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, as well as 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 VA-wide compliance with all applicable privacy laws, regulations, Executive Orders and implementation policies, guidance, directives, and handbooks.

b. Provision of the Freedom of Information Act, Privacy Act, Title 38 United States Code (U.S.C.) (U.S.C. Sections 5701, 5705, 7332), and Standard of Privacy of Individually-Identifiable Health Information, 45 Code of Federal Regulations (CFR) Parts 160 and 164, hence Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

c. Responsibilities for implementing and managing the VHA-wide Privacy Program; and

d. References related to the VHA Privacy Program.

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

4. RESPONSIBLE OFFICE. The VHA Office of Health Data and Informatics (19F) is responsible for the contents of this Directive. Questions may be referred to the VHA Privacy Officer at 727-320-1839.

5. RESCISSIONS. None.

6. RECERTIFICATION. This VHA Directive is scheduled for recertification on or before the last day of March 2010.

S/ Jonathan Perlin, MD, PhD, MSHA, FACP
Acting Under Secretary for Health

DISTRIBUTION: CO: E-mailed 3/22/2005
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 3/22/2005

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 Federal confidentiality laws and regulations.

2. BACKGROUND: The VHA Privacy Program applies to:

a. Personal data that identifies an individual (herein referred to as "individually-identifiable information") that is collected, created, transmitted, used, processed, stored, or disposed of by or for VHA; and

b. VHA components pertaining to all individually-identifiable information, which is maintained in any medium, including hard copy, microfilm, and electronic format and by information systems administrated by, or otherwise under the authority or control of, the Department of Veterans Affairs (VA).

3. POLICY: It is VHA policy that a VHA-wide Privacy Program be implemented through the VHA Privacy Office in the Office of Health Data and Informatics.

4. RESPONSIBILITIES

a. **VHA Chief Health Informatics Officer (CHIO).** The VHA CHIO is responsible for:

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

(2) Seeking technical guidance and requirements for the protection of all privacy–protected data from the VA Privacy Service for the development and approval of cyber security acquisitions, budgeting, and funding.

b. **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 CHIO;

(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 compliance with all Federal privacy law, regulations, and guidance with VHA;

(5) Issuing direction to facility-level Privacy Officers regarding all aspects of implementing the VHA Privacy Program;

(6) Establishing requirements for the responsibilities of facility-level Privacy Officers and providing implementation guidance, as needed;

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

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

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

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

(11) Reporting all actual or suspected breaches of privacy of individually-identifiable information observed or received at the national level to the tracking service designated by the VA Privacy Service;

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

(13) Maintaining a Notice of Privacy Practices; and

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

c. **Veterans Integrated Service Network (VISN) Director and Chief Program Officers.** The VISN Directors and Chief Program Officers are responsible for:

(1) Ensuring compliance within their respective programs with all Federal laws, regulations, VA regulation and policies, and VHA policies relating to privacy;

(2) Ensuring that all personnel within their respective programs attend annual privacy training in accordance with applicable requirements and VHA privacy policy;

(3) Ensuring that all personnel within their respective programs attend privacy training before they are granted access to any individually–identifiable information, and that personnel receive the follow-up privacy training periodically;

(4) Implementing the requirements of the VHA Privacy Program; and

(5) Designating an individual to provide guidance and oversight to ensure compliance with privacy regulations for their respective programs.

d. **Medical Center Director.** The Medical Center Director is responsible for:

(1) Ensuring there is a Privacy Officer at the facility; and

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

e. **Privacy Officer.** The Privacy Officer is assigned responsibility for:

(1) Developing facility privacy policies consistent with national privacy policies and monitoring compliance with such privacy policies;

(2) Reviewing or auditing all programs at the facility on a periodic basis to determine which programs collect, maintain, and store individually-identifiable information in order to ensure compliance with facility privacy policies;

(3) Reporting, in a timely manner, all actual or suspected breaches of privacy of all individually-identifiable information to the tracking service designated by the VA Privacy Service; and

(4) Providing expert guidance to the facility on all privacy related matters such as Privacy Act (PA), Freedom of Information Act (FOIA), HIPAA and 38 U.S.C.

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

(1) Complying with all Federal laws and regulations, VA regulations and policies, and VHA policies relating to privacy;

(2) Completing privacy training at the time of employment, annually thereafter, and within 6 months of a significant change in Federal law and regulation or VHA privacy policy;

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

(4) Using, disclosing, or requesting individually-identifiable information to the minimum amount necessary required to perform their specific job function and to accomplish the intended purpose of the use, disclosure, or request.

5. REFERENCES

a. Title 38 U.S.C. 5701.

b. Title 38 U.S.C. 5705.

c. Title 38 U.S.C. 7332.

d. Title 38 Code of Federal Regulations (CFR) §§1.500-527.

e. Title 38 CFR §§17.500-511.

f. Title 38 CFR §§1.460-496.

g. Title 38 CFR §§1.550-557.

h. Title 38 CFR §§1.575-582.

i. Title 45 CFR, Parts 160 and 164.

j. Public Law 104-191.

k. Office of Management and Budget (OMB) Circular A-130, Appendix I.

l. VA Directive 6502

6. DEFINITIONS

a. **Compliance.** For the purpose of this Directive, the term "compliance" means the act of complying with policies, procedures, directives, laws, and other legal guidance.

b. **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.

c. **Personnel**. For the purpose of this Directive, the term "personnel" includes those officers and employees of the Department; consultants and attending clinicians; without compensation (WOC) 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.*

d. **VHA Privacy Program.** The VHA Privacy Program is the effort within VHA to establish and implement privacy policies and practices that comply with the requirements of all applicable Federal privacy laws and regulations, VA regulations and VA privacy policies. The VHA Privacy Program at a minimum should address privacy policies, privacy training, use and disclosure of information, individual's privacy rights, privacy complaints, notice of privacy practices and privacy compliance monitoring.