Department of Defense
INSTRUCTION

NUMBER 8580.02
August 12, 2015

USD(P&R)

SUBJECT: Security of Individually Identifiable Health Information in DoD Health Care Programs

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD 8580.02-R (Reference (a)) as a DoD instruction (DoDI) in accordance with the authority in DoD Directive (DoDD) 5124.02 (Reference (b)).

b. Establishes policy and assigns responsibilities for security of individually identifiable health information created, received, maintained, or transmitted in electronic form (referred to in this instruction as "electronic protected health information (ePHI)").

c. Implements policy regarding information security as established in sections 300gg and 1320d *et seq.* of Title 42 United States Code (U.S.C.) (Reference (c)); section 1181 *et seq.* of Title 29 U.S.C. (Reference (d)); and parts 160, 162, and 164 of Title 45, Code of Federal Regulations (Reference (e)). References (c), (d), and (e) are collectively known and referred to in this instruction as the "Health Insurance Portability and Accountability Act (HIPAA)."

2. APPLICABILITY

a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD, which are covered entities as defined in DoD 6025.18-R (Reference (f)) (referred to collectively in this instruction as the "DoD Components").

(2) Business associates, where the contract or other written arrangement makes this instruction applicable.

b. This instruction does **not** apply to:

(1) DoD drug-testing programs carried out pursuant to DoDI 1010.01 (Reference (g)) or DoDI 1010.09 (Reference (h).

(2) The provision of health care to foreign national beneficiaries of the Military Health System (MHS) when such care is provided in a country other than the United States.

(3) The Armed Forces Repository of Specimen Samples for the Identification of Remains established and operated pursuant to DoDI 5154.30 (Reference (i)).

(4) The provision of health care to enemy prisoners of war, retained personnel, civilian internees, and other detainees pursuant to DoDD 2310.01E (Reference (j)).

(5) Education records maintained by domestic or overseas DoD-operated schools.

(6) Records maintained by DoD-operated day care centers.

(7) Military Entrance Processing Stations.

(8) Reserve Component medical personnel who are outside the authority of the military treatment facilities (MTFs) and who do not engage in standard electronic transactions covered by this instruction. See Glossary for a list of covered transactions.

(9) Health care providers that participate in Defense Health Agency (DHA)-managed care support contractor provider networks, unless otherwise required by the TRICARE program manuals or other agreements.

c. As required pursuant to the Inspector General Act of 1978, as amended, Title 5, U.S.C., Appendix (Reference (k)), nothing in this instruction will be construed to diminish the authority of any statutory Inspector General, including such authority as provided for in Reference (k).

d. This instruction is based on the requirements of HIPAA, and has common characteristics with sections 3541 through 3544 of Title 44, U.S.C., also known as and referred to in this instruction as the “Federal Information Security Management Act (FISMA) of 2002” (Reference (l)). However, this instruction does not lessen the need for DoD to comply with FISMA, nor does this instruction supersede FISMA.

3. POLICY. It is DoD policy that:

a. In accordance with HIPAA, DoD covered entities and business associates must:

(1) Ensure the confidentiality, integrity, and availability of all ePHI the DoD covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required pursuant to Reference (f).

(4) Ensure compliance with this instruction by its workforce.

(5) Comply with the procedures provided in this instruction with respect to all ePHI they own and/or manage.

b. Security measures implemented to comply with this instruction must be periodically reviewed and assessed, at least annually, pursuant to DoDI 8500.01 (Reference (m)), to ensure DoD continues to provide reasonable and appropriate protection of ePHI.

c. DoD covered entities and business associates may adopt existing policies and procedures as guidance for complying with this instruction to the extent that those policies or procedures meet or exceed the requirements of this instruction.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosures 3 and 4.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the Internet from the DoD Issuances Website at: http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction is effective August 12, 2015.

Brad R. Carson
Acting Under Secretary of Defense for
Personnel and Readiness

Enclosures
1. References
2. Responsibilities
3. Additional Responsibilities for Safeguarding ePHI
4. Administrative, Physical, and Technical Safeguards

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007 (hereby cancelled)

(b) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008

(c) Title 42, United States Code

(d) Title 29, United States Code

(e) Title 45, Code of Federal Regulations

(f) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003

(g) DoD Instruction 1010.01, "Military Personnel Drug Abuse Testing Program (MPDATP)," September 13, 2012

(h) DoD Instruction 1010.09, "DoD Civilian Employees Drug-Free Workplace Program," June 22, 2012

(i) DoD Instruction 5154.30, "Armed Forces Institute of Pathology Operations," March 18, 2003

(j) DoD Directive 2310.01E, "DoD Detainee Program," August 19, 2014

(k) Inspector General Act of 1978, as amended, Title 5, United States Code, Appendix

(l) Title 44, United States Code

(m) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

(n) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

(o) Director, Defense Health Agency Memorandum, "Designation of a Defense Health Agency Health Insurance Portability and Accountability Act Privacy Officer and Health Insurance Portability and Accountability Act Security Officer," September 2, 2014

(p) DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012, as amended

(q) Executive Order 13526, "Classified National Security Information," December 29, 2009

ENCLOSURE 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS (ASD(HA)). Under the authority, direction, and control of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), the ASD(HA):

a. Oversees compliance with this instruction.

b. Ensures reasonable and appropriate guidance and procedures are in place to comply with the requirements of this instruction while taking into account existing DoD cybersecurity-related policies and procedures.

2. DIRECTOR, DHA. Under the authority, direction, and control of the USD(P&R) and the ASD(HA), the Director, DHA:

a. Exercises oversight over DoD covered entities to ensure compliance with this instruction, taking into account other applicable requirements, as described in paragraph 1b of this enclosure.

b. Oversees coordination between the DHA Privacy Office (PO) and the DHA Office of Chief Information Officer (CIO)/Health Information Technology Directorate (HITD).

3. DoD COMPONENT HEADS. The DoD Component heads:

a. Ensure that ePHI within DoD Component-specific assets is protected in accordance with this instruction.

b. Appoint a HIPAA security officer who is responsible for the security of ePHI, in accordance with paragraph 1b of Enclosure 4 of this instruction.

c. Appoint an authorizing official (AO) to make risk-based authorization decisions for DoD information systems (ISs) and platform information technology (PIT) systems in accordance with Reference (m).

d. Appoint a program manager (PM) with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs, in accordance with DoDI 8510.01 (Reference (n)).

e. Ensure awareness, training, and education is provided to all military and civilian personnel, including contractors who are members of the covered entity's workforce before being granted access to ePHI, and on an annual basis. Awareness, training, and education will be commensurate with employees' respective responsibilities for developing, using, operating, administering, maintaining, and retiring:

(1) DoD ISs;

(2) PIT, including network-enabled medical devices; or

(3) Other electronic equipment that creates, receives, maintains, or transmits ePHI.

f. Provide for vulnerability mitigation and an incident response and reporting capability that encompasses ePHI and provides for initiating breach response procedures when a security incident appears to be a breach.

g. Require that contracts include requirements to protect DoD ePHI and are monitored for compliance.

h. Require that access to all DoD ePHI under their purview is granted only on a need-to-know basis consistent with the requirements of Reference (f), and that all personnel who have access are appropriately cleared or qualified.

i. Distribute appropriate notice of security responsibilities and sanction policies to all individuals that develop, use, operate, administer, maintain, or retire DoD Component-owned or -controlled ISs; PITs, including network-enabled medical devices; or other electronic equipment that creates, receives, maintains, or transmits ePHI.

ENCLOSURE 3

ADDITIONAL RESPONSIBILITIES FOR SAFEGUARDING ePHI

1. CHIEF, DHA PO. Under the authority of the Director, DHA and in accordance with Reference (f) and Director, DHA Memorandum (Reference (o)), the Chief of the DHA PO is the designated HIPAA security officer for the DHA and has the overall responsibility for maintaining the confidentiality, availability, and integrity of health information, ensuring compliance with State and federal laws, and developing appropriate organizational initiatives. In addition to the responsibilities outlined in section 2 of this enclosure, the Chief, DHA PO coordinates with the DHA Office of CIO/HITD to:

a. Develop and implement security management processes, including risk analysis, risk management, workforce sanction policy, and IS activity review, to ensure compliance with this instruction.

b. Develop and maintain the DoD organizational initiatives to meet the requirements of this instruction.

c. Develop a compliance monitoring process to report to DHA leadership on a periodic basis, the status of compliance with this instruction.

d. Maintain liaison with the DoD Components to ensure continuous coordination for compliance with this instruction.

2. HIPAA SECURITY OFFICER. In accordance with paragraph 1b of Enclosure 4 of this instruction, each DoD Component designates a HIPAA security officer. DoD Component heads may assign security responsibilities to more than one individual, but a single individual must have overall final responsibility for the Component. Each HIPAA security officer:

a. Fulfills the role of the senior official responsible for the development, implementation, maintenance, oversight, and reporting of security requirements for ePHI. The HIPAA security officer, in conjunction with the DoD Component CIO, must provide strategic and tactical program direction, and exercise authority over all programmatic components, as necessary, to accomplish ePHI security compliance.

b. Ensures that the requirements for ePHI are integrated into all policies and procedures for the planning, procurement, development, implementation, and management of the DoD infrastructure and ISs.

c. Ensures internal audits of data access and use to detect and deter breaches of ePHI. Ensures internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct.

d. Responds to alleged violations of rules, regulations, policies, procedures, and codes of conduct involving ePHI by evaluating or recommending the initiation of investigative procedures in coordination with the DHA PO and in accordance with established DoD Component reporting processes.

e. Ensures consistent action is taken for failure to comply with ePHI security policies for all employees on the workforce, in cooperation with human resources, administration, and legal counsel, as appropriate.

f. Receives and documents reports of security incidents relating to ePHI, takes appropriate action to minimize harm, reports and investigates incidents, initiates breach response procedure when a security incident appears to be a breach, and recommends corrective actions to management.

g. Completes HIPAA Security Officer training before being granted access to ePHI, and on an annual basis.

3. AO. Each DoD Component head appoints an AO to make risk-based authorization decisions for DoD ISs and PIT systems in accordance with Reference (m). For DoD ISs and PIT under the purview of the AO, each AO must:

a. Ensure that requirements for ePHI in accordance with this instruction are incorporated as an element of cybersecurity pursuant to Reference (m).

b. Ensure that a statement of ePHI responsibilities is included in security position assignments, and that appointees to such positions receive appropriate training on ePHI security requirements before being granted access to ePHI, and on an annual basis.

c. As part of the cybersecurity and risk management policy of the DoD in accordance with References (m) and (n), formally approve security safeguards that meet the requirements of this instruction, and issue authorization decisions that are based upon the acceptability of the security safeguards and associated level of residual risk to ePHI.

d. Establish and verify data ownership, accountability, access, and special handling requirements for ePHI.

e. Develop, implement, and maintain a process for managing information security incidents that includes prevention, detection, response, and lessons learned for all ISs; PITs, including network-enabled medical devices; or other electronic equipment that contains ePHI. When a security incident appears to be a breach, the AO will take into account incident response procedures.

4. PM. Each DoD Component head appoints a PM with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet

the user's operational needs, in accordance with Reference (n). If no PM is assigned, then a system manager will carry out these responsibilities. Each PM:

a. Ensures all required resources, including funding and personnel, are appropriately budgeted and available to implement and maintain required safeguards in accordance with this instruction.

b. Ensures the development and implementation of a security management process, as required in paragraph 1a of Enclosure 4 of this instruction, for each IS that creates, receives, maintains, or transmits ePHI.

c. Ensures that the HIPAA security officer responsible for ePHI participates early on in the IS development life cycle to assist with the identification and selection of appropriate security controls, as outlined in Reference (n).

d. Authors, in collaboration with the DHA PO, all required memorandums of understanding (MOUs), memorandums of agreement (MOAs), or business associate agreements (BAAs) to address security requirements for ePHI in systems that interface with and are networked and managed by different AOs, or systems that are networked to non-DoD systems.

e. Completes job-specific training related to the protection of ePHI before being granted access to ePHI, and on an annual basis.

5. IS SECURITY MANAGER (ISSM). A PM appoints an ISSM (who has responsibilities assigned by Reference (m)) to develop, implement, and maintain an organization or system-level cybersecurity program; monitor compliance with cybersecurity policies; ensure the secure implementation and configuration of ISs and PIT systems; and respond to cybersecurity incidents. Each ISSM:

a. Maintains responsibility for the security posture of all ISs; PITs, including network-enabled medical devices; or other electronic equipment under his or her purview that contains ePHI.

b. Ensures that security requirements for ePHI, as specified in this instruction and Reference (n), are incorporated into policies and program guidance that are provided to subordinate activities.

c. Ensures that the information ownership responsibilities that are established for each DoD IS, including accountability, access approvals, and special handling requirements, are in compliance with this instruction.

d. Ensures that all IS security officers (ISSOs) and privileged users receive the necessary technical and security training, education, and awareness to carry out their duties to protect ePHI before being granted access to ePHI, and on an annual basis.

e. Ensures that compliance monitoring occurs, and reviews the results of such monitoring.

f. Ensures that incidents involving ePHI are properly reported to the HIPAA security officer and the DoD reporting chain, and that breach response procedures are initiated when a security incident appears to be a breach.

g. Completes job-specific training related to the protection of ePHI before being granted access to ePHI, and on an annual basis.

6. ISSO. Each PM appoints an ISSO. When circumstances warrant, a single individual may fulfill both the ISSM and the ISSO roles. An ISSO assists with the ISSM's duties and responsibilities, implements and enforces cybersecurity policies and procedures, responds to cybersecurity incidents, and maintains cybersecurity documentation, in accordance with Reference (m). Each ISSO:

a. Ensures that all users have the requisite authority, possess an appropriate personnel security background investigation, and are informed of their security responsibilities before being granted access to a DoD IS that creates, receives, maintains, or transmits ePHI.

b. Ensures that all software, hardware, and firmware that creates, receives, maintains, or transmits ePHI comply with the security requirements in this instruction.

c. Ensures that DoD IS recovery processes are monitored and that security features and procedures for ePHI are properly restored.

d. Ensures that all documentation related to the security of ePHI is current and accessible to properly authorized individuals. Documentation must be maintained for a minimum of 6 years, as required by Reference (f) and this instruction.

e. Ensures that ISs; PITs, including network-enabled medical devices; or other electronic equipment that creates, receives, maintains, or transmits ePHI, are operated, used, maintained, and disposed of in accordance with this instruction and References (m) and (n).

f. Ensures that incidents involving ePHI are properly reported to the ISSM and the DoD reporting chain, and that breach response procedures are initiated when a security incident appears to constitute a breach.

g. Completes job-specific training related to the protection of ePHI before being granted access to ePHI and on an annual basis.

7. PRIVILEGED USERS. All privileged users (e.g., system administrators):

a. Establish and manage authorized user accounts for ISs, including configuring access controls to enable authorized access to ePHI and removing authorizations when access is no longer needed in accordance with Reference (f) or paragraphs 1c(3) and 1d of Enclosure 4 of this instruction.

b. Administer user identification or authentication mechanisms of all ISs; PITs, including network-enabled medical devices; or other electronic equipment that contains ePHI.

c. Coordinate with the ISSO (or in the absence of an ISSO, the ISSM), as required, to enforce password controls, set permissions, perform security management functions, and coordinate or perform preventive and corrective maintenance for all ISs that contain ePHI. Document and report any identified vulnerabilities to the ISSO immediately upon detection.

d. Report to the ISSO (or in the absence of an ISSO, the ISSM) all IS failures that could lead to unauthorized disclosure or any attempt to gain unauthorized access to DoD ISs; PITs, including network enabled medical devices; or other electronic equipment that contains ePHI or data created, received, maintained, or transmitted by that equipment.

e. Complete job-specific training related to the protection of ePHI before being granted access to ePHI and on an annual basis.

8. AUTHORIZED USERS OF HEALTH INFORMATION. All authorized users of health information must:

a. Comply with all applicable policies, issuances, procedures and practices governing the secure operation (e.g., protection of passwords) and authorized use of ISs; PITs, including network-enabled medical devices; or other electronic equipment that creates, receives, maintains, or transmits ePHI.

b. Report all security incidents, potential threats, and suspected vulnerabilities that may affect the confidentiality, integrity, or availability of ePHI to the appropriate HIPAA security officer, ISSO, or ISSM immediately upon detection, and initiate the breach response procedures when a security incident appears to constitute a breach.

c. Complete initial and subsequent annual training, as required by this instruction, for the security of ePHI.

d. Access only that data, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only authorized roles and privileges.

e. Protect all access authenticators, such as individual identities and passwords, commensurate with the classification or sensitivity of the information accessed. Immediately report any compromised or suspected compromise of an authenticator to the appropriate ISSO upon detection.

f. Ensure that electronic media that contain ePHI are properly marked, controlled, stored, transported, and destroyed in accordance with the classification or sensitivity and need-to-know, pursuant to DoD Manual 5200.01 (Reference (p)).

g. Protect terminals, workstations, and other devices containing or processing ePHI under their control from unauthorized access.

h. Observe policies and procedures governing the secure operation and authorized use of any ISs; PITs, including network-enabled medical devices; or other electronic equipment that contains ePHI, to which they have been granted access.

ENCLOSURE 4

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS

1. ADMINISTRATIVE SAFEGUARDS. A DoD covered entity or business associate must implement the administrative actions, policies, and procedures described in this section to protect ePHI.

a. Security Management Process. Implement the following policies and procedures to prevent, detect, contain, and correct security violations:

(1) Risk Analysis. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities with respect to the confidentiality, integrity, and availability of ePHI that it owns or manages in accordance with Reference (n).

(2) Risk Management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with this instruction.

(3) Sanction Policy. Apply appropriate sanctions against workforce members who fail to comply with this instruction and applicable security policies and procedures. Appropriate sanctions are determined based on the severity and circumstances of the violation and may be applied using the standard disciplinary processes already in place, where appropriate. In some cases, the type and severity of sanctions imposed and the categories of violation are at the discretion of the DoD covered entity.

(4) IS Activity Review. Implement procedures to regularly review records of IS activity, such as audit logs, access reports, and security incident tracking reports.

b. Assigned Security Responsibility. Identify, in writing, the HIPAA security officer who is responsible for the development and implementation of the policies and procedures required by this instruction for the DoD covered entity or business associate.

c. Workforce Security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, and to prevent those workforce members who do not have access from obtaining access to ePHI, as provided paragraph 1d of this enclosure.

(1) Authorization or Supervision. Implement procedures for the authorization or supervision of workforce members who work with ePHI or in locations where it might be accessed.

(2) Workforce Clearance Procedures. Implement procedures to determine that the access of a workforce member to ePHI is appropriate.

(3) Termination Procedures. Implement procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member ends or as required by procedures created in accordance with paragraph 1c(2) of this enclosure.

d. Information Access Management. Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements in accordance with Reference (f).

(1) Access Authorization. Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

(2) Access Establishment and Modification. Implement policies and procedures that, based on the DoD covered entity's or business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

e. Security Awareness and Training. Implement a security awareness and training program for all members of its workforce (including management) that includes:

(1) Security Reminders. Periodic security updates.

(2) Protection from Malicious Software. Procedures for guarding against, detecting, and reporting malicious software.

(3) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies.

(4) Password Management. Procedures for creating, changing, and safeguarding passwords.

f. Security Incident Response Procedures

(1) Implement policies and procedures to address security incidents, including initiation of breach response procedures when a security incident appears to constitute a breach.

(2) Identify, report, and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the DoD covered entity or business associate; and document security incidents and their outcomes.

g. Contingency Plan. Develop (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.

(1) Data Backup Plan. Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

(2) Disaster Recovery Plan. Establish (and implement as needed) procedures to restore any loss of data.

(3) Emergency Mode Operation Plan. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

(4) Testing and Revision Procedures. Implement procedures for periodic testing and revision of contingency plans.

(5) Applications and Data Criticality Analysis. Assess the relative criticality of specific applications and data in support of other contingency plan components.

h. Evaluations. Perform periodic technical and non-technical evaluations. Initially these evaluations will be based on the standards implemented in accordance with this instruction. Subsequently the evaluations will be performed in response to environmental or operational changes affecting the security of ePHI, which will establish the extent to which a DoD covered entity's or business associate's security policies and procedures meet the requirements of this instruction.

i. Business Associate Contracts and Other Arrangements

(1) DoD Components (including those covered under this instruction) sometimes perform functions covered under this instruction for other organizations. In other cases, business associate functions may be carried out by other government agencies or by non-governmental entities under contract. This section establishes requirements applicable to all business associates that are:

(a) DoD Components, for which the requirements are established by this instruction, thus not requiring a written BAA. This includes any organization within the DoD that creates, receives, maintains, or transmits ePHI.

(b) Other government agencies, for which the requirements must be incorporated into the MOU or MOA (or incorporated by reference, or by other applicable documentation of the arrangement) between the DoD Component and the other government agency.

(c) Other entities, for which the requirements must be incorporated (or incorporated by reference) into the contract or agreement with the other entity. This includes any contract or agreement containing business associate language in accordance with Reference (f) and requiring compliance, executed on behalf of the DoD that creates, receives, maintains, or transmits ePHI.

(2) A DoD covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on the DoD covered entity's behalf only if the DoD covered entity obtains satisfactory assurances, in accordance with paragraph 1i(5) of this enclosure, that the business associate will appropriately safeguard the information. A DoD covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(3) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with paragraph 1i(5) of this enclosure, that the subcontractor will appropriately safeguard the information.

(4) DoD covered entities and business associates must document the satisfactory assurances required by paragraph 1i(2) or 1i(3) of this enclosure through a written contract or other arrangement with the business associate or subcontractor that meets the applicable requirements of paragraph 1i(5).

(5) The contract or other arrangement required by paragraph 1i(4) of this enclosure must meet the following requirements, as applicable.

(a) Business Associate Contracts. The contract must provide that the business associate will:

1. Comply with the applicable requirements of this instruction.

2. In accordance with paragraph 1i(3) of this enclosure, ensure that any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate agree to comply with the applicable requirements of this instruction by entering into a contract or other arrangement that complies with this section.

3. Report to the DoD covered entity any security incident of which it becomes aware, including breaches of ePHI.

(b) Other Arrangements. The DoD covered entity is in compliance with paragraph 1i(5) of this enclosure if it has another arrangement in place that meets the requirements of section C3.4.3. of Reference (f).

(c) Business Associate Contracts with Subcontractors. The requirements of paragraphs 1i(5)(a) and 1i(5)(b) of this enclosure also apply to the contract or other arrangement between a business associate and a subcontractor required by paragraph 1i(4) of this enclosure.

2. PHYSICAL SAFEGUARDS. A DoD covered entity or business associate must implement the physical measures, policies, and procedures described in this section to protect ePHI.

a. Facility Access Controls. Implement policies and procedures to limit physical access to its electronic ISs and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(1) Contingency Operations. Establish (and implement as needed) procedures in accordance with paragraphs 1g(2) and (3) of this enclosure for a disaster recovery plan and an

emergency mode operation plan that allow facility access in support of restoration of lost data in the event of an emergency.

(2) Facility Security Plan. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(3) Access Control and Validation Procedures. Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.

(4) Maintenance Records. Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).

b. Workstation Use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

c. Workstation Security. Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

d. Device and Media Controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

(1) Disposal. Implement policies and procedures to address the final disposition of ePHI, and the hardware or electronic media on which it is stored in accordance with DoD Component-authorized record disposition authorities.

(2) Media Re-use. Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

(3) Accountability. Maintain a record of the movements of hardware and electronic media and any person responsible for such hardware and media.

(4) Data Backup and Storage. Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

3. TECHNICAL SAFEGUARDS. A DoD covered entity or business associate must implement the technologies, policies, and procedures described in this section to protect ePHI:

a. Access Control. Implement technical policies and procedures for electronic ISs that maintain ePHI to allow access only to those persons or software programs that have been granted access rights, as specified in paragraph 1d of this enclosure.

(1) Unique User Identification. Assign a unique name, number, or both for identifying and tracking user identity.

(2) Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

(3) Automatic Logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(4) Encryption and Decryption. Implement a mechanism to encrypt and decrypt ePHI in accordance with DoD and MHS policy, and taking into account requirements to protect data at rest and in transit, using approved cryptographic modules.

b. Audit Controls. Implement hardware, software, or procedural mechanisms that record and examine activity in ISs that contain or use ePHI.

c. Integrity. Implement policies and procedures to protect ePHI from improper alteration or destruction, including electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

d. Person or Entity Authentication. Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

e. Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

(1) Integrity Controls. Implement security measures to ensure that ePHI being electronically transmitted is not improperly modified during transmission without detection until disposed of.

(2) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate or required by DoD or MHS policy.

4. DOCUMENTATION REQUIREMENTS. A DoD covered entity or business associate must implement the documentation requirements described in this section.

a. Policies and Procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this section, taking into account the RMF described in Reference (n). A DoD covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this paragraph.

b. Documentation

(1) Maintain the policies and procedures implemented to comply with this instruction in written (which may be electronic) form.

(2) If an action, activity, or assessment is required by this instruction to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

c. Time Limit. Retain the documentation required by paragraph 4b of this enclosure for a minimum of 6 years from the date of its creation or the date when it last was in effect, whichever is later.

d. Availability. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

e. Updates. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	authorizing official
ASD(HA)	Assistant Secretary of Defense for Health Affairs
BAA	business associate agreement
CIO	chief information officer
DHA	Defense Health Agency
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
ePHI	electronic protected health information
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HITD	Health Information Technology Directorate
IA	information assurance
IS	information system
ISSM	information system security manager
ISSO	information system security officer
MHS	Military Health System
MOA	memorandum of agreement
MOU	memorandum of understanding
MTF	military treatment facility
PO	Privacy Office
PIT	platform information technology
PM	program manager
U.S.C.	United States Code
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this instruction.

access. The ability or the means necessary to read, write, modify, or communicate data or information, or otherwise use any system resource.

access controls. The process of granting or denying specific requests: for obtaining and using information and related information processing services; and to enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).

administrative safeguards. Administrative actions, and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to safeguard ePHI and to manage the conduct of an organization's workforce in relation to the protection of that information.

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.

availability. The property of being accessible and useable upon demand by an authorized entity.

business associate. A person or entity that performs or assists in the performance of a function or activity (legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services) involving the use or disclosure of PHI on behalf of, or to provide services to, an organization.

compliance monitoring. Collection and evaluation of data, including self-monitoring reports, and verification.

confidentiality. The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

contingency plan. Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability.

covered transactions. The transactions covered by this instruction are the transmission of information between two parties to carry out financial or administrative activities related to health care, including:

Health care claims or equivalent encounter information.

Health care payment and remittance advice.

Coordination of benefits.

Health care claim status.

Enrollment or disenrollment in a health plan.

Eligibility for a health plan.

Health plan premium payments.

Referral certification and authorization.

First report of injury.

Health claims attachments.

Other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation.

cybersecurity. The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication. This includes information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Reference (m) establishes that the term "cybersecurity" replaces the term "information assurance (IA)" within the DoD.

data at rest. Information that resides on electronic media while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated. Data at rest can be archival or reference files that are changed rarely or never. Data at rest also includes data that is subject to regular but not constant change.

data backup plan. A formally documented plan to create and maintain, for a specific period of time, retrievable exact copies of information.

decrypt. Convert enciphered text to plain text by means of a cryptographic system or convert encoded text to plain text by means of a code.

disclosure. Releasing, transferring, provisioning of access to, or divulging in any other manner PHI outside of the entity that maintains or stores the information.

DoD covered entities. All DoD health plans (such as TRICARE), health care providers (such as MTFs), and other entities to the extent that such plans, providers, or entities that are subject to HIPAA. Formerly known as "healthcare entities."

electronic media. Includes memory devices in computers (e.g., hard disks, memory chips) and any removable or transportable digital memory medium, such as magnetic tape or disks, optical disks, digital memory cards, or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, the extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Traditional paper-to-paper facsimile is not included; however, electronic data transmitted using a computer-based facsimile program is included.

ePHI. Individually identifiable health information that is created, received, maintained, or transmitted in electronic form by a covered entity or business associate. ePHI does not include individually identifiable health information in paper or oral form. Reference (f) contains additional requirements for individually identifiable health information created, received, marinated, or transmitted by a covered entity in any form whether electronic, oral, or paper.

emergency mode operation plan. Part of an overall contingency plan. The plan for a process whereby an enterprise would be able to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

employees. Individuals receiving a salary or wages from an organization in exchange for the performance of work for the organization.

encryption. The process of changing plaintext into ciphertext for the purpose of security or privacy.

facility security plan. A plan to safeguard a building's premises (exterior and interior) from unauthorized physical access, and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.

health care. Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to:

Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual, or that affects the structure or function of the body; and

Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

health care provider. Any organization acting as an MTF or a dental treatment facility (collectively known as MTFs). This includes organizations designated as garrison clinics and such groups in a military operational unit, ship, or aircraft, and any other person or organization outside of such organization's workforce who furnishes, bills, or is paid for health care in the normal course of business. This term includes occupational health clinics for civilian employees or contractor personnel.

health information. Any information, whether oral or recorded in any form or medium that:

Is created or received by a health care provider, health plan, public health authority, employer, life insurer, or school or university.

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or past, present, or future payments for the provision of health care to an individual.

HIPAA security officer. An official with statutory or operational authority and responsibility for the development, implementation, maintenance, oversight, and reporting of security requirements for ePHI in accordance with Reference (e).

individually identifiable health information. Information that is a subset of health information, including demographic information collected from an individual, and:

Is created or received by a health care provider, a health plan, or an employer;

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or past, present, or future payments for the provision of health care to an individual; and

Identifies the individual; or

There is a reasonable basis to believe the information can be used to identify the individual.

information security. The system of policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public under the provisions of policy or statute and those established pursuant to the authority of Executive Order 13526 (Reference (q)) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

IS. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, distribution, or disposition of information.

ISSM. The roles and responsibilities of the ISSM, formerly the IA manager, are established in References (m) and (n).

ISSO. The roles and responsibilities of the ISSO, formerly the IA officer, are established in References (m) and (n).

integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

malicious software. Software (e.g., a virus) designed to damage or disrupt a system.

MOA or MOU. A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission, e.g., establishing, operating, and securing a system interconnection.

need-to-know. A method of isolating information resources based on a user’s need to have access to that resource in order to perform their job but no more. The terms “need-to know” and “least privilege” express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

network enabled medical device. An instrument that is intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease.

physical safeguards. Physical measures, policies, and procedures to protect an organization's electronic ISs and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

PIT. Information technology, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

PM. The individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs.

privileged user. A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

risk analysis. Examination of information to identify the risk to an IS.

risk management. The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an IS, and includes:

The conduct of a risk assessment;

The implementation of a risk mitigation strategy;

Employment of techniques and procedures for the continuous monitoring of the security state of the IS; and

Documenting the overall risk management program.

security incident. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an IS.

security or security measures. Encompass all of the administrative, physical, and technical safeguards in an IS.

subcontractor. A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

unauthorized disclosure. Any access to ePHI that is not otherwise required or permitted pursuant to Reference (f).

user. A person or entity with authorized access.

vulnerability. A weakness in IS security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an IS.

workforce. Military and civilian full-time and part-time employees, volunteers, trainees, and other persons (including students and contract personnel) whose conduct, in the performance of work for an organization, is under the direct control of such an entity, whether or not they are paid by the organization.

workstation. An electronic computing device (e.g., a laptop or a desktop computer), or any other device that performs similar functions, and electronic media stored in its immediate environment.