Department of Veterans Affairs
Veterans Health Administration
Washington, DC 20420

VHA Directive 1605
Transmittal Sheet
September 1, 2017

VHA PRIVACY PROGRAM

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive establishes a Veterans Health Administration (VHA)-wide program for the protection of the privacy of Veterans, their dependents, and beneficiaries in accordance with Federal privacy statutes and regulations. This directive also establishes privacy policies to comply with the Department of Veterans Affairs (VA) Directive 6502.

2. SUMMARY OF MAJOR CHANGES: This VHA directive includes the following changes:

a. Revision and update of policy regarding privacy.

b. Inclusion of a Definitions section.

c. Change of the Office of Informatics and Analytics to Office of Informatics and Information Governance.

d. Addition of responsibilities for Deputy Under Secretary for Health for Operations and Management and VHA Personnel.

3. RELATED ISSUES: VHA Directive 1605.01, VHA Handbook 1605.02, and VHA Handbook 1605.03.

4. RESPONSIBLE OFFICE: The VHA Office of Informatics and Information Governance, Information Access and Privacy Office (10P2C1) is responsible for the contents of this directive. Questions may be referred to the VHA Privacy Officer at 704-245-2492.

5. RESCISSION: VHA Directive 1605, dated April 11, 2012, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last day of September 2022. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

Poonam Alaigh, M.D.
Acting Under Secretary for Health

DISTRIBUTION: Emailed to the VHA Publications Distribution List on September 11, 2017.

CONTENTS

VHA PRIVACY PROGRAM

VHA PRIVACY PROGRAM

1. PURPOSE

This Veterans Health Administration (VHA) directive establishes the responsibility requirements and procedures for compliance with all applicable Federal privacy and confidentiality statutes and regulations. **AUTHORITY:** Freedom of Information Act (FOIA), Title 5 United States Code (U.S.C.) 552, implemented by Title 38 Code of Federal Regulations (CFR), Sections 1.550-1.562; 38 U.S.C. 7332; 38 U.S.C. 5701, implemented by 38 CFR Section 1.500-1.527; 38 U.S.C. 5705; and Public Law 104-191, implemented by 45 CFR Parts 160 and 164 (HIPAA).

2. BACKGROUND

The VHA Privacy Program establishes and implements privacy policies and practices that comply with the requirements of all applicable Federal privacy statutes, regulations, and policies. The main components of the program are: privacy policies, privacy training, use and disclosure of information, individuals' privacy rights, privacy complaints and incidents, notice of privacy practices and privacy compliance monitoring. The focus of the policies and procedures involve individually-identifiable information that is collected, created, transmitted, accessed, used, disclosed, processed, stored, or disposed of by or for VHA. All Individually-identifiable information, on Veterans maintained by VHA, is considered protected health information. Additionally, this includes all records maintained in any medium, including hard copy and electronic format, and in information systems administrated by, or otherwise under the authority or control of, the Department of Veterans Affairs (VA).

3. DEFINITIONS

a. **Business Associate.** A business associate is an entity, including an individual, company, or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receiving, maintenance or transmission of protected health information (PHI), or that provides to or for VHA certain services as specified in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule that involve the disclosure of PHI by VHA. Subcontractors of business associates are also considered business associates.

b. **Compliance.** The term compliance is defined as actual and meaningful adherence to the requirements of any law, regulation, or standard applicable to the activity or practice in question.

c. **Disclosure.** For the purpose of this directive, the term disclosure refers to the release, transfer, provision of access to, or divulging in any other manner information outside VHA. Once information is disclosed VHA may retain ownership of the data such as to a Business Associate, contract or other written agreement. There are some cases in which VHA may relinquish ownership of the information. The exception to this definition is when the term is used in the phrase "accounting of disclosures."

d. **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)).

e. **Personally Identifiable Information.** Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be personally identifiable information. ***NOTE:*** *The term "Personally Identifiable Information" is synonymous and interchangeable with "Sensitive Personal Information".*

f. **Personnel.** For the purpose of this directive, the term personnel includes those officers and employees of VHA; consultants and attending clinicians; without compensation (WOC) employees; Intergovernmental Personal Act (IPA) employees; contractors; others employed on a fee basis; medical students and other trainees; and volunteer workers rendering uncompensated services, excluding patient volunteers, providing a service at the direction of VA staff. ***NOTE:*** *Compensated Work Therapy (CWT) workers are not VHA personnel; they are patients receiving active treatment or therapy.*

g. **Sensitive Personal Information.** Sensitive Personal Information (SPI), with respect to an individual, means any information about the individual maintained by VA, including the following:

(1) Education, financial transactions, medical history, and criminal or employment history; and

(2) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records.

NOTE: *SPI is a subset of VA Sensitive Information/Data.*

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

4. POLICY

It is VHA policy that the VHA Privacy Program be implemented by means of the VHA Privacy Office and monitored for compliance with all applicable Federal privacy and confidentiality statutes and regulations.

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for ensuring overall VHA compliance with this directive.

b. **The Assistant Deputy Under Secretary for Health, Office of Informatics and Information Governance .** The Assistant Deputy Under Secretary for Health, Office of Informatics and Information Governance is responsible for:

(1) Ensuring that VHA-wide privacy policies and procedures are implemented through the VHA Privacy Program and

(2) Ensuring the VHA Privacy Program mission and vision are accomplished by supporting resources, funding, and staffing.

c. **Deputy Under Secretary for Health for Operations and Management.** The Deputy Under Secretary for Health for Operations and Management is responsible for:

(1) Ensuring that VISNs and VHA health care facilities implement VHA -wide privacy policies and procedures issued by the VHA Information Access and Privacy (IAP) Office;

(2) Ensuring that the VISNs cooperate with and respond to requests from VHA IAP timely; and

(3) Ensuring VISN and VHA health care facility compliance with mandated VHA-wide privacy policies, including organizational alignment of Privacy Officers.

d. **VHA Privacy Officer.** The VHA Privacy Officer is responsible for:

(1) Performing all privacy duties and responsibilities as designated by the VA Privacy Service and VHA Assistant Deputy Under Secretary for Health, Office of Informatics and Information Governance;

(2) Developing and implementing a VHA Privacy Program;

(3) Developing, issuing, reviewing, and coordinating privacy policy for VHA in conjunction with policy efforts by VA;

(4) Coordinating requirements and monitoring VHA compliance with all Federal privacy laws, regulations, and guidance;

(5) Establishing requirements for the responsibilities of Veterans Integrated Service Network (VISN) and facility-level Privacy Officers and program office Privacy Liaisons and providing implementation guidance, as needed;

(6) Issuing direction to VISN and facility-level Privacy Officers and program office Privacy Liaisons regarding all aspects of implementing the VHA Privacy Program;

(7) Providing VHA-specific privacy training tools and compliance with the annual training requirement;

(8) Examining new or pending legislation, in conjunction with the VA Office of General Counsel (OGC), to determine the actual or potential impact of such legislation on privacy policy and practice at VHA;

(9) Establishing VHA policy on the reporting, tracking, resolution, and auditing of VHA privacy complaints and incidents;

(10) Ensuring Privacy Officers are aware of the process for recording all actual or suspected breaches of privacy observed or reported at the national level in the tracking system designated by the VA Data Breach Resolution Service (e.g., Privacy and Security Event Tracking System (PSETS));

(11) Ensuring VHA resolves all privacy breaches in a timely fashion and in accordance with applicable law;

(12) Coordinating investigation of and response to privacy complaints received from the Department of Health and Human Services, Office for Civil Rights (HHS OCR), Office of Medical Inspector (OMI) and Office of Special Counsel (OSC);

(13) Maintaining a Notice of Privacy Practices for the VHA health care programs;

(14) Providing expert guidance to VHA field staff in regard to the Privacy Act, title 38 U.S.C. 5701, 5705, and 7332, HIPAA Privacy Rule, Health Information Technology for Economic and Clinical Health Act (HITECH) and other applicable Federal privacy laws;

(15) Creating and supporting a compliance monitoring function within VHA that includes conducting independent performance audits of VHA health care facility's compliance with the VHA Privacy Program;

(16) Ensuring Business Associates are periodically monitored to confirm their compliance with the terms of their Business Associate Agreement (BAA) with VHA; and

(17) Reporting compliance-monitoring findings to VHA leadership at a minimum annually.

e. **VISN Directors and Chief Program Officers.** VISN Directors and Chief Program Officers are responsible for:

(1) Ensuring compliance within their respective facilities and programs with all internal and external requirements including Federal statutes and regulations, VA regulations and policies, and VHA policies relating to privacy;

(2) Ensuring policies and procedures consistent with policies contained in this directive are established within their respective programs and distributed to all personnel;

(3) Ensuring that all personnel within their respective facilities complete privacy training in accordance with VHA privacy policy before they are granted access to any individually-identifiable information and that personnel receive the privacy training annually;

(4) Implementing the requirements of the VHA Privacy Program as it applies to their respective facilities and programs;

(5) Designating an individual with privacy experience which may include certification such as Certified Information Privacy Professional (CIPP) to serve as the VISN Privacy Officer or Program Office Privacy Liaison to provide guidance and oversight to ensure compliance with privacy regulations for their respective programs; and

(6) Ensuring that all personnel within their respective facilities and programs are timely and thorough in completing all monitoring and remediation activities as requested by VHA IAP.

f. **Program Office Privacy Liaisons.** The Program Office Privacy Liaison is responsible for:

(1) Developing program office privacy practices consistent with the VHA Privacy Program;

(2) Conduct privacy assessments of all program office programs or activities on a schedule set forth by the VHA Privacy Compliance Assurance (PCA) Office to ensure compliance with program office privacy policies;

(3) Providing guidance to the program office on all privacy-related matters such as the Privacy Act, FOIA, HIPAA Privacy Rule, and title 38 confidentiality statutes, and seeking guidance and advice from VHA IAP to resolve any questions or concerns about privacy-related issues;

(4) Ensuring that the program office responds to requests from the VHA IAP by the required deadline;

(5) Ensuring that all complaints, incidents and actual or suspected breaches of privacy are recorded (by the Privacy Liaison or other responsible party, as appropriate to the circumstances) within one hour in the tracking system (e.g., PSETS) designated by the VA Data Breach Resolution Service and these complaints, incidents and actual or suspected breaches of privacy must also be investigated and resolved in coordination with VHA IAP;

(6) Coordinating with VHA IAP on any Memorandums of Understanding/Agreement (MOU/MOA) or Data Use Agreements (DUA) when sharing personally identifiable information with an outside entity;

(7) Assisting with issues resulting from the review of presentation material by the VHA Privacy Office to ensure compliance as required by VA or VHA policy; and

(8) Tracking privacy training annually and reporting the compliance to IAP upon request.

g. **VISN Privacy Officer.** The VISN Privacy Officer is responsible for:

(1) Developing VISN privacy policies consistent with the VHA Privacy Program;

(2) Conducting privacy assessments of all VISN-level programs on a schedule set forth by VHA IAP to ensure compliance with VISN privacy policies and monitoring that the facility Privacy Officers are conducting their Facility Self-Assessment (FSA) quarterly at the facility-level as required by VHA IAP;

(3) Providing expert privacy guidance to each VISN facility and VISN staff on all privacy related matters such as the Privacy Act, FOIA, HIPAA Privacy Rule, and title 38 confidentiality statutes, and seeking guidance and advice from the VHA Privacy Office to resolve any questions or concerns about privacy-related issues;

(4) Ensuring that the VISN office and all facilities within the VISN respond to requests from VHA IAP by the required deadline;

(5) Ensuring that all complaints, incidents and actual or suspected breaches of privacy are reported (by the VISN Privacy Officer or other responsible party, as appropriate to the circumstances) within one hour to the tracking service designated by the VA Privacy Service and these complaints, incidents and actual or suspected breaches of privacy must be investigated and resolved;

(6) Monitoring facility Privacy Officers within their respective VISN to ensure they are completing Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), contract reviews and Business Associate Agreements (BAA) for facility-level systems and agreements, and reporting any deficiencies to the appropriate Medical Center Director;

(7) Conducting privacy-related reviews, such as contract security reviews for VISN-level contracts, and VISN privacy presentation or publication reviews as required by VA or VHA policy;

(8) Ensuring a BAA is in place for VISN-level contracts or other agreements (e.g., MOU/ISA) involving the disclosure of personally identifiable information (PII) to the contractor or other outside entity; and

(9) Partnering with new Privacy Officers within their VISN to ensure that they have the necessary resources and training to build a privacy program.

h. **VA Medical Center Director.** The VA Medical Center Director is responsible for:

(1) Designating an individual with privacy experience which may include Certified Information Privacy Professional (CIPP) or other related experience, to serve as the Privacy Officer;

(2) Ensuring compliance within the facility with all Federal laws, regulations, VA regulation and policies, and VHA policies relating to privacy;

(3) Ensuring facility policies and procedures consistent with policies contained in this directive are established and distributed to all employees;

(4) Ensuring that all personnel within the facility obtain privacy training before they are granted access to any individually-identifiable information, and that personnel receive the follow-up privacy training periodically;

(5) Ensuring that all personnel within the facility obtain annual privacy training in accordance with applicable requirements and VHA privacy policy;

(6) Implementing the requirements of the VHA Privacy Program as it applies to VHA facilities;

(7) Ensuring that all complaints, incidents and actual or suspected breaches of privacy are recorded (by the Privacy Officer or other responsible party, as appropriate to the circumstances) within one hour in the tracking system designated by the VA Data Breach Resolution Service (e.g., PSETS);

(8) Ensuring the facility Privacy Officer completes PTAs, PIAs, contract reviews and BAAs for facility-level systems and agreements;

(9) Ensuring that the facility Privacy Officer is conducting the FSA quarterly as required by VHA IAP; and

(10) Making their facility, documentation and personnel available for assessment by VHA Privacy Compliance Assurance and ensuring that personnel within the facility are timely and thorough in completing remediation activities as requested by VHA IAP.

i. **Facility Privacy Officer.** The facility Privacy Officer is responsible for:

(1) Reporting directly to the facility Director or Associate Director for responsibilities as the designated facility Privacy Officer(s) and for activities of the facility Privacy Program;

(2) Performing duties as needed to ensure a robust, effective and compliant facility privacy program, including training, monitoring, analysis, or other specific responsibilities outlined in VA or VHA privacy policies;

(3) Using the facility privacy policy template to develop facility privacy policies consistent with the VHA Privacy Program;

(4) Reviewing or auditing all programs at the facility and outlying Community Based Outpatient Clinics quarterly to ensure compliance with national and facility privacy policies;

(5) Completing and submitting the FSA quarterly as required by VHA IAP;

(6) Providing all documentation and other materials for assessment by VHA Privacy Compliance Assurance timely and completing remediation activities as requested by the VHA IAP;

(7) Providing expert guidance to the facility on all privacy-related matters, such as the Privacy Act, FOIA, HIPAA Privacy Rule, and title 38 confidentiality statutes, and seeking guidance and advice from their VISN privacy officer or privacy liaison to resolve any questions or concerns about privacy-related issues;

(8) Ensuring that the facility responds to requests from the VHA IAP by the required deadline;

(9) Ensuring that all complaints, incidents and actual or suspected breaches of privacy of Individually-identifiable information are reported within 1 hour to the tracking service designated by the VA Data Breach Resolution Service (e.g. PSETS) and these complaints, incidents and actual or suspected breaches of privacy are investigated and resolved;

(10) Conducting privacy-related reviews, such as contract security reviews, PTAs, PIAs, BAAs, facility walk through assessments, privacy presentation or publication reviews and research protocol privacy reviews, as required by VA or VHA policy;

(11) Reviewing any MOU/MOA or DUA when sharing or disclosing facility-level personally identifiable information with an outside entity; and

(12) Ensuring that the facility complies with all corresponding privacy directives associated with this policy.

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

(1) Complying with all Federal laws and regulations, VA regulations and policies, national VHA policies and local (VISN, program office and/or facility) policies relating to privacy;

(2) Completing all applicable VA- and VHA-required privacy training at the time of employment, annually thereafter, and as directed when changes are made to update the required training;

(3) Reporting all actual or suspected breaches of privacy in a timely and complete manner to the appropriate privacy official, according to established policy;

(4) Seeking guidance and advice from their local Privacy Officer or Privacy Liaison to resolve any questions or concerns about privacy-related issues;

(5) Ensuring privacy authority exists, which may require consultation with an appropriate privacy official, prior to sharing or disclosing PII outside VA; and

(6) Using, disclosing, or requesting the minimum amount of individually-identifiable information necessary to perform their specific job function. The minimum necessary standard does not apply to treatment purposes.

6. REFERENCES

a. 38 U.S.C. 5701.

b. 38 U.S.C. 5705.

c. 38 U.S.C. 7332.

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

e. FOIA, 5 U.S.C. 552.

f. Privacy Act, 5 U.S.C. 552a.

g. VA Directive 6502, VA Enterprise Privacy Program.

h. VHA Directive 1605.01, Privacy and Release of Information.

i. VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information.

j. VHA Handbook 1605.03, Privacy Compliance Assurance Program and Privacy Compliance Monitoring.