

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 guidelines 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 guidelines and technical standards will be reviewed for revision or renewal, as appropriate, on their fifth anniversary or sooner, if indicated.

Each practice guideline 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, requiring the approval of the Commission on Quality and Safety as well as the ACR Board of Chancellors, the ACR Council Steering Committee, and the ACR Council. The practice guidelines 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 guideline and technical standard by those entities not providing these services is not authorized.

Revised 2009 (Resolution 3)*

ACR–SIIM PRACTICE GUIDELINE FOR ELECTRONIC MEDICAL INFORMATION PRIVACY AND SECURITY

PREAMBLE

These guidelines are an educational tool designed to assist practitioners in providing appropriate radiologic care for patients. They are not inflexible rules or requirements of practice and are not intended, nor should they be used, to establish a legal standard of care. For these reasons and those set forth below, the American College of Radiology cautions against the use of these guidelines 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 physician or medical physicist in light of all the circumstances presented. Thus, an approach that differs from the guidelines, 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 the guidelines 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 the guidelines. However, a practitioner who employs an approach substantially different from these guidelines 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 these guidelines 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 these guidelines is to assist practitioners in achieving this objective.

I. INTRODUCTION

The guideline for electronic medical information privacy and security was developed and written collaboratively by the American College of Radiology (ACR) 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 this 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.

The goal of this guideline 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.

II. POLICY STATEMENTS

Policies should include the following topics:

- A. Security awareness training for the staff in the department.
- B. Security issues for electronic personal health information.
- C. Designation of responsibility for:
 1. Providing security awareness training.
 2. Developing procedures in support of proper security measures.
 3. Providing appropriate computer training.
 4. Assuring that policies and procedures are followed.
 5. Resolving security problems.
- D. 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.
- E. Provision of backup for all systems.
- F. Proper storage and retention for all electronic data.
- G. System downtime and recovery plans for unexpected computer downtimes.
- H. Maintenance of a support manual and how to guide for computer systems and information.
- I. 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 the Health Insurance Portability and Accountability Act (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 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 their 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 shall 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 shall be identified and given authority by administration.
 - d. Obtaining access privileges requires contracted 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.
 - g. Ensure authentication for log in process.
 - h. Define who monitors all vendor access to radiology equipment and interfaces.
 - i. Require secure remote application access with a virtual private network (VPN) or secure socket layer (SSL).

6. Activity review

- a. Define a process to determine who has accessed radiology 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.
 - 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 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

The following formal components of security must be addressed by an electronic medical information system: authorization (e.g., access controls), authentication (digital signing, biometrics, etc.), availability (such as fault tolerance and denial of service [DOS] resistance), confidentiality (including encryption when required), data integrity, and nonrepudiation (digital signing). This section surveys the methods available for each of these tasks. Some methods can be used in more than one role.

A. 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 processes a user can reach and what hours they can use them and audit their usage.

1. Access control lists assign rights and privileges of users to resources. Controls can be implemented at the computer’s operating system level. For large applications such as Radiology Information System (RIS) and the Picture Archiving and Communication System (PACS), the permitted user list should be stored and managed centrally in a “single sign-on” database.
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 critical computers is necessary to prevent console-based attacks, power interruptions, or other threats.

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, log in is granted.
2. Two-factor authentication, often referred to as strong identification, requires 2 independent ways to establish user identity and associated privileges.
3. Human authentication is the verification that a person rather than a computer program initiated the transaction.

C. Availability

The system administrators must defend against various threats to continuous availability.

1. Virus detection
The need for viral defense is widely recognized. Even servers behind firewalls can be attacked by user-infected laptops 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 Message Digests of key configuration files on a computer system. Then the file containing the Message Digests 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
Critical computers must have redundant hardware, data archives, power and networking systems, and the ability to support automatic fail over. 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.

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 fail over, the enterprise is at risk whenever that person is unavailable. All persons charged with maintaining a critical system must should be equipped with full documentation and trained in executing downtime/fail over procedures.
5. Physical safety
Servers should be located to protect them from physical damage, intentional or accidental, and from environmental disasters.

D. 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. Public and private key systems
Private key systems use a single key among all members in a group to encode/decode information. Private key systems have 1 private key that an agent keeps to himself and 1 public key that is shared at large. Agents wishing to send a secure note to the recipient use the recipient’s public key to encode the note. The methods can be used on individual computer storage units (e.g., CD-ROM, DVD), computer networks, or even paper files. They decrease the risk of a security breach, even if a message falls into the wrong hands.

E. Data Integrity

When transferring information it is necessary to verify that the information arrived as it was sent and not modified.

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. Message digest (hashing)
Mathematical operations known as hashes can be used to compute a unique value Message Digest

for a given input text. Any alteration in the text will alter the value of the Message Digest. If the sender of a message computes the Message Digest 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.

F. 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.

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 CFR¹ 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.

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

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. 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 the Health Insurance Portability and Accountability Act (HIPAA) requires an understanding of rules and regulations, maintaining appropriate documentation (e.g., patient authorization, IRB waiver) and working with the IRB/Privacy Board to ensure compliance.

VI. MEDICAL-LEGAL CONSIDERATIONS

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

- A. Joint Commission.
- B. HIPAA.
- C. Local and state laws.
- D. Family Educational Rights and Privacy Act.
- E. Americans with Disabilities Act.
- F. Rehabilitation Act.
- G. Gramm-Leach-Bliley Act.
- H. Children's Online Privacy Protection Act.

ACKNOWLEDGEMENTS

This guideline was revised according to the process described under the heading *The Process for Developing ACR Practice Guidelines and Technical Standards* on the ACR web page (<http://www.acr.org/guidelines>) by the Guidelines and Standards Committee of the ACR Commission on Medical Physics in collaboration with the SIIM.

Collaborative Subcommittee:

ACR

J. Anthony Seibert, PhD, FACR, Co-Chair
 John S. Kent, MS, FACR
 Richard A. Geise, PhD, FACR
 Alan H. Rowberg, MD
 Richard L. Morin, PhD, FACR

SIIM

Katherine P. Andriole, PhD, Co-Chair
 Steve G. Langer, PhD
 Paul Nagy, PhD
 Eliot L. Siegel, MD, FACR

ACR Guidelines and Standards Committee

Richard A. Geise, PhD, FACR, Chair
 William K. Breeden, III, MS
 Martin W. Fraser, MS
 Laurie E. Gaspar, MD, MBA, FACR
 Bruce E. Hasselquist, PhD
 Mahadevappa Mahesh, MS, PhD, FACR
 Tariq A. Mian, PhD, FACR
 James T. Norweck, MS
 Janelle L. Park, MD
 J. Anthony Seibert, PhD, FACR
 James M. Hevezi, PhD, FACR, Chair, Commission

REFERENCES

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

1. 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). *Mita Security and Privacy Documents*. Available at: <http://www.medicalimaging.org/policy/security.cfm>. Assessed September 25, 2008.
3. Reiner BI, Siegel EL, Dwyer SJ. 2000. *SCAR University Primer One: Security Issues in the Digital Medical Enterprise*. Society for Imaging Informatics in Medicine Available at: <http://www.siiimweb.org>. Accessed September 24, 2008
4. 2006 Cookbook for the Security Section of the IHE Profiles (Risk Management in Healthcare IT Whitepaper). ACC/HIMSS/RSNA Available at: http://www.ihe.net/technical_framework/upload/IHE_ITI_TF_White_Paper_Security_Cookbook_PC_2006_08_30.pdf. Accessed September 24, 2008

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. 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.

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 two-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 U.S. 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, Internet Protocol (IP) address numbers, vehicle identifiers – license plate/serial numbers, 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 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 (e.g., 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.

*Guidelines and 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 guidelines and standards published before 1999, the effective date was January 1 following the year in which the guideline or standard was amended, revised, or approved by the ACR Council.

Development Chronology for the Guideline

2004 (Resolution 12)

Revised 2009 (Resolution 3)