DoD 8580.02-R

DoD HEALTH INFORMATION SECURITY REGULATION

July 12, 2007

ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS

THE ASSISTANT SECRETARY OF DEFENSE
1200 DEFENSE PENTAGON
WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

JUL 12 2007

FOREWORD

This Regulation is issued under the authority of DoD Directive 5136.1 (Reference (a)). It assigns the Assistant Secretary of Defense for Health Affairs (ASD(HA)) the authority, direction, and control to establish policies, procedures, and standards that shall govern DoD medical programs.

Although this Regulation is based on the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191 (1996) (Reference (b)), and title 45 Code of Federal Regulations parts 160, 162, and 164 (Reference (c)), it covers much of the same ground as the Federal Information Security Management Act (FISMA) (Reference (d)). This Regulation in no way impacts the need for the Department of Defense to comply with the FISMA. This law has not been superseded and has been taken into consideration in developing this Regulation.

This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

The reporting requirements in this Regulation are exempt from licensing in accordance with paragraphs C4.4.2., C4.4.4., and C4.4.7. of DoD 8910.1-M (Reference (e)).

This Regulation is effective immediately and is mandatory for use by all DoD Components.

Send recommended changes to this Regulation to the following address:

TRICARE Management Activity
Privacy Office
Skyline Five, Suite 810, 5111 Leesburg Pike
Falls Church, Virginia 22041-3206

This Regulation is approved for public release with unlimited distribution and is available via the World Wide Web at: http://www.dtic.mil/whs/directives.

S. Ward Casscells
Assistant Secretary of Defense
for Health Affairs

TABLE OF CONTENTS

REFERENCES

(a) DoD Directive 5136.1, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," May 27, 1994
(b) Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996"
(c) Parts 160, 162, and 164 of title 45, Code of Federal Regulations
(d) Sections 3541 to 3544 of title 44, United States Code, "Federal Information Security Management Act of 2002" (FISMA)
(e) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
(f) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
(g) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," as amended
(h) Executive Order 12958, "Classified National Security Information," April 20, 1995, as amended
(i) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(j) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(k) DoD 5200.1-R, "Information Security Program," January 14, 1997
(l) DoD Directive 1010.1, "Military Personnel Drug Abuse Testing Program," December 9, 1994
(m) DoD Directive 1010.9, "DoD Civilian Employees Drug Abuse Testing Program," August 23, 1988
(n) DoD Directive 5154.24, "Armed Forces Institute of Pathology (AFIP)," October 3, 2001
(o) DoD Directive 2310.01E, "The Department of Defense Detainee Program," September 5, 2006
(p) Appendix 3 of title 5, United States Code, "Inspector General Act of 1978," as amended
(q) Section 552a of title 5, United States Code, "Privacy Act of 1974," as amended
(r) Chief Information Officer Memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance," July 6, 2006
(s) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007
(t) DoD 5200.2-R, "Personnel Security Program," Change 3, February 23, 1996
(u) DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004
(v) Chief Information Officer Memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
(w) "Joint Concept of Operations for Global Information Grid NetOps," version 3, August 4, 2006
(x) Assistant Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001
(y) Assistant Secretary of Defense Memorandum, "Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," June 2, 2006

(z) DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004

(aa) Chairman of the Joint Chiefs of Staff Instruction 5610.01D, "Information Assurance (IA) and Computer Network Defense (CND)," June 15, 2004

DL1. DEFINITIONS

DL1.1. Access. The ability or the means necessary to read, write, modify, or communicate data and/or information, or to otherwise use any system resource.

DL1.2. Access Controls. Limiting access to information system resources only to authorized users, programs, processes, or other systems.

DL1.3. Administrative Safeguards. Administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to safeguard electronic protected health information (PHI) and to manage the conduct of an organization's workforce in relation to the protection of that information.

DL1.4. Authentication. For the purpose of this Regulation, the corroboration that a person is the one claimed.

DL1.5. Availability. The property that data or information is accessible and useable upon demand by an authorized person.

DL1.6. Biomedical 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.

DL1.7. 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, as defined in DoD 6025.18-R (Reference (f)).

D.1.8. Compliance Monitoring. Collection and evaluation of data, including self-monitoring reports, and verification.

DL1.9. Confidentiality. The property that data or information is not made available or disclosed to unauthorized persons or processes.

DL1.10. Contingency Plan. For the purpose of this Regulation, a plan maintained for emergency response, backup operations, and post-disaster recovery for an information system to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

DL1.11. 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.

DL1.12. Data Backup Plan. A formally documented plan to create and maintain, for a specific period of time, retrievable exact copies of information.

DL1.13. Data Integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

DL1.14. Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

DL1.15. Disclosure. Releasing, transferring, provisioning of access to, or divulging in any other manner PHI outside of the entity that maintains or stores the information.

DL1.16. 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.

DL1.17. 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.

DL1.18. Employees. Individuals receiving a salary or wages from an organization in exchange for the performance of work for the organization.

DL1.19. Encryption. The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.

DL1.20. Facility. The physical premises and the interior and exterior of a building or buildings.

DL1.21. 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.

DL1.22. Healthcare. Care, services, or supplies related to the health of an individual. Healthcare includes, but is not limited to, the following:

DL1.22.1. 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

DL1.22.2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

DL1.23. Healthcare entities. Department of Defense health plans (such as TRICARE), healthcare providers (such as medical treatment facilities), and other entities to the extent that

such plans, providers, or entities are subject to Reference (b) (hereafter referred to as "organizations").

DL1.24. Healthcare Provider. Any organization acting as a Medical Treatment Facility (MTF) or a Dental Treatment Facility (DTF). 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 healthcare in the normal course of business. This term includes occupational health clinics for civilian employees or contractor personnel.

DL1.25. Health Information. Any information, whether oral or recorded in any form or medium that:

DL1.25.1. Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, or school or university; and

DL1.25.2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or past, present, or future payments for the provision of healthcare to an individual.

DL1.26. Individually Identifiable Health Information. Information that is a subset of health information, including demographic information collected from an individual, and:

DL1.26.1. Is created or received by a healthcare provider, a health plan, or an employer; and

DL1.26.2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or past, present, or future payments for the provision of healthcare to an individual; and:

DL1.26.2.1. Identifies the individual; or

DL1.26.2.2. There is a reasonable basis to believe the information can be used to identify the individual.

DL1.27. Health Insurance Portability and Accountability Act (HIPAA) Security Officer. Official with statutory or operational authority and responsibility for the development, implementation, maintenance, oversight, and reporting of security requirements for electronic PHI in accordance with the "Health Insurance Reform: Security Standards; Final Rule" (Reference (c)).

DL1.28. Information Assurance. See Joint Publication 1-02 (Reference (g)) for definition.

DL1.29. Information Assurance Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with "Information Systems Security Manager."

DL1.30. Information Assurance Officer (IAO). An individual who reports to the IAM and is responsible for ensuring that the appropriate operational IA posture is maintained for a DoD information systems or organization. While the term IAO is favored within the Department of Defense, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Networks Security Officer, or Terminal Area Security Officer).

DL1.31. Information Security. For the Purpose of this Regulation, 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 under the authority of Executive Order 12958 (Reference (h)) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

DL1.32. Information System. For the purpose of this Regulation, a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced information technology (IT)-based processes, and platform IT interconnections.

DL1.33. Integrity. The property that data or information have not been altered or destroyed in an unauthorized manner.

DL1.34. Malicious Software. Software (e.g., a virus) designed to damage or disrupt a system.

DL1.35. Memorandum of Agreement (MOA). Memorandums that define general areas of conditional agreement between two or more parties - what one party does depends on what the other party does (e.g., one party agrees to provide support, if the other party provides the materials).

DL1.36. Memorandum of Understanding (MOU). Memorandums that define general areas of understanding between two or more parties - explains what each party plans to do; however, what each party does is not dependent on what the other party does (e.g., does not require reimbursement or other support from receiver).

DL1.37. Need-To-Know. For the purpose of this Regulation, the necessity for access to, or knowledge or possession of, specific official information required to carry out official duties.

DL1.38. Non-repudiation. The ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

DL1.39. Password. For the purpose of this Regulation, confidential authentication information composed of a string of characters.

DL1.40. Physical Safeguards. Physical measures, policies, and procedures to protect an organization's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

DL1.41. Plan of Action and Milestones (POA&M). A tool that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for weaknesses found in programs and systems.

DL1.42. Privileged User. An authorized user who has access to system control, monitoring, or administration functions.

DL1.43. Program Manager (PM). The individual with responsibility for managing an acquisition program or the development life cycle of an information system.

DL1.44. Protected Health Information (PHI). Individually identifiable health information that is created, received, or maintained by a covered entity, as defined in DoD 6025.18-R (Reference (f)).

DL1.45. Risk Analysis. Examination of information to identify the risk to an information system.

DL1.46. Risk Assessment. For the purpose of this Regulation, risk assessment is the process of analyzing threats to and vulnerabilities of an information system, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

DL1.47. Risk Management. For the purpose of this Regulation, risk management is the process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

DL1.48. Security Incident. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

DL1.49. Security Measures. Encompass all of the administrative, physical, and technical safeguards in an information system.

DL1.50. Technical Safeguards. The technology and the policy and procedures for its use that safeguard electronic PHI and control access to it.

DL1.51. Threat Assessment. Formal description and evaluation of threat to an information system.

DL1.52. User. A person or entity with authorized access.

DL1.53. Vulnerability. See Reference (g) for definition.

DL1.54. 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.

DL1.55. 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.

C1. CHAPTER 1

GENERAL INFORMATION

C1.1. PURPOSE

This Regulation:

C1.1.1. Implements the HIPAA of 1996 (Reference (b)) and parts 160, 162, and 164 of title 45, C.F.R. (Reference (c)).

C1.1.2. Implements policy and assigns responsibilities for applying the standards for security of individually identifiable health information under Reference (c).

C1.1.3. Complements DoD information assurance controls in accordance with DoD Directive 8500.1 (Reference (i)), DoD Instruction 8500.2 (Reference (j)), and information security requirements, in accordance with DoD 5200.1-R (Reference (k)).

C1.2. APPLICABILITY AND SCOPE

C1.2.1. This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all organizational entities within the Department of Defense that use or disseminate Health Information (hereafter collectively referred to as the "DoD Components").

C1.2.2. Except as otherwise provided, the requirements adopted under this Regulation apply to the following entities, as defined in Reference (f):

C1.2.2.1. The health plans of the Military Health System.

C1.2.2.2. Healthcare providers that transmit health information in electronic form in connection with a transaction covered by this Regulation.

C1.3. NON-APPLICABILITY

This Regulation does not apply to:

C1.3.1. A drug-testing program of the Department of Defense carried out under the authority of DoD Directive 1010.1 (Reference (l)) or DoD Directive 1010.9 (Reference (m)).

C1.3.2. The provision of healthcare to foreign national beneficiaries of the Department of Defense when such care is provided in a country other than the United States.

C1.3.3. The Armed Forces Repository of Specimen Samples for the Identification of Remains, established and operated under the authority of DoD Directive 5154.24 (Reference (n)).

C1.3.4. The provision of healthcare to enemy prisoners of war, retained personnel, civilian internees, and other detainees under the provisions of DoD Directive 2310.01E (Reference (o)).

C1.3.5. Education records maintained by domestic or overseas schools operated by the Department of Defense.

C1.3.6. Records maintained by day care centers operated by the Department of Defense.

C1.3.7. Military Entrance Processing Stations.

C1.3.8. Reserve component medical activities that are not practicing in a medical treatment facility (MTF).

C1.3.9. Reserve Components practicing outside of the authority of MTFs, who do not engage in electronic transactions covered by this Regulation.

C1.4. INSPECTOR GENERAL

As required under appendix 3 of title 5 United States Code (Reference (p)), nothing in this Regulation shall be construed to diminish the authority of any statutory Inspector General, including such authority, as provided for in the Inspector General Act of 1978, as amended (Reference (p)).

C1.5. POLICY

It is DoD policy, under References (b) and (c), that procedures shall be prescribed to administer the protection of PHI.

C1.6. RESPONSIBILITIES

C1.6.1. The Assistant Secretary of Defense for Health Affairs (ASD(HA)), under the Under Secretary of Defense for (Personnel and Readiness), shall:

C1.6.1.1. Exercise oversight to ensure compliance with this Regulation.

C1.6.1.2. Ensure reasonable and appropriate guidance and procedures are in place to comply with the requirements of this Regulation.

C1.6.2. TRICARE Management Activity Privacy Office shall:

C1.6.2.1. Develop and implement a process to ensure compliance, as specified in subparagraph C1.6.1.1.

C1.6.2.2. Develop and maintain the DoD Health Information Security Program to meet the requirements of this Regulation.

C1.6.2.3. Develop a compliance monitoring process to report on a periodic basis, the status of compliance with this Regulation.

C1.6.2.4. Maintain liaison with the DoD Components to ensure continuous coordination of the DoD Health Information Security Program.

C1.6.3. The Heads of the DoD Components shall:

C1.6.3.1. Ensure that electronic PHI within DoD Component-specific assets is protected in accordance with this Regulation.

C1.6.3.2. Appoint a HIPAA Security Officer who is responsible for the security of electronic PHI, in accordance with section C2.3. of this Regulation.

C1.6.3.3. Ensure that awareness, training, and education are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems, biomedical devices, or other electronic equipment that contains, creates, processes, transmits, or stores electronic PHI.

C1.6.3.4. Provide for vulnerability mitigation and an incident response and reporting capability that encompasses electronic PHI.

C1.6.3.5. Ensure that contracts include requirements to protect DoD electronic PHI, and are monitored for compliance.

C1.6.3.6. Ensure that access to all DoD electronic PHI under their purview is granted only on a need-to-know basis consistent with the requirements of References (c) and (f), and that all personnel having access are appropriately cleared or qualified.

C1.6.3.7. Ensure that appropriate notice of security responsibilities and sanction policies are provided to all individuals that develop, use, operate, administer, maintain, or retire DoD Component-owned or -controlled information systems, biomedical devices, or other electronic equipment that contains, creates, processes, transmits, or stores electronic PHI.

C1.6.4. Healthcare Entities shall:

C1.6.4.1 Ensure the confidentiality, integrity, and availability of all electronic PHI the organization creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

C1.6.4.2. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under References (f) and (q).

C1.6.4.3. Ensure compliance with this Regulation by its workforce. All security safeguards delineated by this Regulation are required by DoD unless specified as addressable. When safeguards are designated as addressable, an organization must:

C1.6.4.3.1. Assess whether the safeguard is reasonable and appropriate in its environment, when analyzed with reference to the likely contribution to protecting the organization's electronic PHI.

C1.6.4.3.2. Take into consideration the following factors when deciding what is reasonable and appropriate:

C1.6.4.3.2.1. The size, complexity, and capabilities of the organization;

C1.6.4.3.2.2. The organization's technical infrastructure, hardware, and software security capabilities;

C1.6.4.3.2.3. The costs of security measures; and

C1.6.4.3.2.4. The probability and criticality of potential risks to electronic PHI.

C1.6.4.3.3. Implement the safeguards, if reasonable and appropriate.

C1.6.4.3.4. If implementing the safeguards is not reasonable and appropriate, an organization must:

C1.6.4.3.4.1. Document why it would not be reasonable and appropriate to implement the safeguards; and

C1.6.4.3.4.2. Implement an equivalent alternative measure, if reasonable and appropriate.

C1.6.4.4. Implement and maintain reasonable and appropriate policies and procedures to comply with the requirements of this Regulation with respect to all electronic PHI.

C1.6.4.5. Maintain a written record(which may be in electronic form) of the actions, activities, or assessments that require documentation by this Regulation.

C1.6.4.5.1. Retain the implemented policies and procedures for 6 years from the date of their creation or the date when they were last in effect, whichever is later.

C1.6.4.5.2. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

C1.6.4.5.3. Review documentation, at a minimum, annually, and update, as needed, in response to environmental or operational changes affecting the security of the electronic PHI.

C1.6.4.6. Perform routine risk assessments throughout the life cycle of information systems and following significant changes to the organizational security posture.

C1.6.4.7. When necessary, provide a POA&M to identify security vulnerabilities and the actions required to resolve them.

C1.6.5. Each HIPAA Security Officer who has electronic PHI protection responsibilities shall:

C1.6.5.1. Fulfill the role of the senior official responsible for the development, implementation, maintenance, oversight, and reporting of security requirements for electronic PHI. The HIPAA Security Officer, in conjunction with the Chief Information Officer, shall provide strategic and tactical program direction, and exercise authority over all programmatic components, as necessary, to accomplish electronic PHI security compliance.

C1.6.5.2. Ensure that the requirements for electronic PHI are integrated into all policies and procedures for the planning, procurement, development, implementation, and management of the DoD infrastructure and information systems.

C1.6.5.3. Ensure internal audits of data access and use to detect and deter breaches of electronic PHI. Ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct.

C1.6.5.4. Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct involving electronic PHI by evaluating or recommending the initiation of investigative procedures.

C1.6.5.5. Ensure consistent action is taken for failure to comply with electronic PHI security policies for all employees on the workforce. Work in cooperation with human resources, administration, and legal counsel, as appropriate.

C1.6.5.6. Receive and document reports of security breaches relating to electronic PHI, take appropriate action to minimize harm, report and investigate breaches, and make recommendations to management for corrective action.

C1.6.5.7. Complete job-specific training related to the protection of electronic PHI on an annual basis.

C1.6.6. Each DAA, shall:

C1.6.6.1. For DoD information systems or enclaves under the purview of the DAA, ensure that requirements for electronic PHI are incorporated as an element of the DoD information system life-cycle management processes.

C1.6.6.2. For DoD information systems or enclaves under the purview of the DAA, ensure that when security positions are assigned in writing, a statement of electronic PHI responsibilities are included, and that appointees to such positions receive appropriate training on electronic PHI security requirements.

C1.6.6.3. For DoD information systems or enclaves under the purview of the DAA, as part of the system annual security review, required by sections 3541 to 3544 of title 44, United States Code, the Federal Information Security Management Act (FISMA) (Reference (d)) and Defense Information Assurance Certification and Accreditation Process (Reference (r)), formally approve security safeguards that meet the requirements of this Regulation, and issue accreditation statements that are based upon the acceptability of the security safeguards and associated level residual risk to electronic PHI for each information system under his or her purview.

C1.6.6.4. For DoD information systems or enclaves under the purview of the DAA, establish and verify for each information system under the purview of the DAA data ownership, accountability, access rights, and special handling requirements.

C1.6.6.5. For DoD information systems or enclaves under the purview of the DAA, ensure a process for managing information security incidents that includes prevention, detection, response, and lessons learned is developed, implemented and maintained for all information systems, biomedical devices, or other electronic equipment that contains electronic PHI under the purview of the DAA.

C1.6.7. Each PM shall:

C1.6.7.1. Maintain responsibility for the security posture of all information systems and data under his/her purview that contain electronic PHI.

C1.6.7.2. Ensure all required resources, to include funding and personnel, are appropriately budgeted and available to implement and maintain required administrative, physical, technical, organizational, and procedural safeguards in accordance with this Regulation.

C1.6.7.3. Ensure the development and implementation of a Security Management Process, as required in section C2.2. for each information system that contains, creates, processes, transmits, or stores electronic PHI.

C1.6.7.4. Ensure that the Security Officer responsible for electronic PHI participates early on in the information system development life cycle to assist with the identification and selection of appropriate security controls.

C1.6.7.5. Author all required MOU/MOAs or Business Associate Agreements to address security requirements for electronic PHI in systems that interface with and are networked and managed by different DAAs, or systems that are networked to non-DoD entities.

C1.6.7.6. Complete job-specific training related to the protection of electronic PHI on an annual basis.

C1.6.8. Each IAM, shall:

C1.6.8.1. Ensure that security requirements for electronic PHI, as specified in this Regulation, are incorporated into policies and program guidance that are provided to subordinate activities.

C1.6.8.2. Ensure that the information ownership responsibilities that are established for each DoD information system, to include accountability, access approvals, and special handling requirements, are in compliance with this Regulation.

C1.6.8.3. Ensure that all IAOs and privileged users receive the necessary technical and security training, education, and awareness to carry out their duties to protect electronic PHI.

C1.6.8.4. Ensure that compliance monitoring occurs, and review the results of such monitoring.

C1.6.8.5. Ensure that incidents involving electronic PHI are properly reported to the designated security official and the DoD reporting chain, in accordance with DoD 5400.11-R, DoD Privacy Program (Reference (s)).

C1.6.8.6. Complete job-specific training related to the protection of electronic PHI on an annual basis.

C1.6.9. Each IAO, shall:

C1.6.9.1. Ensure that all users have the requisite authority, possess an appropriate personnel security background investigation and are aware of their security responsibilities before being granted access to a DoD information system that contains, creates, processes, transmits, or stores electronic PHI.

C1.6.9.2. Ensure that all software, hardware, and firmware that contain, create, process, transmit, or store electronic PHI comply with the security requirements in this Regulation.

C1.6.9.3. Ensure that DoD information system recovery processes are monitored and that security features and procedures for electronic PHI are properly restored.

C1.6.9.4. Ensure that all documentation related to the security of electronic PHI is current and accessible to properly authorized individuals. Documentation must be maintained for a minimum of 6 years, as required by Reference (c) and this Regulation.

C1.6.9.5. Ensure that information systems, biomedical devices, or other electronic equipment that contains creates, processes, transmits, or stores electronic PHI, are operated, used, maintained, and disposed of in accordance with this Regulation and all applicable information assurance policies and procedures.

C1.6.9.6. Ensure that incidents involving electronic PHI are properly reported to the IAM and the DoD reporting chain, in accordance with Reference (s).

C1.6.9.7. Complete job-specific training related to the protection of electronic PHI on an annual basis.

C1.6.10. Privileged Users (e.g., System Administrators and Network Security Officers), shall:

C1.6.10.1. Establish and manage authorized user accounts for information systems, including configuring access controls to enable authorized access to electronic PHI and removing authorizations when access is no longer needed.

C1.6.10.2. Administer user identification or authentication mechanisms of all information systems, biomedical devices, or other electronic equipment that contains electronic PHI.

C1.6.10.3. Coordinate with the IAO, as required, to enforce password controls, set permissions, perform security management functions, and coordinate and/or perform preventive and corrective maintenance for all information systems that contain electronic PHI. Document and report any identified vulnerabilities to the IAO immediately upon detection.

C1.6.10.4. Report to the IAO all information system failures that could lead to unauthorized disclosure or any attempt to gain unauthorized access to DoD information systems, biomedical devices, or other electronic equipment that contains electronic PHI and/or data created, processed, stored and/or transmitted by that equipment.

C1.6.10.5. Complete job-specific training related to the protection of electronic PHI on an annual basis.

C1.6.11. Authorized Users of Health Information shall:

C1.6.11.1. Observe all applicable policies, issuances, procedures and practices governing the secure operation (e.g., protection of passwords) and authorized use of information systems, biomedical devices, or other electronic equipment that contains, creates, processes, transmits, or stores electronic PHI.

C1.6.11.2. Report all security incidents, potential threats, and suspected vulnerabilities that may affect PHI to the appropriate HIPAA Security Officer, IAO, or IAM immediately upon detection.

C1.6.11.3. Complete initial and annual training as required by this Regulation for the security of electronic PHI.

C1.6.11.4. 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.

C1.6.11.5. Protect all access authenticators, such as individual IDs 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 IAO upon detection.

C1.6.11.6. Ensure that electronic media that contain electronic PHI are properly marked, controlled, stored, transported, and destroyed in accordance with the classification or sensitivity and need-to-know.

C1.6.11.7. Protect terminals, workstations, and other devices containing or processing electronic PHI under their control from unauthorized access.

C1.6.11.8. Observe policies and procedures governing the secure operation and authorized use of any information systems, biomedical devices, or other electronic equipment that contains electronic PHI, to which they have been granted access.

C2. CHAPTER 2

ADMINISTRATIVE SAFEGUARDS

C2.1. OVERVIEW

Administrative safeguards are administrative actions, policies, and procedures that manage the selection, development, implementation, and maintenance of security measures through initial and subsequent organizational risk assessments due to changes in the organizational security posture. Administrative safeguards are measures designed to protect electronic PHI and to manage the conduct of the organization's workforce in relation to the protection of that information.

C2.2. SECURITY MANAGEMENT PROCESS

C2.2.1. Implementation. Implement a security management process, including policies and procedures, to prevent, detect, contain, and correct security violations.

C2.2.2. Establishment. Establish the security management process and related activities as the foundation of the organization's security program. Utilize a life-cycle approach to security that requires an assessment of the security posture of the organization and work to reduce risks on a continual basis as the security, environment, and needs of the organization change.

C2.2.3. Risk Analysis

C2.2.3.1. Conduct a risk analysis that includes an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic PHI created, received, stored, or transmitted by the organization.

C2.2.3.2. Include a threat assessment, vulnerability pairing, and residual risk determination in the risk analysis. Consider both organizational and technical assessments that address all areas of security in the risk analysis or risk assessment. Take into account all relevant losses that would be expected if security measures were not in place, including losses caused by unauthorized uses and disclosures, as well as losses of data integrity or accuracy.

C2.2.4. Risk Management

C2.2.4.1. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with section C1.5. Organizations must ensure the confidentiality, integrity, and compliance by its workforce and protect against reasonably-anticipated threats and hazards to the security of electronic PHI and unauthorized uses and disclosures of electronic PHI.

C2.2.4.2. Develop plans and take actions to implement safeguards in response to the findings of the risk analysis. Conduct re-assessments regularly to determine the effectiveness of implemented safeguards.

C2.2.5. Sanction Policy

C2.2.5.1. Ensure that sanction policies are in place and applied appropriately against workforce members who fail to comply with the security policies and procedures of the organization.

C2.2.5.2. Ensure that the workforce is notified of the sanction policy.

C2.2.5.3. Use standard disciplinary processes, when appropriate, to determine specific sanctions according to the severity and circumstances of violations. The type and severity of sanctions imposed, and the categories of "violation," are at the discretion of the organization.

C2.2.6. Information System Activity Review

C2.2.6.1. Implement procedures for regular review of records of information system activity such as audit logs, access reports, and security incident tracking reports.

C2.2.6.2. Examine records of system use (such as audit and system logs) for potential breaches of security policy. Determine the frequency of reviews for both automated and manual logs. Reports must be reviewed based on the organization's risk analysis and risk process determination.

C2.3. ASSIGNED SECURITY RESPONSIBILITY

C2.3.1. Identify and assign in writing the organization HIPAA Security Officer who is responsible for the development and implementation of the policies and procedures required by this Regulation. While more than one individual may be given security responsibilities, a single individual must be designated as having the overall final responsibility.

C2.3.2. The number and type of personnel required to implement an organization's security policies in a manner consistent with this Regulation depends on the size and structure of the organization. Document and validate the actual workforce numbers with a breakdown of responsibilities as part of the security management process.

C2.4. WORKFORCE SECURITY

C2.4.1. Access. Implement policies and procedures to ensure that all members of the workforce have appropriate access to electronic PHI, as provided under Implementation Access Management (section C2.5.). Prevent those workforce members who do not have authorized access, either physical or electronic, from accessing electronic PHI.

C2.4.2. Workforce. The term "workforce" includes military and civilian full-time and part-time employees, contract personnel, volunteers, students, and trainees. Ensure that individuals such as cleaning personnel and facility maintenance or repair contractors are considered and addressed in policies and procedures.

C2.4.3. Authorization and/or Supervision

C2.4.3.1. Implement procedures for the authorization and/or supervision of workforce members. A workforce member working with or in locations accessible to electronic PHI must either be authorized to be there, supervised while there, or both.

C2.4.3.2. The organization may employ various procedures across different types of workers depending on the results of the risk analysis, cost, and the organization's resources and business processes as long as these procedures are documented.

C2.4.4. Workforce Clearance Procedures

C2.4.4.1. Implement procedures to determine the appropriate access of workforce members to electronic PHI.

C2.4.4.2. Implement personnel security background investigation procedures for access to electronic PHI that determine a person's trustworthiness in accordance with DoD 5200.2-R (Reference (t)). A workforce member's access to electronic PHI is dependent on assessments of their job responsibilities including the amount and type of supervision.

C2.4.4.3. Implement a screening process for each job position or role and document the procedures to be followed in conducting that check. While some roles may require job references or a National Agency Check, others may only require an interview.

C2.4.5. Termination Procedures

C2.4.5.1. Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends, or as required by the organization's workforce clearance and access procedures required by sections C2.4.4., C2.5.4., and C2.5.5.

C2.4.5.2. Termination procedures must focus on two common threats: (1) continued access to information by terminated workforce personnel and (2) continued access to information by those who are still part of the workforce but whose access is no longer appropriate. Workforce status ends for many different reasons, such as retirement, change of jobs, or unsatisfactory performance, and each reason potentially poses different threats to information assets. Depending upon its risk assessment, an organization may require different procedures for terminating a former employee's access to information versus changing the access permissions for a current employee.

C2.5. INFORMATION ACCESS MANAGEMENT

C2.5.1. Access. Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of References (d) and (f).

C2.5.2. Differentiation. Differentiate information access provided to different categories of workers, as based on the organization's risk analysis, size, structure, individual access requirements and business needs.

C2.5.2.1. Establish a policy that lists and describes the different categories of workers.

C2.5.2.2. Determine the types of information needed by each of those categories of workers.

C2.5.2.3. Establish the permitted uses (read, write, amend, delete) of each type of information for each category. Only grant each worker access to the minimum amount of information needed according to their access requirements and/or to achieve the purpose of its use.

C2.5.3. Management. Establish policies and procedures for workforce configuration management that describe how the workforce is given access to information and determine the process for implementing workforce accounts, including how to make modification to permission to existing accounts. Include periodic reviews for requesting, establishing, issuing, and closing workforce accounts to ensure that they are current and accurate.

C2.5.4. Access Authorization - Implement policies and procedures for granting an individual access to electronic PHI through multiple venues to include: access to a workstation, transaction, program, process, or other mechanism. Include clear delineation on the required authorizations and clearances needed before an account can be established.

C2.5.5. Access Establishment and Modification - Based upon the organization's access authorization policies, implement additional policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

C2.5.6. Integration. The policies and procedures listed in sections C2.5.4. and C2.5.5. are very similar to those of the workforce security section (C2.4.). This redundancy reflects the importance of a formal configuration management process and documented policies and procedures that define the level of access for personnel authorized access to electronic PHI, including how the access is granted, modified, and terminated.

C2.6. SECURITY AWARENESS AND TRAINING

C2.6.1. Awareness and Training Program. Develop and implement a security awareness and training program for all members of the workforce that complements the requirements of Reference (j) and Reference (u).

C2.6.2. Awareness and Training. Awareness and training are separate activities. Security "awareness" exists to continuously heighten workforce members' familiarity with security. Security "training" teaches security practices.

C2.6.3. Record Maintenance. Maintain records documenting the implementation and delivery of the security awareness and training program. Include, at a minimum, who, where, when, and what was taught.

C2.6.4. Security Reminders. Implement annual (or more frequently, if necessary) security updates that serve as a security reminder to increase security awareness. Security reminders include e-mail messages, newsletters, posters, etc.

C2.6.5. Protection from Malicious Software. Implement security awareness and training that cover procedures for guarding against, detecting, and reporting malicious software. Part of these procedures must include an education plan for all users of electronic PHI that addresses:

C2.6.5.1. The threat of malicious software.

C2.6.5.2. Procedures in place for alerts about potential harm from malicious software.

C2.6.5.3. Methods of virus prevention.

C2.6.5.4. Response to virus detection.

C2.6.6. Log-in Monitoring. Implement security awareness and training that cover procedures for monitoring log-in attempts and reporting discrepancies to the appropriate security official. Ensure that the workforce is trained to be alert to possible unauthorized access attempts from that workstation. Training should include how to recognize an unauthorized access attempt on the type of system the user will be using, steps users can take in response to unauthorized access attempts, and reporting procedures.

C2.6.7. Password Management. Implement security awareness and training that covers procedures for creating, changing, and safeguarding passwords. Train personnel on the organization's password policies and how to create, change, and protect passwords, including how to handle lost or compromised passwords.

C2.7. SECURITY INCIDENT PROCEDURES

C2.7.1. Security Incidents. Implement policies and procedures to address security incidents. Security incidents, as defined for the purposes of this Regulation, include, but are not limited to, policy violations by users, denial of service attacks, intrusions, unauthorized disclosures, theft and/or loss of information.

C2.7.2. Response and Reporting. Establish response procedures for all levels of incidents that demonstrate how the organization will:

C2.7.2.1. Identify and respond to suspected or known security incidents.

C2.7.2.2. Report all suspected or known security incidents to the appropriate authorities in accordance with References (h), (i), (j), (r), (s), (v), and (w).

C2.7.2.3. Mitigate, to the extent practical, harmful effects of security incidents.

C2.7.2.4. Document security incidents and their outcomes.

C2.8. CONTINGENCY PLAN

C2.8.1. Emergency Response. Establish and review, annually, policies and procedures for responding to an emergency or other occurrence, such as a fire, vandalism, system failure, or a natural disaster that damages systems that contain electronic PHI. Review and update the contingency plan and all of the subsections of this requirement as needed.

C2.8.2. Data Backup Plan. Establish policies and procedures to create and maintain retrievable exact copies of electronic PHI that ensure information will not be lost in the event of a major system failure. Based on the risk assessment, system capabilities, and business processes, assign priority and frequency to backups (real time, hourly, daily, weekly, etc.). Policies and procedures must identify:

C2.8.2.1. The most appropriate method to backup the information (magnetic tapes, paper, etc.).

C2.8.2.2. The frequency for data backups.

C2.8.2.3. Maintenance of the backups (i.e., offsite, in an air-conditioned compartment or other conditions, tape(s) life cycle, system(s) of tapes, labeling and archiving of tapes for historical data).

C2.8.2.4. How long the backups should be maintained.

C2.8.2.5. Testing of the backups by executing a restore function test periodically.

C2.8.3. Data Recovery Plan. Establish and implement, annually, policies and procedures to restore any loss of data. Disasters, including fire, vandalism, natural disaster, or system failure, have the possibility of damaging PHI. Contingency plans must include a strategy and method for recovering lost or inaccessible PHI in a timely manner after a disaster.

C2.8.4. Emergency Mode Operation Plan. Establish and implement, annually, policies and procedures to enable continuation of critical business processes for the protection of the security of electronic PHI while operating in emergency mode. Contingency plans must contain an

emergency operations plan that establishes an alternate means of protecting electronic PHI during an emergency.

C2.8.5. Testing and Revision Procedures. Implement procedures for annual testing and revision of written contingency plans to look for any weaknesses. Revise the plan based on the results of testing, if necessary, and to ensure that it remains appropriate as business processes and the environment change over time.

C2.8.6. Applications and Data Criticality Analysis. As part of an organization's risk assessment, assess the relative criticality of specific applications and data in support of other contingency plan components. Utilize the results of this analysis to assign priority to information resources and determine the best strategy to protect those resources.

C2.9. EVALUATION

C2.9.1. Perform an annual (or more frequently, if necessary) technical and non-technical evaluation of the security program based upon this Regulation and in response to environmental or operational changes affecting the security of electronic PHI. Establish the extent to which the organization's security policies and procedures meet the requirements of this Regulation.

C2.9.2. Assess how changes in the environment (e.g., security-related regulations and laws and new threats) and operations (e.g., changing mission, business practices, upgraded, or new technology) affect compliance.

C2.9.3. Include all organizational safeguards and systems, as well as a review of information systems, in technical and non-technical assessments. Security evaluations can either be performed by an organization's own workforce or by an outside organization.

C2.10. BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS

C2.10.1. Business associates are authorized to create, receive, maintain, or transmit electronic PHI on behalf of the organization provided that reasonable and satisfactory assurances are presented to the organization that the business associate will appropriately safeguard the information on its behalf. Satisfactory assurances that meet the applicable requirements of this Regulation must be documented through a written contract or other legal arrangement with the business associate.

C2.10.1.1. DoD Components (including some that are themselves covered under this Regulation) sometimes perform functions for other organizations that are covered functions under this Regulation. 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:

C2.10.1.1.1. DoD Components, for which the requirements are established by this Regulation, thus not requiring a written Business Associate agreement. This includes any organization within the Department of Defense that creates, receives, maintains, or transmits electronic PHI.

C2.10.1.1.2. Other Government Agencies, for which the requirements shall be incorporated into the MOU/MOA (or incorporated by reference, or by other applicable documentation of the arrangement) between the DoD Component and the other Government Agency.

C2.10.1.1.3. Other entities, for which the requirements shall 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 (i) and requiring compliance, executed on behalf of the DoD that creates, receives, maintains, or transmits electronic PHI.

C2.10.1.2. An organization that violates the satisfactory assurances it provided as a business associate of another organization will be in noncompliance with this Regulation.

C2.10.2. The contract or other arrangement requires the business associate to:

C2.10.2.1. Implement administrative, physical, and technical safeguards that will protect the confidentiality, integrity, and availability of electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the organization.

C2.10.2.2. Ensure that all agents or subcontractors to whom the business associate provides electronic PHI will also implement reasonable and appropriate safeguards to protect the information.

C2.10.2.3. Report all security incidents to the organization as directed in the organization's contract.

C2.10.2.4. Authorize termination of the contract or other arrangement if the organization finds that the business associate has violated the terms of the contract. The organization may omit this authorization of the termination if such authorization is inconsistent with the statutory obligations of the organization or its business associate.

C2.10.3. An organization that becomes aware of a violation of its contract or other arrangement is required to:

C2.10.3.1. Take the necessary steps to mitigate the violation.

C2.10.3.2. Terminate the contract or arrangement if those steps do not successfully end the violation.

C2.10.3.3. Report the problem to the appropriate chain of command if termination is not reasonable.

C2.10.4. When an organization and its business associate are both governmental entities, the organization is in compliance with section C2.10. if:

C2.10.4.1. The organization enters into an MOU/MOA with the business associate and that MOU/MOA contains terms that accomplish the objectives of section C2.10.2.

C2.10.4.2. Other laws (including issuances adopted by the organization or its business associate) contain requirements applicable to the business associate that accomplish the objectives of section C2.10.2.

C2.10.5. If a business associate is required by law to perform a function or activity on behalf of an organization or to provide a service as described in paragraph DL1.7. to an organization, the organization may permit the business associate to create, receive, maintain, or transmit electronic PHI on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of this Regulation. The organization must attempt in good faith to obtain satisfactory assurances that the business associate will appropriately safeguard the information on its behalf and document the attempt. The organization must also document any reason why these assurances cannot be obtained.

C2.10.6. Business associate contracts or other arrangements are not required for transmissions by an organization of electronic PHI to a health care provider concerning the treatment of an individual.

C2.10.7. The organization can make assumptions about the good faith of those with whom and which it enters into contractual arrangements. A business associate is also not required to have the same level of security that exists at the organization. Organizations, however, are free to implement more demanding levels of security as deemed necessary.

C2.10.8. Organizations are not required to enter into new contractual or other arrangements to meet this Regulation’s requirements if existing written specifications already fulfill minimum standards or can be amended to do so.

C3. CHAPTER 3

PHYSICAL SAFEGUARDS

C3.1. OVERVIEW

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

C3.2. FACILITY ACCESS CONTROLS

C3.2.1. Limited Physical Access. Implement policies and procedures to limit physical access to information systems or biomedical devices and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

C3.2.1.1. Limit physical access to all buildings or business suites and to areas dedicated to the storage and use of both electronic equipment and media.

C3.2.1.2. Employ physical access controls that permit entry to individuals with appropriate authorization and deny entry to individuals lacking appropriate authorization.

C3.2.2. Physical Access Controls. Physical access controls reinforce both administrative and technical policies and procedures on information access management by permitting only authorized individuals to create, review, transmit, or modify only that information for which they have a "need-to-know."

C3.2.3. Contingency Operations. Establish and implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. Focus these procedures on the functioning of the facility and its access control mechanisms (both administrative and technical) during and after an emergency or disaster.

C3.2.4. Facility Security Plan. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. The Facility Security Plan includes policies and procedures for controlling physical access to facilities and equipment that handles electronic PHI during routine and emergency operations.

C3.2.5. Access Control and Validation Procedures. Implement procedures to control and validate identification and authentication of a person's access to facilities based on their role or function, including visitor control and control of access to firmware, hardware, and/or software programs for testing and revision.

C3.2.5.1. Establish procedures that provide individuals with physical access only to the minimum necessary data they need-to-know in order to fulfill their job responsibilities. Procedures must include:

C3.2.5.1.1. Identify and document validation access authorizations of people requesting access to a building, suite, controlled rooms and/or computer equipment prior to allowing access.

C3.2.5.1.2. Controls on visitor flow through facilities that include customers or patients, vendors, and visitors.

C3.2.5.1.3. Restrictions on access to software program testing and revision sites that only allow entrance for authorized personnel.

C3.2.5.2. Under section C.2.4., organizations must implement controls that establish different levels of access to information depending on work needs. Controlling physical access to areas within the facility with "need-to-know" procedures supports and strengthens the protective function of differentiating levels of general access to information stored and processed within the facility.

C3.2.6. Maintenance Records

C3.2.6.1. Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, or locks). Such procedures ensure accountability and aid in maintaining the facility security plan and other safeguards.

C3.2.6.2. Document policies and procedures for maintenance records even when the organization does not control the building it occupies or where they share space with other organizations. If facility security is in part based on the efforts of third parties (e.g., the building's own security force), that must be documented and be reasonable and appropriate to the circumstances.

C3.3. WORKSTATION USE

C3.3.1. Implement policies and procedures concerning workstations that specify the authorized 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 a class of workstation that can access electronic PHI.

C3.3.2. Workstation is any electronic computing device and electronic media stored in its immediate environment. These electronic computing devices include laptop or desktop computers, personal digital assistants, tablet computers, and other portable/wireless devices that can access, store, and transmit electronic PHI.

C3.3.3. For conventional desktop computing devices, include requirements to lock or logoff before leaving a workstation unattended and requirements concerning the positioning of the workstation. For portable devices that can leave the organization's premises, ensure that policies and procedures delineate the types of information users may enter into the device.

C3.4. WORKSTATION SECURITY

C3.4.1. Implement physical safeguards for all workstations that access electronic PHI. Ensure that workstation access is only granted to authorized users and prevent workstation access to unauthorized users.

C3.4.2. For fixed location devices, safeguards must include specifications for secure locations based on the sensitivity of the information accessed and the operational needs of the workforce. Safeguards for portable workstations must include limitations on what devices can leave the facility.

C3.5. DEVICE AND MEDIA CONTROLS

C3.5.1. Receipt and Removal. Implement policies and procedures for device and media controls that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility.

C3.5.2. Controls for Hardware and Movable Media. Include controls that guard the electronic PHI on both hardware and movable media. Media includes drives (permanent and removable), diskettes, compact discs, tapes, biomedical devices and any other device that is capable of accessing, storing, or transmitting electronic information. Protect the movement of these devices within a facility and when they enter or exit a facility.

C3.5.3. Disposal. Implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored. Procedures must include approved methods of disposal such as use of commercial or public disposal services, sale or donation of electronic devices and the process for ensuring that electronic PHI processed by or stored on the hardware and electronic media is no longer accessible.

C3.5.4. Media Re-Use. Implement procedures for removal of electronic PHI from electronic media before the media is made available for re-use. Methods for removing electronic PHI include reformatting and writing over existing data. Procedures must comply with the ASD Memorandum (Reference (x)).

C3.5.5. Accountability. Maintain a record of the movements of hardware and electronic media and any person responsible therefore. Implement procedures for safely managing electronic devices and media, including records of who has the devices or media, when they had possession, and where they kept the devices or media from the time of original receipt to time of

final disposal or transfer to another entity. The mechanism used for recording this documented information may be manual or automated.

C3.5.6. Data Backup and Storage. Create a retrievable, exact copy of electronic PHI before movement of equipment. Because electronically stored information can be lost, stolen, damaged, or destroyed if stored improperly or when equipment is moved, a organization must establish procedures for the secure movement of equipment, media shelf life and retention periods, the conditions of short and long-term storage locations, and physical protection measures for media repositories.

C4. CHAPTER 4

TECHNICAL SAFEGUARDS

C4.1. OVERVIEW

Technical safeguards are the technology, as well as the policies and procedures for its use that protect electronic PHI and control access to it. Technical safeguards are designed to protect electronic PHI being created, processed, stored, or transmitted.

C4.2. ACCESS CONTROLS

C4.2.1. Restricted Access. Implement technical policies and procedures for information systems and electronic devices containing PHI that allow access only to those persons or software programs that have been granted access rights as specified in section C2.4. http://privacy.med.miami.edu/glossary/xd_information_access_mgmt.htm

C4.2.2. Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. System processes will use this name and/or number to identify the user and to associate the user with tracked actions taken by or on behalf of that user. Unique user identifiers are the foundations of audit logs that help assess inappropriate access to electronic PHI by individual users.

C4.2.3. Emergency Access Procedure

C4.2.3.1. Establish, and implement as needed, procedures for obtaining necessary electronic PHI during an emergency. Develop technical procedures for obtaining electronic PHI when standard procedures fail due to a crisis situation including system failure or the unavailability of authorized users.

C4.2.3.2. Develop procedures to grant temporary access to otherwise unauthorized medical personnel when a patient's authorized providers may not be available (such as during admission to a hospital emergency department).

C4.2.4. Automatic Logoff (Addressable)

C4.2.4.1. Assess the need to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

C4.2.4.2. Based on the organization's risk assessment, implement an automatic logoff if reasonable and appropriate.

C4.2.4.3. Based on the organization's risk assessment, if implementing an automatic logoff is not reasonable and appropriate:

C4.2.4.3.1. Document why it is not reasonable and appropriate to implement the automatic logoff, and

C4.2.4.3.2. Implement an equivalent alternative measure if reasonable and appropriate. Document that alternative measure and how it achieves the same objective.

C4.2.5. Encryption and Decryption (Addressable)

C4.2.5.1. Encrypt all electronic PHI stored, processed, or transmitted using wireless local-area network devices, systems, and technologies in accordance with References (j), (y), and (z).

C4.2.5.2. Encrypt all electronic PHI assigned to a High PII Impact Category processed or stored on any mobile computing device or removable electronic media in accordance with References (j), (v), and (z).

C4.2.5.3. When encryption is not specifically required by other policy, assess the need to implement a mechanism to encrypt and decrypt electronic PHI at rest and during transmission as a means of controlling access to the electronic PHI.

C4.2.5.4. Based on the organization's risk assessment, implement a mechanism to encrypt and decrypt electronic PHI at rest if reasonable and appropriate in accordance with encryption requirements in Reference (j).

C4.2.5.5. Based on the organization's risk assessment, if implementing a mechanism to encrypt and decrypt electronic PHI at rest is not reasonable and appropriate:

C4.2.5.5.1. Document why it is not reasonable and appropriate to implement a mechanism to encrypt and decrypt electronic PHI at rest.

C4.1.5.5.2. Implement an equivalent alternative measure if reasonable and appropriate. Document the alternative measure and how it achieves the same objective.

C4.3. AUDIT CONTROLS

C4.3.1. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

C4.3.2. Select and implement a technical service to document system activity to establish the foundation for the audit requirement found in section C2.2.6.1. Use organizational policies, risk assessments, good industrial practice, and issuances such as the privacy standard to determine the organization's choice and pattern of auditing events.

C4.4. INTEGRITY

C4.4.1. Data Integrity. Implement policies and procedures to protect electronic PHI from improper or unauthorized access, use, disclosure, modification, alteration or destruction. While organizations assure data integrity through a combination of many controls including administrative, physical, and technical, this standard requires the deployment and use of technical policies and procedures to protect data integrity. Technical policies and procedures include access controls, virus protection, and encryption.

C4.4.2. Mechanism to Authenticate Electronic PHI

C4.4.2.1. Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

C4.4.2.2. Employ technical mechanisms such as check sums, message authentication codes, and digital signatures to authenticate the integrity of electronic PHI in automated information systems.

C4.4.2.3. Determine to what degree of assurance electronic PHI should be authenticated.

C4.5. PERSON OR ENTITY AUTHENTICATION

C4.5.1. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed and provide the appropriate level of non-repudiation in accordance with the Chairman of the Joint Chiefs of Staff Instruction 5610.01D (Reference (aa)). Install and use technical procedures that verify the identification and authentication of human users and other machines that transfer or request information.

C4.5.2. Organizations may use many methods with varying degrees of assurance and levels of robustness that balance business needs, cost of controls, and the sensitivity of the protected information.

C4.6. TRANSMISSION SECURITY

C4.6.1. Technical Security Mechanisms. Implement technical security mechanisms to guard against unauthorized access, use, disclosure, modification, alteration, or destruction to PHI that is being transmitted over an electronic communications network. Assess and install appropriate technical controls that mitigate threats to data security in transit over all types of networks including, but not limited to, wireless networks, the Internet, corporate intranets, dedicated lease lines, and dial-up connections.

C4.6.2. Integrity Controls. Implement security mechanisms to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

Integrity controls must provide assurance that a transmitted message arrives at its destination exactly as it left its origin.

C4.6.3. Encryption (Addressable)

C4.6.3.1. Assess the need to encrypt electronic PHI in transit to protect the confidentiality and integrity of the data during transmission over a network or other electronic means.

C4.6.3.2. Based on the organization's risk assessment, implement encryption of electronic PHI if reasonable and appropriate in accordance with encryption requirements in Reference (j) and DoDI 8520.2 (Reference (z)).

C4.6.3.3. Based on the organization's risk assessment, if implementing encryption of electronic PHI is not reasonable and appropriate:

C4.6.3.3.1. Document why it would not be reasonable and appropriate to implement a mechanism to encrypt and decrypt electronic PHI in transmission; and

C4.6.3.3.2. Implement an equivalent alternative measure if reasonable and appropriate. Document the alternative measure and how it achieves the same objective.