Procedia of Engineering and Life Science Vol. 6 2024
The 3rd International Scientific Meeting on Health Information Management (3rd ISMoHIM)
Asosiasi Perguruan Tinggi Rekam Medis dan Manajemen Informasi Kesehatan Indonesia - Universitas Muhammadiyah Sidoarjo

Security of Electronic Medical Information and Patient Privacy

Katherine P. Andriole[1*], Sings[2]
[1,2]Indian Institute of Technology Delhi
*Correspondence author: katherineandriole@gmail.com

Abstract. Tujuan penelitian ini adalah untuk mengeksplorasi implementasi keamanan sistem Rekam Medis The responsibility that physicians have to protect their patients from harm extends to protecting the privacy and confidentiality of patient health information including that contained within radiological images. The intent of HIPAA and subsequent HIPAA Privacy and Security Rules is to keep patients' private information confidential while allowing providers access to and maintaining the integrity ofrelevant information needed to provide care. Failure to comply with electronic protected health information (ePHI) regulations could result in financial or criminal penalties or both. Protected health information refers to anything that can reasonably be used to identify a patient (eg, name, age, date of birth, social security number, radiology examination accession number). The basic tools and techniques used to maintain medical information security and patient privacy described in this article include physical safeguards such as computer device isolation and data backup, technical safeguards such as firewalls and secure transmission modes, and administrative safeguards including documentation of security policies, training of staff, and audit tracking through system logs. Other important concepts related to privacy and security are explained, including user authentication, authorization, availability, confidentiality, data integrity, and nonrepudiation. Patient privacy and security of medical information are critical elements in today's electronic health care environment. Radiology has led the way in adopting digital systems to make possible the availability of medical information anywhere anytime, and in identifying and working to eliminate any risks to patients.
Keywords: Medical Record Security, HIPAA Compliance, ePHI, Patient Privacy, Radiology

I.BACKGROUND

HIPAA was enacted in 1996 to serve 2 main purposes: (1) to protect health insurance coverage for workers and their families when they change or lose their jobs (Title I); and (2) to require the establishment ofnational standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers (Title II) [1,2]. The intent was to keep patients' private information confidential while allowing providers and health insurance plans to access information needed to provide care. The standards were meant to improve the efficiency and effectiveness of the nation's health care system by encouraging widespread use of electronic data interchange in the US health care system. The Administrative Simplification Statute and Rules (Title II of HIPAA) further address the security and privacy of health data. The US Department of Health and Human Services published a final Privacy Rule in December 2000 (modified in August 2002) that set standards for the protection of individually identifiable health information. It also published a Security Rule in February 2003 that set standards for protecting the confidentiality, integrity, and availability of electronic protected health information (PHI) [1]. Compliance with the Privacy Rule and Security Rule has been required for all health plans since 2004 and 2006, respectively. Failure to comply with state and federal regulations related to electronic PHI (ePHI) could result in financial or criminal penalties or both. This law requires that loss or theft of medical records be reported; failure to comply subjects the perpetrator to financial and criminal penalties. A person found to have violated this law may be fined up to $250,000 and imprisoned for up to 10 years. The underlying principle ofthis law is that patients should have basic rights to: (1) access their own medical records; (2) maintain confidentiality over their medical records; and (3) know who has accessed their records.

Radiological images and other clinical information (eg, lab test results, medications, allergies, medical history) are increasingly being acquired, transmitted, and stored digitally and viewed on computers for primary interpre- tation and review. Because digital or electronic health information includes radiological images as well as nonimage data, HIPAA rules apply to image and infor- mation management systems such as a PACS, a hospital information system (HIS), a radiology information system (RIS), a computerized physician order entry (CPOE) system, and a speech recognition report generation system used by radiologists in their daily practice. The ways and means of making this information available to various kinds of providers, for the benefit of the patient, are rapidly expanding. The Health IT for Economic and Clinical Health (HITECH) Act is intended to foster interoperable IT systems so that providers are appropriately aware of information relevant to the decisions they make, and high-quality nonredundant care can be pro- vided. Health information exchanges (HIEs) and personal health records are new and exciting paradigms for improving availability of health information. However, However, the increasing number of places in which digital information resides provides more opportunity for inappro- priate exposure. For patients to accept these emerging mechanisms as a means to enhance their care, they must trust that the appropriate safeguards are in

place to maintain their privacy and confidentiality. It behooves the radiology profession to proactively provide such assurance to patients. This article discusses the definition and importance of and current practices related to patient privacy, the security of electronic medical information, and the safeguarding of medical images. The responsibilities of the radiologist are summarized, and the basic techniques used to keep medical information (images and relevant nonimage data) secure and private are covered. A glossary of common terms and references for other resource documents is provided. The radiologist are summarized, and the basic techniques used to keep medical information (images and relevant nonimage data) secure and private are covered. A glos- sary of common terms and references for other resource documents is provided.

II.PHI

The responsibility that physicians have to protect their patients from harm extends to protecting the privacy and confidentiality of patient health information. Although privacy and confidentiality are often used interchangibly, patient privacy specifically refers to the right of patients to determine when, how, and to what extent their health information is shared with others. The concept encompasses maintaining confidentiality while sharing identifying data or PHI with only those health care providers and related professionals who need it in the course of caring for a patient.Anything that can reasonably be used to identify a patient is considered PHI, including obvious things such as name, age, date of birth, social security number, telephone numbers, license numbers, postal address, all date elements (except year), e-mail addresses, web addresses, Internet provider addresses, account numbers, and health insurance identification numbers. In addition, this information includes internal identifiers such as medical record number, radiology accession number, date of examination, or any other identification numbers. A DICOM medical image is full of PHI and should not be used outside a clinical setting without full anonymization. Biometric identifiers such as fingerprints, voice or retinal scans, fullface photos, and other comparable images are also considered PHI.

Information security includes the measures that health care providers must take to protect patients' PHI from unauthorized access or breach. In addition, security involves maintaining the integrity of electronic medical information and ensuring availability to those authorized individuals who need access to clinical data, including images, for the purposes of patient care. Research and educational activities are not exempt from the privacy and security requirements for PHI. Institutional policies must protect individually identifiable health information while allowing reasonable access to medical information by the researcher, educator, or trainee

III.SECURITY AND PRIVACY SAFEGUARDS

The basic techniques involved in maintaining medical information security and patient privacy include physical, technical, and administrative safeguards. Physical safeguards include device isolation; allowing direct physical access to authorized personnel only; methods for backing up data 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 or a Secure Sockets Layer, and encryption techniques. Administrative safeguards include re- quirements for documenting departmental security policies; training staffon these policies; maintaining audit trails ofall system logs by user identification, activity, and date and time ofaccess; 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 Audit trails and tools can be employed in various ways to enhance security and privacy. To the extent that is practical, audit trails should be granular, with information ranging from who logged into a system at any given time, to what they looked at, added, changed, or deleted. System administrators and security personnel should design routine audits, random spot-check audits, in addition to providing custom audits and investigations when analyzing a potential breach or other problem. All users of a system should be well educated as to the audit processes in place. This approach provides clarity as to what behaviors are expected and emphasizes commitment to protecting patients' privacy. At times, well-meaning individuals may not fully appreciate what constitutes privacy; providing knowledge ofwhat is to be audited may help reinforce what is meant by PHI and privacy. Publicly relating examples of how audit trails have been used to enforce the protection of PHI can be an extremely effective tool in promulgating good practices.

IV.TOOLS TO MAINTAIN SECURITY AND PRIVACY

PACS, HIS-RIS, CPOE, other image management systems, and medical IT solutions must incorporate the following

components within their system security policies and procedures: authentication, authorization, availability, confidentiality, data integrity, and non-repudiation. Authentication is the process of verifying the identity of a user by a computer system and can be accomplished using log-ins/ usernames and passwords, digital certificates, smartcards, and biometrics. Authen- tication only verifies the identity ofan individual; it does not define their access (authorization) rights. Authori- zation defines what the user can do once authenticated. Methods available for authorization or access controls include single sign-on (SSO) databases or lists assigning rights and privileges of users to access certain resources; automatic account logoff (timeouts) after a specified period of inactivity to prevent access by invalid users; and physical access controls. Vital clinical systems (eg, electronic medical records, PACS, CPOE) must be continuously accessible or available to avoid compromising clinical care, and system administrators must defend against various threats, pro- vide fault tolerance for their systems (eg, redundant 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 level of prevention can be accomplished by blocking ac- cess to the data using such technologies as switched networks, and by encrypting the data so that even if it is obtained, it cannot be read by unauthorized users.

Portable media such as flash drives, laptops, and online storage services such as Dropbox are major potential risks for PHI loss. Removable USB drives in particular present a hazard and should be avoided, as they can store a vast amount of clinical information and can be easily lost. Refer to your organization's policy on removable media. Encrypting a drive can provide a basic level ofprotection, but if the drive is lost, it still must be reported. Maintaining data integrity is essential when transferring information and can be accomplished by verifying that the information arrived as it was sent and was not modified in any way. Methods of maintaining data integrity include intrusion detection such as Tripwire (security and regulatory compliance software), and message digest or hashing, also known as digital fingerprints or checksums, 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 ofall user activity are methods of nonrepudiation.

V.POLICY

Physicians are responsible for protecting patient information, ensuring patient 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 members must be trained in security policies, and every clinical professional is responsible. Provisions must be made 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. The Department of Health and Human Services Office for Civil Rights enforces the HIPAA rules [1,2].

Patients' rights include the ability to communicate with health care providers in confidence and to have any and all PHI protected. The patient is responsible for authorizing any release of PHI, except when release is required by law. Federal rules created to enforce the HIPAA legislation specify the 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 of information or the privacy of the patient. Should a breach occur, care providers are required to present all. Patient privacy and security of electronic medical information are critical elements in today's electronic health care environment. Radiology has led the way in establishing the availability of information anytime and anywhere through the pervasive deployment of digital systems. Although this principle greatly enhances patient care by making information easily available, it opens the door to the inappropriate exposure of private information. No longer is there a single copy of information on paper or film in one location, often under the direct observation of personnel. Information can be seen by multiple users in multiple locations simultaneously. Fortunately, practical means are available to permit this access only when appropriate. Radiologists must understand their responsibilities around electronic medical information, know their patients' rights, and educate themselves in the techniques used to keep medical information private and secure.

VI.GLOSSARY

Anonymization: the process of removing all indentifiers or codes that directly or indirectly link a sample or data to a specific, identifiable person. Audit: an information system log that keeps a record of all user activity by user identification and time and date of access. Authentication: the process of verifying the identity of a person/user by a computer system, or

assuring that a computer program is a trusted one.Authorization: controls that restrict system access to authorized users only; access controls assign user rights and privileges to resources via single sign-on databases; auto logoff procedures prevent someone other than the valid user from continuing a computer session; physical access controls are used for critical computers to prevent console-based malicious attacks, power interruptions, or other threats to security of the systems. Biometrics: requires a user to provide a fingerprint, voice sample, retinal scan, or the like, which is compared to a stored record ofthe user's biological signature before the user can gain access to the computer. Data integrity: complete data; in transfer, data that arrived exactly as they were sent unmodified. Deidentification: the process ofmodifying identifiers within medical

ACKNOWLEDGMENT

Thanks to 3rd ISMOHIM organized by APTIRMIKI in collaboration with PORMIKI so that this article can be published.

REFERENCES

[1]US Department of Health and Human Services. Health information privacy. Available at: http://www.hhs.gov/ocr/ privacy. Accessed August 8, 2023.

[2]CMS. HIPAA—general information. Available at: http://www.cms.hhs. gov/ HIPAAGenInfo. Updated April 2, 2013.Accessed August 28, 2014.

[3]ACR/RSNA. Glossary of terms. Available at http://www.radiologyinfo. org/en/ glossary/glossary1.cfm?pid¼1. Accessed August 8, 2024.

[4]Medical Imaging and Technology Alliance. Security and privacy. Available at: http:// www.medicalimaging.org/policy-and- positions/joint-security-and-privacy- committee-2/. Accessed August 28, 2014.

[5]Dwyer SJ, Reiner BI, Siegel EL. Security issues in the digital medical enterprise. 2nd ed. Society for Computer Applications in Radiology; Leesburg, VA 2024.

[6]Integrating the Healthcare Enterprise. Cookbook: preparingthe IHEprofilesecurity section (risk management in healthcare IT). Available at: http://www.ihe.net/Technical_ Framework/upload/IHE_ITI_Whitepaper_ Security_Cookbook_2008-11-10.pdf. Accessed August 8, 2024.

[7]Integrating the Healthcare Enterprise. IHE IT infrastructure white paper on health information exchange (HIE) security and privacy through IHE profiles. Version 2.0. Available at: http://www.ihe.net/Technical_ Framework/upload/IHE_ITI_Whitepaper_ Security_and_Privacy_of_HIE_ 2008-08-22-2.pdf. Accessed August 8, 2024.

[8]Andriole KP, Khorasani R. Patient privacy and security of electronic medical information for radiologists: the basics. J Am Coll Radiol 2020;7:397-9.

[9]Branstetter B IV. Practical imaging informatics: foundations and appli- cations for PACS professionals. New York, NY: Springer; 2019.