Patient Privacy and Security of Electronic Medical Information

Summary

At A Glance

- Patients have the right to determine how their health information is shared.
- Radiologists and other physicians are working to ensure that electronic medical information is properly protected.
- Patients who believe their health information has been misused should contact their physician or physician's administrative staff immediately.

Interest is increasing in the security of electronic medical information, or patient health information, that is digitally stored. Sometimes this information needs to be accessed for physicians to be able to make the best decisions about patient care. Patients have the right to determine how and when their health information is shared.

Radiologists are at the forefront of trying to protect confidential electronic medical information from being misused. Several radiology organizations are currently working to develop policies and standards related to the protection of medical information, as well as improving technology to ensure this information is safeguarded.

Physicians have responsibilities when it comes to protecting electronic medical information. Radiologists and other physicians must document all use of patient information, share privacy and security policies with their patients, and report any loss of information. Patients should contact their physician or physician's administrative staff immediately if they suspect misuse of their electronic health information.

For more detailed information on patient privacy and security of electronic medical information, continue reading.

What is security of electronic medical information?

Radiologic images, lab test results, medications, allergies, and other clinical information are increasingly being stored and viewed on computers. The responsibility that physicians have to protect their patients from harm extends to protecting patient information, privacy and confidentiality. Patient information security includes the steps healthcare providers must take to guard patients' "protected health information"
commonly referred to as PHI, from unauthorized access or breaches of privacy or confidentiality. Security also refers to maintaining the integrity of electronic medical information, and ensuring availability to those who need access and are authorized to view such clinical data, including images, for the purposes of patient care. The federal government requires the secure handling of electronic media and PHI with standards put forth in the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Research and educational activities are not exempt from the privacy and security requirements for PHI. Institutional policies protect the privacy of individually identifiable health information, while allowing reasonable access to medical information by the researcher, educator or trainee.

What is patient privacy?

Patient privacy refers to the right of patients to determine when, how and to what extent their health information is shared with others. It involves maintaining confidentiality and sharing identifying data, known as protected health information (PHI), only with healthcare providers and related professionals who need it in order to care for the patient.

Why are security and patient privacy important?

The secure management of electronic medical information may have an impact on the quality of patient care, patient rights, and healthcare professionals and their current work practices and legal responsibilities. Doctors can make the best decisions about medical care if they have access to all relevant information in their patients' medical histories. Inability to access data may delay clinical management decisions and could adversely impact patient care. Patients have the right to maintain privacy and confidentiality of their PHI. Methods of protection must include considerations for timely and easy access to clinical information by the authorized healthcare professionals.

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

Radiologists have been at the forefront of adopting digital medical imaging and electronic health information. They have recognized the many benefits and are working to eliminate risks. Through organizations like the American College of Radiology (ACR), Radiological Society of North America (RSNA) and Society for Imaging Informatics in Medicine (SIIM), healthcare professionals have worked with scientists, industry and health policy leaders to develop standards, create policies and procedures, adapt technologies, educate other physicians and health professionals, and experiment with promising new methodologies to provide high quality medical care to patients in a safe and secure environment.

What are the responsibilities of the radiologist and patient?
Radiologists are physicians and as such are responsible for protecting patient information, privacy and confidentiality, and securing patient data from loss or corruption. Physicians must document their privacy and security policies and communicate this information to their patients. All staff must be trained in security policies. There must be provisions for backup of all computer systems, proper storage and retention of all electronic data, maintenance of computers, system downtime procedures and recovery plans, incident reporting and resolution of security issues. Failure to comply with state and federal Electronic Protected Health Information (ePHI) state and federal regulations could result in financial and/or criminal penalties.

It is the patient's right to communicate with healthcare providers in confidence and to have any PHI protected. The patient is responsible for authorizing any release of PHI, except when required by law.

What should you do if you think your health information has been accessed inappropriately?

If you believe that your PHI has been accessed or used inappropriately, report your concerns to your physician or administrative staff of the physician office or hospital immediately. Federal rules created to enforce the HIPAA legislation specify steps that care providers and their business 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 are required to provide all individuals affected by any such breaches with a description of the incident, including information about what steps they should take to protect themselves and what steps the care provider will take to recover the loss and avoid further breaches. The report must include contact information of an individual assigned to answer questions from individuals affected by the breach.

How is medical information kept secure and private?

Physical, technical and administrative safeguards are in place to protect the privacy, security and integrity of recorded patient information, while at the same time allowing appropriate access to health providers for the care and management of patients. Physical safeguards include device isolation, allowing direct physical access only to authorized personnel; data backup and maintaining copies, emergency contingency protocols, and proper device disposal. 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 requirements for documenting departmental security policies, training staff about these policies, maintaining 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, adhering to specific methods for incident reporting and resolution of security issues, and clearly documenting accountability, sanctions and disciplinary actions for violation of policies and procedures.

Electronic medical records (EMR) must incorporate the following components within their system
security policies and procedures: authorization, authentication, availability, confidentiality, data integrity and nonrepudiation. The methods available for authorization or access controls include single sign-on databases or lists assigning rights and privileges of users to access certain resources, automatic account logoff after a specified period of inactivity to prevent access by invalid users, and physical access controls.

Authentication is the process of verifying the identity of a user to a computer system and can be accomplished 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.

EMRs must be continuously available and system administrators must defend against various threats providing fault tolerance for their systems (duplicated hardware, data archives, power and networking systems), provide physical safety of servers, and incorporate preventative virus and intrusion detection.

To maintain confidentiality, unauthorized third parties must be prevented from accessing and viewing medical data. This can be accomplished by preventing physical access to the data using such technologies as switched networks, and by encrypting the data so that even if it is physically obtained, it cannot be read.

It is essential to maintain data integrity when transferring information 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 ensures that a transferred message has been sent and received by the parties claiming to have sent and received the message, providing a record of the transaction. Digital signatures and system audit logs of all user activity are methods of nonrepudiation.

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

This material is copyrighted by either the Radiological Society of North America (RSNA), 820 Jorie Boulevard, Oak Brook, IL 60523-2251 or the American College of Radiology (ACR), 1891 Preston White Drive, Reston, VA 20191-4397. Commercial reproduction or multiple distribution by any traditional or electronically based reproduction/publication method is prohibited.