Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6066
Transmittal Sheet
April 2, 2008

PROTECTED HEALTH INFORMATION (PHI)

1. REASON FOR ISSUE: This Directive sets policies, roles, and responsibilities for VA components that enter into Business Associate Agreements (BAAs) and Memoranda of Understanding (MOUs) that cover the handling of Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive sets forth policies and responsibilities for the protection and safeguard of PHI and EPHI. This policy requires compliance, where appropriate, with regulations issued by the Department of Health and Human Services, as mandated by HIPAA, 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule").

3. RESPONSIBLE OFFICE: Office of the Assistant Secretary for Information and Technology (005), Office of Privacy and Records Management.

4. RELATED HANDBOOKS: VHA Handbook 1605.1, Privacy and Release of Information; VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information; VHA Handbook 1600.01, Business Associate Agreements; VA Handbook 6500, Information Security Program.

5. RESCISSIONS: None.

CERTIFIED BY:

/S/
Robert T. Howard
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/S/
Robert T. Howard
Assistant Secretary for
Information and Technology

Distribution: Electronic Only

PROTECTED HEALTH INFORMATION

1. PURPOSE AND SCOPE

a. This Directive establishes the policies and responsibilities for compliance with regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule").

b. The provisions of this Directive apply to all Department of Veterans Affairs (VA) components with a Business Associate Agreement (BAA) or Memorandum of Understanding (MOU) with Veterans Health Administration (VHA), or other Covered Entity, that pertain to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI). VA components meeting these criteria are herein referred to as "Business Associates." The provisions of this Directive do not apply to:

(1) PHI or EPHI provided to a non-covered entity under authority of 45 CFR 164.512(k)(1)(iii); or

(2) Official investigations by the Office of Inspector General.

c. HIPAA is the outcome of the health care initiatives of the early 1990s. The legislation was designed to combat fraud and waste, promote medical savings accounts, improve access to long-term care services and coverage, simplify the administration of health insurance, and ensure the privacy and security of health information. The legislation required the promulgation of rules on privacy, electronic transactions, code sets, security, and standard unique identifiers for payers and standard unique identifiers for providers.

d. Generally, the same rules on privacy apply across VA. However, with the passage of the HIPAA of 1996, there is a distinction between the VHA and VA in regards to privacy practices. VHA, as a health plan and health care provider, is considered to be a "Covered Entity" under HIPAA.

e. Although VHA is the Covered Entity under HIPAA, other VA Administrations and Staff Offices may have access to PHI and EPHI in the course of providing benefits and services to veterans through a BAA or MOU with the Covered Entity. A BAA or MOU must be in place in order for a Covered Entity to disclose PHI or EPHI to an organization that is not a Covered Entity, unless the transaction is provided under the authority of Title 45 CFR 164.512(k)(1)(iii) and used to adjudicate claims processed under Title 38 CFR.

f. When the phrase “Protected Health Information” and the abbreviation “PHI” are used in this Directive, they include the phrase “Electronic Protected Health Information” and the abbreviation “EPHI”. Other terms not specifically defined within this Directive should be considered to reflect the definition found in a widely accepted dictionary.

2. POLICY. Adherence to Agreements. All Business Associates will fully understand and adhere to all obligations and requirements set forth in such agreements. Failure to comply with all aspects of such agreements can result in non-compliance with Federal law, which carries penalties for VA and potentially for individual(s) responsible for non-compliance. The requirements set forth within the agreement must be followed.

3. RESPONSIBILITIES

a. **The Assistant Secretary for Information and Technology.** The Assistant Secretary for Information and Technology, as the VA Chief Information Officer (CIO), is the identified security official who is responsible for the development and implementation of the policies and procedures as required by 45 CFR Part 164, Subpart C, §164.306 (a)(2), and the designated privacy official who is responsible for the development and implementation of the policies and procedures as required by 45 CFR Part 164, Subpart E, §164.530 (a)(1)(i). The CIO shall establish department-wide requirements, and provide oversight and guidance related to the protection of personally identifiable information including PHI throughout VA.

b. **The Deputy Assistant Secretary (DAS), Office of Information Protection and Risk Management.** The DAS, Office of Information Protection and Risk Management shall ensure department-wide compliance with privacy and records management law, policies, and standards.

c. **The Associate Deputy Assistant Secretary (ADAS) , Office of Privacy and Records Management.** The ADAS for Privacy and Records Management shall advise the DAS for Information Protection and Risk Management, as well as, the VA Assistant Secretary for Information and Technology, Under Secretaries, Assistant Secretaries, and Other Key Officials on privacy policy compliance; effective privacy practices and security controls over VA information systems; and other matters relevant to protecting all personally identifiable information including PHI, and all information systems carrying said data.

d. **Director, Privacy Service**. The Director shall:

(1) Perform all privacy duties and responsibilities as designated by the Associate Deputy Assistant Secretary for Privacy and Records Management; and

(2) Provide technical guidance to Under Secretaries, Assistant Secretaries, and Other Key Officials regarding requirements for the protection of all personally identifiable information, including PHI.

e. **The Associate Deputy Assistant Secretary (ADAS) for Cyber Security.** The ADAS for Cyber Security shall:

(1) Perform all security duties and responsibilities as designated by the Assistant Secretary of Information and Technology;

(2) Advise the VA Assistant Secretary of Information and Technology, Under Secretaries, Assistant Secretaries, and Other Key Officials on security policy compliance; effective security practices and controls for VA information systems; and other matters relevant to protecting all personally identifiable information including PHI, and all information systems carrying said data;

f. **The General Counsel**. This Office is responsible for:

(1) Interpreting applicable laws, regulations, and Directives;

(2) Rendering legal opinions on the compliance of each Administration or staff office with applicable laws, regulations and Directives; and

(3) Rendering legal advice and services regarding privacy and security issues to Under Secretaries, Assistant Secretaries, and other key officials.

g. **Under Secretaries, Assistant Secretaries, and Other Key Officials.**

(1) Ensure that Business Associates comply with Federal laws, regulations, policies and procedures associated with this Directive;

(2) Establish procedures and rules of conduct necessary to implement this Directive to ensure compliance with applicable privacy mandates;

(3) Ensure the Covered Entity receives notification within one hour of an incident involving PHI and that the Covered Entity is provided a written incident report within twenty-four hours, or as stipulated in the agreement, whichever is shorter;

(4) Provide an inventory of all employees, contractors, subcontractors or agents of the Business Associate that have access to PHI under a BAA or MOU to the organization's Privacy and Information Security Officers. Inventories shall not include personal information beyond an individual's full name;

(5) Provide to the organization's Privacy and Information Security Officers within 30 days of any change to the inventory of employees, contractors, subcontractors or agents of the Business Associate that have access to PHI under the BAA found in VHA Handbook 1601, Appendix B or through a negotiated MOU along with the details of said change; and

(6) Track and report numbers of employees, contractors, subcontractors or agents of the Business Associate that have received VHA Privacy Policy Training, or equivalent, to the organization's Privacy Officer, at their request.

h. **Privacy Officers.** Privacy Officers shall:

(1) Ensure that Under Secretaries, Assistant Secretaries, and Other Key Officials receive adequate notification of when to report training numbers for employees that have access to PHI under the BAA found in VHA Handbook 1601, Appendix B or through a negotiated MOU; and

(2) Identify and implement mechanisms to ensure all employees that are identified in the inventory as having access to PHI have received the VHA Privacy Policy Training or equivalent.

i. **Information Security Officers.** Information Security Officers shall identify and implement mechanisms to ensure all employees that are identified in the inventory as having access to PHI have received annual security awareness training.

j. **Business Associates.** As users of VA systems with access to PHI and EPHI, all employees, contractors, subcontractors, volunteers, interns, or any other agent of the Business Associates shall:

(1) Sign the BAA found in VHA Handbook 1600.01, Business Associate Agreements, Appendix B or other Statement of Understanding and/or Rules of Behavior. This agreement will provide a comprehensive understanding of their responsibilities as they relate to protection and confidentiality of PHI;

(2) Comply with VA Handbook 6500, Information Security Program;

(3) Access records containing PHI only when the information is needed to carry out their official duties related to the services being performed under the agreement;

(4) Disclose PHI only in accordance with applicable laws, regulations, and VA policies and procedures;

(5) Take VHA's Privacy Policy Training, or equivalent, on an annual basis;

(6) Take security awareness training on an annual basis; and

(7) Report all actual or suspected incidents involving PHI to their Privacy Officer immediately upon discovery of the incident.

(8) Comply with VA and VHA policy as it relates to personnel suitability and security program requirements for background screening of both employees and non-employees who have access to VA information systems and data.

4. REFERENCES

a. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191, 42 USC § 201 et seq.

b. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 CFR Parts 160 and 164.

c. Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II), Security Rule, 45 CFR Parts 160, 162, and 164

d. Privacy Act of 1974, 38 CFR 1.575-582, 5 U.S.C.552 a.

e. VA Directive 6300, Records and Information Management

f. VA Directive 6500, Information Security Program

g. VA Directive 6502, VA Privacy Program

h. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA)

i. VA Handbook 6300.5; 6300.5/1, Procedures for Establishing and Managing Privacy Act Systems of Records.

j. VA Handbook 6502.1, Privacy Violation Tracking System (PVTS)

k. VHA Directive 0710, Personnel Suitability and Security Program

l. VHA Directive 1605, VHA Privacy Program

m. VHA Directive 2003-025, Confidential Communications

n. VHA Handbook 1600.01, Business Associate Agreements

o. VHA Handbook 1605.1, Privacy and Release of Information

p. VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information

5. DEFINITIONS

a. **Business Associate.** A person who or entity that is not an employee or volunteer of, or intern or other student sponsored by the Covered Entity who, on behalf of the Covered Entity, performs or assists in the performance of:

(1) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or

administration, utilization review, quality assurance, billing, benefit management, practice management, repricing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services; or

(2) Any other function or activity regulated by the HIPAA Privacy Rule.

b. **Covered Entity.** An organization or individual that is one or more of the following:

(1) A health care provider that conducts certain transactions in electronic form (called here a “covered health care provider”),

(2) A health care clearinghouse, or

(3) A health plan.

NOTE: See Department of Health and Human Services Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification standards for more information.

c. **Data Aggregation** means the combining of such protected health information by the Business Associate with the protected health information received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.

d. **De-identify.** Health Information may be determined to be de-identified only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(a) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(b) Documents the methods and results of the analysis that justify such determination; or

(2) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed and the Covered Entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(a) Names;

(b) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits

of a zip code if, according to the current publicly available data from the Bureau of the Census:

1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(c) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(d) Telephone numbers;

(e) Fax numbers;

(f) Electronic mail addresses;

(g) Full or partial Social Security Numbers;

(h) Health record numbers;

(i) Health plan beneficiary numbers;

(j) Account numbers;

(k) Certificate/license numbers;

(l) Vehicle identifiers and serial numbers, including license plate numbers;

(m) Device identifiers and serial numbers;

(n) Web Universal Resource Locators (URLs);

(o) Internet Protocol (IP) address numbers;

(p) Biometric identifiers, including finger and voice prints;

(q) Full face photographic images and any comparable images; and

(r) Any other unique identifying number, characteristic, or code.

e. **Designated Record Set.** A group of records maintained by or for a Covered Entity that is:

(1) The health records and billing records about individuals maintained by or for a covered health care provider;

(2) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(3) Used, in whole or in part, by or for the Covered Entity to make decisions about individuals. For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a Covered Entity.

f. **Disclosure** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

g. **Electronic Protected Health Information (EPHI)**. EPHI is Protected Health Information (PHI) in electronic form. The HIPAA Security Rule specifically applies to PHI in electronic form, or EPHI, rather than the broader category of PHI which can be in any form or medium.

h. **Incident.** Any physical, technical or personal activity or event that increases the Covered Entity's risk to inappropriate or unauthorized use or disclosure of PHI or causes the Covered Entity to be considered non-compliant with the Administrative Simplification provisions of HIPAA as determined by the Department of Health and Human Services.

i. **Protected Health Information (PHI).** PHI is health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium, and relates to:

(1) The past, present, or future physical or mental health, or condition of an individual;

(2) Provision of health care to an individual; or

(3) Past, present, or future payment for the provision of health care to an individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

(4) If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. For further guidance, see Part II, 45 CFR 164.501.

j. **Privacy Act System of Records.** A group of any records containing personal information under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

k. **Required By Law.** A mandate contained in law that compels a Covered Entity to make a use or disclosure of protected health information and that is enforceable in a court of law.

l. **Use** means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.