrooks. If more attention was put forth into making frequent backups, better backup practices, and updates to disaster recovery and incident response plans so that specifics for ransomware events were included, there would be significantly fewer successful ransomware attacks within the healthcare industry.

— Answered by Rebecca Herold

Q: With the evolving threat landscape, how should HIPAA training programs be updated to ensure that all staff members are well versed in compliance requirements?

A: Security awareness training is the most important investment that an organization can make to help ensure that its staff members keep the organization safe and compliant. Good information security awareness training can help to:

- Prevent breaches and fend off phishing attacks
- Create a culture of security by building security values into the fabric of your organization
- Bolster your technology against cyberthreats
- Reassure your customers and patients that the organization cares about keeping their information safe
- Meet compliance requirements

A staggering portion of cybersecurity incidents are linked to people: therefore, one of the key ways to help people improve their security behaviors is via cybertraining. If you are considering instituting a training program at your organization, the following topics and categories are critical for understanding the fundamentals of cybersecurity:

- The use of passphrases (rather than traditional, difficult-to-remember passwords) and the use of multifactor authentication for added security.
- Identifying and avoiding scams. From phishing to smishing, people need to feel confident about their ability to spot a scam. A simulated phishing attack can (when done well) transform how people respond to threats.
- Different types of malware and how to identify the signs of infection.
- Robust device security—help people to make their devices into Fort Knox. Teach them how to configure antivirus software and firewalls and set up automatic updates.
- The optimism bias. People don't believe they'll be a victim of cybercrime. By directly addressing this bias, you'll boost the effectiveness of your campaign. Why? Because if people think it'll never happen to them, why would they listen in the first place?
- Preventing identity theft—a key element of good cybersecurity training. Your program needs to help people spot

warning signs and clean up their passwords.
- How to browse securely and how to avoid tracking or form auto-filling. Break it down with step-by-step guides on browser configuration.
- The risks of unsecured public Wi-Fi—and how to use a VPN for protection.

— Answered by Julia Huddleston

Q: For the final rule "HIPAA Privacy Rule to Support Reproductive Health Care Privacy," what are the highlights for HIPAA compliance officers?

A: The HIPAA Privacy Rule to Support Reproductive Health Care Privacy aims to strengthen HIPAA privacy protections by "prohibiting the disclosure of [PHI] related to lawful reproductive health care in certain circumstances."

Previously, medical record privacy was at risk, particularly when patients sought legal reproductive healthcare across state lines. The new level of HIPAA privacy includes the following provisions:

- "Prohibits the use or disclosure of PHI when it is sought to investigate or impose liability on individuals, healthcare providers, or others who seek, obtain, provide, or facilitate reproductive healthcare that is lawful under the circumstances in which such healthcare is provided, or to identify persons for such activities."
- "Requires a regulated healthcare provider, health plan, clearinghouse, or their business associates, to obtain a signed attestation that certain requests for PHI potentially related to reproductive health care are not for these prohibited purposes."
- "Requires regulated healthcare providers, health plans, and clearinghouses to modify their Notice of Privacy Practices (NPP) to support reproductive healthcare privacy."

Compliance with the final rule is required 180 days after the effective date, which means organizations must be compliant by December 23, 2024. OCR is allowing a deferred date for required NPP changes of February 16, 2026, to accommodate other recent regulatory changes that impact NPPs. OCR has also stated that it will make available a model attestation no later than December 23, 2024.

In the meantime (and remembering that December is the height of the holiday season), CEs should:

- Review and revise current policies and procedures regarding PHI disclosures, in addition to BAAs, to ensure they comply with the final rule
- Begin updating employee trainings when appropriate to help employees understand the new rule and obtain necessary attestations before disclosing PHI potentially related to reproductive healthcare

— Answered by Julia Huddleston

Q: Can you discuss the importance of integrating security and privacy controls into medical devices and what specific risks need to be addressed to comply with HIPAA regulations?

A: The HIPAA Privacy and Security rules include many specific types of controls that must be incorporated into all healthcare CEs and BAs. Medical devices are some of the most patient-impactful elements within those ecosystems. The use of medical devices is often the difference between life and death for the associated patients. This potentially fatal impact provides even more reasons for building security and privacy controls around medical devices.

These devices not only should be used to provide treatment to patients; medical devices that collect, derive, transmit, receive, process, or store data about patients must also provide capabilities that facilitate HIPAA security and privacy requirements. Manufacturers and engineers designing medical devices need to ensure that the following security and privacy capabilities are built into the devices themselves:

- **Access controls:** capabilities for accessing the device (utilizing unique user IDs with strong authentication methods, such as multifactor authentication or passkeys); and capabilities for accessing, changing, copying, and deleting data
- **Activity logging:** capabilities to create logs for all the types of access previously listed, with associated details (e.g., audit trails)
- **Remote administration:** capabilities for authorized personnel to locate devices, disable devices, remotely wipe data from devices, and other types of activities supporting the purpose of the medical device and mitigating associated risks
- **Encryption:** capabilities to strongly encrypt and decrypt data based on established risks in the device's digital environment
- **Automatic session logout:** capabilities for authorized connections to be inactivated and/or logged off as

reasonable and appropriate for the associated purpose and use of the medical device
- **System updates:** capabilities to automatically apply system and application updates
- **Malicious code protection:** capabilities for protecting the device and associated components from malicious software
- **Terminating access:** capabilities to terminate access for established user accounts when access to the device is no longer authorized
- **Data backup:** capabilities for automating and/or manually backing up medical device data to remote, secured backup media
- **Data destruction:** capabilities for irreversibly deleting data from the medical device and all associated components

For each of the capabilities listed, if they are not possible due to the purpose of the device, or if the capability is lacking in a device that is already being used or must be used, then CEs should ensure that the manufacturer and/or vendor provides clear instructions for how CEs and BAs can completely delete all data.

It is important to note that manufacturers and vendors supporting medical devices and in possession of patient data are considered to be BAs and are thus subject to HIPAA’s compliance standards.

— Answered by Rebecca Herold