ATTACH #15

Department of Veterans Affairs
Veterans Health Administration
Veterans Integrated Service Network (VISN 23)

Network Policy V23-DND-020
February 18, 2009

# VISN 23 PRIVACY POLICY

1. **PURPOSE**: This memorandum implements VISN 23 privacy policy in compliance with Veterans Health Administration (VHA) Handbook 1605.1 and establishes responsibilities and procedures for the privacy protection of information that is collected, maintained, used, disclosed, amended and/or disposed by the staff and systems of VISN 23.

   In this document, the term workforce refers to on-site or remotely located employees, residents, students, Without Compensation (WOC) staff, volunteers, and any other appointed workforce members. Contractors will be held responsible for adhering to these policies and procedures in accordance with contracts and business associate agreements.

2. **POLICY**:

   a. VISN 23 will develop, implement, maintain, and enforce a structured program to safeguard individually identifiable information. The privacy program is designed to allow continued operation of mission-critical activities while ensuring the integrity, availability, confidentiality, and authenticity of data and information; minimum necessary access to protected health information; and a continuing awareness of the need for, and the importance of, information privacy within the facility.

   b. All members of the workforce are responsible for complying with this privacy policy, applicable federal laws and regulations, VA regulations and policies, VHA policies, as well as the procedures and practices developed in support of these policies. All facility privacy policies and procedures must be consistent with VHA Directive 1605, VHA Handbooks 1605.1 and 1605.2.

   c. All privacy, and other, personnel responsible for implementing and complying with these policies and procedures will be provided copies of, or access to, this policy.

   d. Violations of privacy policies or procedures will be brought to the attention of management for appropriate disciplinary action and/or sanctions, and reported in accordance with national and local policy. Privacy violations will be reported through the Privacy Violation Tracking System (PVTS) to the VA Security Operations Center (SOC) by the Privacy Officer (PO) within one hour of discovery.

   e. All policies and procedures, and any actions/activities taken as a result of these policies, must be documented in writing. In addition to policies and procedures, privacy-related communications, decisions, actions, and activities or designations, including any signed authorizations, must be documented. All documentation must either be retained in accordance with the VA records control schedule (RCS-10).

   f. All documentation related to the information privacy program will be reviewed and updated as needed in response to operational changes affecting the privacy of individually identifiable information (III).

   g. The current Chief of Health Information Management (HIM) for the Nebraska Western Iowa Health Care System (NWIHCS) is designated as the VISN Privacy Officer (PO). This is a collateral responsibility. The VAMC St. Cloud Privacy Officer is the VISN Alternate Privacy Officer. This is a collateral responsibility. The Administrative Secretary to the VISN Director is designated as the VISN FOIA Officer. This is also a collateral responsibility.

**3. RESPONSIBILITY**:

a. Executive Management (VISN 23 Network Director, and VISN 23 Deputy Network Director) is responsible for:

(1) Providing the necessary resources (funding and personnel) to support the Privacy Program and ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy and other federal legislation [e.g., Freedom of Information Act (FOIA) [5 U.S.C. 552], Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [45 C.F.R. Parts 160 and 164], the Privacy Act (PA) [5 U.S.C. 552a], the VA Claims Confidentiality Statute [38 U.S.C. 5701], Confidentiality of Medical Quality Assurance Review Records [38 U.S.C. 5705], and Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records [38 U.S.C. 7332]].

(2) Ensuring adequate Privacy Officer (PO) coverage for the VISN Offices. The VISN Privacy Officer will report and privacy concerns or problems to the VISN 23 Deputy Network Director

(3) Ensuring POs are fully involved in all projects concerning the collection, maintenance, use and/or disclosure, and amendment and/or disposal of III.

(4) Ensuring that new and revised Memorandums of Understanding and/or Data Use Agreements which involve the collection, transmission, use or sharing of information are reviewed by the facility Privacy Officer prior to approval by Executive Leadership

b. Privacy Officer, or designee, is responsible for:

(1) Developing, implementing and updating VISN specific privacy policies and procedures.

(2) Conducting periodic assessments, compliance reviews and/or audits of the facility's collection, use, storage and maintenance of personal information.

(3) Establishing effective working relationships with the Information Security Officer (ISO), FOIA Officer, Facility Chief Information Officer (FCIO), Contracting Officer, Compliance Officer and Human Resources personnel to assure that local policies and procedures which may impact the privacy program support and complement each other.

(4) Ensuring that executive leadership is apprised of all privacy related issues.

(5) Coordinating with the VISN ISO for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule or other federal privacy statutes.

(6) Serving as the facility's point of contact for matters relating to the privacy policies and procedures.

(7) Work with the Minneapolis VAMC Employee Education service and the Minneapolis VAMC Privacy Officer to ensure that members of the workforce receive training and education about privacy policies and procedures as required by VHA Privacy Program.

(8) Ensuring that members of the workforce know who to contact when a privacy complaint, incident or observation is identified or received.

(9) Monitoring the VISN office and workforce compliance with VHA privacy policies and procedures as well as compliance with local privacy policies and procedures.

(10) Ensuring processes are in place for the appropriate accounting of disclosures of individually identifiable information made by the facility and appropriate utilization of the Release of Information (ROI) Records Management software.

(11) In collaboration with various program officials and the Contracting Officer, ensuring identification of all entities meeting the definition of business associates.

(12) Ensuring that all business associates have either signed a business associate agreement or are in the process of completing an agreement, and that current agreements are maintained.

(13) In partnership with the VISN Records Management Officer ensures that the facility does not maintain any unauthorized Privacy Act system of records.

(14) Ensuring all facility developed paper, web-based or electronic forms that collect personal information contain the appropriate Privacy Act statements.

(15) Reviewing and approving all Memorandums of Understanding or Data Use Agreements when required for the sharing of VA privacy protected data between the facility and another party.

(16) Ensuring prompt investigation and follow-up on allegations or known occurrences of privacy incidents, complaints and/or observations including logging the complaint, incident or observation in the PVTS and completion of the Formal Event Review and Evaluation Tool (FERET). The completion of the PVTS and FERET tools should be conducted prior to investigation of the complaint, incident or observation.

(17) Ensuring that a Privacy Impact Assessment (PIA) is completed on all Local Area Networks (LAN).

(18) Requests for amendment of records will be referred to the appropriate system manager, or VAMC as appropriate. The PO and/or designee is responsible for reviewing requests to amend any information or record retrieved by an individual's name and contained in a VA system of records, which includes designated record sets, and coordinating such amendments with the author of the document, system owner, or facility Privacy Officer as appropriate.

(19) Other responsibilities as defined by the VHA Information Access and Privacy Office

c. Information Security Officer is responsible for:

(1) Coordinating with the VISN Privacy Officer for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule or other federal privacy statutes.

(2) Coordinating, facilitating, and updating the establishment of information security policies and procedures, to work in tandem with privacy policies and procedures.

(3) Establishing effective working relationships with the Privacy Officer, FOIA Officer, FCIO, Contracting Officer, Compliance Officer, and Human Resources personnel to assure that information technology (IT) security and HIPAA/FOIA/PA/Federal Information Security Management Act (FISMA) policies and procedures complement and support each other.

(4) Reviewing and evaluating the security program impact(s) of any proposed facility information privacy policy and procedure changes.

(5) Collaborating on addressing/resolving privacy complaints, investigations, and access rights to audits and other information maintained by the ISO, on issues related to common facility impacts from privacy and security requirements.

d. FOIA Officer is responsible for:

(1) Coordinating with the Privacy Officer and ISO to assure HIPAA/FOIA/PA policies and procedures complement and support each other.

(2) Processing FOIA requests for non-individually identifiable information (III} disclosures.

(3) Submitting the annual FOIA report in coordination with the PO.

e. VISN Chief Information Officer or designee is responsible for:

(1) Coordinating with ISO and PO to provide technical advice and other assistance relative to the reasonable safeguards requirements of privacy statutes and regulations dealing with implementation of IT systems, policies and procedures.

(2) Identifying each locally maintained computer system that contains III and providing technical input for various mandated documents, reports, and investigations.

(3) Assuring all computer rooms meet acceptable reasonable safeguards and that minimum necessary access is maintained.

f. VISN 23 Chief, Human Resources Management Service (HRMS), and/or designees are responsible for:

(1) Providing guidance to supervisors and managers regarding personnel actions, sanctions, or other actions to be taken when employees have violated information privacy practices, laws, regulations, policies and procedures, and rules of behavior (see VA Directive 5021).

(2) Providing appropriate information to PO for completion of PVTS entries.

(3) Coordinating with PO on the privacy of personnel records and other records maintained by HRMS.

(4) Ensuring that personnel records maintained by the HRMS are maintained in compliance with applicable privacy policies, statutes and regulations.

g. VA Contracting Officer/Contracting Officer Technical Representative (COTR) is responsible for:

(1) Working in collaboration with the PO to ensure that privacy responsibilities are listed in all contracts (see FAR Part 24).

(2) Ensuring through the COTR that contractors are aware of, and abide by, those privacy responsibilities as stated in contracts with VA and VHA.

(3) Ensuring that business associate agreements are enacted for all in which the contractor meets the definition of a business associate. Business Associate Agreements (BAA) should be a separate document from the contract.

(4) Ensuring that contract performance meets privacy requirements including mediating and/or terminating the contract if information privacy requirements are not being met.

h. Local Managers, Supervisors, and their designees (e.g. ADPAC) are responsible for:

(1) Identifying and protecting all III used by supervised personnel, including contractors and other workforce members.

(2) Ensuring that III, whether computerized or printed, is secured when work areas are unattended.

(3) Training new personnel on roles and responsibilities for protecting III.

(4) Assigning functional categories and ensuring that supervised personnel have only the minimum necessary access level required to carry out their authorized functions or assigned duties; assigning functional categories.

(5) Ensuring each supervised workforce member (including volunteers, residents, students and without compensation employees) completes formal privacy and information security training within 30 days upon hire and annually thereafter. Responsible for ensuring that such training is documented.

(6) Ensuring supervised workforce members sign the Rules of Behavior as required by VA Handbook 6500, Information Security Program.

(7) Ensuring that media (paper, electronic, CDs, disks, portable devices, etc.) with III is disposed of via approved means. The Minneapolis VAMC Privacy Officer will be contacted when media other than paper is to be discarded. He will ensure that the VISN media is disposed of in the same secure manner as the Minneapolis VAMC media.

(8) Assists the PO and Human Resources with the investigation and resolution of privacy incidents involving their workforce and/or program(s).

i. The VISN 23 Quality Manager serves as Quality Management (QM) Confidentiality Officer and is responsible for coordinating with the PO and FOIA Officer on requests for copies of or access to VISN QM documents. The PO serves as the final approval authority for determining which documents are classified as quality management

documents in accordance with VHA Directive 2004-051, Quality Management (QM) and Patient Safety Activities That Can Generate Confidential Documents.

j. All individuals who have access to sensitive information are responsible for:

(1) Accessing the minimum necessary data for which they have authorized privileges and on a need-to-know basis in the performance of their official VA duties.

(2) Protecting an individual's rights to privacy and ensuring proper use and disclosure of information. All workforce members will be held accountable for compliance with these policies, procedures, and applicable laws.

(3) Appropriately safeguarding printed and electronic III.

(4) Reporting complaints and/or violations of privacy policies or procedures to the Privacy Officer in a timely manner.

(5) Consulting the Privacy Officer and VHA Handbook 1605.1 for guidance in privacy situations not addressed in this document.

**4. PROCEDURES**: Outlined in Attachments A, B, C

**5. RESCISSIONS**: None

**6. FOLLOW-UP RESPONSIBILITY:** VISN 23 Privacy Officer

**7. REVIEW DATE**: February 2012

/S/

**ROBERT A. PETZEL, M.D.**
**Network Director**

**ATTACHMENTS**: A, B, C

**APPENDIX:** I, II, III

**DISTRIBUTION**: All members of the VISN 23 Facility Workforce

**Attachment A**

## Administrative Requirements

### *1. Compliance with Privacy Policies*

a. The facility and its workforce will comply with the contents of this policy, VHA Handbook 1605.1, and all other applicable privacy laws, regulations, and VA policies.

b. The facility Privacy Officer will monitor compliance with this policy through various means, including continuous assessment for privacy compliance.

### *2. Documentation*

a. This policy and any changes thereto, must be maintained in writing, either on paper or in electronic form, for a period of at least six (6) years.

b. Changes in VHA Handbook 1605.1: In the event that there is a change in VHA Handbook 1605.1, which necessitates alteration of facility policies and procedures, the VISN 23 privacy policies and procedures will be revised without delay by the VISN 23 Privacy Officer.

### *3. Complaint Process*

a. All privacy complaints received by the facility are to be referred immediately to the VISN Privacy Officer or the VAMC St Cloud Privacy Officer who will act in the role of Alternate VISN 23 Privacy Officer

b. The VISN Privacy Officer will enter all facility privacy complaints, regardless of validity, into the VA Privacy Violation Tracking System (PVTS) and complete the Formal Event Review and Evaluation Tool (FERET), if applicable, within one hour of notification/discovery.

c. The VISN Privacy Officer is responsible for investigating complaints regarding facility privacy practices, documenting the results of the investigations, and responding to all privacy complaints in writing.

d. The Privacy Complaint File containing all of the documentation of the privacy complaint and investigation will be retained by the facility Privacy Office indefinitely per the RCS 10-1.

e. All complaints received from the Department of Health and Human Services (HHS) – Office for Civil Rights (OCR) are to be forwarded immediately to the VHA Information Access and Privacy Office in VHACO for appropriate processing. The facility does not have authority to respond to HHS-OCR complaints. If an investigation arises as a result of a HHS-OCR complaint, VISN 23 and its business associates must permit the Secretary of HHS access to information, during normal business hours, after coordinating with the VHA Information Access and Privacy Office.

f. The VISN Privacy Officer is responsible for cooperating in a timely manner with the VHA Information Access and Privacy Office on all HHS-OCR complaints and all other privacy complaints submitted to VHACO.

g. When addressing complaints or contemplating employee disciplinary action, staff should refer to VA Directive 5021 and VA Handbook 5021, Employee/Management Relations, and the Privacy Complaint and Violation Resolution Guide available at http://vaww.vhaco.va.gov/privacy/ComplaintTracking.htm.

h. All employees are required to fully cooperate with the VISN Privacy Officer and/or the VHA Information Access and Privacy Office throughout the complaint investigation process.

***4. Reasonable Safeguards***

a. All VISN workforce members shall ensure that appropriate administrative, technical, and physical safeguards are used to maintain the security and confidentiality of III, including protected health information (PHI), and to protect against any anticipated threats or hazards to their security or integrity. The facility's workforce shall make reasonable efforts to limit III to the minimum necessary to accomplish the intended purpose of any use, disclosure, or request.

b. All workforce members may access and use information contained in VHA records as required for their official duties related to treatment, payment, and health care operations purposes.

(1) Supervisors, with input from the VISN Privacy Officer will be responsible for determining which persons in the workforce need access to PHI or III for their duties, the category or categories of protected health information to which access is needed, and any conditions appropriate to such access.

c. When disclosing VHA information, all applicable laws and regulations are reviewed and applied to the request in order to assure utilization of the most stringent provisions for all uses and/or disclosures of data in order to provide the greatest rights to the individual and the minimum necessary of III. III disclosure is mandatory with a valid written authorization, signed by the individual but disclosure must be limited to only the information necessary to satisfy the purpose of the request.

d. Disposal of documents: Staff disposes of paper and electronic documents that contain III by placing in secure locked shredding bins. Employees will contact the Minneapolis VAMC Privacy Officer when it is necessary to dispose of media and electronic media storage devices such as CD and portable thumb drives. He will ensure that the media is disposed of securely with the media from the Minneapolis VAMC. Data that is not destroyed at the site of production, such as that which is transported for contracted shredding, must be secured in locked containers or in locked areas until it is removed for destruction. See VA Handbook 6500 and VA Directive 6371 for more detailed procedures.

e. Maintaining auditory privacy: Staff only discusses patient care and personnel issues in appropriate areas, which allow the maintenance of auditory privacy. Facility staff does not discuss patient information in areas not conducive to confidentiality (e.g., canteen, elevators, or hallways). VHA health care providers and staff must refrain from discussing patient

information within hearing range of anyone who is not on the patient's treatment team or does not have a need to know the specific patient information unless an emergent condition arises whereby auditory privacy cannot be maintained.

f. Use of facsimile (fax): When using fax technology, facility staff adheres to VHA Handbook 1907.1, Health Information Management and Health Records. III is only transmitted via facsimile (fax) when absolutely necessary. Receipt of faxed information containing or requesting individually-identifiable patient information must be forwarded to the Privacy Officer at the appropriate VAMC for appropriate processing. Any staff member utilizing facsimile as a means of transferring individually-identifiable information must take the following steps to ensure that individually-identifiable information is sent to the appropriate destination and not to a machine accessible to the general public:

(1) Verify the fax number prior to sending the fax and, in order to prevent misdialing, pre-program and test the destination numbers. Periodically verify the fax numbers of frequent recipients. Ask those frequent recipients to notify the facility of any fax number changes.

(2) Ensure that a fax cover sheet with an appropriate confidentiality statement, instructing the recipient of the transmission to notify the facility if received in error, must be sent with all outgoing faxes.

(3) Notify the recipient before sending the fax in order to ensure that someone is present to receive the information or that the fax machine is in a secure location (e.g. locked room).

(4) Review the fax confirmation slip to verify that the confidential information went to the proper destination number. If there has been an error, immediately contact the incorrect recipient and request return or destruction of the fax.

g. Electronic mail (e-mail) and information messaging applications and systems are used as outlined in VA policy (VA Directive 6301 and VA Handbook 6500). These types of messages never should contain III, unless the authentication mechanisms have been secured appropriately (see VA Handbook 6500).

h. To the extent practicable, VISN 23 mitigates any harmful effect known to have resulted from an improper use or disclosure of III. Mitigation may include, but is not limited to: operational and procedural corrective measures; re-training, reprimanding, or disciplining workforce members; addressing problems with any involved business associates; incorporating the chosen mitigation solution(s) into facility procedures. The VISN 23 workforce may report reports improper uses or disclosures of III or any other privacy incident through their supervisor or directly to the VISN Privacy Officer.

***5. Sanctions***

a. All individuals who use or gain access to VA information systems or sensitive information must sign and adhere to the Rules of Behavior, which bind them to the legal and moral responsibility of preventing unauthorized disclosure. (See VA Handbook 6500, Information Security Program) VISN 23 has established sanctions, which are applied against members of its workforce as appropriate, for failures to comply with privacy policies and procedures and Rules of Behavior.

b. VISN 23 has established a set of rules that describes the information privacy operations of the facility and clearly delineates the responsibilities and expected behaviors of all workforce members. These rules address all significant aspects of using III and the consequences of inconsistent behavior or non-compliance. The entire workforce of VISN 23 will have access to a copy of these rules for purposes of review. A signed (manually or electronically) acknowledgement of these rules is necessary for each workforce member.

c. The Privacy Officer will determine information privacy violations and provide evidence thereof. The employee's supervisor will determine appropriate actions and may, in conjunction with human resources, take necessary steps and apply appropriate sanctions for any employees who are non-compliant with privacy policies and procedures. Penalties will be assessed against any individual(s) who knowingly and/or willfully use, disclose, or obtain information without the patient's written authorization or not as authorized by law.

d. Appropriate legal authorities outside of VHA may levy civil or criminal sanctions for privacy violations. Depending on the statute, penalties range from $5,000 and/or one year in jail to $250,000 and/or up to ten years in jail, per offense. If a penalty is levied, the offending employee, not VA, is responsible for payment. In addition, other adverse actions, administrative or disciplinary may be taken against employees who violate the statutory provisions. Adverse actions may include, but are not limited to, progressive discipline. The facility will follow processes and procedures outlined in VA Handbook 5021 for adverse actions in compliance with the stated Table of Penalties.

***6. Privacy Training and Education***

a. The VISN Privacy Officer, in coordination with the Minneapolis VAMC Education Coordinator or Education Office, is responsible for developing a local-level privacy training policy that outlines the facility procedures for ensuring compliance with the annual privacy training requirement of VHA Directive 1605 and VHA Handbook 1605.1.

(1) VHA Privacy Policy training is to be completed by the VISN 23 workforce annually and no later than June 30th each year. Executive Privacy Training in addition to VHA Privacy Policy training (for those managers GS-14 and above) is required and must be completed no later than June 30th each year. Education of VISN 23 employees will be tracked through the Minneapolis VAMC Education department and reported. Non compliance with privacy training requirements will be reported to the VISN 23 Deputy Director who will enforce the required compliance.

(2) The Minneapolis VAMC Privacy Officer, in conjunction with the Minneapolis VAMC Education Service will conduct privacy awareness training at all facility New Employee Orientation programs and shall ensure that all new personnel are trained in accordance with VHA Directive 1605 and VHA Handbook 1605.1.

b. The VISN Privacy Officer is responsible for developing a VISN training strategy in conjunction with the Minneapolis VAMC Education Coordinator or Education Office. VISN 23 workforce members will be included in all local Minneapolis VAMC activities to heighten awareness of facility and personnel privacy requirements and patient privacy rights. The VISN Privacy Officer will also send periodic messages to VISN staff and ensure that appropriate Privacy Posters are visible in the VISN facility. These activities will be designed

to ensure a privacy culture and posture is maintained throughout the VISN facility and that personnel are kept aware of how the privacy policies apply to their specific work duties. The VISN Director will make the strategy available to the VHA Information Access and Privacy Office upon request.

c. The VISN Privacy Officer, in coordination with the Minneapolis VAMC Education Coordinator or Education Office, department heads and supervisors, shall maintain a process of compiling annual training records in order to report the VISN privacy training completion status to the VHA Privacy Office and to the health care facility Director upon request. VISN administrative staff shall compile this information from the LMS and TEMPO systems and report to the VISN Privacy Officer.

   (1) The annual training records of completion of privacy training must be kept for all employees, volunteers, students, and contractors in order for reporting of facility privacy training completion numbers by each group.

   (2) The VISN Director will certify annual training completion to the VHA Information Access and Privacy Office for all personnel based on the reports generated by the health care facility Privacy Officer and Education Coordinator or Education Office upon request.

d. The health care facility Privacy Officer shall conduct other activities within the facility to enhance awareness of privacy and that have a positive impact on the overall privacy culture and posture of the facility. These activities shall include, but are not limited to, participation in VA's annual Privacy Week activities, posting privacy posters and announcements throughout the facility, and conducting one-on-one training with personnel who have been observed displaying negative privacy culture behaviors.

**Attachment B**

**Uses and Disclosures**

***1. Minimum Necessary***

a. The minimum necessary requirements do not apply to disclosures to, or requests by, a health care provider who requires the information for treatment purposes.

b. All facility staff should have minimum necessary (for completion of job duties) access to PHI. Specific minimum necessary policies and procedures, including appropriate staff access levels, are explained in VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information.

c. Supervisors will assign functional categories to staff and ensure that the only access given for access to PHI and III is required to perform their assigned duties.

***2. Forwarding a Request for Release of Information***

a. All requests for release of information received in the VISN offices will be forwarded to the ROI Department at the appropriate VAMC for processing. Requests for billing information will be forwarded to the appropriate VAMC Medical Care Cost Recovery (MCCR) Coordinator for processing. The VISN Privacy Officer will be consulted on any requests received that are unusual or are not addressed in this policy.

(1) If the record requested does not contain individually-identifiable information, process the request in accordance with section D. Freedom of Information Act.

(2) Copying fees may be charged for copies of records provided to requestors. Only copying fees as stated in 38 CFR 1.577(f) or subsequent regulations may be charged. The facility is prohibited for charging more for copies than is allowed in VA regulations.

***3. Contracts and Business Associate Agreements***

a. In contracts/agreements that involve the use or disclosure of PHI, appropriate privacy requirements, specifications, and statements of work must state that privacy requirements and specifications should be properly implemented before the contract/agreement goes into operation.

b. All contracts must meet the contracting requirements dictated by VA's Office of Acquisition and Material Management and the Federal Acquisitions Regulations (FAR). Any contract which necessitates the use of III must conform to the policies and procedures in FAR Subpart 24.1, Protection of Individual Privacy.

c. All contracts, agreements, and relationships must be assessed to determine if a business associate relationship exists. (See Appendix III for the Business Associate Decision Tree).

d. The facility contracting officer, the Privacy Officer, and the ISO will work together to identify those entities that qualify as Business Associates under HIPAA and ensure that Business

Associate Agreements (BAAs) are enacted for these identified entities in accordance with HIPAA BAA policies and procedures (Note: a business associate relationship exists if the facility is required to release PHI to a contractor or business partner for the provision of services on the facility's behalf.)

e. If a business associate relationship is determined to exist, a business associate agreement is enacted utilizing only the most current version of the VHA Information Access and Privacy Office-approved BAA language available at http://vaww.vhaco.va.gov/privacy/baa.htm. If a business associate is determined to serve more than one VA facility, the facility Privacy Officer contacts the VHA Information Access and Privacy Office to discuss enacting a national BAA. BAAs are kept updated and documented as long as the agreement is in force. (Refer to VHA Handbook 1600.01, Business Associate Agreements)

f. Per the agreement, business associates will:

(1) Not use or further disclose the information other than as permitted or required by the contract or by law;

(2) Use appropriate safeguards to prevent inappropriate use or disclosure of the information;

(3) Ensure any employee of a business associate, contractor, subcontractor or agent of the business associate receives at a minimum, annual privacy and security training that conforms to the requirements of VHA Privacy Training and VA Cyber Security training;

(4) Report to VHA any inappropriate use or disclosure of the information of which it becomes aware;

(5) Ensure that any agents, including subcontractors, to whom it provides PHI received from, or created or received by, the associate, on behalf of the facility/VA, agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(6) Utilize only contractors, subcontractors, or agents who are physically located within a jurisdiction subject to the laws of the United States. Business associate will ensure that it does not use or disclose protected health information received from the VA in any way that will remove the protected health information from such jurisdiction.

(7) Make III available to the individual to whom it pertains in accordance with federal privacy statutes, confidentiality statutes, and Paragraph 7 of VHA Handbook 1605.1.

(8) Make III available for amendment and incorporate any amendments to IIHI in accordance with federal privacy statutes, confidentiality statutes, and Paragraph 8 of VHA Handbook 1605.1.

(9) Make III available in order to provide an accounting of disclosures in accordance with federal privacy statutes, confidentiality statutes, and Paragraph 9 of VHA Handbook 1605.1.

(10) Make its internal practices and records relating to the use and disclosure of III from, or created or received by, the business associate on behalf of VHA, available to the

Secretary of HHS for purposes of determining compliance with Title 45 Code of Federal Regulations (CFR) Parts 160 and 164;

(11) At termination of the contract, return or destroy all III received from, or created or received by, the associate on behalf of VHA. If the Business Associate will destroy the records on behalf of VHA, the method of destruction must be outlined in the BAA.

(12) Authorize termination of the contract by VHA, if VHA determines the associate has violated a material term of the contract.

g. If a pattern of activity or practice of the business associate constitutes a material breach or violation of the business associate's obligation under the contract or other agreement is discovered, the facility Privacy Officer reports the problem to the VHA Information Access and Privacy Office and works with the Privacy Office to find a solution to the problem.

h. The COTR will monitor compliance with the applicable privacy policies required under the Business Associate Agreement.

**Attachment C**

## Freedom of Information Act (FOIA)

### *1. General*

a. The FOIA requires disclosure of VA records, or any reasonably segregable portion of a record, to any person upon signed, written request.

b. A FOIA request may be made by any person (including foreign citizens), partnerships, corporations, associations, and foreign, State, or local governments with some exceptions. The following types of request are not proper FOIA requests:

(1) Requests for records by Federal agencies and their employees acting in their official capacity.

(2) Requests for records by fugitives from justice seeking records related to their fugitive status.

c. VHA administrative records not retrieved by name, social security number, or other identifier must be made available to the greatest extent possible in keeping with the spirit and intent of the FOIA.

d. Before releasing records in response to a FOIA request, the record must be reviewed by the facility FOIA Officer to determine if all or only portions of the record cannot be released, in accordance with the nine (9) exemptions provided in the FOIA. The process of deleting portions of documents before releasing them is referred to as "redaction."

### *2. Requests for Copies of Records*

a. Records or information customarily furnished to the public in the regular course of the performance of official duties (e.g., information posted on VAMC Internet site) may be furnished without a written request.

b. Requests for official records under FOIA must be in writing over the signature of the requester and reasonably describe the records so that they may be located. This procedure should not be waived for reasons of public interest, simplicity, or speed. Generally, the request does not have to be designated a FOIA request and the individual does not have to explain why access to official records is desired.

### *3. Processing a FOIA Request*

a. A request for records received at the VISN facility must be promptly referred for action to the facility's FOIA Officer. Prompt referral of any request for facility records to the facility FOIA Officer is required in order to ensure the below time limitations are met.

b. All FOIA requests must be tracked in the FOIAXpress web-based FOIA tracking system.

c. The VISN FOIA Officer will process VISN specific FOIA request and assess appropriate fees.

d. Once the requester has been notified of a determination to comply with the request, the document(s) must be made available promptly. When the agency determines that response to a FOIA request will take longer than ten (10) or more business days, the FOIA requester must be notified and provided a tracking number for his/her FOIA request. The 10-day time limitation begins upon receipt of the request by the facility.

e. In unusual circumstances, extensions of not more than 10 workdays (for a total of 20 workdays from receipt of the request by the facility) may be approved by advising a requester in writing whether VA will grant or deny the request.

f. For FOIA releases that require a payment by the requestor, the VISN FOIA officer will inform the requestor of the anticipated charge before the request is completed. Amounts due of greater than $50 will be collected before the records are released. For billing amounts of less than $50.00 the billing invoice may be included with the records that are released.

g. NOTE: Refer to VHA Handbook 1605.1 Privacy and Release of Information paragraph 32 Freedom of Information Act for additional information on processing FOIA requests.

***4. Coordination of Releases with Regional Counsel***

a. In any case where a FOIA request involves matters or subjects involved in ongoing or anticipated litigation, administrative proceedings, or criminal or civil investigation, health care facility personnel must coordinate the facility's response to the FOIA request with the Regional Counsel.

b. If a request involves matters pertaining to ongoing litigation, the Regional Counsel must be informed of the request to ensure coordination of the VA's position in the litigation with any release of documents.

c. Coordination with the VHA FOIA Officer is also advisable when the facility receives a FOIA request of high visibility or importance to the Department.

***5. Annual Report of Compliance with FOIA***

a. The FOIA requires each agency to submit to the Congress a report, on or before March 1 of each year, of its activities and efforts to administer the FOIA during the preceding fiscal year. The facility FOIA Officers must submitted the Annual FOIA Report to the FOIA Officer by mid-October each fiscal year.

b. The VISN 23 FOIA Officer will maintain a tracking log of all FOIA requests received and processed at the VISN 23 facility to ensure that all requirements are met.

c. The VISN FOIA Officer will submit an annual report via the VA Intranet for use in compiling the Department report. The VHA FOIA Officer will send out instructions for submitting the report and time limits for the preparation and submission of the health care facility annual FOIA report. The VHA Directive Annual Report of Compliance with the Freedom of Information Act (FOIA) is available on the following web site: http://vaww.vhaco.va.gov/privacy/FOIA/

## APPENDIX I: Glossary of Terms

*Access* means the ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

*Authentication* means corroboration that a person is the one claimed.

*Availability* means that data or information is accessible and useable upon demand by an authorized person.

*Business associate* means a person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right.

*Computer matching* describes the computerized comparison of records from two or more automated systems of records. For more information, reference VHA Handbook 1605.1, section 37.

*Confidentiality* means that property, data, or information is not made available or disclosed to unauthorized persons or processes.

*De-identified information* is heath information that does not identify an individual and provides no reasonable basis to believe that the information can be used to identify the individual.

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

*Electronic media* means:
(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

*Facility* means the physical premises and the interior and exterior of a building(s).

*Information system* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

*Individual* means the person who is the subject of protected health information.

*Individually-identifiable health information* is a subset of health information, including demographic information collected from an individual, that:

i. Is created or received by a health care provider, health plan, or health care clearinghouse.
ii. Relates to the past, present, or future condition of an individual and provision of, or payment for, health care; and
iii. Identifies the individual or provides a reasonable basis to believe it can be used to identify the individual.

*Integrity* means the property of data or information having not been altered or destroyed in an unauthorized manner.

*Limited Data Set* is comprised of PHI that excludes specific direct identifiers of the individual or of relatives, employers, or household members of the individual. A limited data set is not de-identified data and can only be used for the purposes of research, public health, or health care operations, and can only be disclosed for the purpose of research.

*Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

*Password* means confidential authentication information composed of a string of characters.

*Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

*Positive identification* refers to the validation of a unique username and password combination; or the validation of picture, social security number, and/or date of birth. Positive identification is the first step in the authorization of an individual or entity seeking access to sensitive information systems or to a secure physical location.

*Protected health information* means individually identifiable health information that is:
(i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.
*Protected health information* excludes individually identifiable health information in:
(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) Records described at 20 U.S.C. 1232g (a4Biv); and

(iii) Employment records held by a covered entity in its role as employer.

*Right of access* is an individual's right to have access to (e.g., look at, view) or obtain a copy of records pertaining to the individual that contain individually-identifiable information.

*Security or Security measures* encompass all of the administrative, physical, and technical safeguards in an information system.

*Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

*Sensitive data* refers to data/information whose loss, misuse, or unauthorized access to (or modification of) could adversely affect national or departmental interest, the conduct of Federal or departmental programs, or the privacy to which individuals are entitled. This data/information includes, but is not limited to: medical, benefits, personal, and individually identified health data/information in electronic or any other form, and copyright-protected software.

*System of records* refers to any group of records under the control of the Department from which a record is retrieved by personal identifier such as the name of the individual, number, symbol, or other unique retriever assigned to the individual.

*Technical safeguards* mean the technology, and the policy and procedures for its use that protect electronic protected health information and control access to it.

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

*User* means a person or entity with authorized access.

*Workforce* means on-site or remotely located employees, contractors, students, WOC, volunteers, and any other appointed workforce members.

*Workstation* means an electronic computing device. For example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

**APPENDIX II: Acronyms**

ADPAC: Automated Data Processing Application Coordination

ADUSH: Assistant Deputy Under Secretary for Health

AIB: Administrative Investigation Board

AIS: Automated Information System(s)

AITC: Austin Information Technology Center

AOD: Administrative Officer of the Day

ARC: Allocation Resource Center

BAA: Business Associate Agreement

CCA: confidential communications address

C&A: Certification and Accreditation

CFR: Code of Federal Regulations

CMS: Centers for Medicare and Medicaid Services

COTR: Contracting Officer Technical Representative

CPRS: Computerized Patient Record System

DSS: Document Storage Systems, Inc.

DTA: Data Transfer Agreement

DUA: Data Use Agreement

EEO: Equal Employment Opportunity

FAR: Federal Acquisitions Regulations

FCIO: Facility Chief Information Officer

FERET: Formal Event Review and Evaluation Tool

FISMA: Federal Information Security Management Act

FOIA: Freedom of Information Act

HHS: Department of Health and Human Services

**APPENDIX II**

HIPAA: Health Insurance Portability and Accountability Act

HRMS: Human Resources Management Service

IA: Information Assurance

IIHI: Individually Identifiable Health Information

III: Individually Identifiable Information

IRB: Institutional Review Board

IRM: Information Resources Management

ISO: Information Security Officer

IT: Information Technology

MCCR: Medical Care Cost Recovery

MOU: Memorandum of Understanding

OCIS: Office of Cyber and Information Security

OCR: Office of Civil Rights

OGC: Office of General Counsel

OI: Office of Information

OIG: Office of the Inspector General

ORM: Office of Resolution Management

PA: Privacy Act

PHI: Protected Health Information

PO: Privacy Officer

POA: Power of Attorney

PVTS: Privacy Violation Tracking System

QM: Quality Management

R&D: Research and Development

RCS: Records Control Schedule

ROI: Release of Information

**APPENDIX II**

SF: Standard Form

SOC: Security Operations Center

SSN: Social Security Number

TIU: Text Integrated Utilities

USC: United States Code

VA: Department of Veterans Affairs

VAMC: Department of Veterans Affairs Medical Center

VHA: Veterans Health Administration

VHACO: Veterans Health Administration Central Office

VIC: Veteran Identification Card

VIReC: VA Information Resource Center

VISN: Veterans Integrated Service Network

VistA: Veterans Health Information Systems and Technology Architecture

VSSC: VHA Support Service Center

WOC: Without Compensation Employee

## Appendix III: Business Associate Decision Tree

### DECISION TREE FOR BUSINESS ASSOCIATE AGREEMENTS

***NOTE:*** *This Decision Tree applies to any agreement vehicle (i.e. Purchase Order, Purchase Card, Memorandum of Agreement), not just contracts.*

### 1. START

a. **Does the business associate provide a service, function, or activity to the Veterans Health Administration (VHA) or on behalf of VHA?**

**YES.** KEEP GOING! This arrangement might require a business associate agreement (BAA).

**NO**. STOP! This arrangement does not require a BAA.

b. **Does the business associate need Protected Health Information (PHI) from VHA to perform the service, function, or activity?** *or* **Does VHA need to provide the business associate access to PHI so that the service, function, or activity can be performed?** *or* **Does the business associate see PHI when performing the service, function or activity (e.g., shredding company)?**

**YES.** KEEP GOING! This arrangement might require a BAA. Proceed to the following exclusion and exemption questions.

**NO.** STOP! This arrangement does not require a BAA.

***NOTE:*** *If you are uncertain if PHI will be required or viewed by the business associate in order to perform the service, obtain more information from the Program Office or Business Line with whom the business associate works or the VHA Information Access and Privacy Office.*

### 2. EXCLUSION AND EXEMPTION QUESTIONS

a. **Workforce Exclusion: Is the business associate a member of the VHA workforce as defined in the Privacy Rule?** *(A member of the VHA workforce is an individual who has a VHA appointment or who is required, under VHA policy, to have a VHA appointment. Included in the definition of VHA workforce are all paid employees, employees under an Interpersonal Agreement (IPA) and all Without Compensation (WOC) employees (whether paid directly or through disbursement agreements). Examples of WOC employees include, but are not limited to: students, residents, interns, trainees, and volunteers. Contract employees, including those under Fee Basis Agreement, are not considered members of the VHA workforce for the purposes of a BAA.)*

**YES.** STOP! This is not a business associate relationship and does not require a BAA.

**NO.** KEEP GOING! You must answer the following exclusion and exemption questions.

***NOTE:*** *A business associate agreement (BAA) may be required in order to provide other VA components performing a service, function or activity for VHA or that benefits VHA with PHI (e.g., VA Office of Information & Technology). All BAAs with other VA components will be negotiated by the VHA Information Access and Privacy Office and should not be negotiated locally.*

b. **Treatment Exemption: Is the business associate a health care provider as defined by the Social Security Act?** and **Is the PHI being disclosed and/or used for treatment of an individual?** *(Treatment is the provision, coordination, or management of health care or related services by one or more health care provider. This includes the coordination of health care by a health care provider with a third-party, consultation between providers relating to a patient, or the referral of a patient from one health care provider to another.)*

If the answers to both questions are "**YES**," STOP! This arrangement does not require a BAA.

If the answer to either question is "**NO**," proceed with the following exclusion and exemption questions.

***NOTE:*** *If you are uncertain if someone is considered a health care provider under the Social Security Act, contact the VHA Information Access and Privacy Office for assistance.*

c. **Research Exclusion: Is the service, function, or activity research as defined in the Common Rule or as in Title 38 Code of Federal Regulations (CFR) 16.102(g), or VHA Handbook 1200.5?** and **Is the PHI being disclosed and/or used for research purposes?**

If the answer to both of these questions is "**YES,**" STOP! This arrangement does not require a BAA. ***NOTE:*** *Although a BAA is not required, other requirements must be met to disclose for research purposes (see VHA Handbook 1605.1).*

If the answer to all questions is "**NO**," proceed with the following exclusion and exemption questions.

d. **Health Plan-to-Health Care Provider Exclusion: Is the PHI being disclosed/and or used in VHA's role as a health plan to pay for services to a health care provider?**

**YES**. STOP! If the answer is "**YES**," then this arrangement does not require a BAA as it is part of the payment activities of VHA.

**NO.** KEEP GOING! If the answer is "**NO**," proceed with the following exclusion and exemption questions.

e. **Government Reporting Purposes Exclusion: Is the business associate a government agency to whom you are providing PHI for legally-mandated reporting purposes?**

**YES.** STOP! If the answer is "**YES**," then this arrangement does not require a BAA.

***NOTE***: *Although a BAA is not required, other legal requirements must be met in order to disclose PHI (see VHA Handbook 1605.1, for details on disclosing information in these situations).*

**NO.** KEEP GOING! If the answer is "**NO**," proceed to "Final Steps."

**3. FINAL STEPS**

If it has been determined that the arrangement is not exempt or excluded from the business associate agreement requirement, utilize the latest Business Associate Agreement Template http://vaww1.va.gov/cbo/hipaa/baa/fourthtemplate.doc to execute a business associate agreement.

***NOTE:*** *Numerous national-level BAAs have been signed for various services provided to VHA. Local agreements are not required with business associates who have signed national-level BAAs.*

**4. ADDITIONAL INFORMATION**

a. **Examples of Business Associate Functions, Activities, and Services Include, but are not Limited to:**

(1) Accounting

(2) Accreditation

(3) Actuarial Work

(4) Administrative

(5) Benefit management

(6) Billing

(7) Claims processing or administration

(8) Consulting

(9) Data aggregation

(10) Data analysis, processing, or administration

(11) Financial

(12) Legal ***NOTE:*** *VHA has a national-level BAA with VA Office of General Counsel; Individual facilities do not need to sign a separate BAA with Regional Counsel.*

(13) Management

(14) Practice management

(15) Re-pricing

(16) Shredding

(17) Transcription Services

(18) Utilization review

(19) Quality assurance

(20) Other health care operations not specifically tied to treatment, research, and/or payment

b. **For Your Information, Examples of Health Care Providers Include, but are not Limited to:**

(1) Community Residential Care (CRC) Programs

(2) Dentists

(3) Durable Medical Equipment (DME) suppliers

(4) Hospices

(5) Hospitals

(6) Home health agencies

(7) Nursing homes

(8) Pharmacies

(9) Physicians and/or group practice