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 considering 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 variables such as the condition of the patient, limitations of available resources, or advances in knowledge or technology after publication of this document. However, a practitioner who employs an approach substantially different from the guidance in this document may consider documenting in the patient record information sufficient to explain the approach taken.

The practice of medicine involves the science, and 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 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, 831 N.W.2d 826 (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).

Across most advanced economies, medical imaging and related patient information are now 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 all health care employees have to protect patients from harm extends to protecting patient privacy and patient information. Health care facilities and other entities engaged with assisting and providing health care should carefully document 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 one of a growing set of security requirements 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. Health care employees also must assess whether they have to comply with the European Union's General Data Protection Regulation (GDPR). The GDPR strictly limits using and sharing a patient's personal data, such as health care data. See https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

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[1].

[1] 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. A report April 28, 2015, is available at http://www.fas.org/sgp/crs/misc/R42507.pdf.

II. POLICY STATEMENTS

A. In today's security environment, organizations should assume they have already been breached and enact policies and actions to establish their response rather than focusing primarily on compliance. Policies should include the following topics:

1. Security awareness training for all staff in the organization
2. Security issues for ePHI and personally identifiable information (PII)
3. Designation of responsibility for:
    a. Providing security awareness training
    b. Point of contact position for all access control functions specific to department and enterprise
    c. Developing procedures in support of proper security measures
    d. Providing appropriate computer training

    e. Assuring that policies and procedures are followed
    f. Resolving security problems
    g. Ensuring appropriate mobile device management is enabled and configured for secure access
    h. Responding to a systems breach
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 with means to withstand ransomware attacks
6. Proper storage and retention for all electronic data
7. System downtime and recovery plans for unexpected computer downtime
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 security safeguards:
        i. Physical safeguards
        ii. Technical safeguards
        iii. Administrative safeguards
    b. Share assessment findings and risk analysis with appropriate institutional departments or service providers and vendors.
    c. Establish a policy for risk management for incorporating medical devices [1]
        i. Define the policy for determining acceptable risk, taking into account relevant international standards and national or regional regulations [1]
        ii. Ensure the provision of adequate resources
        iii. Ensure the assignment of qualified personnel for management, performance of work, and assessment activities
        iv. Review the results of risk management activities, including event management at defined intervals, to ensure the continuing suitability and the effectiveness of the IT risk management process
    d. Procurement of medical devices and security verification checklist
        i. Medical device manufacturer disclosure of security-related features [2]
        ii. Review and validate response of manufacturers prior to connection of device to medical IT network [2]
2. Security awareness and operational training
    a. Use radiology and specialty-oriented training tools
        i. Provide HIPAA/HITECH security training for all personnel
        ii. Inform staff of departmental policies.
    b. Maintain individual documentation of staff training
    c. Conduct annual security training relevant to enterprise and radiology
    d. Provide training for all employees and stakeholders encompassing the following:
        i. Operational computer training of all personnel on systems needed to perform their jobs
        ii. Emergency operational and communication procedures for computer downtime
        iii. Operational and communication procedures for planned computer downtime
        iv. Emergency operational and communication procedures to be used during a disaster
        v. Downtime recovery procedures and restoration to normal operation
    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. Attestation may be obtained through enterprise educational portals

3. Incident reporting and resolution of security issues
    a. Develop procedure for reporting of incidents or vulnerabilities to a department security officer, risk manager, or designee
    b. Document and implement corrective actions for minor problems
    c. Initiate corrective action with the involvement of the appropriate institutional departments, vendors, or service providers
    d. Maintain complete documentation of incidents and actions for Process Quality Improvement (PQI)
4. Accountability and sanctions
    a. Develop, review, and document manager's responsibilities for overseeing the security plan within their areas of responsibility
    b. Develop and confirm personnel responsibility for following the policies and procedures that have been established
    c. Develop, document, and share sanctions and disciplinary actions for violation of policies and procedure*s*
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 facility (or 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:
        i. Limits access to information/systems according to "need to know" as determined by staff member's manager
        ii. 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:
        i. Syntax
        ii. Expiration cycle
        iii. Reuse rules
    h. Ensure authentication for login process.
    i. Define who monitors all vendor access to departmental equipment and interfaces.
    j. Develop a methodology for comprehensive monitoring of access logs, unauthorized access, and reporting procedures for all IT solutions [3].
    k. Require secure remote application access with current encryption methods with embedded access control

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 the frequency and level of detail for monitoring and reporting.
    d. Define frequency of system privilege audits to ensure proper access level appropriate for current role
    e. Develop a process for data analysis, investigation, verification, reporting, and mitigation.

III. PROCEDURES

B. Physical Safeguards

Physical safeguards are physical measure, policies, and procedures enacted to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

1. Facility Access Controls:
    a. Policies and procedures for contingency operations
        i. Access rules for restoration of lost data under disaster recovery and emergency operations
        ii. Procedures to address major hardware and software recovery following system downtime
        iii. Identification of personnel performing data restoration and physical access to facility
    b. Policies and procedures for facility security plan
        i. Description of safeguards used to protect the facility from unauthorized physical access, tampering, or theft
        ii. Risk analysis data on workforce access to specific facilities and equipment
        iii. Methods to control access (door locks, electronic access, signage, security service/patrol, alarms video monitoring)
        iv. Methods to control property (property control tags, engraving of equipment)
        v. Methods for personnel control (identification badges, visitor badges, escorts)
        vi. Roles and training of staff and employees
    c. Policies for access control and validation procedures
        i. Alignment of person's access to information necessary for role or function in the organization
        ii. Methods to identify individuals with authorized access
        iii. Methods for visitors: sign-in, visitor badges, escort rules
        iv. Periodic review of employee restricted access list
    d. Policies and procedures for maintenance records
        i. Specification of all physical security components (locks, routine maintenance, new devices)
        ii. Special circumstances for terminated workforce members with access to large amounts of ePHI
2. Workstation (and equipment) use
    a. Policies and procedures to specify proper functions to be performed by computing devices
        i. Identification of workstations that can access ePHI from those that cannot
        ii. Internet accessibility to whitelisted sites, inaccessibility to blacklisted sites
    b. Assessment of physical surroundings to protect ePHI; risk to address possible negative impacts
        i. Sign-on, sign-off procedures, password protection, use of privacy screens, screensavers
    c. Rules for use of workstation devices in remote locations and for access of ePHI
3. Workstation (and equipment) security
    1. Policies and procedures to physically protect workstations that access ePHI
        i. Identification of all workstations that access ePHI (including laptops, personal digital assistants)
        ii. Restriction of physical access to workstations by authorized users only (secure room, area)
4. Device and media controls
    a. Policies and procedures for disposal
        i. Process to ensure unusable and inaccessible ePHI in final disposition of devices/media
        ii. Address data contained on storage devices and media from obsolete computers
    b. Policies and procedures for media reuse
        i. Electronic media reuse – ensuring complete removal of ePHI
        ii. Define how computers that are being repaired and/or stored will be handled
    c. Policies and procedures for accountability
        i. Maintain a record of movements of hardware and electronic media
        ii. Identify individual devices through serial numbers or other tracking mechanisms
        iii. Maintain a record of responsible person(s)
    d. Policies and procedures for data backup and storage
        i. Create a retrievable, exact copy of ePHI, when needed, before movement of equipment
        ii. Develop a policy for backing up data and maintaining copies
        iii. Develop a policy for retention and storage of electronic data

III. PROCEDURES

C. Technical Safeguards

1. Firewalls and secure transmission modes for staff communication
    a. Establish secure external firewalls for any network with a connection to the Internet or an outside network.
    b. Network separation for internal health care systems, which if compromised, could risk patient health. This could be done by air gapping or a second internal firewall.
    c. Establish encryption tools to allow secure transmission through the firewall.
    d. Ensure the security of e-mail communication.
        i. If e-mail is provided, make sure it is encrypted or otherwise secure for communication between staff and customers outside of the firewall.
        ii. Ensure that communication directly with patients over the Internet is authorized by the patient and that appropriate security precautions are in place.
2. Systems log aggregators to centralize application and server logs and provide automatic monitoring for anomalies.
3. Intrusion detection system to identify breaches earlier
4. Intelligent multifactor authentication to apply different levels of challenges to users as they attempt to access systems from known low-risk zones or high-risk zones
5. Encryption of data storage for mobile devices, desktop devices, and data center storage

IV. SECURITY AND PRIVACY TOOLS USED

The key provisions for handling ePHI in health care systems are outlined in 21CFR11, Subpart B and C. These rules require that all electronic record systems have methods for validation, protection, and auditing of records. The control and protection of any electronic record, both in health care and in industry, is termed cybersecurity, and includes methods for the protection of all components in the data stream, ie, computers, networks, programs, as well as control from unintended or unauthorized access, change, or use. Tools that can be used to minimize the risk from loss of control are changing continuously, and so a review of the requirements to address the privacy and security issues is given here to assist in selection of the appropriate one. In general, any tool should include 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) [4-11].

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 three levels:

1. Deidentification: Defined under HIPAA as being one of two 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: The process by which medical data are made unlinkable to the original patient.
3. Pseudonymization: Retrievably preventing linkage of medical data with an individual, using personal identifiers that have been replaced with artificial identifiers, or pseudonyms [12,13].

IV. SECURITY AND PRIVACY TOOLS USED

A. Deidentification

Deidentification requirements apply to images, reports, and other associated image-associated information, though the processes and tools used may be different.

In some situations (eg, research), the removal of patient information from the record can be used to eliminate security risks. The requirements for deidentification are defined by HIPAA/HITECH through CFR§164.514. One means of satisfying the deidentification requirement is to remove all of the following:

1. Names (this includes names of the individual and their relatives, employers, or household members)
2. Geographic subdivisions smaller than a state, with exceptions for the use of part of the zip code
3. All dates, except year, and all ages over 89
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers and license plate numbers
13. Device identifiers and serial numbers
14. URLs
15. IP addresses
16. Biometric identifiers
17. Full-face photographs and any comparable images
18. Any other unique, identifying characteristic or code

For some clinical trials and other defined research projects, not all of the 18 elements listed above need to be removed to be considered compliant with deidentification. The requirements for this specialized use of PHI should be defined by the Institutional Review Board (IRB) prior to any use[1].

Satisfactory image and report deidentification features may or may not be included in the operational clinical infrastructure (eg, PACS, Radiology Information System (RIS), electronic medical record (EMR)). It may be necessary to use commercial or open-source third-party tools. Whatever tools are used, they should be tested and validated for compliance with standard and national, regional and local (site) policies regarding what information needs to be removed or retained. The manner of their configuration and use shall be addressed in the site's security risk assessment policies and procedures.

DICOM defines standard data elements with specific values and usage, which can be classified as being at risk for leakage of various categories of identifying information. These are listed in DICOM PS3.15 Annex E, together with the appropriate action to be taken during the deidentification, whether it be to satisfy the 18 elements requirement of the HIPAA Privacy Rule or some other deidentification standard.

As an alternate to performing complete deidentification, PHI can be extracted from the record and used for statistical and scientific analysis without the need for patient identification. This can be used if there is no reasonable mechanism to identify an individual from the data. Protection for this type of data use can be achieved by the application of statistical disclosure limitation procedures. This type of PHI use is considered anonymization.

IV. SECURITY AND PRIVACY TOOLS USED

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 the user's 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 local management of a combination of user name and passphrase. This involves the use of a unique user name and secret passphrase used as a security measure against unauthorized access to data. Minimal criteria should be met to ensure sufficient resistance against guessing or brute-force attacks, most importantly a length of at least eight characters and vetting

against repetitive or easily predictable passphrases (ie, 12345678) and dictionaries of passwords or passphrases that are known to have been breached. Requirements for arbitrary password complexity (ie, numbers, special characters, etc) and regularly scheduled password rotation are no longer considered necessary to ensure security per National Institute of Standards and Technology (NIST) Special Publication 800-63B (https://pages.nist.gov/800-63-3/sp800-63b.html). Central management of authentication is preferred, but if passwords are managed locally, they should not be stored as plaintext as any breach of the system could expose all username and password combinations. Rather, passwords should be stored using modern one-way hash algorithms.

2. Management of users and passphrases can, and arguably should, be performed centrally by an institution using Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory (AD), or other similar mechanisms. Advantages are that authentication is managed centrally, more comprehensive institutional oversight is enabled, and the same credentials can be used for multiple applications throughout the institution. Passphrase requirements should be implemented as in Item 1.
3. Users should generally be required to reauthenticate after 30 minutes of inactivity or after 12 hours of use regardless of activity to ensure the user is still present and actively using the system. Some exceptions may be made in particular settings, such as operating or procedure rooms where physical security can be ensured and periodic reauthentication is not feasible.
4. Two-factor authentication, often referred to as strong identification, can strengthen authentication and requires two independent ways to establish user identity and associated privileges. The second factor is often a physical device or application on a personal device, such as a smartphone, but this may more commonly transition to a biometric feature (fingerprint, face, voice) if the agent is a human. Indeed biometric feature authentication is becoming more common in smartphone and other personal devices, which, in some cases, provide access to the second factor. However, biometric features should be limited to the second factor rather than the primary method of authentication as they are probabilistic rather than deterministic and could be potentially fraudulently replicated (ie, photographs or latent fingerprints). Alternately, if the agent is another computer, the second factor is often a cryptographic certificate, which must be preapproved by the authenticating system. Multifactor authentication should be configurable to apply higher and lower degrees of secondary authentication depending on the trust of the device authenticating. For example, a device on a trusted network may only need a second form of authentication once a month, whereas a device coming from a foreign nation known to have an active hacking community may require a second form of authentication for each login. Hardware-based two-factor authentication (2FA) should be considered. Other methods of 2FA such as text/SMS are vulnerable to SIM swaps where the telephone's text could be forwarded to another number. App based software tokens may be more secure for 2FA than text/SMS. However, with a SIM swap attack on one's mobile device, the capture of the token could allow an attacker unlimited access to all two-factor codes. A hardware device has no moving parts, is easy to use and generally can be carried into secure working environments such as military bases [14].
5. Many other advanced methods of passphrase and authentication security can be found in the NIST publication referenced above, depending on the resources available to the practice.

IV. SECURITY AND PRIVACY TOOLS USED

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, how they can use them, and what hours they can use. 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 or combinations of controls can be implemented at the institution level using LDAP or AD, operating system or application level. Institutional management of at least broad roles is recommended to centralize control and monitoring but some applications, such as the RIS and the PACS, may also store user information with more granular controls within the application.

2. Auto-logoff is a method of automatically logging off an account after a specified period of inactivity to deter someone besides the valid user from using the session. As above, this should generally be 30 minutes, but exceptions can be made depending on the needs and physical security of the space in which the system is used.
3. Physical access control for critical computers is necessary to prevent console-based attacks, power interruptions, or other threats. Physical controls may vary depending on use case and sensitivity of data.
4. Access control mechanisms should be reviewed regularly to ensure old or inactive accounts have been removed.

IV. SECURITY AND PRIVACY TOOLS USED

D. Auditing (HIPAA, Other Requirements)

Secure, computer-generated, time-stamped audit trails that record activity must be maintained in information systems that contain or use ePHI to stay compliant with HIPAA, HITECH, and other federal regulations [21 C.F.R. § 11.10(e), [45 C.F.R. § 164.312(b)]. Additionally, these audit trails and system activity should be reviewed periodically to assess for any irregular patterns, suspicious activity, or breaches [45 C.F.R. § 164.308(a)(1)(ii)(c)]. This requires fairly detailed logging at a granular level.

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

IV. SECURITY AND PRIVACY TOOLS USED

E. Application Availability

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

1. Malware detection
   The need for malicious software 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 one 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. Documentation should be reviewed periodically to ensure it is up to date and relevant. Reviewed and approved copies of documentation need to be accessible in both online and offline formats. Online formats include internal wiki sites or online notebooks, offline formats would include flash media stored physically onsite that contain the latest copy of approved documentation.

5. Physical safety

Servers must be located to protect them from physical damage, intentional or accidental, and from environmental disasters.

6. Mobile devices used to access patient data need to be managed through mobile device management that can enforce password minimums for device access, report device location if lost, and allow for remote wipe capabilities of device if lost and unrecoverable.

7. Encryption controls need to be set for any media storage used in the practice. Storage media containing patient data that is not actively being processed need to be encrypted.

IV. SECURITY AND PRIVACY TOOLS USED

F. Confidentiality

The object of confidentiality is to prevent data from being observed by unauthorized third parties. There are two 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.

Preventing third parties from gaining access

1. Network-based controls
   This method attempts to protect confidentiality via the first strategy: denial of data access within the network. One of the most basic tools is the use of switched networks rather than hubs. Additionally, network jacks within publicly accessible areas should not be enabled when not used for a piece of networking equipment. This prevents a malicious attacker from plugging in to an open jack and gaining access to the network. Highly sensitive systems, such as those who could directly harm patients if compromised, should be protected with an inner network tool, such as a firewall, or a separate network without open access to the larger private local area network (LAN).

2. Physical-based controls: This method ensures that physical access to data is limited and monitored. This includes controlling physical access to data center rooms or rooms where devices such as personal computers (PC) are accessible from a person passing by.
3. Encryption
   There exist multiple methods of data encryption; however greater amounts of computer processing power have meant that encryption schemes are increasingly vulnerable to various methods of attack. Therefore a static recommendation of an encryption method that provides a reasonable degree of protection cannot be made. However, organizations like NIST do regularly recommend types of encryption. What can be stated is that all health data in motion must be encrypted, all health data at rest on a mobile device should be encrypted, and data at rest on nonmobile devices should strongly be considered a candidate for encryption.

IV. SECURITY AND PRIVACY TOOLS USED

G. Data Availability

The corollary to application availability is data availability. There are two components to data availability: (1) ensuring the systems that deliver the data are always functioning and (2) backing up data to guard against system failure or data loss. Both of these components can be achieved by eliminating single points of failure, preparing for a disaster and having a mechanism to recover data if a disaster occurs, and monitoring the functioning of all equipment to recognize and reduce potential failure scenarios.

Removing single points of failure and providing disaster recovery can be done through data mirroring, network storage, clustered and distributed file systems, cloud systems, and virtualization.

1. Data mirroring can be used to replicate all computing function and data storage. The mirrored systems can also be used during normal maintenance or during a disaster to improve efficiency.
2. Network storage can be used to reduce a single point of failure for data storage by moving this function to

remote locations or locations that have disaster protection (eg, power backup). Network-attached storage (NAS) refers to dedicated data storage that exists on the same network. A storage area network (SAN) uses a separate network to provide redundant data access.

3. Clustered and distributed file systems make storage and computing available to multiple computers over a network. In general, these systems are a set of client and server services that allow a file to be viewed by multiple servers or workstations at the same time, although none of the client or servers using the data actually store the data.
4. Data stored in the cloud is a form of distributed computing accessed via the Internet. Cloud computing allows access to data from multiple workstations or devices, and there is normally no technical limitations on the amount of data that can be stored. Cloud systems should have similar safeguards to ensure data availability as in-house systems.
5. Virtualization is technology that allows you to create multiple simulated environments on a single physical hardware system. Virtualization can be done for a server, network, or desktop. A virtual system can replicate all functionality and data similar to data mirroring, but because multiple instances are running on a single hardware, it reduces the total hardware needed. Therefore, instead of purchasing multiple redundant hardware for each application, multiple applications run virtually on a single system, and separate systems can be set up to provide automatic failover for redundancy.

Regardless of the computing systems and data storage redundancy used, if the network between systems fails, data availability is lost. Therefore it is essential that the network architecture be robust and have redundancy. There are many methods for ensuring network availability (eg, multihoming) that can reduce slow data processing, or failure may be corrected by automatically rerouting network traffic. These methods are always changing, and the user should query the network provider to supply the method and assurances of uptime with their technique.

IV. SECURITY AND PRIVACY TOOLS USED

H. Data Integrity

Data integrity refers to the validity, accuracy, consistency, and reliability of data over their entire lifecycle. Integrity is indicated by an absence of any alteration in the data between two or more updates of a data record. Data is recorded exactly as intended, and upon later retrieval, the data is the same as it was when it was originally recorded. It is imposed at the design stage using standard rules and procedures and is maintained using error checking and validation routines. When transferring or storing information, whether textual, numerical, graphical, annotations, medical images, or a combination, it is necessary to verify that the information has not been modified after the original event (unless an intended change is authorized and documented). Any unintended change to data because of a processing or storage operation, hardware problem, or human error is a failure of data integrity. This change could be benign, potentially harmful, or even catastrophic in the delivery of medical care, resulting in misdiagnosis, mistreatment, or loss of human life. If there is evidence of unauthorized access, there might also be issues of data security.

1. Input validation – quality control checks and corrections to prevent incorrect data entry
2. Access controls, assignment of read/write privileges, auditing
3. Data backup to store a copy of the data in an alternate location
4. Data encryption to lock data by cipher
5. Data validation to certify uncorrupted contents of transmitted or received data
    a. Hash function and hash value

IV. SECURITY AND PRIVACY TOOLS USED

I. Nonrepudation

Nonrepudiation ensures that a transferred message or data 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 their 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. Trusted (digital) timestamping

    - Issued by a trusted third party acting as a time stamping authority to prove existence of data without the possibility of backdating the timestamps

3. Auditing

    - An information system that logs all user activity by user identification

IV. SECURITY AND PRIVACY TOOLS USED

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[1] Part 46, Subpart A) and/or Food and Drug Administration (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 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. The data use agreement must follow the specifications in 45 CFR§164.514(e)(1)-(4).

The standard for deidentification of DICOM objects is defined by the DICOM Standard PS 3.15-2011, Digital Imaging and Communications in Medicine (DICOM), Part 15: Security and System Management Profiles (http://dicom.nema.org/medical/dicom/current/output/html/part15.html). It is up to the user doing the deidentification to ensure that PHI is removed or cleaned according to the laws and practices in place at the time deidentification occurs. Further details on deidentification are explained at The Cancer Imaging Archive Public Access wiki, (https://wiki.cancerimagingarchive.net/display/Public/De-identification+Knowledge+Base). Volume rendering of high-resolution MR or CT head and neck images might produce recognizable visual features unless an effort is made to remove the facial features. Opinion varies about the likelihood of this risk for practical reidentification scenarios weighed against the utility of the data.

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.

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

VI. MEDICAL-LEGAL CONSIDERATIONS

Physicians and health care professionals should evaluate whether their use and disclosure of electronic medical information might implicate one or more of the following laws and rules. This is not an exhaustive list. Physicians and professionals should consult a qualified health care lawyer in their relevant jurisdiction to obtain counsel on specific medical-legal matters.

1. Joint Commission
2. HIPAA/HITECH
3. GDPR – General Data Protection Regulation
4. Local and state laws
5. Family Educational Rights and Privacy Act
6. Americans with Disabilities Act
7. Genetic Information Nondiscrimination Act of 2008
8. Rehabilitation Act
9. Gramm-Leach-Bliley Act

10. 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 (https://www.acr.org/Clinical-Resources/Practice-Parameters-and-Technical-Standards) by the Committee on Practice Parameters and Technical Standards – Medical Physics of the ACR Commission on Medical Physics in collaboration with the AAPM and the SIIM.

Writing Committee – members represent their societies in the initial and final revision of this technical standard

ACR	AAPM	SIIM
J. Anthony Seibert, PhD, FACR, Chair	Donald J. Peck, PhD, FACR	Ross W. Filice, MD
Adam E. Flanders, MD		Tom Kern, CIIP
		James T. Whitfill, MD

Committee on Practice Parameters and Technical Standards – Medical Physics

(ACR Committee responsible for sponsoring the draft through the process)

Maxwell R. Amurao, PhD, MBA, Chair

Mary Ann Keenan, DMP, Vice Chair

Priscilla F. Butler, MS, FACR

Chee-Wai Cheng, PhD, FAAPM

William R. Geiser, MS

Per H. Halvorsen, MS, FACR

Loretta M. Johnson, PhD

Lijun Ma, PhD, FAAPM

Tariq A. Mian, PhD, FACR

Jonathon A. Nye, PhD

Matthew A. Pacella, MS, FACR

Anshuman Panda, PhD

Douglas E. Pfeiffer, MS, FACR

Premavathy Rassiah, PhD

Christopher J. Watchman, PhD

Mahadevappa Mahesh, MS, PhD, FACR, Chair, Commission on Medical Physics

Jacqueline Anne Bello, MD, FACR, Chair, Commission on Quality and Safety

Matthew S. Pollack, MD, FACR, Chair, Committee on Practice Parameters and Technical Standards

Mary S. Newell, MD, FACR, Vice Chair, Committee on Practice Parameters and Technical Standards

Comments Reconciliation Committee

Eric B. Friedberg, MD, FACR, Chair

Sonia Gupta, MD, Co-Chair

Maxwell R. Amurao, PhD, MBA

Jacqueline A. Bello, MD, FACR

David A. Clunie, MB, BS

Bruce H. Curran, MS, ME, FACR

Richard Duszak, Jr., MD, FACR

Ross W. Filice, MD

Adam E. Flanders, MD

Martin W. Fraser, MS, FACR

Tobin C. Hyman, MS

Candice A. Johnstone, MD

Mary Ann Keenan, DMP

Tom Kern, CIIP

Paul A. Larson, MD, FACR

Mahadevappa Mahesh, MS, PhD, FACR

Mary S. Newell, MD, FACR

Donald J. Peck, PhD, FACR

Matthew S. Pollack, MD, FACR

Henri Primo, MD

J. Anthony Seibert, PhD, FACR

Timothy L. Swan, MD, FACR

James T. Whitfill, MD

Writing Committee – members represent their societies in the initial and final revision of this technical standard

ACR	AAPM	SIIM
J. Anthony Seibert, PhD, FACR, Chair	Donald J. Peck, PhD, FACR	Ross W. Filice, MD

Adam E. Flanders, MD

Tom Kern, CIIP

James T. Whitfill, MD

Committee on Practice Parameters and Technical Standards – Medical Physics

(ACR Committee responsible for sponsoring the draft through the process)

Maxwell R. Amurao, PhD, MBA, Chair

Mary Ann Keenan, DMP, Vice Chair

Priscilla F. Butler, MS, FACR

Chee-Wai Cheng, PhD, FAAPM

William R. Geiser, MS

Per H. Halvorsen, MS, FACR

Loretta M. Johnson, PhD

Lijun Ma, PhD, FAAPM

Tariq A. Mian, PhD, FACR

Jonathon A. Nye, PhD

Matthew A. Pacella, MS, FACR

Anshuman Panda, PhD

Douglas E. Pfeiffer, MS, FACR

Premavathy Rassiah, PhD

Christopher J. Watchman, PhD

Mahadevappa Mahesh, MS, PhD, FACR, Chair, Commission on Medical Physics

Jacqueline Anne Bello, MD, FACR, Chair, Commission on Quality and Safety

Matthew S. Pollack, MD, FACR, Chair, Committee on Practice Parameters and Technical Standards

Mary S. Newell, MD, FACR, Vice Chair, Committee on Practice Parameters and Technical Standards

Comments Reconciliation Committee

Eric B. Friedberg, MD, FACR, Chair

Mary Ann Keenan, DMP

Comments Reconciliation Committee

Sonia Gupta, MD, Co-Chair

Maxwell R. Amurao, PhD, MBA

Jacqueline A. Bello, MD, FACR

David A. Clunie, MB, BS

Bruce H. Curran, MS, ME, FACR

Richard Duszak, Jr., MD, FACR

Ross W. Filice, MD

Adam E. Flanders, MD

Martin W. Fraser, MS, FACR

Tobin C. Hyman, MS

Candice A. Johnstone, MD

Tom Kern, CIIP

Paul A. Larson, MD, FACR

Mahadevappa Mahesh, MS, PhD, FACR

Mary S. Newell, MD, FACR

Donald J. Peck, PhD, FACR

Matthew S. Pollack, MD, FACR

Henri Primo, MD

J. Anthony Seibert, PhD, FACR

Timothy L. Swan, MD, FACR

James T. Whitfill, MD

REFERENCES

1. [-3197782] International Organization for Standardization. Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities ;. 2016.
2. [-3197783] National Electrical Manufactures Association. HIMSS/NEMA Standard HN 1-2013: Manufacturer disclosure statement for medical device security (MDS2); . 2013.
3. [-3197784] Federal Committee on Statistical Methodology. Subcommittee on disclosure limitation methodology, Federal Committee on Statistical Methodology. Report on statistical disclosure limitation methodology. Statistical Policy Working Paper2, Office of Management and Budget – PDF. May 1994. Revised by the Confidentiality and Data Access Committee 2005; Available at: https://www.hhs.gov/sites/default/files/spwp22.pdf.
4. [18280936] FetzerDavid TDTDepartment of Diagnostic and Interventional Imaging, The University of Texas Health Science Center at Houston Medical School, 6431 Fannin Street, MSB 2.100, Houston, TX 77030, USA., WestO ClarkOC. The HIPAA privacy rule and protected health information: implications in research involving DICOM image databases. Acad Radiol 15:390-5, .
5. [22038512] FreymannJohn BJBSAIC-Frederick, Inc., Rockville, MD 20892, USA. freymannj@mail.nih.gov, KirbyJustin SJS, PerryJohn HJH, ClunieDavid ADA, JaffeC CarlCC. Image data sharing for biomedical research--meeting HIPAA requirements for De-identification. J Digit Imaging 25:14-24, .
6. [28405948] MonteiroErikssonE0000-0001-6201-1977University of Aveiro, DETI/IEETA, Aveiro, Portugal. eriksson.monteiro@ua.pt., CostaCarlosCUniversity of Aveiro, DETI/IEETA, Aveiro, Portugal., OliveiraJosé

LuísJLUniversity of Aveiro, DETI/IEETA, Aveiro, Portugal.. A De-Identification Pipeline for Ultrasound Medical Images in DICOM Format. J Med Syst 41:89, .
7. [25969931] MooreStephen MSMFrom the Mallinckrodt Institute of Radiology, Washington University School of Medicine, 510 S Kingshighway Blvd, St Louis, MO 63110 (S.M.M., D.R.M., K.E.S., K.W.C., B.A.V., L.R.T., F.W.P.); and Leidos Biomedical Research, Bethesda, Md (J.S.K., J.B.F.)., MaffittDavid RDR, SmithKirk EKE, et al. De-identification of Medical Images with Retention of Scientific Research Value. Radiographics 35:727-35, .
8. [25147130] NewhauserWayneWDepartment of Physics and Astronomy, Medical Physics Program, Louisiana State University, 202 Nicholson Hall, Baton Rouge, LA 70803, USA; Department of Medical Physics, Mary Bird Perkins Cancer Center, 4950 Essen Lane, Baton Rouge, LA 70809, USA. Electronic address: newhauser@lsu.edu., JonesTimothyTDepartment of Physics and Astronomy, Medical Physics Program, Louisiana State University, 202 Nicholson Hall, Baton Rouge, LA 70803, USA; Department of Medical Physics, Mary Bird Perkins Cancer Center, 4950 Essen Lane, Baton Rouge, LA 70809, USA., SwerdloffStuartSELEKTA Impac Software, 100 South Mathilda Avenue, Sunnyvale, CA 94086, USA., et al. Anonymization of DICOM electronic medical records for radiation therapy. Comput Biol Med 53:134-40, .
9. [17191099] NoumeirRitaREcole de Technologie Supérieure, 1100 Notre-Dame West, Montreal, QC, Canada H3C 1K3. noumeir@ele.etsmtl.ca, LemayAlainA, LinaJean-MarcJM. Pseudonymization of radiology data for research purposes. J Digit Imaging 20:284-95, .
10. [19745435] OnkenMichaelMOFFIS - Institute for Information Technology, 26121 Oldenburg, Germany. onken@offis.de, RiesmeierJörgJ, EngelMarcelM, YabanciAdemA, ZabelBernhardB, DesprésStefanS. Reversible anonymization of DICOM images using automatically generated policies. Stud Health Technol Inform 150:861-5, .
11. [29224856] SilvaJorge MiguelJMDETI/IEETA, University of Aveiro, Portugal. Electronic address: jorge.miguel.ferreira.silva@ua.pt., PinhoEduardoEDETI/IEETA, University of Aveiro, Portugal., MonteiroErikssonEBMD Software, Portugal., SilvaJoão FigueiraJFDETI/IEETA, University of Aveiro, Portugal., CostaCarlosCDETI/IEETA, University of Aveiro, Portugal.. Controlled searching in reversibly de-identified medical imaging archives. J Biomed Inform 77:81-90, .
12. [-3197785] National Institute of Standards and Technology. De-identification of personal information. 2015; Available at: https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf.
13. [-3197786] IHE International I. IHE infrastructure handbook. 2014; Available at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.1_2014-06-06.pdf.

14. [-3197787] Bazzell M, Carroll J. The Complete Privacy and Security Desk Reference. Vol I. San Bernadino, CA; 2016.

Appendix A

A. Research Inside Firewall of Institution
1. Data
   a. Loss
      i. Risk: moderate
      ii. Cost: low (assuming can be regenerated from PHI source)
   b. Unauthorized access
      i. Risk: moderate
      ii. Cost: low (if data anonymized)
   c. Tampering
      i. Risk: moderate
      ii. Cost: high (invalidate research)
2. Applications
   1. Downtime
      i. Risk: moderate
      ii. Cost: low
   2. Unauthorized access
      i. Risk: moderate
      ii. Cost: low (if data anonymized)
   3. Tampering
      i. Risk: moderate

ii. Cost: high (invalidate research)

3. Requirements
Legal: 21CFR11 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

B. Research performed at multiple sites

1. Data
a. Loss
i. Risk: moderate
ii. Cost: moderate (data has to be regenerated from PHI at all sites)
b. Unauthorized access
i. Risk: moderate
ii. Cost: low (if data anonymized)
c. Tampering
i. Risk: moderate
ii. Cost: high (invalidates research)

2. Applications
a. Downtime
i. Risk: moderate
ii. Cost: low
b. Unauthorized access
i. Risk: moderate
ii. Cost: low (if data anonymized)
c. Tampering
i. Risk: moderate
ii. 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
i. Risk: variable (depends on data availability tools used)
ii. Cost: high (patient care, medicolegal)
b. Unauthorized access
i. Risk: moderate (most FDA products have basic controls)
ii. Cost: high (legal and confidentiality loss)
c. Tampering
i. Risk: moderate (most FDA products have basic controls)
ii. Cost: high (patient care, medicolegal)

2. Applications
a. Downtime
i. Risk: variable (depends on application availability tools used)

ii. Cost: high (patient care, revenue loss)

b. Unauthorized access
i. Risk: moderate (most FDA products have basic controls)
ii. Cost: high (legal and confidentiality loss)

c. Tampering
i. Risk: moderate (most FDA products have basic controls)
ii. Cost: high (patient care, medicolegal)

3. Requirements
a. Legal: all PHI controls of 21CFR11 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
i. Risk: moderate (most cloud providers have redundant storage)
ii. Cost: high (patient care, medicolegal)
b. Unauthorized access
i. Risk: high (many more agents have potential access)
ii. Cost: high (legal and confidentiality loss)
c. Tampering
i. Risk: high (many more agents have potential access)
ii. Cost: high (patient care, medicolegal)

2. Applications
a. Downtime
i. Risk: moderate (most cloud services are redundant)
ii. Cost: high (patient care, revenue loss)
b. Unauthorized access
i. Risk: high (many more agents have potential access)
ii. Cost: high (legal and confidentiality loss)
c. Tampering
i. Risk: high (many more agents have potential access)
ii. 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.

EHR – Electronic health record – more encompassing version of EMR

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.

GDPR - General Data Protection Regulation – the GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the European Union.

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.

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 law and rules.

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

IP – Internet Protocol – 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.

Revised 2019 (Resolution 22)

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.

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.

TPO – treatment payment or administrative operation.

URL – Uniform Resource Locator – a reference (an address) to a resource that specifies its location on a computer network (eg, the Internet) and a mechanism for retrieving it.

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)

Revised 2019 (Resolution 22)
Amended 2023 (Resolution 2c)