Security101

Strengthening privacy and security

in the modern healthcare landscape

Step into the ever-changing landscape of ***healthcare data protection***. Discover the vital need for robust policies that not only ***secure patient information*** but also ***enhance privacy and safety***. Uncover the challenges faced by healthcare organizations, insurers, and researchers in ***safeguarding patient confidentiality*** within the ***intricate healthcare structure***.

Security101

Contents

Introduction

Protection of medical records has been a permanent concern in the health care industry. For centuries, physicians have adhered to the oath of Hippocrates to keep confidential the information they learn from patients. Nowadays, the practice of medicine is drastically more complex and vulnerable, since it goes beyond the patient-provider relationship to a more intricate structure where there are organizations collecting and analyzing individuals' health information.

As insurers, managed care organizations, public health officials and researches continue to need patient information, it is paramount to follow with rigor the policies and practices that truly protect the data they collect and boost patient safety and privacy. In a time of increasing advanced communications and technologies, it is also fundamental to acknowledge the proper measures to keep electronic health records (EHR) secure and out of the wrong hands.

In accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), there are national standards to be followed by covered entities for the protection of individually identifiable health information. Besides abiding by those policies, advances in physical security are indispensable to implement in order to safeguard the integrity of medical records, limit the inappropriate disclosure of personal data to unauthorized parties, and guarantee the safety of patients.

Medical records management

The procedures and protocols utilized to handle patient information throughout the entire data lifecycle is called medical records management. Managing patient records efficiently and accurately is critical to avoid numerous threats, including medication errors, missed diagnoses, treatment lapses, and other events that can put the lives of patients at risk.

Likewise, not protecting patient data can compromise the privacy and security of the individual by exposing highly sensitive personal information to unauthorized parties. In addition, hospitals and clinics are aware of the urgency of enhancing the quality of their service to attract and retain more patients, which places a massive value on proper medical record management.

Data breaches are a main concern that should not be underestimated. When they happen, patients are unwilling to share their full medical history as they do not feel confidence in their provider, inducing a defective outcome in the medical treatment. Second, poor record management leaves healthcare facilities vulnerable to expensive fines, lawsuits, and criminal charges.

The process of safeguarding Protected Health Information (PHI)[1] — any individually identifiable health data — starts at the moment a patient record is created. It must be then adequately stored, secured, and maintained for a specified retention period to finally be properly destroyed.

[1] *The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights regarding that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.*

SECURITY & STORAGE

According to HIPAA, there are some security measures that must be observed to ensure the integrity of PHI:

1. Identify and proactively protect data against anticipated security threats.
2. Train employees in medical records security procedures.
3. Ensure records are stored where there is controlled access.
    - Locked file cabinets, desks, closets, offices.
    - Wireless locks
    - Alarm keypad systems
    - Biometric authentication
4. Implement hardware, software, and procedures to control access.

Moreover, it is recommended that medical records are placed out of sight of unauthorized individuals, but if they must be in accessible places, they should be stored in locked cabinets with no open shelves.

ACCESS, RELEASE, AND RETENTION TIMELINES

In conformity with HIPAA, a patient or patient designated representative has the right to access medical records. To ensure records are released correctly, providers and insurers are severely restricted from sharing data.

The backbone of a defensible record and information management program is a solid retention schedule that meets all applicable and operational requirements, including federal and state laws. The retention parameters vary per state.

DATA DESTRUCTION

Data destruction is the last step of the medical records management process. After the retention period expires, properly destroying information is important to prevent it from being used in any illegal or unauthorized manner. HIPAA provides strict data destruction protocols. The main goal is to make PHI essentially unreadable, indecipherable, and unable to be reconstructed.

The methods of destruction entail:

- Shredding
- Burning
- Pulping
- Pulverizing

Further, labeled prescription bottles and other PHI should be placed in opaque bags in a secure area. In regard to electronic health records (EHR), clearing (overwriting media with non-sensitive data), purging (exposing media to strong magnetic fields to disrupt the magnetic domains), and destruction of media (disintegration, pulverization, melting, incineration, or shredding) might be necessary.

Protecting patient privacy

Confidentiality of health care data is being questioned by people. Such concerns are growing as more sensitive information, such as HIV status, psychiatric files, and genetic information, is being stored in medical records. Addressing these concerns requires a better understanding of the vulnerabilities of health information in paper and electronic form and the various mechanisms available for protecting such information.

Covered entities (health plans, health care clearinghouses, and healthcare providers who electronically transmit any health information) must apply appropriate administrative, technical, and physical safeguards, as mandated by HIPAA, to protect the privacy of PHI, including the disposal of such information.

Protected Health Information must not be disposed in dumpsters or other containers that are accessible by the public or other unauthorized persons. In addition, the disposal of certain types of PHI such as name, social security number, driver license number, credit card numbers, diagnosis, and treatment information require more attention as it can potentially be used for identity theft, discrimination, and harm to the patient's reputation.

The concerns of privacy are based on two premises:

1. Individuals have a fundamental right to control the dissemination and use of information about themselves.
2. Information about an individual, revealed to a party not willingly designated by the individual, may be used to harm their economic or social interests.

ELECTRONIC HEALTH RECORDS

Moving from paper records to electronic health records (EHR) allows providers to use information more effectively and improve the quality and efficiency of patient care. Electronic Protected Health Information (ePHI) is still very vulnerable to malicious attacks, thereby requires advanced security efforts to protect confidential data.

In addition to applying administrative and physical safeguards, covered entities must adhere to reasonable policies and procedures and comply with HIPAA Privacy Rule to protect confidentiality, integrity, and availability of data.

In order to protect information in electronic form, healthcare providers must make changes and incorporate the latest physical security solutions to effectively reduce risks. It is also important to have strong cybersecurity strategies in place to prevent, detect, and respond to attacks against patient information.

These are some important questions to consider to improve the security practices put in place to safeguard medical records:

- Where is the documentation stored?
- Where are the backups stored?
- What are the backup and recovery routines?
- Is information encrypted?
- Is emergency access possible?
- Do authorized employees have user-based access control?
- Are employees trained on medical records best practices?
- How are identities authenticated?

KEY STEPS

Protecting patient privacy and complying with HIPAA Privacy Rule can be achieved by strictly following a few best practices and adopting essential physical security technologies.

Comply with regulations

Besides acting in accordance to HIPAA guidelines, clearly define the policies and procedures for maintaining medical record security within the campus. Update as necessary or responding to organizational changes. The effort should be multidisciplinary and welcome all departments involved with handling records.

Label records accurately

Medical errors are a substantial cause of death in the United States. For this reason, a robust taxonomy and indexing system, that covers all types of records, is necessary. This is vital to ensure patient safety by eliminating the possibility of wrong diagnoses or treatments. Further, it improves retention schedules and makes searching more efficient, saving time and money.

Increase data security

Ensure there is a detailed audit trail. Further, lock paper records in a room with restricted access. Records stored off-site should be held in certified, climate-controlled facilities. At the end of their life cycle, paper and electronic records should be securely destroyed. Access control systems and wireless locks are highly recommended to prevent unauthorized individuals from retrieving private information.

Solutions

Regardless if it is paper records or ePHI, covered entities should avoid a breach of security at all costs. However, it is necessary to understand that by adhering to HIPAA mandates, hospitals are still not doing enough. Additional security measures such as data encryption and staff training are key to ensure patient data is being governed adequately, and smart decisions are always taken.

Moreover, advanced physical security solutions are important to help improve the safety of medical information. With the proper integration of access control systems, biometric authentication, and wireless locks, healthcare institutions can be more efficient in their operations and take proactive steps in protecting their patients' health and data. These are some of the solutions that can be utilized by healthcare leaders to protect medical records.

ACCESS CONTROL

A first-class access control platform can help healthcare facilities protect sensitive medical information by only granting access to systems and documents to authorized people. The solutions include door devices, locks, alarms, cloud-based monitoring, and activation systems.

Medical record storage requires an access control system that allows access to only authorized people and ensures environmental isolation. Further, a sophisticated solution can ensure that only one person can enter a secured doorway for each authorized car read by using infrared sensor beams to detect tailgating.

Door locks could be remotely controlled and monitored from a centralized platform. This could be a valuable solution to detect doors that are propped or held open. Local door alarms and multi-zone annunciators could be activated in this scenario. Having access to cabinets and lockers where PHI is stored, without the use of keys, is also ideal.

In addition, wireless locks are an outstanding addition to hospitals, as they can enhance security and compliance. Wireless cabinet locks provide unparalleled access control, auditing, accountability, and loss /misuse of data prevention. Wireless readers can also be attached directly to glass doors and have a clean aesthetic.

Access control solutions can be programmed for specific days and hours, increasing accountability, reducing loss and liability, and improving the security of patient information.

BIOMETRICS

Biometric technology such as facial recognition and iris scanners are promising solutions for the reliable identification of patients and employees. Verifying people are who they say they are, guaranteeing caregivers are taking care of the right patient, and ensuring healthcare workers have access to only authorized information is vital to decrease costs and augment hospital security.

As healthcare organizations digitize patient records, biometrics can provide a fast, safe, upgraded, trustworthy, and effective way to grant access to spaces or information. Biometric authentication can decrease medical errors by distinguishing people dependent on their unique biometric characteristics.

More than ever, biometric technology is demanded by hospitals because of the high number of identification procedures performed in campus. Customary patient labeling is a vulnerable process that can lead to serious emergencies and even death. Improving the accuracy of patient authentication is, without a doubt, imperative.

In addition, it is important to keep an audit trail of each time a doctor or healthcare professional accesses a patient's record. Implementing biometric authentication not only guarantees that authorized medical personnel is getting access to the information, but it records who and when utilized this data. This is highly important to maintain the confidentiality of the information, avert medicinal extortion, and provide patients with the right treatment and medication.

Conclusion

Healthcare institutions are highly vulnerable targets of malicious data attacks. As they collect and maintain patients' sensitive information, it is necessary to take pertinent steps to protect the confidentiality, integrity, and availability of data at all times. Ensuring individuals' health information is safe from theft results in better health outcomes, smarter spending, and healthier patients.

Unfortunately, when a proactive approach is not taken, people might feel a lack of trust in the discretion and accuracy of the PHI management system, which can lead to the withholding of crucial health information and even life-threatening consequences. Providing patients with peace of mind will supply physicians with a more comprehensive context of every medical case and help them take better health decisions.

Irrespective of the type of records utilized in the hospital — paper, electronic, or both — abiding by HIPAA regulations is essential to protect patients' data. In addition, covered entities are required to follow The Privacy Rule, a mandate that calls for safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

Improving the security of medical records access, storage, release, and destruction can be achieved when the proper technologies are adopted. Access control, wireless locks, and first-class biometric authentication are solutions that can help health care facilities keep unauthorized persons away from confidential data, reduce medical errors, remain compliant, and avoid costly penalties and litigation.