Patient Privacy and Security of Electronic Medical Information

Summary

At A Glance

- The right to share your personal health information is a decision between you and your doctor.
- Radiologists ensure that your electronic medical information is secure.
- If you suspect someone of improperly accessing your health information, contact your doctor's office immediately.

As medical records are routinely digitized, cybersecurity is becoming a growing concern for the medical community. Doctors need access to your information to make important, quick decisions about your health care. However, you have the right to decide how and when they may access or share your information.

Radiologists have developed safeguards to prevent the misuse of confidential medical information. In fact, several radiology organizations have policies and standards in place to protect your records. As doctors develop new radiology technology, they are also improving the technology they use to secure your health information.

Doctors have a responsibility to help protect electronic medical information. They must document all use of your information, share their privacy and security policies with you, and report any loss of information. Contact your doctor's office immediately if you suspect someone is misusing your electronic health information.

What is electronic medical information security?

Most doctors and hospitals store images, test results, medications, allergies, and other data electronically. This allows them to view the data on computers. Doctors have a responsibility to first "do no harm." This responsibility extends to protecting patient information, privacy, and confidentiality. Patient information security outlines the steps doctors must take to guard your "protected health information" (PHI) from unauthorized access or breaches of privacy/confidentiality. Security also refers to maintaining the integrity of electronic medical information. It makes sure that those who need to can access and view the data, including images, to provide medical care. The federal government regulates the management of electronic media and PHI through the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Research and educational activities also must comply with PHI privacy and security requirements. Institutions must protect the privacy of individually identifiable health information, while allowing reasonable access by the researcher, educator, or trainee.

What is patient privacy?

Patient privacy is your right to decide when, how, and to what extent others may access your health information. Patient privacy maintains confidentiality and only shares PHI with those who need it to provide or improve medical care. If your PHI is used for research purposes, researchers must obtain your informed consent. This may include using your medical information anonymously to conduct research.

Why are security and patient privacy important

Electronic medical information security can affect the quality of patient care and patient rights. It can also impact the work practices and legal responsibilities of health care professionals. Doctors can make the best decisions for your care if they can access all relevant information in your medical history. If the doctor cannot access the data, this can delay important medical decisions and potentially harm your medical care. Any protection methods must maintain PHI privacy and confidentiality while still allowing authorized individuals to quickly and easily access it.

What are radiology professionals doing to safeguard medical images and patient information?

Radiologists are some of the first doctors to adopt digital medical imaging and electronic health information. They recognize the many benefits of these technologies and are working to eliminate risks. This work is done through organizations like the Radiological Society of North America (RSNA) (http://www.radiologyinfo.org/en/info/about-rsna) , American College of Radiology (ACR) (http://www.radiologyinfo.org/en/info/about-acr) ,and Society for Imaging Informatics in Medicine (SIIM) (https://siim.org/) . Together, these health care professionals, scientists, and industry/health policy leaders are developing standards and creating policies and procedures. They are also adapting technologies, educating other health care professionals, and trying new ways to safely and securely provide high quality patient care.

What are the responsibilities of the radiologist and patient?

As doctors, radiologists are responsible for protecting your information, privacy, and confidentiality. They are also responsible for securing patient data from loss or corruption. Doctors must document their privacy and security policies and share them with their patients. All staff must be trained in security policies. Policies must provide for computer system backups and maintenance, proper data storage and retention, system downtime procedures and recovery plans, incident reporting, and security issue resolutions. Failure to comply with state and federal Electronic Protected Health Information (ePHI) state and federal regulations could result in financial and/or criminal penalties.

As a patient, you have a right to talk to your doctor in confidence and to have any PHI protected. You are responsible for authorizing any release of PHI, except when required by law or in the event of an emergency.

What should you do if you think someone is inappropriately accessing your health information?

If you believe someone is misusing your PHI, contact your doctor's office immediately. Federal rules enforce HIPAA legislation. These rules outline steps that care providers and their associates must take to investigate, report, and address any unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the information. Care providers must provide all affected individuals with a description of the incident and outline what steps they should take to protect themselves. The care provider must also outline what steps they will take to recover the loss and avoid further breaches. This report must identify who you should contact with any questions about the breach.

How is medical information kept secure and private?

Physical, technical, and administrative safeguards protect the privacy, security, and integrity of recorded patient information. At the same time, these safeguards allow appropriate access to health providers for patient care. Physical safeguards include:

- Use of encrypted storage or devices
- Restricting physical access to authorized personnel only
- Preserving copies and conducting data backups
- Maintaining emergency contingency protocols
- Disposing outdated devices properly.

Technical safeguards include firewalls and secure transmission modes for communication such as virtual private networks (VPN) or secure sockets layer (SSL) and encryption techniques.

Administrative safeguards include:

- Requiring documentation of departmental security policies
- Training staff about security policies
- Conducting audit trails of all system logs by user identification and activity
- Enforcing policies for storage and retention of electronic data and backup of all systems
- Providing specific methods to report incidents and resolve security issues
- Documenting accountability, sanctions, and disciplinary actions for any violation of policies and procedures.
- Institutional review board (IRB) approval for any study involving PHI or human subjects

Electronic medical records (EMRs) must incorporate the following components within their system security policies and procedures:

- authorization
- authentication
- availability
- confidentiality
- data integrity
- nonrepudiation.

Authorization or access control methods include single sign-on databases or lists assigning users' rights and privileges to access certain resources. They also include automatic account logoff after a specified period of inactivity to prevent access by invalid users, frequent password changes and physical access controls (i.e. chip-based ID cards).

Authentication verifies a user's identity to a computer system using login passwords, digital certificates, smart cards, and biometrics. Authentication only verifies the identity of an individual. It does not define their access (authorization) rights.

The EMR must be continuously *available,* and system administrators must defend against various threats. They must provide fault tolerance for their systems (duplicated hardware, data archives, power, and networking systems). They must also keep servers physically safe and incorporate preventative virus and intrusion detection.

To maintain confidentiality, administrators must block unauthorized third parties from accessing and viewing medical data. Switched networks and data encryption can help prevent physical access.

It is essential to maintain data integrity when transferring information. This is done by verifying that the information arrived as it was sent and was not modified in any way. Methods to maintain data integrity include intrusion detection, such as tripwire and message digest, or hashing to detect any alteration of the data.

Nonrepudiation provides a record of the transaction. This ensures that a transferred message has been sent and received by the parties claiming to have sent and received it. Nonrepudiation methods include digital signatures and system audit logs of all user activity.

If you still have questions about how your medical information is secured and protected, please ask to your doctor and any facility where you receive medical tests or procedures.

Disclaimer

This information is copied from the RadiologyInfo Web site (http://www.radiologyinfo.org) which is dedicated to providing the highest quality information. To ensure that, each section is reviewed by a physician with expertise in the area presented. All information contained in the Web site is further reviewed by an ACR (American College of Radiology) - RSNA (Radiological Society of North America) committee, comprising physicians with expertise in several radiologic areas.

However, it is not possible to assure that this Web site contains complete, up-to-date information on any particular subject. Therefore, ACR and RSNA make no representations or warranties about the suitability of this information for use for any particular purpose. All information is provided "as is" without express or implied warranty.

Please visit the RadiologyInfo Web site at **http://www.radiologyinfo.org** to view or download the latest information.

Note: Images may be shown for illustrative purposes. Do not attempt to draw conclusions or make diagnoses by comparing these images to other medical images, particularly your own. Only qualified physicians should interpret images; the radiologist is the physician expert trained in medical imaging.

Copyright