10 Best Practices for Protecting Confidential Health Information

ENCRYPT DATA

Data encryption is required by HIPAA when transmitting PHI over open networks as a way of safeguarding PHI. Data encryption scrambles text to make it unreadable if it gets in the hands of a person who doesn't have a "key" to unlock it. Many software programs have data encryption capabilities built-in, or you can use third-party resources. It's important for everyone in the practice to understand what steps to take to encryptdata that includes PHI. However, data encryption is not completely fail-safe, so experts caution that you shouldn't rely on data encryption as your only defense against healthcare cybersecurity breaches.

ENCOURAGE BEST PRACTICES IN THE OFFICE

Every person in the office plays a role in ensuring privacy as part of your company culture. Demonstrate a commitment to privacy from the very moment patients enter the practice. This includes offering ample space for filling out forms and providing insurance information in a discreet manner. Always discuss individual patient health matters in private rooms, never within earshot of other patients or staff members who don't have a need to know the information. And don't leave patient forms sitting out in the open. Keep all files secure and confidential. When everyone on the care team adheres to these practices, it reinforces and reminds us all that they are important.

NEVER SHARE PASSWORDS

Passwords should be changed regularly and should be complex, so they can't easily be guessed. Use a combination of uppercase and lowercase letters, numbers, and special symbols. It's also a good idea to change passwords regularly. Never share passwords with anyone else on the clinical care team, or with anyone at home. Each staff member should have their own access code, and always use their own password when accessing confidential PHI.

DEVELOP AN INCIDENT RESPONSE PROCESS

In an ideal world, errors in handling PHI would never happen. But it's wise to have a process in place if they do. Consult with a privacy expert or legal representative to ensure you understand what steps are required in the event of a privacy breach. Requirements likely vary based on the specifics of the situation. It can be helpful to compose a guide or decision-support tool that staff can easily reference in case of an incident. Include contact information for anyone who needs to be alerted right away.

EDUCATE STAFF

Make sure everyone in the office fully understands the importance of protecting confidential PHI. Privacy compliance should be an essential component of employee onboarding training, with regular refreshers for all staff. Keep privacy rules and policies posted where they easily can be seen, and keep an open dialog about patient privacy. Finally, consider appointing a privacy officer to be in charge of monitoring patient privacy practices in your office.

10 Best Practices for Protecting Confidential Health Information (continued)

CONDUCT A RISK ANALYSIS

Evaluate the potential privacy pitfalls that occur in your practice. It can be a humbling and eye-opening experience to investigate where there may be lapses in your process. A risk analysis is the first step toward making changes that can have a real impact on protecting PHI for your patients.

EVALUATE RISKS WITH PARTNERS AND VENDORS

Extend your risk analysis to include risks with partners and vendors. Security of patient information doesn't begin and end with just the clinical care team. If you work with vendors and other partners, you need to ensure that their systems are HIPAA-compliant and that they're following proper procedures as well.

DEVELOP DIFFERENT LEVELS OF ACCESS

HIPAA mandates that you should only access patient health information that you need to do your job. Some roles require greater access than others. Setting access based on roles can help prevent people from accidentally seeing information not necessary for their jobs. This improves security and helps you protect confidential patient health information.

SHRED PAPER FILES WITH PHI

Do you use paper forms for collecting information, and then transfer all the data into your EMR platform? Maintain the highest level of security by shredding paper forms and files you don't need to keep. Have special bins for the shreds rather than throwing them in the regular trash containers. PHI you should shred includes patient forms, data reports, or insurance billing information. Never leave printed PHI in the open, and don't keep them longer than you need to.

SHARE PATIENT RECORDS SECURELY

There are many situations when you need to share patient information with other healthcare providers. For example, you may need to share information about a diagnosis or treatment plan to coordinate care, or you may request records from another practice. You'll also receive medical records requests from a patient, insurance companies, or other entities.

Recent updates to the 21st Century Cures Act encourages greater cooperation between clinicians to support better healthcare decision-making. This includes securely sharing electronic health information. In these situations, it's crucial to ensure that the right documents get to the right person at the right time.

There's a lot at stake when it comes to protecting confidential health information. Follow these best practices to develop policies and practices to ensure you're protecting both your patients and your medical practice.

Vivlio offers a secure solution for doing just that. We go above and beyond, offering the highest level of security to seamlessly and securely transfer medical records across multiple electronic medical records (EMR) platforms, in accordance with the Cures Act.

vivlio health

vivliohealth.com

info@vivliohealth.com

vivlio-health