

Protecting Patient Data

The security of patient health information is extremely important to health care providers and their patients. While health care practices already follow HIPAA rules and regulations, practices must recognize that electronic health records (EHRs) present different challenges than paper charting systems. Practices need to adjust behaviors and institutional procedures to make sure their patients' electronic health information is kept safe and private.

According to recent surveys, patients worry that their personal health information might not be kept private and secure if stored electronically. Patients are especially concerned about who will have access to their records.

Despite these concerns, patient health information has not been the target of most electronic privacy breaches. Rather, data that can be used for financial fraud and identity theft (such as Social Security numbers) are at highest risk. In order to protect patients, practices must do everything to maximize the security of their patients' electronic data and health information.

To ensure the safety of your patients' information:

I. Choose an EHR product that has all of the recommended security features (*front*).

II. Follow the proper procedures and practices to maintain data security (*back*).

I. Choose an EHR product that has all of the recommended security features.*

1. Role-Based Access

- > Allows the practice to define access privileges of each staff person and ensures that only authorized health care providers can see patients' health information. Administrative staff should be restricted to basic information such as address, date of birth and other demographic information.
- > Practice leadership should be the only people who are responsible for establishing the access privileges of staff members.

2. Audit Trails

- > Audit trails track activities within the EHRs. Documented events in an audit trail include: a staff member logging in or out of the system, opening, modifying, creating or deleting a record, scheduling a patient, signing a chart, querying the system or printing personal health information.
- > Audit trails also document the date and time of an event, where the event occurred and who performed the event.
- > Only authorized administrators should have access to read these records. No one, not even the office administrator, should be able to modify or delete audit trails.

3. Password Protection

- > EHRs must require a password to access the system.
- > EHRs should be able to support additional passwords or identifiers for each user. For example, a practice could use passwords and biometrics (e.g., fingerprint or retinal scans) to confirm the identity of people logging into EHRs.
- > The practice administrator should be able to define the rules for password complexity and expiration. (*e.g., the practice may require all users to have passwords with five letters and at least one number, and that staff members change their password every three months.*)
- > The system must automatically log out a staff member if they forget to log out or leave the screen inactive for a period of time. The system must also require the user to enter his/her password to get back into the system.
- > If someone repeatedly tries to enter the wrong password, the system should lock the user out. This keeps people from guessing other users' passwords.

4. Data Encryption

- > EHRs should encrypt patient data, which helps to protect data if hardware is stolen, or messages are intercepted.

5. Consent

- > EHRs should have the ability to print, store and display patient consent forms.

*Security features are recommended by the Certification Commission for Health Information Technology (CCHIT).

II. Follow the proper procedures and practices to maintain data security.

1. Continue following the rules and regulations set forth by HIPAA.

- > Do not leave printed patient health information where others have access to it.
- > When scanning information into a patient's EHR, destroy the paper copy when it is no longer needed.
- > Unlike paper charts, it is easy to see a computer screen from across the room. Computer screens should not be visible from the waiting room, check-in area, or any place an unauthorized person may be able to see a patient's EHR.
- > Install privacy filters on monitors to block anyone from viewing the computer from a side view.

2. Install antivirus, intrusion detection and firewall software.

3. Do not use Social Security numbers as a unique patient identifier.

4. Patients have the right to control who sees their information.

- > Whether or not an EHR system is in place, do not share patients' health information with anyone unless the patient has personally authorized it or such disclosure is authorized by law (e.g., mandated disease reporting).
- > Ensure that employers, marketers and law enforcement or immigration officers do not have access to patient records.
- > If your practice is part of a Health Information Exchange network, patients have the right to choose whether or not they will participate.
- > Patients have the right to revoke their consent for sharing information.

5. Patients should understand their rights to consent, as listed in #4 above.

6. Always log out of the EHR system when leaving the computer.

- > If EHRs are left open on the screen, other people can access and/or modify patient information. This activity will be logged as the user's and he/she may be held accountable for any privacy violations.

7. Keep all passwords safe and secret.

- > Create a password carefully. Passwords should not be obvious, such as birthdays, pets' names or favorite sports teams. Think of something that is easy for you to remember, but impossible for anyone else to guess.
- > Never share passwords. If anyone asks a staff member for his/her password, the staff member should report that person immediately to the practice administrator.
- > Passwords should not be posted or written down near the staff members' desks.
- > Change passwords every three months.

8. Ensure hardware is safe and secure.

- > Portable computers are easy to steal. Computers, servers and other equipment that contain data should be locked in a secure place when not being used.

9. Be careful when accessing EHRs from outside of the office.

- > When opening a patient's EHR in public, make sure no one can see the computer screen.
- > Only access EHRs from a secure Internet connection.

10. Train all staff members on data security policies and procedures.

- > Make sure everyone in the practice understands and observes the policies and procedures for protecting patient health information.

11. Keep up with staffing changes.

- > If an employee leaves the practice, change the user's status to inactive. This means they can no longer sign in with their old password.

12. Review audit trails periodically.

- > Reviewing audit trails can alert practices to potential system abuse or misuse.
- > Some staff members forget to log out of their system, as well as access parts of the EHRs that are beyond their practice function. Audit trails can let practice administrators know when this occurs and take appropriate action.

Improve Quality of Care Through Electronic Health Records

For more information, visit www.nyc.gov/pcip