VHA PRIVACY PROGRAM

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

2. SUMMARY OF CONTENTS/ MAJOR CHANGES. This VHA Directive sets forth:

a. Policy for the VHA Privacy Program. This policy requires VHA-wide compliance with all applicable privacy laws, regulations, Executive Orders and implementation policies, directives, and handbooks:

b. Responsibilities for implementing, managing and monitoring the VHA Privacy Program; and

c. References related to the VHA Privacy Program.

3. RELATED HANDBOOKS. VHA Handbook 1605.1, VHA Handbook 1605.2, and VHA Handbook 1605.03.

4. RESPONSIBLE OFFICE. The VHA Office of Informatics and Analytics, 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. RESCISSIONS. VHA Directive 1605, dated March 17, 2005, is rescinded.

6. RECERTIFICATION. This VHA Directive is scheduled for recertification on or before the last day of April 30, 2017.

Robert A. Petzel, M.D.
Under Secretary for Health

DISTRIBUTION: E-mailed to the VHA Publications Distribution List 4/12/2012

VHA PRIVACY PROGRAM

1. PURPOSE: This VHA Directive provides policy and responsibilities for the VHA Privacy Program and covers the responsibilities and requirements for compliance with all applicable Federal confidentiality statutes and regulations.

2. BACKGROUND: The goal of the VHA Privacy Program is to establish and implement privacy policies and practices that comply with the requirements of all applicable Federal privacy statutes, regulations, and policies.

a. The VHA Privacy Program addresses privacy policies, privacy training, use, and disclosure of information, individuals' privacy rights, privacy complaints, notice of privacy practices, and privacy compliance monitoring.

b. The VHA Privacy Program applies to sensitive personal information (SPI) that is collected, created, transmitted, used, disclosed, processed, stored, or disposed of by, or for, VHA and that is maintained in any medium, including hard copy, electronic format, and by information systems administrated by, or otherwise under the authority or control of, the Department of Veterans Affairs (VA). Individually-identifiable information is a subset of SPI.

3. POLICY: It is VHA policy that a VHA Privacy Program must be implemented through the VHA Privacy Office and monitored through the Privacy Compliance Assurance (PCA) Office within the Office of Informatics and Analytics.

4. RESPONSIBILITIES

a. **The Assistant Deputy Under Secretary for Health for Informatics and Analytics.** The Assistant Deputy Under Secretary for Health for Informatics and Analytics is responsible for:

(1) Ensuring that Department and Administration-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.

b. **VHA Privacy Officer.** The VHA Privacy Officer, or designee, 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 for Informatics and Analytics.

(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) Monitoring VHA compliance with all Federal privacy laws and regulations.

(5) Establishing responsibilities for Veterans Integrated Service Network (VISN) and facility-level Privacy Officers; issuing direction regarding all aspects of implementing the VHA Privacy Program; and providing implementation guidance, as needed to facility-level Privacy Officers and program office Privacy Liaisons.

(6) Providing VHA-specific privacy training tools and monitoring compliance with the annual training requirement.

(7) 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.

(8) Establishing VHA policy on the reporting, tracking, resolution, and auditing of VHA privacy violations and complaints.

(9) Ensuring that all complaints and actual or suspected breaches of privacy of SPI are recorded within 1 hour of notification during business hours, and as soon as possible outside of normal business hours, in the tracking system designated by the VA Privacy Service.

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

(11) Coordinating investigation of and response to privacy complaints received from the Department of Health and Human Services, Office for Civil Rights.

(12) Maintaining a Notice of Privacy Practices for VHA health care programs.

(13) Providing expert guidance to VHA field staff in regard to the Privacy Act, Title 38 United States Code (U.S.C.) 5701, 5705, and 7332; the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule; and other applicable Federal privacy laws.

(14) Conducting assessments of each VHA health care facility's compliance with the privacy program at a minimum of every 3 years.

(15) Monitoring Business Associates to ensure their compliance with the terms of their Business Associate Agreements (BAA) with VHA.

(16) Reporting compliance-monitoring findings from the VHA PCA Office, at least annually, to VHA leadership.

c. **VISN Directors and Chief Program Officers.** Each VISN Director and Chief Program Officer is responsible for:

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

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

(3) Ensuring that all personnel within their respective facilities and programs complete privacy training annually, in accordance with applicable requirements and VHA privacy policy, before being granted access to any individually-identifiable information; and that appropriate personnel, periodically, receive follow-up privacy training.

(4) Designating an individual with privacy experience to serve as the VISN Privacy Officer or as the Program Office Privacy Liaison to provide oversight in ensuring compliance with privacy regulations.

(5) Ensuring that all remediation activities, as requested by the VHA PCA Office, are completed in a timely and thorough manner.

d. **Program Office Privacy Liaison.** The Program Office Privacy Liaison is responsible for:

(1) Developing program office privacy policies consistent with the VHA Privacy Program.

(2) Conducting privacy assessments of all program office programs and activities on a schedule set forth by the VHA PCA Office to ensure compliance with program office privacy policies.

(3) Providing expert guidance to the program office on all privacy-related matters such as the Privacy Act (PA), Freedom of Information Act (FOIA), HIPAA Privacy Rule, and Title 38 confidentiality statutes.

(4) Seeking guidance and advice from the VHA Information Access and Privacy Office to resolve any questions or concerns about privacy-related issues.

(5) Ensuring that the program office responds to requests from the VHA Information Access and Privacy Office or the VHA Privacy Compliance Assurance Office by the required deadline.

(6) Ensuring that all complaints and actual or suspected breaches of privacy of SPI are recorded within 1 hour of notification during business hours, and as soon as possible outside of normal business hours, in the tracking system designated by the VA Privacy Service.

(7) Ensuring all complaints and actual or suspected breaches of privacy are investigated and resolved.

(8) Conducting privacy-related reviews, such as contract security reviews for Program Office contracts, as required by VA or VHA policy.

(9) Reviewing presentation material to ensure compliance with VA or VHA policy.

e. **VISN Privacy Officers.** 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 the VHA PCA Office to ensure compliance with VISN privacy policies.

(3) Ensuring that the facility Privacy Officers are conducting the Facility Self Assessment quarterly as required by VHA PCA Office.

(4) Providing expert privacy guidance to each VISN facility and VISN staff on all privacy related matters such as the PA, FOIA, HIPAA Privacy Rule, and Title 38 confidentiality statutes.

(5) Seeking guidance and advice from the VHA Information Access and Privacy Office to resolve any questions or concerns about privacy-related issues.

(6) Ensuring that the VISN office and all facilities within the VISN respond to requests from the VHA Information Access and Privacy Office by the required deadline.

(7) Ensuring that all complaints and actual or suspected breaches of privacy of SPI are recorded within 1 hour of notification during business hours, and as soon as possible outside of normal business hours, in the tracking system designated by the VA Privacy Service.

(8) Ensuring all complaints and actual or suspected breaches of privacy are investigated and resolved.

(9) Conducting privacy-related reviews, such as contract security reviews for VISN-level contracts, and VISN privacy presentation or publication reviews with VA or VHA policy.

f. **Medical Facility Director.** The Medical Facility Director is responsible for:

(1) Ensuring compliance within the facility of all Federal laws and regulations, and VA and VHA policies relating to privacy, including implementation of the VHA Privacy Program as it applies to the facility.

(2) Ensuring facility policies and procedures, consistent with policies contained in this Directive, are established and distributed to all employees.

(3) Ensuring all employees are aware of the necessity of:

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

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

(c) Using, disclosing, or requesting the minimum amount of SPI necessary to perform their specific job function. ***NOTE:*** *The minimum necessary standard does not apply to treatment purposes.*

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

(5) Ensuring that all complaints and actual or suspected breaches of privacy of SPI are recorded within 1 hour of notification during business hours, and as soon as possible outside of normal business hours, in the tracking system designated by the VA Privacy Service.

(6) Ensuring that documentation and personnel are available for assessment by the VHA PCA Office.

(7) Ensuring remediation activities, as requested by the VHA PCA Office, are completed in a timely and thorough manner.

(8) Ensuring facility compliance this Directive.

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

(1) Reporting directly to the facility Director or Associate Director for responsibilities 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, and other specific responsibilities outlined in VHA policy.

(3) Developing facility privacy policies consistent with the VHA Privacy Program.

(4) Auditing all programs at the facility and affiliated community-based outpatient clinics quarterly to ensure compliance with facility privacy policies.

(5) Providing expert guidance to the facility on all privacy-related matters, such as the PA, FOIA, HIPAA Privacy Rule, and Title 38 confidentiality statutes.

(6) Seeking, as needed and appropriate, guidance and advice from the VISN Privacy Officer or Program Office Privacy Liaison to resolve any questions or concerns relating to privacy-related issues.

(7) Ensuring the facility responds to deadlines requested from the VHA Information Access and Privacy Office.

(8) Ensuring that all complaints and actual or suspected breaches of privacy of SPI are recorded within 1 hour of notification during business hours, and as soon as possible outside of normal business hours, in the tracking system designated by the VA Privacy Service.

(9) Conducting privacy-related reviews, such as contract security reviews, privacy impact assessments, facility walk-through assessments, privacy presentation or publication reviews, and research protocol privacy reviews, as required by VA or VHA policy.

5. REFERENCES

a. Title 5 U.S.C. 552, Freedom of Information Act (FOIA).

b. Title 5 U.S.C. 552a, Privacy Act.

c. Title 38 U.S.C. 5701.

d. Title 38 U.S.C. 5705.

e. Title 38 U.S.C. 7332.

f. Title 38 U.S.C. §§ 5721-28.

g. Title 45 Code of Federal Regulations Parts 160 and 164.

h. VA Directive 6502.

6. DEFINITIONS

a. **Access.** Access is the obtaining or using of information, electronically, on paper or other medium, for the purpose of performing an official function

b. **Compliance.** For the purpose of this Directive, the term "compliance" means the act of satisfying all requirements of policies, procedures, directives, and laws.

c. **Disclosure.** Disclosure is 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. **Health Information.** Health information is any information created or received by a health care provider 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.

e. **Individually-identifiable Information.** Individually-identifiable information is any information, including health information maintained by VHA, pertaining to an individual that

also identifies the individual and, except for individually-identifiable health information, is retrieved by the individual's name or other unique identifier. Individually-identifiable health information is covered regardless of whether or not the information is retrieved by name.

f. **Minimum Necessary Standard.** The Minimum Necessary Standard is the minimum necessary amount of data, including paper and electronic data, that VHA personnel may use or disclose.

g. **Personnel.** For the purpose of this Directive, the term "personnel" includes those VHA officers and employees; 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.*

h. **Sensitive Personal Information (SPI).** SPI, with respect to an individual, means any information about the individual maintained by an agency including the following: education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace the individual's identity, including: name, social security number (SSN), date of birth, mother's maiden name, or biometric records.

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

j. **VHA Notice of Privacy Practices.** VHA Notice of Privacy Practices describe how medical information about an individual may be used or disclosed and how an individual can obtain access to this information.