The American College of Radiology, with more than 30,000 members, is the principal organization of radiologists, radiation oncologists, and clinical medical physicists in the United States. The College is a nonprofit professional society whose primary purposes are to advance the science of radiology, improve radiologic services to the patient, study the socioeconomic aspects of the practice of radiology, and encourage continuing education for radiologists, radiation oncologists, medical physicists, and persons practicing in allied professional fields.

The American College of Radiology will periodically define new practice parameters and technical standards for radiologic practice to help advance the science of radiology and to improve the quality of service to patients throughout the United States. Existing practice parameters and technical standards will be reviewed for revision or renewal, as appropriate, on their fifth anniversary or sooner, if indicated.

Each practice parameter and technical standard, representing a policy statement by the College, has undergone a thorough consensus process in which it has been subjected to extensive review and approval. The practice parameters and technical standards recognize that the safe and effective use of diagnostic and therapeutic radiology requires specific training, skills, and techniques, as described in each document. Reproduction or modification of the published practice parameter and technical standard by those entities not providing these services is not authorized.

Revised 2014 (Resolution 37)*

ACR–AAPM–SIIM PRACTICE PARAMETER FOR ELECTRONIC MEDICAL INFORMATION PRIVACY AND SECURITY

PREAMBLE

This document is an educational tool designed to assist practitioners in providing appropriate radiologic care for patients. Practice Parameters and Technical Standards are not inflexible rules or requirements of practice and are not intended, nor should they be used, to establish a legal standard of care[1]. For these reasons and those set forth below, the American College of Radiology and our collaborating medical specialty societies caution against the use of these documents in litigation in which the clinical decisions of a practitioner are called into question.

The ultimate judgment regarding the propriety of any specific procedure or course of action must be made by the practitioner in light of all the circumstances presented. Thus, an approach that differs from the guidance in this document, standing alone, does not necessarily imply that the approach was below the standard of care. To the contrary, a conscientious practitioner may responsibly adopt a course of action different from that set forth in this document when, in the reasonable judgment of the practitioner, such course of action is indicated by the condition of the patient, limitations of available resources, or advances in knowledge or technology subsequent to publication of this document. However, a practitioner who employs an approach substantially different from the guidance in this document is advised to document in the patient record information sufficient to explain the approach taken.

The practice of medicine involves not only the science, but also the art of dealing with the prevention, diagnosis, alleviation, and treatment of disease. The variety and complexity of human conditions make it impossible to always reach the most appropriate diagnosis or to predict with certainty a particular response to treatment. Therefore, it should be recognized that adherence to the guidance in this document will not assure an accurate diagnosis or a successful outcome. All that should be expected is that the practitioner will follow a reasonable course of action based on current knowledge, available resources, and the needs of the patient to deliver effective and safe medical care. The sole purpose of this document is to assist practitioners in achieving this objective.

[1] Iowa Medical Society and Iowa Society of Anesthesiologists v. Iowa Board of Nursing, ___ N.W.2d ___ (Iowa 2013) Iowa Supreme Court refuses to find that the *ACR Technical Standard for Management of the Use of Radiation in Fluoroscopic Procedures* (Revised 2008) sets a national standard for who may perform fluoroscopic procedures in light of the standard's stated purpose that ACR standards are educational tools and not intended to establish a legal standard of care. See also, Stanley v. McCarver, 63 P.3d 1076 (Ariz. App. 2003) where in a concurring opinion the Court stated that "published standards or guidelines of specialty medical organizations are useful in determining the duty owed or the standard of care applicable in a given situation" even though ACR standards themselves do not establish the standard of care.

I. INTRODUCTION

The practice parameter for electronic medical information privacy and security was revised collaboratively by the American College of Radiology (ACR), the American Association of Physicists in Medicine (AAPM), and the Society for Imaging Informatics in Medicine (SIIM).

Medical imaging and related patient information are increasingly being managed via digital acquisition, transmission, storage, display, and interpretation. The secure management of these data may have an impact on the quality of patient care, on patient's rights, and on health care professionals and their current practices and legal responsibilities.

The responsibility that physicians have to protect their patients from harm extends to protecting patient privacy and patient information. Physicians should carefully document their privacy and security policies and communicate this information to their patients. The responsibility to protect patient privacy and to secure patient data from loss or corruption is a critical requirement for the provision of medical care. Additionally, failing to comply with Electronic Protected Health Information (ePHI) state or federal regulations could result in financial and/or criminal penalties as described in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequently strengthened by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 regarding civil and criminal enforcement of HIPAA rules.

The goal of this practice parameter is to recommend actions for the protection, privacy, security, and integrity of recorded patient information while allowing appropriate access for care and management of patients. Policy and procedure recommendations (sections II and III) are provided, and the tools available to ensure privacy and security are described in section IV. Use cases for specific situations (eg, research use of PHI) are given in Appendix A of this document to elucidate risks and costs for data and applications, as well as the specific legal and practice requirements and the tools used to ensure compliance. Research, educational, and marketing uses of patient information requirements are outlined in section V. The practice parameter concludes in section VI with a list of medical/legal entities and government agencies that may have more restrictive rules and considerations for security and privacy.

An additional resource is a compilation of authoritative report and resource links for a broad scope of cybersecurity issues, which is available from the Congressional Research Service.[2]

II. POLICY STATEMENTS

A. Policies should include the following topics:

1. Security awareness training for the staff in the department
2. Security issues for electronic personal health information
3. Designation of responsibility for:
   a. Providing security awareness training
   b. Developing procedures in support of proper security measures
   c. Providing appropriate computer training
   d. Assuring that policies and procedures are followed
   e. Resolving security problems
4. Initial and subsequent periodic assessment and risk analysis of all processes related to the handling of ePHI; the findings from these audits should be used to guide the development of future policies and procedures.
5. Provision of backup for all systems
6. Proper storage and retention for all electronic data
7. System downtime and recovery plans for unexpected computer downtimes

[2] The United States Congress has been actively involved with cybersecurity issues since 2001. A document with links to selected authoritative reports and resources on cybersecurity law and legislation is periodically updated. As of November, 2013, a report dated October 25, 2013, is available at http://www.fas.org/sgp/crs/misc/R42507.pdf.

8. Maintenance of a support manual and how-to-guide for computer systems and information
9. Business associate contracts and trust agreements; all current vendors and other entities that have or need access to ePHI must have business associate agreements as required by HIPAA; these agreements should be obtained through the normal purchasing process.

III. PROCEDURES

A. Administrative Safeguards

1. Perform an audit and assessment of existing practices.
   a. The audit will address the following:
      - Physical safeguards
      - Technical safeguards
      - Administrative safeguards
   b. Share assessment findings and risk analysis with appropriate institutional departments or service providers.
2. Security awareness and operational training
   a. Use radiology specialty oriented training tools.
      - Provide HIPAA security training for all personnel.
      - Inform staff of policies specific to radiology.
   b. Maintain individual documentation of staff training.
   c. Conduct annual security training.
   d. Provide universal training for the following:
      - Operational computer training of all personnel on systems needed to perform their jobs
      - Emergency operational procedures for computer downtime
      - Emergency operational procedures to be used during a disaster
      - Computer recovery procedures
   e. Require all personnel to sign a responsibility statement for information security and confidentiality. This security applies to all information in the department, such as patient data, research, and financial information.
3. Incident reporting and resolution of security issues
   a. Reporting of incidents or vulnerabilities to a responsible individual
   b. Implementing corrective action for minor problems
   c. Initiating corrective action with the involvement of the appropriate institutional departments or service providers
   d. Documentation of incidents and actions
4. Accountability and sanctions
   a. Manager's responsibilities for overseeing the security plan within his/her areas of responsibility
   b. Personnel responsibility for following the policies and procedures that have been established
   c. Sanctions and disciplinary actions for violation of policies and procedures
5. Access controls
   a. All systems maintained by the facility or contracted entity must be subject to the facility's policies and procedures.
   b. Approval of access to all systems is the responsibility of the local administration.
   c. Parties responsible for creating, changing, and disabling accounts must be identified and given authority by administration.
   d. Obtaining access privileges requires person's or entity's signature on a responsibility and confidentiality statement.

e. Require user identification sign-on code:
   - Limits access to information/systems according to "need to know" as determined by staff member's manager
   - Allows for tracking of user activity

f. Require separate user defined password or biometric identification.
g. Minimum requirement/best practice for password considerations include consideration of:
   - Syntax
   - Expiration cycle
   - Reuse rules

h. Ensure authentication for login process.
i. Define who monitors all vendor access to radiology equipment and interfaces.
j. Require secure remote application access with a virtual private network (VPN) or secure sockets layer (SSL).

6. Activity review
   a. Define a process to determine who has accessed ePHI.
   b. Define who will review firewall "real-time logs" in a timely and reactive manner to determine if inappropriate activity is taking place.
   c. Define who within radiology will notify various system entities at the time of employee termination and/or status change.
   d. Define the frequency and level of detail for monitoring and reporting.

B. Physical Safeguards

1. Develop a device and hardware disposal and electronic media reuse policy.
   a. Develop a policy to address data contained on storage devices/media from obsolete computers.
   b. Define how computers that are being repaired and/or stored will be handled.
2. Document the process of backing up data and maintaining backup copies of ePHI.
3. Develop an emergency contingency protocol that includes:
   a. Procedures to address major hardware and software recovery following system downtime
   b. A system disaster recovery plan
4. Develop a policy for retention and storage of electronic data.
5. Ensure that workstations and remote printers are physically safeguarded to prevent unauthorized access to data.
6. Define safeguards for laptop computer/tablet/smartphone/flash drive use when connecting to institutional network.

C. Technical Safeguards

1. Firewalls and secure transmission modes for staff communication
   a. Establish secure firewalls for systems that may be vulnerable to security breaches.
   b. Establish a VPN or SSL to allow secure transmission through the firewall.
   c. Ensure the security of e-mail communication.
      - If e-mail is provided, make sure it is encrypted or otherwise secure for communication between staff and customers outside of the VPN or SSL.
      - Ensure that communication directly with patients over the Internet is authorized by the patient and that appropriate security precautions are in place.

IV. SECURITY AND PRIVACY TOOLS USED

The key provisions for handling PHI on health care systems are outlined in 21CFR11; Subpart B details controls for medical records, and Subpart C details requirements for electronic signatures. The following tools can be used to address the privacy and security issues of Subpart B in an electronic medical information system, including anonymization (elimination of PHI from the electronic files), authentication (digital signing, biometrics, etc),

authorization (eg, access controls), auditing (ensuring compliance to HIPAA and other regulations), application availability (fault tolerance and denial of service [DOS] resistance), confidentiality (including encryption when required), data availability, data integrity, and nonrepudiation (digital signing). This section describes these tools. Some tools can be used in more than one role.

A. Anonymization

Removing patient information is a cornerstone of performing research on clinical information. HIPAA/HITECH requires that only those involved in direct patient care should have access to the patient identity or identifying characteristics. A distinction is made between 2 levels:

1. De-identification: Is defined under HIPAA as being one of 2 methods: the Safe Harbor method details 18 features that must be removed, and the Statistical Method requires a statistician to document that there is a small likelihood that a given record could be traced back to the patient.
2. Anonymization: Is the process by which medical data are made unlinkable to the original patient.

De-identified data are still coded to an alias; an agent in possession of the table could link a record back to the real patient. Fully anonymized data is not linkable to the original patient. It is important to realize that not all PHI is always confined to the "digital object" metadata and headers. It is also possible that some PHI resides in the pixel data of the image. At least 2 open source applications are available to perform both tag and raster anonymization: the RSNA Clinical Trials Processor (http://mircwiki.rsna.org/index.php?title=CTP-The_RSNA_Clinical_Trial_Processor) and the DICOM Cleaner (http://www.dclunie.com/pixelmed/software/webstart/DicomCleanerUsage.html).

Note: Anonymization of "image pixel data" is ultimately the responsibility of the anonymization site even if "applications" are used to anonymize the data. Anonymization of data burned into the image itself (ie, image pixel data) is notoriously difficult. Review of all such images for accurate anonymization is strongly recommended when such images are batch anonymized by computer application.

B. Authentication

Authentication is the process of verifying the identity of a user to a computer system. This verification can be accomplished using a variety of approaches including passwords, digital certificates, smart cards, and biometrics. Authentication only verifies the identity of an individual but does not define his or her access rights (authorization). The term authentication also refers to a confirmation that a message, file, or other data has not been altered or forged. "Challenge response authentication" refers to a family of protocols in which a challenge (question) by the computer is met with a response from a user or computer client.

1. The simplest example of challenge response authentication is the traditional user name/password authentication. This involves the use of a user name and a password that consists of a secret word or code used as a security measure against unauthorized access to data. This password typically requires a combination of letters, numbers, and/or characters. If it matches the information on the computer's access control list, login is granted.
2. Two-factor authentication, often referred to as strong identification, requires 2 independent ways to establish user identity and associated privileges. The second factor is often a biometric feature (fingerprint, voice recognition) if the agent is a human. Alternately, if the agent is another computer the second factor is often a cryptographic certificate.

C. Authorization (access controls)

Restricting access to a system to only authorized users is of primary concern. Sophisticated access controls also define and limit what exact applications and processes a user can reach and what hours they can use them and audit their usage. Propagation of access controls to mobile devices, specifically smartphones and tablet computers, must also

have methods for restricted database and system access via device identification, encryption, passwords, and auto-logoff among many controls.

1. Access control lists assign rights and privileges of users to resources. Controls can be implemented at the operating system or application level. For example, large applications such as Radiology Information System (RIS) and the picture archiving and communication system (PACS) store the permitted user in the application.
2. Auto-logoff is a method of automatically logging off an account after a specified period of inactivity to prevent someone besides the valid user from using the session.
3. Physical access control for **c**ritical computers is necessary to prevent console-based attacks, power interruptions, or other threats.

D. Auditing (HIPAA, Other Requirements)

21CFR11 Subpart B also requires the use of "secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records."

Audit records must be retained for at least as long as the statutory requirement of the medical record itself.

E. Application Availability

System administrator must defend against various threats to continuous availability of applications.

1. Virus detection
   The need for viral defense is widely recognized. Even servers behind firewalls can be attacked by user-infected laptops or other mobile devices if they leave the facility and re-enter the "secure" network, or if a virus gets into a facility before virus protection is in place.
2. Intrusion detection
   The system must not be compromised by an unauthorized party. An effective way of preventing this is to compute the hash value of key configuration files on a computer system. Then the file containing the hash value of the configuration files can itself be encrypted or written to write-only media. Thereafter, periodic retests compare the state of the computer to the original state. Any differences should be cause for concern.
3. Fault tolerance and business continuity considerations
   Critical computers must have redundant hardware, data archives, power and networking systems, and the ability to support automatic failover. Such systems should consist of 2 or more nodes (ideally in separate data centers), and they should be capable of supporting software upgrades without system downtime. Solutions such as offsite cloud-based disaster recovery should be identified and described in policies and procedures of the institution.
4. Documentation and staff availability
   Redundant human resources are essential for maintaining high system uptime. If only 1 person knows how to perform a system failover, the enterprise is at risk whenever that person is unavailable. All persons charged with maintaining a critical system must be equipped with full documentation and trained in executing downtime/failover procedures.
5. Physical safety
   Servers must be located to protect them from physical damage, intentional or accidental, and from environmental disasters.

F. Confidentiality

The object of confidentiality is to prevent data from being observed by unauthorized third parties. There are 2 main strategies for this: prevent third parties from having physical access to the data, and encrypt the data so that even if it is captured by third parties it cannot be read.

1. Switched networks
   This method attempts to protect confidentiality via the first strategy: denial of data access. An instantaneous circuit is created between the 2 agents who intend to communicate. This approach makes it more difficult for eavesdropping to occur.
2. Encryption: public and private key systems
   These methods can be used on individual computer storage units (eg, CD-ROM, DVD) or computer networks. They decrease the risk of a security breach, even if a message falls into the wrong hands.
   - Private key systems use a single key among all members in an application group to encode/decode information.
   - Public key systems have 1 private key that an agent keeps to himself/herselfand 1 public key that is shared at large. Agents wishing to send a secure note to the agent use the agent's public key to encode the note, and the agent decodes it with its private one.

G. Data Availability

The corollary to application availability is data availability. The chief method to maintain data availability is redundancy. Data storage file systems use redundancy in several methods. Within a single storage unit, storage disks make use of several algorithms all named RAID X (where X is a varying number). Sites may also "mirror" entire storage systems on a second storage unit, either in the same data center or "in the cloud." Popular RAID types are as follows:

1. RAID 1: A simple mirror among 2 disks. System can lose 1 disk without data loss. However, the second disk essentially provides no additional storage.
2. RAID 5: System can support loss of 1 disk, but the system has a higher utilization. For example, 75% of each disk may contain unique data, and 25% of the data are used to reconstruct another disk if it is lost.
3. RAID 6: A system that can survive the loss of 2 disks without data loss; other advantages are similar to RAID 5.

H. Data Integrity

Whether transferring information or storing it, it is necessary to verify that the information has not been modified. The same cryptographic methods outlined under IV.F. Confidentiality have application here.

1. Intrusion detection (tripwire)
   As described in section IV.C.2, an intrusion detection system can inform system administrators if the system has been compromised. Any breach should be cause to view all data on that system with suspicion.
2. Hash function and hash value
   Mathematical operations known as hash functions can be used to compute a unique hash value for given input text or data. Any alteration in the data will alter the hash value. If the sender of a message computes the hash value and encodes it with his or her private key, the recipient can decode the hash with the sender's public key and compare the value with a new hash computation on the message. If there is a difference, the message has been altered. A third party cannot fake a new hash value after the message alteration because he or she does not have the sender's private key.

I. Nonrepudiation

Nonrepudiation ensures that a transferred message has been sent and received by the parties claiming to have sent and received the message and is a way to guarantee that the sender cannot later deny having sent the message nor can the recipient deny having received the message. Methods of nonrepudiation include:

1. Digital signature
   With the use of public key infrastructure, the sender signs the message/data with his or her unique private key to encrypt the contents. The contents and signature can only be decoded by the sender's public key. Denial of sending the information is to claim that the original distributed public key was fake or the private key was stolen.
2. Auditing
   An information system that logs all user activity by user identification can also defeat repudiation claims.

J. Use Cases

Representative use cases that deal with both research and clinical scenarios, within the medical center or in the cloud, are listed in Appendix A to use as guidance on when to use the tools listed in this section.

V. RESEARCH, EDUCATIONAL, AND MARKETING USES OF PATIENT DATA; INSTITUTIONAL REVIEW BOARD, AND PRIVACY REQUIREMENTS

Research and educational activities are not exempt from the privacy and security requirements for protected health information. Privacy and security policies protect the privacy of individually identifiable health information while allowing reasonable access to medical information by the researcher/educator.

Most human research operates under the common rule (45 CFR[3] Part 46, Subpart A) and/or FDA human subject protection regulations (21 CFR Parts 50 and 56). The HIPAA Privacy Rule provision for research (45 CFR 164.502(d) and 45 CFR 164.514) builds on existing federal protections and creates equal standards of privacy protection for research governed by federal regulations as well as research that is not.

The privacy rule under HIPAA regulations covers all human beings, living or dead. Researchers may use patient PHI under the following stipulations:

A. Research Authorization Form

The privacy rule allows a single authorization form for the use and disclosure of PHI by the researcher and may be combined with the research consent form. For specific criteria, see 45 CFR§164.508(b)(3)(i).

B. Waiver of Authorization

Research use and disclosure of PHI by the researcher without individual authorization can occur with an exemption (waiver) approved by the IRB/privacy board. Documentation must include identification of the IRB or privacy board, date of alteration/waiver documentation, and satisfaction of waiver criteria as provided in 45 CFR§164.512(i)(2).

C. Review Preparatory to Research

This review is a mechanism used when researchers need to assess the feasibility of conducting research prior to the beginning of a study. The review is initiated by submitting a request to the IRB or privacy board detailing the proposed study and recognizing the conditions set forth in 45 CFR§164.510(i)(ii).

D. Data Use Agreement

A covered entity for research and educational purposes may use or disclose health information that has been de-identified by eliminating the following unique identifying characteristics: name, postal address, all date elements (except year), telephone number, fax number, e-mail address, URL address, IP address, social security numbers, account numbers, license numbers, medical record number, health plan beneficiary number, device identifiers and

[3] Code of Federal Regulations (found in the Federal Register).

their serial numbers, vehicle identifiers and serial number, biometric identifiers (finger and voice prints), full face photos and other comparable images, and any other unique identifying characteristics, numbers, or codes. Special situations in radiology might arise, for instance, in soft-tissue volume-rendered magnetic resonance imaging (MRI) or computed tomography (CT) datasets that might lead to patient identification. The data use agreement must follow the specifications in 45 CFR§164.514(e)(1)-(4).

E. Research on PHI of Decedents Requires

1. A representation by the researcher that use/disclosure being sought is solely for research on PHI of decedents
2. PHI for which access is sought is necessary for the research purpose
3. Documentation of the death of individuals about whom information is being sought when requested by the covered entity

For more information see 45 CFR§164.510(i)(iii).

F. Accounting for Research Disclosures

Under the Privacy Rule, individuals have the right to receive an accounting of disclosures of PHI during the 6 years prior to the individual's request but no earlier than April 14, 2003, and must include specific information regarding each disclosure. For subsequent multiple disclosures to the same person a more general accounting is permitted.

The success of medical research and educational uses under HIPAA requires an understanding of rules and regulations, maintaining appropriate documentation (eg, patient authorization, IRB waiver), and working with the IRB/privacy board to ensure compliance.

VI. MEDICAL-LEGAL CONSIDERATIONS

A. The following entities may have more restrictive rules to consider. This is not an exhaustive list.

1. Joint Commission
2. HIPAA/HITECH
3. Local and state laws
4. Family Educational Rights and Privacy Act
5. Americans with Disabilities Act
6. Rehabilitation Act
7. Gramm-Leach-Biley Act
8. Children's Online Privacy Protection Act

ACKNOWLEDGEMENTS

This practice parameter was revised according to the process described under the heading *The Process for Developing ACR Practice Parameters and Technical Standards* on the ACR website (http://www.acr.org/guidelines) by the Committee on Practice Parameters and Technical Standards-Nuclear Medicine and Molecular Imaging of the ACR Commission on Medical Physics in collaboration with the AAPM and the SIIM.

Collaborative Committee
Members represent their societies in the initial and final revision of this practice parameter.

ACR
Richard L. Morin, PhD, FACR, FAAPM, Co-Chair
J. Anthony Seibert, PhD, FACR, FAAPM, Co-Chair
Adam E. Flanders, MD

Christoph Wald, MD, PhD, FACR

AAPM
Bruce H. Curran, MS, ME, FAAPM
Michael J. Flynn, PhD, FAAPM
Jeff P. Masten, MA, JD, BS, MS

SIIM
Katherine P. Andriole, PhD
Steve G. Langer, PhD
Paul Nagy, PhD

Committee on Practice Parameters and Technical Standards-Nuclear Medicine and Molecular Imaging
(ACR Committee responsible for sponsoring the draft through the process)

Tariq A. Mian, PhD, FACR, FAAPM, Chair
Charles M. Able, MS
Maxwell R. Amurao, PhD, MBA
Ishtiaq H. Bercha, MSc
Chee-Wai Cheng, PhD, FAAPM
Ralph P. Lieto, MS, FACR, FAAPM
Matthew A. Pacella, MS
William Pavlicek, PhD
Doug Pfeiffer, MS, FACR, FAAPM
Thomas G. Ruckdeschel, MS
Christopher J. Watchman, PhD
Gerald A. White, Jr., MS, FACR, FAAPM
John W. Winston, Jr., MS

Richard A. Geise, PhD, FACR, FAAPM, Chair, Commission on Medical Physics
Debra L. Monticciolo, MD, FACR, Chair, Commission on Quality and Safety
Julie K. Timins, MD, FACR, Chair, Committee on Parameters & Standards - Q&S

Comments Reconciliation Committee
Tariq A. Mian, PhD, FACR, FAAPM, Chair
Timothy L. Swan, MD, FACR, Co-Chair
Katherine P. Andriole, PhD
Kimberly E. Applegate, MD, MS, FACR
Bruce H. Curran, MS, ME, FAAPM
Adam E. Flanders, MD
Michael J. Flynn, PhD, FAAPM
Richard A. Geise, PhD, FACR, FAAPM
William T. Herrington, MD, FACR
Steve G. Langer, PhD
Paul A. Larson, MD, FACR
Jeff P. Masten, MA, JD, BS, MS
Debra L. Monticciolo, MD, FACR
Richard L. Morin, PhD, FACR, FAAPM
Paul Nagy, PhD
Anne S. Patterson, MS
J. Anthony Seibert, PhD, FACR, FAAPM
William F. Sensakovic, BA, BS, PhD
Julie K. Timins, MD, FACR
Christoph Wald, MD, PhD, FACR

REFERENCES

All references to the CFR refer to the Code of Federal Regulations (found in the Federal Register).

1. US Department of Health and Human Services. Official documents (Copy 45 CFR Part 164, December 28, 2000 and August 14, 2002) (amendments to final rule 45); CFR Part 160, general administrative requirements.
2. Medical Imaging and Technology Alliance (MITA). Security and Privacy. MITA website. http://www.medicalimaging.org/policy-and-positions/joint-security-and-privacy-committee-2/. Accessed August 19, 2013.
3. IHE. IHE Security and Privacy for HIE. IHE Wiki. http://wiki.ihe.net/index.php?title=IHE_Security_and_Privacy_for_HIE#Current_Draft. Accessed August 19, 2013
4. US Department of Health and Human Services. HITECH Act Enforcement Interim Final Rule. US Department of Health and Human Services website. http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html. Accessed August 19, 2013.

APPENDIX A

Use Cases

A. Research Inside Firewall of Institution

1. Data
   a. Loss
      - Risk: moderate
      - Cost: low (assuming can be regenerated from PHI source)
   b. Unauthorized access
      - Risk: moderate
      - Cost: low
   c. Tampering
      - Risk: moderate
      - Cost: high (invalidate research)
2. Applications
   a. Downtime
      - Risk: moderate
      - Cost: low
   b. Unauthorized access
      - Risk: moderate
      - Cost: moderate
   c. Tampering
      - Risk: moderate
      - Cost: high (invalidate research)
3. Requirements
   Legal: 21CFR11 Safe Harbor anonymization, audit trails of who accessed and annonymized
4. Tools used
   a. Application and data hashes to detect tampering
   b. Anonymizer tools
   c. Auditing trails at the PHI source and at the anonymization tool

B. Research performed at multiple sites

1. Data
   a. Loss
      - Risk: moderate
      - Cost: moderate (data has to be regenerated from PHI at all sites)
   b. Unauthorized access
      - Risk: moderate
      - Cost: low
   c. Tampering
      - Risk: moderate
      - Cost: high (invalidates research)
2. Applications
   a. Downtime
      - Risk: moderate
      - Cost: low
   b. Unauthorized access
      - Risk: moderate
      - Cost: moderate
   c. Tampering
      - Risk: moderate
      - Cost: high (invalidates research)
3. Legal Requirements
   21CFR 11 Safe Harbor anonymization, audit trails of who accessed and anonymized
4. Tools used
   a. Application and data hashes to detect tampering
   b. Anonymizer tools
   c. Auditing trails at the PHI source and at the anonymization tool
   d. Digital signing to verify identity of remote senders

C. PHI Care Inside Firewall

1. Data
   a. Loss
      - Risk: variable (depends on data availability tools used)
      - Cost: high (patient care, medicolegal)
   b. Unauthorized access
      - Risk: moderate (most FDA products have basic controls)
      - Cost: high (legal and confidentiality loss)
   c. Tampering
      - Risk: moderate (most FDA products have basic controls)
      - Cost: high (patient care, medicolegal)
2. Applications
   a. Downtime
      - Risk: variable (depends on application availability tools used)
      - Cost: high (patient care, revenue loss)
   b. Unauthorized access
      - Risk: moderate (most FDA products have basic controls)
      - Cost: high (legal and confidentiality loss)
   c. Tampering
      - Risk: moderate (most FDA products have basic controls)
      - Cost: high (patient care, medicolegal)

3. Requirements
    a. Legal: all PHI controls of 21CF11 are required including report controls and digital signing
    b. Practice: high uptime, case of use, responsive behavior, clinical imaging tools
4. Tools used
    a. Redundant storage and applications
    b. Authentication controls
    c. Access controls based on user role
    d. Auditing
    e. Digital signing

D. PHI Care in the Cloud (HIE or Cloud-Based Provider)

1. Data
    a. Loss
        - Risk: moderate (most cloud providers have redundant storage)
        - Cost: high (patient care, medicolegal)
    b. Unauthorized access
        - Risk: high (many more agents have potential access)
        - Cost: high (legal and confidentiality loss)
    c. Tampering
        - Risk: high (many more agents have potential access)
        - Cost: high (patient care, medicolegal)
2. Applications
    a. Downtime
        - Risk: moderate (most cloud services are redundant)
        - Cost: high (patient care, revenue loss)
    b. Unauthorized access
        - Risk: high (many more agents have potential access)
        - Cost: high (legal and confidentiality loss)
    c. Tampering
        - Risk: high (many more agents have potential access)
        - Cost: high (patient care, medicolegal)
3. Requirements
    a. Legal: all PHI controls of 21CF11 are required including report controls and digital signing
    b. Practice: high uptime, ease of use, responsive behavior, clinical imaging tools
4. Tools used
    a. Redundant storage and applications
    b. Authentication controls
    c. Access controls based on user role
    d. Auditing
    e. Digital signing
    f. Encrypted data transmission beyond the firewall
    g. Digital signing to verify identity of remote senders

APPENDIX B

Glossary

Anonymization – the process of removing of all identifiers or codes that directly or indirectly link a particular data point or sample to an identifiable person. These data/samples become irreversibly unlinked from any subject identifiers.

Biometrics – in this case, the user may pass a smartcard through the card reader and then have to provide a fingerprint or voice sample (which is compared to a stored record before the central computer admits the user).

De-identification – the process of modifying identifiers within data/samples so that the information does not involve Protected Health Information (PHI). There are 18 items to exclude for de-identification as listed in 45 CFR 64.514(b)(2).

Digital Certificate – accompanies an electronic message to verify the identity of a user sending the message and also enables a user to encrypt the message.

Domain Name System (DNS) – a distributed internet delivery service that is mainly used to translate between domain names and internet protocol (IP) addresses, and to control Internet e-mail delivery.

Electronic Media – refers to electronic storage media in PCs and removable/transportable digital memory medium such as magnetic tapes or disks, CDs, pen drives or flash drives, optical disks, or digital memory cards; or transmission media, such as the intranet, extranet, leased lines, dial-up lines, and/or private networks.

Electronic Medical Information – patient information including images stored on electronic media.
EMR – Electronic medical record.

Firewall – a program or hardware device that filters information coming through the Internet connection into a private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.

HIPAA – Health Insurance Portability and Accountability Act of 1996.

HIPAA Security Standards – the Federal Government's requirements for the handling of electronic media and protected health information. The standards address the following:

1. Ensuring confidentiality, integrity, and availability of all electronic protected health information (ePHI) the covered entity creates, receives, maintains, or transmits.
2. Protecting against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
3. Protecting against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required.
4. Ensuring compliance by the workforce.

HIS – Hospital information system.

HITECH – Health Information Technology for Economic and Clinical Health Act of 2009; addresses the privacy and security concerns associated with the electronic transmission of health information through provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Information security – the measures taken to protect personal health information from unauthorized breaches of privacy.

IP – basic communication language of the Internet; can also be used in private networks (intranet or extranet) and is the lower layer of a 2-layer system that handles addresses and sees that the e-mail gets to the correct destination.

IRB – institutional review board – a specially constituted review body established or designated by an entity to protect the welfare of human subjects recruited to participate in biomedical or behavioral research.

LAN – local area network, a short-distance network used to link a group of computers together within a department.

Nonrepudiation – the concept of ensuring that a party cannot repudiate or refute the validity of a statement or contract. The most common application of electronic nonrepudiation is in the verification and trust of digital signatures.

PACS – picture archiving and communication system.

Patient Privacy – refers to the right of patients to determine when, how, and to what extent their health information is shared with others.

PHI – protected health information is any information relating to one's physical or mental health, the provisions of one's health care, or the payment for that health care. The US Department of Health and Human Services (DHHS or HHS) defines all of the following as individually identifiable health information:

1. Names and addresses (all geographic subdivisions smaller than a state)
2. Dates that identify – dates of birth, admission and/or discharge date(s), dates of death
3. Specific age if over 89
4. Telephone and/or fax numbers, Social Security numbers, medical record and/or account numbers, employee numbers, health plan numbers, email addresses, Web/URLs, IP address numbers, and vehicle identifiers such as license plate/serial numbers and/or certificate/license numbers.
5. Full face images and/or comparable images, biometric identifiers, such as finger prints and/or voice prints.
6. Any unique identification numbers, codes, and/or characteristics that may be traced back to an individual.

RIS – radiology information system.

Smartcards – devices in a credit card form factor that contain electronic information or tokens that identify and validate the user in conjunction with other biometric or password information.

SSL – Secure Sockets Layer – a cryptographic protocol (encode/decode) that provides secure communications on the Internet for data transfers.

TPO – treatment payment or administrative operation.

Virtual Private Network (VPN) – a computer network in which links between nodes are carried by open connections or virtual circuits (eg, the Internet) instead of by physical wires. Software uses encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

---

*Practice parameters and technical standards are published annually with an effective date of October 1 in the year in which amended, revised, or approved by the ACR Council. For practice parameters and technical standards published before 1999, the effective date was January 1 following the year in which the practice parameter or technical standard was amended, revised, or approved by the ACR Council.

Development Chronology for the Practice Parameter
2004 (Resolution 12)
Revised 2009 (Resolution 3)
Revised 2014 (Resolution 37)