RadiologyInfo.org
For patients

Medical Information Privacy

Summary

- You have the right to decide whether to share your confidential medical information.
- Healthcare groups must keep your electronic medical information secure.
- If you suspect someone has improperly accessed your information, contact your healthcare provider immediately.

Your medical information is stored in an electronic format. There are many rules and regulations — including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) — that exist to protect your medical information.

Doctors need to access your information to make important, quick decisions about your medical care. However, you have the right to decide whether they may access your information or share it with others.

Healthcare groups have developed safeguards to protect your medical information. As technology improves, healthcare groups are also improving the ways they secure your information.

Doctors must help protect your information. They must document all use of your information, share their privacy/security policies with you, and report any data loss or breach. Contact your doctor's office immediately if you suspect someone is misusing your information.

What is electronic medical information security?

Healthcare groups store images, test results, physician notes, medications, allergies, and other data electronically. Doctors have a responsibility to first "do no harm." This responsibility includes protecting your information, privacy, and confidentiality. Patient information security outlines the steps healthcare workers must take to guard your "protected health information" (PHI). Security also refers to maintaining the integrity of electronic medical information. It makes sure that those who need to can access your information to provide medical care. The federal government regulates the management of electronic records and your protected health information.

Research and educational activities also must comply with privacy and security requirements. Institutions must protect the privacy of your health information, while allowing reasonable access by researchers, educators, or trainees.

What is patient privacy?

Patient privacy is your right to decide when, how, and to what extent others may access your protected health information (PHI). Patient privacy maintains confidentiality and only shares your information with those who need it to provide medical care. If your information is used for research purposes, researchers must request approval from their local institution research board (IRB). This may include making your information anonymous before using it 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 healthcare professionals. Doctors can make the best decisions for your care if they can access your complete medical history. Lack of access can delay important decisions and harm your medical care. Protection methods must keep your information private and confidential while still allowing authorized individuals to quickly 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 groups like the Radiological Society of North America (RSNA) (https://www.radiologyinfo.org/en/info/about-rsna) , American College of Radiology (ACR) (https://www.radiologyinfo.org/en/info/about-acr) ,and Society for Imaging Informatics in Medicine (SIIM) (https://siim.org/) . Together, these healthcare leaders are developing standards and creating policies to ensure your radiology information remains secure but can be shared easily so you can receive high-quality patient care.

What are the responsibilities of the radiologist and patient?

Radiologists work with IT professionals to protect your information, privacy, confidentiality, and integrity. Doctors must document their privacy and security policies and share them with you. All staff must be trained in security policies. These policies must provide for computer system backups and maintenance, proper data storage, system failure and recovery plans, incident reporting, and security issue resolutions. Failure to comply with state and federal Electronic Protected Health Information (ePHI) regulations may result in financial and/or criminal penalties.

As a patient, you have a right to talk to your doctor in confidence and have your information protected. You choose whether to release it, 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 health information, contact your doctor's office immediately. Federal rules outline steps that care providers must take to investigate, report, and address any unauthorized use of your healthcare information that compromises your privacy. If your information has been exposed, your care provider must provide you with a description of the incident and outline what steps you should take to protect yourself. The care provider must also tell you what they will do to recover the loss and avoid further breaches. This report must identify whom you should contact if you have any questions about the breach.

How is medical information kept secure and private?

Many different safeguards protect the privacy, security, and integrity of your information. At the same time, these safeguards give your doctors access so they can provide you with medical care. Physical safeguards include:

- Using encrypted storage or devices
- Restricting physical access to authorized personnel only
- Preserving copies and conducting data backups
- Maintaining emergency protocols
- Properly disposing outdated devices

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

Administrative safeguards include:

- Documenting department security policies
- Training staff about security policies

- Conducting audit trails of all system logs by user identification and activity
- Enforcing policies for storing electronic data and system backups
- Providing specific methods to report incidents and resolve security issues
- Documenting accountability, sanctions, and disciplinary actions for any violation of policies and procedures
- IRB approval for any study involving protected healthcare information or human subjects

Electronic medical records (EMRs) must include the following in their security policies and procedures:

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

Authorization/access control methods include single sign-on databases or lists assigning user access rights and privileges. They also include automatic account logoff after a certain period of inactivity. This helps prevent access by invalid users. Frequent password changes and physical access controls (such as chip-based ID cards) may also be used.

Authentication verifies your identity to a computer system using login passwords, digital certificates, smart cards biometrics, and multi-factor approaches. Authentication only verifies your identity. It does not define what resources you can access.

The EMR must be continuously *available*, and system administrators must defend against various threats. They must provide back-up for their systems (duplicated hardware, data archives, power, and networking systems). They must also keep computer servers physically safe and defend against computer viruses and hacking.

Confidentiality means that all unauthorized access of your medical data is blocked.

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. IT personnel use a variety of methods to maintain data integrity and detect any attempts to modify the data, such as digital signatures.

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. Methods include digital signatures and system logs of all user activity.

If you still have questions about how your private information is protected, please talk with your healthcare provider.

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