Briefings on HIPAA

HIPAA Q&A: Medical devices, social media, and reproductive healthcare

by Rebecca Herold, CDPSE, FIP, CISSP, CIPM, CIPP/US, CIPT, CISM, CISA, FLMI

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 covered entities (CE) and business associates (BA). 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.

Q: With the rise of social media, what are some best practices for healthcare organizations to prevent unintentional HIPAA violations when employees and patients share information online?

A: This is an important issue for every type of CE to consider when establishing policies, procedures, rules, and training. BAs, however, should also take this into consideration to ensure that important PHI does not end up publicly accessible online.

For example, in 2019, Elite Dental Associates in Dallas paid $10,000 to the Office for Civil Rights (OCR) and had to adopt a corrective action plan to settle HIPAA Privacy Rule violations after posting a patient's last name and details of their health conditions to the internet.

Here is a high-level checklist of items to keep in mind when dealing with social media and HIPAA:

- Establish social media and other types of online security and privacy policies.

- Establish supporting procedures for each business unit regarding compliance with the unit's policies.
- Assign a role/position/person with the responsibility for monitoring public social media sites for information about the CE and associated BAs, and ensure that workers know and understand the policies and supporting procedures.
- Provide training to all employees, including BAs (at least once a year), covering the online posting policies. Also, provide ongoing reminders.
- Consistently apply sanction policies for those who violate policy and post PHI or related information online.

Q: OCR released a HIPAA rule in April 2023 that became effective April 22, 2024, including changes related to reproductive healthcare privacy rights. What steps should CEs and BAs take to ensure compliance with these new requirements?

A: The final rule:

- 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 BAs to obtain signed attestations that certain requests for PHI potentially related to reproductive healthcare are not for these prohibited purposes
- Requires CEs to modify their Notice of Privacy Practices (NPP) to support reproductive healthcare privacy

CEs and BAs need to:

- Update their applicable privacy and security policies and procedures to include the attestations and actions specific to requests from individuals who are not involved with treatment, payment, or operations of the patient and who are not authorized to access reproductive health data. Such updates, or creation of new policies and procedures if they do not yet exist, should include:
    - Information indicating that reproductive healthcare and the associated data is protected by HIPAA and the United States Constitution, regardless of the state where an individual is pursuing access to the data.
    - Procedures for BAs to follow if any type of entity ever asks a BA to turn over PHI. The BA should contact the associated CE as soon as possible and notify them of the request.
    - A statement that the decision to release PHI upon a request must be made by the CE, not the BA, no matter what the entity requesting the PHI says.
        - Update the NPPs that they provide to patients and insureds. Most BAs will not need to do this, but those that support the provisioning of NPPs to patients and insureds will need to ensure the NPPs for each of their associated CEs are updated to align with their CE clients.
        - Provide training on how to respond to requests for reproductive health data for workers who would, or could, be involved with such situations.

Q: How can healthcare organizations balance the need for patient safety and data security with the demands of legal compliance, and what role does ongoing training and awareness play in achieving this balance?

A: HHS has created some useful and informative guidance for CEs and BAs about deciding how to meet such legal compliance demands. You can see such guidance here. There are some good examples included.

Privacy and security officers within CEs and BAs should make use of these guidance documents and incorporate them within their organizational training courses. For these types of situational compliance activities, online training can be provided, but often it is more effective to provide live in-person training to allow for questions and other types of interactions that will help support long-term retention of the concepts covered.

CEs and BAs also should send short excerpts and/or reminders about these issues on an ongoing basis. This will help to ensure all personnel who would be involved in these situations will understand the key requirements and respond consistently in relevant scenarios.

Editor's note: Herold is the CEO of Privacy & Security Brainiacs SaaS services, providing HIPAA security and privacy training and other compliance services.

"Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro, or the Copyright Clearance Center at 978-750-8400. Opinions expressed are not necessarily those of RCA. Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions."