Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6066
Transmittal Sheet
September 2, 2014

PROTECTED HEALTH INFORMATION (PHI) AND BUSINESS ASSOCIATE AGREEMENTS MANAGEMENT

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

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

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

4. RELATED HANDBOOKS: VA Handbook 6500, Information Security Program, VHA Handbook 1605.1, Privacy and Release of Information; VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information; VHA Handbook 1605.05, Business Associate Agreements.

5. RESCISSIONS: VA Directive 6066, Protected Health Information (PHI), April 2, 2008.

CERTIFIED BY:

/s/
Stephen W. Warren
Executive in Charge
and Chief Information Officer
for Office of Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Stephen W. Warren
Executive in Charge
and Chief Information Officer
for Office of Information and Technology

Distribution: Electronic Only

PROTECTED HEALTH INFORMATION (PHI) AND BUSINESS ASSOCIATE AGREEMENTS MANAGEMENT

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 Subparts A and E of Part 164, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), and 45 CFR Parts 160 and Subparts A and C of Part 164, the Security Standard ("Security Rule") and 45 CFR Parts 160 and Subpart D of Part 164, Breach Notification Rule.

b. The provisions of this Directive apply to all Department of Veterans Affairs (VA) components that are Business Associates, as defined by HIPAA, of the Veterans Health Administration (VHA). VA components meeting these criteria are herein referred to as "Business Associates." The provisions of this Directive do not apply to:

(1) Protected Health Information (PHI) or Electronic Protected Health Information (EPHI) provided to VA components, such as the Veterans Benefits Administration (VBA) or the National Cemetery Administration, under authority of 45 CFR 164.512(k)(1)(iii), i.e., determination of eligibility for or entitlement to, or provide, benefits under the laws administered by the Secretary of Veterans Affairs; or

(2) Official investigations, audits, and inspections conducted by the Office of Inspector General.

c. HIPAA is the product 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 HIPAA, there is a distinction between the VHA and VA in regards to health care privacy practices. VHA, as a health plan and health care provider, is 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 performing certain functions or activities on behalf of, or providing certain services to VHA through a Business Associate Agreement (BAA). A BAA must be in place in order for VHA to disclose PHI or EPHI to a VA component that is Business Associate as defined under paragraph 1b.

2. POLICY. All Business Associates will fully understand and adhere to all obligations and requirements directly applicable to Business Associates as set forth in VA and VHA policy implementing HIPAA and documented in a BAA. Failure to comply with all aspects of HIPAA requirements applicable to Business Associates can result in non-compliance with Federal law, which carries penalties for VA and potentially for individual(s) responsible for non-compliance. All Business Associates also understand that they are subject to periodic HIPAA compliance reviews conducted by VHA.

3. RESPONSIBILITIES

a. **The Assistant Secretary for Information and Technology.** The Assistant Secretary for Information and Technology, as the VA Chief Information Officer (CIO), and on behalf of the Office of Information and Technology, a Business Associate of VHA, 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). Further, the Assistant Secretary for Information and Technology, as the VA CIO and on behalf of OIT, a Business Associate of VHA, 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 will establish department-wide requirements, and provide oversight and guidance related to the protection of personally identifiable information (PII) including PHI throughout VA.

b. **The Deputy Assistant Secretary (DAS) for Information Security.** The DAS for Information Security shall develop policies and guidance which require department-wide compliance with privacy and records management law, policies, and standards.

c. **The Associate Deputy Assistant Secretary (ADAS), Policy, Privacy & Incident Response.** The ADAS for Policy, Privacy & Incident Response will advise the DAS for Information Security, as well as, the Assistant Secretary for Information and Technology, Under Secretaries, Assistant Secretaries, and Other Key Officials on privacy policy compliance; effective privacy controls and security controls for VA information systems; and other matters relevant to protecting PII including PHI, and all information systems collecting, storing or transmitting PII or PHI, and perform all security duties and responsibilities as designated by the Assistant Secretary for Information and Technology.

d. **Director, Office of Privacy and Records Management (OPRM)**. The Director, OPRM will act as a liaison for the Director, Privacy Service to the ADAS, Policy, Privacy, & Incident Response on matters of privacy policy compliance; effective privacy controls for VA information systems; and other matters relevant to protecting PII and PHI.

e. **Director, Privacy Service**. The Director, Privacy Service will:

(1) Perform all privacy duties and responsibilities as designated by the Director, OPRM; and

(2) Provide policy guidance to Under Secretaries, Assistant Secretaries, and Other Key Officials regarding requirements for the protection of PII and PHI.

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 within their respective areas comply with Federal laws, regulations, VA 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 and security mandates;

(3) Ensure that Privacy Officers report, within one hour of discovery, all actual or suspected breaches involving PII and record within a tracking system designated by VA Privacy Service for audit purposes;

(4) Provide an inventory of all subcontractors of the Business Associate that have access to PHI or EPHI to the organization's Privacy Officers and Information Security Officers;

(5) Provide to the organization's Privacy and Information Security Officers an updated inventory within 30 days of any change to the inventory of subcontractors of the Business Associate that have access to PHI and/or EPHI under the BAA found in VHA Handbook 1605.05; and

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

h. **Privacy Officers.** Privacy Officers will:

(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 1605.05, Business Associate Agreements;

(2) Understand and apply federal laws, statutes, guidance and VA policies and procedures related to privacy;

(3) Serve as advisors on all aspects of privacy to their administrations, staff offices, and/or program areas

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

(5) Use and disclose PHI processed by a VA covered entity or BA in accordance with the HIPAA Privacy and Security Rules, including providing individuals with the following rights:

(a) Right to receive prior to service a Notice of Privacy Practices (NoPP) regarding the uses and disclosures of PHI and their Individual rights;

(b) Right to access and amend PHI in a designated record set;

(c) Right to request an accounting of disclosures;

(d) Right to request restrictions on disclosures;

(e) Right to specify the method for confidential communications; and

(f) Right to have any complaints about how their PHI is processed resolved.

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 will have received annual security awareness training.

j. **Business Associates.** As users of VA systems with access to PHI and EPHI, Business Associates will:

(1) Directly comply with the HIPAA Security Rule, the use and disclosure provisions of the HIPAA Privacy Rule, and the HIPAA Enforcement Rule as set forth by the Department of Health and Human Services (HHS) regulations, 45 CFR Parts 160 and 164.

(2) Provide VHA with written assurances required by the HIPAA Privacy and Security Rules by signing the BAA found in VHA Handbook 1605.05, Business Associate Agreements. This agreement will provide a comprehensive understanding of their responsibilities as they relate to protection and confidentiality of PHI;

(3) Comply with VA Handbook 6500, Managing Information Security Risk: VA Information Security Program;

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

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

(6) Ensure all employees, volunteers, interns, contractors or subcontractors of the Business Associate with access to PHI take VHA's Privacy and HIPAA Training, or equivalent, on an annual basis;

(7) Ensure all employees, volunteers, interns, contractors or subcontractors of the Business Associate take security awareness training on an annual basis; and

(8) Report all actual or suspected privacy incidents into the designated data breach reporting system within one hour of discovery;

(9) 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.

(10) Obtain satisfactory written assurances that meet the same requirements that apply to arrangements between a Covered Entity and Business Associate from a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

(11) Maintain records and compliance reports regarding HIPAA Security and Privacy Rule compliance in order to provide such information to VHA and/or HHS upon request to ascertain whether the Business Associate is complying with the applicable provisions under HIPAA.

4. REFERENCES

a. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub.L. 111-5, 42 U.S.C. § 300jj et seq

b. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191, 42 U.S.C. § 201 et seq

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

d. Health Insurance Portability and Accountability Act, Security Rule, 45 CFR Parts 160 and 164

e. Privacy Act of 1974, 5 U.S.C.552a

f. VA Directive 6300, Records and Information Management

g. VA Directive 6500, Information Security Program

h. VA Directive 6502, VA Privacy Program

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

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

k. VA Handbook 6500, Managing Information Security Risk: VA Information Security Program

l. VA Handbook 6502.1, Privacy System Event Tracking System (PSETS)

m. VHA Directive 0710, Personnel Suitability and Security Program

n. VHA Directive 1605, VHA Privacy Program

o. VHA Directive 2003-025, Confidential Communications

p. VHA Handbook 1605.1, Privacy and Release of Information

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

r. VHA Handbook 1605.05, Business Associate Agreements

5. DEFINITIONS

a. **Business Associate.** A person or entity who is not a member of VHA's workforce, who, creates, receives, maintains, or transmits PHI on behalf of VHA in the performance of:

(1) A function or activity involving claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, 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.

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

e. **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.

f. **Notice of Privacy Practices (NoPP).** A Notice of Privacy Practices documents the uses and disclosures of PHI that may be made by a covered entity and of the individual's rights and the covered entity's legal duties with respect to PHI.

g. **Privacy 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.

h. **Personally Identifiable Information (PII).** Personally Identifiable Information, for purpose of this VA Privacy Service directive, is considered to be the same as VA sensitive personal information/data. PII is any information about an individual that can be used to distinguish or trace an individual's identity, alone, or when combined with other information which is linked or linkable to a specific individual, such as: name, social security number, date and place of birth, mother's maiden name, telephone number, driver's license number, credit card number, photograph, finger prints, biometric records, education, financial transactions, medical history, and criminal or employment history, etc.

i. **Protected Health Information (PHI). Protected Health Information (PHI)** Protected Health Information, for purposes of this VA Privacy Service directive, will be considered a subcategory of PII. This term applies only to individually-identifiable health information that is under the control of VHA, as VA's only Covered Entity under HIPAA. PHI is health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium. PHI excludes employment records held by an employer in its role as employer, records of a person deceased for more than 50 years, and some education records. It includes genetic information.

j. **Sensitive Personal Information (SPI).** Sensitive Personal Information, as defined in VA Handbook 6500, is any information about the individual maintained by an agency, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) 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. For purposes of this directive, the term SPI is interchangeable with the term PII.

k. **Subcontractor.** A Subcontractor is one that enters into a subcontract and assumes the obligations of the prime. For the purposes of this Directive, the subcontractor is an entity or person to whom a Business Associate delegates a function, activity, or service regulated by the HIPAA Privacy Rule, other than in the capacity of a member of the workforce of such Business Associate. A subcontractor shall refer to a contractor of the Business Associate that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

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