Home health & HIPAA compliance

HIPAA compliance is a journey, not a destination, and that journey is often long, complex, and loaded with obstacles. Overcoming those obstacles is difficult for all healthcare organizations, regardless of size or stature, but for home health agencies, whose workers are more mobile than most, achieving and maintaining HIPAA compliance comes with some unique challenges.

As care workers come and go between multiple locations, home health organizations face a difficult balancing act between providing their staff with the necessary information and lines of communication required to carry out their job effectively, whilst simultaneously ensuring best practice security and privacy standards are adhered to at all times.

A major step in achieving, and crucially conserving HIPAA compliance in the home health arena is understanding these unique challenges, and providing staff with the necessary training and tools to deliver uncompromised levels of care, without jeopardizing the integrity of patients' health records. This guide explores some common HIPAA compliance challenges faced by home health organizations, and offers some solutions for overcoming them.

Challenge 1. Misplaced devices

The portability of smartphones makes them particularly susceptible to loss or theft, and for home health workers, the likelihood of misplacing a device is increased due to the amount of traveling involved; from devices being left behind after appointments, to being stolen from parked vehicles, taking a mobile device into the field increases risk. While for most people the loss or theft of a device presents little more than a costly inconvenience, in healthcare the repercussions can be much more severe.

If a misplaced device contains electronic protected health information (ePHI), either stored within an app or on the device itself, then it needs to be reported as a breach under the HIPAA Breach Notification Rule. In almost all situations, there are only two reasons a lost device may not have to be reported:

1. No PHI was on the device
2. The PHI is encrypted to FIPS 140-2 standards, rendering the data unusable

In both cases, documentation must be provided to support the final decision. Simply writing the device off and hoping for the best is not an option. By implementing a few straightforward security best practices, it is possible to reduce vulnerabilities and ensure sensitive data remains protected, should a device wind up in the wrong hands.

- Encourage employees to implement strong passwords, PINs, and other methods of user authentication, and ensure these credentials are frequently updated
- Deploy multi-factor authentication where possible
- Encrypt devices to help prevent unauthorized parties accessing confidential data
- Install remote wiping and/or remote disabling

Challenge 2. Secure communication

When working out in the field, be it in a patient's home, a care home environment, or in a public space in between appointments, care workers need to maintain a reliable and secure line of communication with coworkers. Whether sending, receiving, or gaining access to ePHI, the process of doing so must not be at the expense of patient privacy.

Smartphones, in particular, provide home health professionals with a convenient way of communicating with their colleagues when in the field, but this convenience can easily lead to a HIPPA violation if ePHI is exchanged through nonsecure channels such as email, text message (SMS) or other popular messaging apps like Skype, Facebook Messenger or WhatsApp. While some of these platforms encrypt data while it is in transit, thus checking some of HIPAA's security boxes, a lack of secure storage or access controls mean there is still significant risk involved when communicating via these channels. What's more, these platforms also present significant potential for human error, as messages could be sent to the wrong recipient/s. Even after a message has been sent, there's rarely any way of knowing whether the intended recipient has received or read it.

To avoid these pitfalls, home health organizations should establish policies that regulate security procedures and prohibit the use of non-secure applications for medical communication, and ensure all staff are trained to follow best practices. Critically, organizations must invest in HIPAA-secure tools that provide a secure alternative to the likes of email and text messaging, but also offer the convenience and familiarity of a mobile application so not to negatively affect workflows. This allows care teams to communicate easily while on the road, without the worry that ePHI is being put at risk.

Challenge 3. Wi-Fi roulette

Accessing the internet via unsecured wireless networks in public spaces such as coffee shops, airports, and service stations presents significant risks. While public Wi-Fi networks can provide a convenient, and often critical means of accessing important information while away from a desk, they also present an easy way for unauthorized users to access and intercept sensitive data.

As a primary precaution, home health caregivers should be encouraged to change the settings on their devices to ask permission before automatically joining any unrecognized networks, and where possible, use a secure browser connection or VPN (virtual private network) to route traffic through a secure tunnel even when a device is connected to public Wi-Fi.

Challenge 4. Disclosure of information

Under the HIPAA Privacy Rule, patients have the right to request that details of their medical condition are withheld from some or all third parties, including family. In home environments, where close family and friends may be present, this can cause awkward situations, and can even prevent a care worker from doing their job properly. It is impossible to predict if and in what context such a situation may arise, but in order to protect themselves and the integrity of their patients' health information - and in turn minimize a potential HIPAA violation - carers should be trained to never discuss patient information with anyone other than the patient or their authorized representative.

Challenge 5. Paper records

Electronic health record (EHR) adoption among healthcare organizations is at an all time high, with the vast majority of home health agencies now utilizing digital records to improve workflows and manage patient care more effectively. While the digitization of healthcare may have driven down paper usage within most care environments, it's paper charts are still very previland in home health.

Protecting the integrity of paper records within the relative safety of practice walls can be achieved through securely locked cabinets and cupboards, but as soon as paper leaves the building, it becomes vulnerable. Loss and theft is one thing, but even reading physical records in a public space could become a problem if it was to be left behind or seen by a curious bypasser.

Any old or unwanted documentation containing PHI, no matter how insignificant it may seem, should be disposed of properly to a point where the information is indecipherable - simply tossing it in the trash will not suffice. HIPAA's privacy and security rules do not require a particular disposal method, but the steps taken to safeguard PHI must be reasonable, for example shredded, burnt, or pulped to an extent that it is rendered unreadable and cannot be reconstructed.

PHI on paper is the same as PHI on a computer or mobile device, and both need to be protected from unauthorized access. To avoid potential HIPAA violations caused by paper documents, care workers should be educated to recognize the 18 PHI identifiers as listed by HIPAA. While some of these identifiers are more obvious than others - names, addresses, full face photographs - others are less so, and could, therefore, be misconstrued as non-sensitive data. Even the smallest detail could, in theory, be tied back to a patient, so when it comes to paper, it's best to err on the side of caution and assume everything is private.

Responsibilities

Ultimately it is the responsibility of the employer to ensure home health workers remain HIPAA compliant at all times, through the implementation of thorough training programs, ongoing risk analysis, and clearly communicated policies. In the event of an unauthorized disclosure of PHI, it would be the employer's responsibility to report the beach to the Department of Health & Human Services (HHS), even if it was the negligence of a healthcare worker that caused the breach in the first place.