HEALTH CARE INFORMATION SECURITY POLICY AND REQUIREMENTS

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive establishes policy for VHA's Health Care Information Security Program in accordance with the Health Insurance Portability and Accountability Act Security Rule.

2. SUMMARY OF CONTENT: This VHA directive sets forth:

a. VHA's Health Care Information Security Program policy;

b. Requirements for Department-wide compliance with the HIPAA Security Rule, and VA-issued information security policy directives and handbooks when electronic protected health information is created, received, maintained, or transmitted by VHA;

c. Responsibilities for implementing, managing, and monitoring VHA's Health Care Information Security Program; and

d. Program integration with VA policies and processes related to VHA's Health Care Information Security Program.

3. RELATED ISSUES: VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014; VA Directive 6500, VA Cybersecurity Program, dated January 23, 2019; VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008; VA Directive 6509, Duties of Privacy Officers, dated July 30, 2015; VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, dated March 10, 2015; VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, dated March 12, 2019; VA Handbook 6500.3, Assessment, Authorization and Continuous Monitoring of VA Information Systems, dated February 3, 2014; VHA Directive 1605, VHA Privacy Program, dated September 1, 2017; VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016; VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information, dated April 4, 2019; VHA Handbook 1605.03, Privacy Compliance Assurance Program and Privacy Compliance Monitoring, dated April 13, 2009; VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015; and VHA Handbook 1605.05 Business Associate Agreements, dated July 22, 2014.

4. RESPONSIBLE OFFICE: VHA's Office of Health Informatics (OHI), Health Care Security Requirements (HCSR) Office (10A7) is responsible for the contents and maintenance of this directive.

5. RESCISSIONS: None.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of April 2024. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded. ***NOTE:*** *This VHA directive is to be reviewed annually to ensure compliance with all legislative requirements and remain properly integrated with other VA security policies and procedures.*

CERTIFIED BY:	**BY DIRECTION OF THE UNDER SECRETARY FOR HEALTH:**
/s/ Steven Lieberman, MD, MBA, FACHE Acting Principal Deputy Under Secretary for Health	/s/ Steven Lieberman, MD, MBA, FACHE Acting Principal Deputy Under Secretary for Health

NOTE: *All references herein to VA and VHA documents incorporate by reference subsequent VA and VHA documents on the same or similar subject matter.*

DISTRIBUTION: Emailed to the VHA Publications Distribution List on May 1, 2019.

CONTENTS

HEALTH CARE INFORMATION SECURITY POLICY AND REQUIREMENTS

HEALTH CARE INFORMATION SECURITY POLICY AND REQUIREMENTS

1. PURPOSE

This directive establishes VHA's policy for its Health Care Information Security Program in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. **AUTHORITY:** Title 45, Code of Federal Regulations (CFR) parts 160 and 164.

2. BACKGROUND

a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law (Pub. L.) 104-191, required the Department of Health and Human Services (HHS) develop regulations to ensure that covered entities make secure the electronic protected health information (e-PHI) of individuals. These regulations, referred to as the HIPAA Security Rule, are located at 45 CFR part 160 and subparts A and C of part 164. As the covered entity (CE) within VA responsible for ensuring the security of e-PHI of Veterans, dependents, and beneficiaries, VHA is required to comply with, and implement, the provisions of the HIPAA Security Rule. VHA's Health Care Information Security program, implemented through this VHA directive, serves as VHA's compliance with the HIPAA Security Rule provisions. Additionally, this program complies with the Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. 111-5, which requires business associates of covered entities comply with the HIPAA Security Rule.

b. Through VA's Directive and Handbook 6500 series, VA complies with Federal Information Security Management Act of 2014 (FISMA), Public Law No: 113-283, Chapter 35 of Title 44 United States Code (U.S.C), which requires a framework for addressing risk management in information systems. These directive and handbook series also meet the requirements of the HIPAA Security Rule. VHA implements and complies with FISMA and the HIPAA Security Rule through integration with the VA 6500 series, the VHA's Information Security Program, and this directive.

c. The goal of VHA's Health Care Information Security Program is to provide policy, procedures, guidance, and oversight, designed to ensure the confidentiality, integrity and availability of e-PHI when it is created, received, maintained, or transmitted by VHA; a business associate (BA), other entities within VA; or affiliates. VHA's Health Care Security Requirements (HCSR) Office, which is responsible for this program, works to:

(1) Provide HIPAA subject matter expertise for health care information security policies, procedures, and practices to VHA, the Office of Information & Technology (OI&T), and other BAs;

(2) Ensure compliant health care system security architecture requirements;

(3) Ensure compliant health care application and system development;

(4) Develop, implement, and maintain HIPAA Security Rule compliance assessments and remediation monitoring in alignment with VA's FISMA Risk Management Framework program; and,

(5) Ensure health care information security awareness and outreach in alignment with VA's cybersecurity strategy.

3. DEFINITIONS

a. **Access.** Access is the ability to obtain or use information electronically, (read, write, modify, or communicate data/information for the purpose of performing an official function.

b. **Breach.** For purposes of this directive, "breach" means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under subpart E of 45 CFR Part 164 (i.e., the HIPAA Privacy Rule), which compromises the security or privacy of the PHI, except:

(1) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or a BA, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of 45 CFR Part 164 (i.e., the HIPAA Privacy Rule);

(2) Any inadvertent disclosure by a person who is authorized to access PHI by a CE or a BA to another person authorized to access PHI by the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of 45 CFR Part 164 (i.e., the HIPAA Privacy Rule); or

(3) A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. ***NOTE:*** *See the definition of breach at 45 CFR 164.402. This is a subset of Data Breach under Title 38 of CFR.*

c. **Business Associate.** A business associate (BA) is an entity, including an individual (other than a member of VHA's workforce), company, organization, or another CE, that performs or assists in the performance of a function or activity on behalf of VHA that involves the creating, receiving, maintaining or transmitting of PHI, or that provides to or for VHA certain services as specified in the HIPAA Privacy Rule that involve the disclosure of PHI by VHA. Subcontractors of business associates are also considered business associates. ***NOTE*****:** The HIPAA Security Rule applies only to e-PHI, which is a subset of PHI.

d. **Covered Entity.** A covered entity (CE) is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulations (see

45 CFR parts 160 and 164). VHA is a covered entity because VHA is both a health plan and a health care provider.

e. **Disclosure.** Disclosure is the release, transfer, provision of access to, or divulging in any other manner, of information outside VHA. Once information is disclosed, VHA may retain ownership of the data, such as to a BA, contract, or other written agreement. There are some cases in which VHA may relinquish ownership of the information.

f. **Electronic Protected Health Information.** Electronic Protected Health Information (e-PHI) refers to individually-identifiable health information which is covered under the HIPAA Privacy Rule located at 45 CFR part 160 and part 164 subparts A and E, and is created, received, maintained, or transmitted in electronic form by a covered entity. Users of e-PHI must abide by the HIPAA Security Rule regardless of the type of electronic device when managing or handling e-PHI at rest, being processed, used, transferred, or transmitted electronically.

g. **Health Information.** Health information is any information, including genetic information, whether oral or records in any form or medium, created or received by a health care provider, public health authority, employer, life insurers, school or university, or health care clearinghouse or health plan, that 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 payment for the provision of health care to an individual. Health information includes information pertaining to examinations, medical history, diagnosis, and findings or treatment, including laboratory examination, X-rays, microscopic slides, photographs, prescriptions, and the like.

h. **HIPAA Privacy Rule.** The Department of Health and Human Services, Office for Civil Rights regulation on the Standards for Privacy of Individually Health Identifiable Information promulgated at 45 CFR Part 164, Subpart E.

i. **HIPAA Security Rule.** The HIPAA Security Rule, located at 45 CFR part 160 and part 164 subparts A and C, requires covered entities to maintain reasonable and appropriate safeguards to ensure confidentiality, integrity and availability of all e-PHI under their control.

j. **Individually-Identifiable Information.** Individually-identifiable information is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as individually identifiable health information regardless of how it is retrieved. Individually-identifiable information is a subset of sensitive personal information or personally identifiable information and is protected by the Privacy Act (5 U.S.C. 552a (e)(10)).

k. **Individually-Identifiable Health Information.** Individually-identifiable health information is a subset of health information, including demographic information collected from an individual, that: (1) is created or received by a health care provider, health plan, or health care clearinghouse (e.g., a HIPAA-covered entity, such as VHA);

(2) relates to the past, present, or future physical or mental condition of an individual, or provision of or payment for health care to an individual; and (3) identifies the individual or where a reasonable basis exists to believe the information can be used to identify the individual. ***NOTE:*** *VHA uses the term individually-identifiable health information to define information covered by the Privacy Act and the Title 38 confidentiality statutes, in addition to HIPAA. Individually-identifiable health information does not have to be retrieved by name or other unique identifier to be covered by this directive.*

l. **Personnel.** For the purpose of this directive, the term personnel includes officers and employees of VHA; health care providers; without compensation (WOC) workers; contractors; others employed on a fee basis; medical students and other clinical or health profession trainees; VA employees who are covered under a business associate agreement; and volunteer workers, excluding patient volunteers rendering uncompensated services at the direction of VHA staff. The term does not include Compensated Work Therapy patients.

m. **Use.** Use includes the viewing, sharing, employment, application, utilization, examination, or analysis of information within VHA.

4. POLICY

It is VHA policy to comply with the HIPAA Security Rule by implementing and maintaining an information security program wherever e-PHI is present, through the use of VA's risk management framework (VA Directive and Handbook 6500 series). It is also VHA policy that, as required by HIPAA, this compliance requirement will apply to any entity that handles, processes, or uses e-PHI for which VHA is responsible. This includes all relevant components of VA and any other external partners who function as business associates.

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for ensuring overall VHA compliance with this directive and the HIPAA Security Rule at 45 CFR part 160 and subparts A and E of part 164.

b. **Assistant Deputy Under Secretary for Health, Office of Health Informatics (OHI).** The Assistant Deputy Under Secretary for Health, OHI is responsible for:

(1) Designating, in writing, the HCSR Director as VHA's HIPAA Security Officer, responsible for development, implementation, and monitoring the Health Care Information Security Program.

(2) Ensuring VA and VHA information security policies and procedures are implemented throughout VHA via VHA's Health Care Information Security Program.

(3) Ensuring the HCSR office receives necessary and appropriate funding and staffing to implement a HIPAA compliant VHA Health Care Information Security Program.

c. **Health Care Security Requirements Office Director.** The HCSR Office Director is responsible for:

(1) Performing all e-PHI security duties and responsibilities as designated by VHA's Assistant Deputy Under Secretary for Health, Office of Health Informatics.

(2) As designated in section 5.b.(1), serving as VHA's HIPAA Security Officer.

(3) Representing VHA Leadership and working in collaboration with OI&T Leadership to plan, coordinate, and support the Office of Inspector General's (OIG), FISMA and Federal Information Systems Controls Audit Manual (FISCAM) audits. These audits determine the extent to which VA complies with FISMA/FISCAM requirements as well as applicable standards and guidance issued by the Office of Management and Budget, Department of Homeland Security, and National Institute of Standards and Technology (NIST).

(4) Working in collaboration with internal and external partners and organizations, to achieve VHA's strategic goals and enhance the security of VHA's health care delivery system and administrative processes that benefit the Veteran.

(5) Conveying the technical needs and direction of VHA leadership to VA security teams and OI&T relative to the overall health care environment and provide innovative, architecturally sound standards-based security and privacy solutions to VHA health care line of business.

(6) Overseeing the development, implementation, and monitoring of VHA Health Care Information Security Program's policy and guidance as needed.

(7) Oversee and monitor the implementation and integration of VHA's Healthcare Information Security Program with all VHA and VA processes related to the healthcare line of business and technology.

(8) As requested, reviewing new or pending legislation, in conjunction with VA's Office of General Counsel (OGC), to determine the actual or potential impacts of such legislation on e-PHI security policy and practice in VHA.

(9) Working in collaboration with VHA's Information Access and Privacy (IAP) Office to coordinate investigation of, and response to, complaints received from the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) involving e-PHI.

(10) Advancing and enabling VHA health information exchange by creating interoperable security and privacy technical and vocabulary standards for use within VA and across the nation.

(11) Assessing compliance with the HIPAA Security Rule in VA medical facilities, business associates and other VHA entities through periodic reviews.

d. **Veteran Integrated Service Network Directors and VHA Chief Program Officers.** Veteran Integrated Service Network (VISN) Directors and VHA Chief Program Officers are responsible for:

(1) Ensuring all personnel within their respective facilities or program offices comply with this directive; and e-PHI-related VA policy, Federal statutes, and regulations.

(2) Ensuring all personnel within their respective facilities or program offices are made aware of their responsibility to protect e-PHI, and complete e-PHI-related VA training required by VA Directive 6500 and VHA Directive 1605 before being granted access to e-PHI.

(3) Awareness and oversight of HIPAA compliance assessment remediation activities within their respective facility or program office in a timely and thorough manner.

(4) Assisting HCSR Office Director in the investigation of, and response to, e-PHI security complaints received from HHS OCR.

(5) Seeking subject matter expertise from VHA's Health Care Security Requirements Office on security of e-PHI prior to entering any formal agreements, electronic solution projects, research, or contractual arrangements which involve e-PHI.

e. **VISN Privacy Officers, VHA Facility Privacy Officers and VHA Program Office Privacy Liaisons.** VISN Privacy Officers, VHA Facility Privacy Officers, and VHA Program Office Privacy Liaisons are responsible for:

(1) Collaborating with their respective Information System Security Officer (ISSO) to ensure reasonable and appropriate security controls safeguards are in place to protect the privacy of e-PHI in accordance with VA Directive 6502, VA Enterprise Privacy Program; VA Directive 6509, Duties of Privacy Officers; and VHA Directive 1605, VHA Privacy Program.

(2) Ensuring all complaints and incidents involving e-PHI are reported, investigated, and resolved in accordance with VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information.

(3) Assisting the VHA Health Care Security Requirements Office in the investigation of, and response to, security complaints regarding e-PHI received from HHS OCR as appropriate.

f. **Program Office, Regional Information Security Director (RISO), District Information Security Managers (ISMO), and Information Systems Security Officers (ISSO).** Through a National Business Associate Agreement (BAA) between VA OI&T and VHA, the Program Office, Regional Information Security Director

(RISO)District Information Security Managers (ISMO), and Information Systems Security Officers (ISSO) are responsible for:

(1) Ensuring the HIPAA Security Rule is properly implemented in accordance with this directive.

(2) Conducting continuous monitoring as set forth by VA policy to ensure continued compliance with HIPAA Security Rule standards and specifications.

(3) Ensuring all complaints, incidents, or suspected breaches of e-PHI are investigated and resolved promptly in accordance with the Department's incident response policy.

(4) Conducting security-related reviews for contracts, research project proposals, and affiliate agreements involving e-PHI in accordance with Department and VHA policy.

g. **VA Medical Facility Directors.** The VA medical facility Directors are responsible for:

(1) Ensuring all personnel within their respective facilities are aware of their responsibility to protect e-PHI and comply with e-PHI security requirements especially:

(a) Report all actual or suspected breaches of e-PHI privacy or security in a timely and complete manner to the appropriate privacy or security official, as required by VA Handbook 6500.2.

(b) Seek guidance and advice from their local Privacy Officer and/or ISO to resolve any privacy or security questions or concerns about e-PHI.

(c) Use, disclose, or request the minimum amount of access to e-PHI necessary to perform their specific job function. ***NOTE:*** *The minimum necessary standard does not apply to treatment purposes. For further information, see VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information.*

(d) Complete applicable VA and VHA e-PHI security required trainings in accordance with VA Directive 6500, VA Cybersecurity Program, and VHA Directive 1605, VHA Privacy Program, before being granted access to e-PHI.

(2) Implementing the requirements of the VHA Health Care Information Security Program within their facility.

(3) Ensuring facility related ePHI procedures are consistent with this directive and are distributed to all employees who have access to e-PHI.

(4) Ensuring appropriate security documentation and necessary personnel are available to participate in compliance assessments conducted by the HCSR Office related to e-PHI.

(5) Awareness and oversight of HIPAA compliance assessment remediation activities within their respective facility or program office in a timely and thorough manner.

h. **VHA Personnel.** All VHA personnel are responsible for:

(1) Complying with all Federal and State laws, regulations, and VA and VHA policies relating to security of e-PHI.

(2) Completing all applicable VA- and VHA-required e-PHI security training.

(3) Reporting all actual or suspected breaches of e-PHI security in a timely and complete manner to the appropriate ISO, according to established policy in accordance with VA Handbook 6500.2.

(4) Seeking guidance and advice from their local ISO or privacy officer to resolve any questions or concerns about e-PHI security issues.

(5) Using, disclosing, or requesting the minimum amount of e-PHI necessary to perform their specific job. ***NOTE:*** *The minimum necessary standard does not apply to treatment purposes. For further information, see VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information.*

6. TRAINING

All VA, VHA staff, BA's, affiliates and business partners who have, or will request access to e-PHI must complete all the VA's annual security, privacy, and HIPAA privacy related awareness courses as required by Department and VHA policies.

7. RECORDS MANAGEMENT

All records regardless of format (paper, electronic, electronic systems) created in this directive shall be managed per the National Archives and Records Administration (NARA) approved records schedules found in VHA Records Control Schedule 10-1. If you have any question to the regarding any aspect of records management, you should contact your facility Records Manager or your Records Liaison.

8. REFERENCES

a. 44 U.S.C. 3541-3559, Federal Information Security Modernization Act of 2014.

b. Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA).

c. Public Law 111-5, Health Information Technology for Economic and Clinical Health Act.

d. 45 CFR Parts 160 and 164, HIPAA Security Rule.

e. VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014.

f. VA Directive 6500, VA Cybersecurity Program, dated January 23, 2019.

g. VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008.

h. VA Directive 6509, Duties of Privacy Officers, dated July 30, 2015.

i. VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, dated March 10, 2015.

j. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information, dated March 12, 2019.

k. VA Handbook 6500.3, Assessment, Authorization and Continuous Monitoring of VA Information Systems, dated February 3, 2014.

l. VHA Directive 1605, VHA Privacy Program, dated September 1, 2017.

m. VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.

n. VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information, dated April 4, 2019.

o. VHA Handbook 1605.03, Privacy Compliance Assurance Program and Privacy Compliance Monitoring, dated April 13, 2009.

p. VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015.

q. VHA Handbook 1605.05, Business Associate Agreements, dated July 22, 2014.

r. National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

s. NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.