PRIVACY COMPLIANCE ASSURANCE PROGRAM AND PRIVACY COMPLIANCE MONITORING

1. PURPOSE. This Veterans Health Administration (VHA) Handbook establishes the Privacy Compliance Assurance Program and the required activities and procedures to monitor and validate compliance within VHA with Federal privacy laws, regulations and Department of Veterans Affairs (VA)-VHA privacy policy.

2. SUMMARY OF CONTENTS. This is a new Handbook which provides the procedures necessary to show compliance with all applicable Federal privacy laws and regulations, and to monitor VHA's implementation of the privacy policies issued to fulfill the requirements of these laws and regulations.

3. RELATED ISSUES. VHA Directive 1605, VHA Handbook 1605.1, and VHA Handbook 1605.2.

4. FOLLOW-UP RESPONSIBILITY. The VHA Office of Health Information (19) is responsible for the contents of this Handbook. Questions may be referred to the VHA Privacy Officer, at 727-320-1839.

5. RESCISSIONS. None.

6. RECERTIFICATION. This VHA Handbook is scheduled for recertification on or before the last working day of April 2014.

Michael J. Kussman, MD, MS, MACP
Under Secretary for Health

DISTRIBUTION: CO: E-mailed 4/14/09
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 4/14/09

CONTENTS

PRIVACY COMPLIANCE ASSURANCE PROGRAM AND PRIVACY COMPLIANCE MONITORING

PARAGRAPH **PAGE**

CONTENTS Continued...

PARAGRAPH **PAGE**

APPENDIX

PRIVACY COMPLIANCE ASSURANCE PROGRAM AND PRIVACY COMPLIANCE MONITORING

1. PURPOSE

This Veterans Health Administration (VHA) Handbook establishes the Privacy Compliance Assurance Program and the monitoring activities required for validating compliance with Federal privacy laws, regulations, and Department of Veterans Affairs (VA) and VHA privacy policy as required in VHA Directive 1605. It establishes the procedures and the VHA Privacy Compliance Assurance Office within the VHA Information Access and Privacy Office for implementing these monitoring activities.

2. BACKGROUND

a. VHA, as a component of a government agency and a health plan and health care provider, must comply with all applicable Federal privacy and confidentiality statutes and regulations. The six statutes and sets of regulations most commonly encountered are listed in and are the basis for the privacy policies issued by VHA. VHA Handbook 1605.1 applies all six statutes and sets of regulations simultaneously to govern the collection, maintenance, and release of information from VHA records. They are:

(1) **The Freedom of Information Act (FOIA), Title 5 United States Code (U.S.C.) 552, implemented by Title 38 Code of Federal Regulations (CFR), Sections 1.550-1.559.** FOIA compels disclosure of reasonably described VHA records or a reasonably segregated portion of the records to any person upon written request, unless one or more of nine exemptions apply to the records (see 38 CFR 1.554(a)(1)-(9)). A FOIA request may be made by any person (including foreign citizens), partnerships, corporations, associations, and foreign, State, or local governments. VHA administrative records are made available to the greatest extent possible in keeping with the spirit and intent of FOIA. All FOIA requests must be processed in accordance with the statute, regulations, and current VHA policy.

(2) **The Privacy Act, 5 U.S.C. 552a, implemented by 38 CFR Section 1.575-1.584.** Generally, the Privacy Act provides for the confidentiality of individually-identified and retrieved information about living individuals that is maintained in a Privacy Act system of records and permits disclosure of Privacy Act-protected records only when specifically authorized by the statute. The Privacy Act provides that the collection of information about individuals is limited to that which is legally-authorized, relevant, and necessary. All information must be maintained in a manner that precludes unwarranted intrusion upon individual privacy. Information is collected directly from the subject individual to the extent possible. At the time information is collected, the individual must be informed of the authority for collecting the information, whether providing the information is mandatory or voluntary, the purposes for which the information will be used, and the consequences of not providing the information. The Privacy Act requires VHA to take reasonable steps to ensure that its Privacy Act-protected records are accurate, timely, complete, and relevant. ***NOTE:*** *The information collection requirements of the Paperwork Reduction Act must be met, where applicable.*

(3) **The VA Claims Confidentiality Statute, 38 U.S.C. 5701, implemented by 38 CFR Section 1.500-1.527.** This statute provides for the confidentiality of all VA patient and claimant names and home addresses (and the names and home addresses of their dependents) and permits disclosure of the information only when specifically authorized by the statute. Title 38 CFR Sections 1.500-1.527, are not to be used in releasing information from patient medical records when in conflict with 38 CFR 1.575-1.584, 38 CFR 1.460-1.496, or 45 CFR Parts 160 and 164.

(4) **Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332, implemented by 38 CFR Section 1.460-1.496.** This statute provides for the confidentiality of certain patient medical record information related to drug and alcohol abuse, HIV infection, and sickle cell anemia; it permits disclosure of the protected information only when specifically authorized by the statute.

(5) **Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law (Pub. L.) 104-191) implemented by 45 CFR Parts 160 and 164.** This statute provides for the improvement of the efficiency and effectiveness of health care systems by encouraging the development of health information systems through the establishment of standards and requirements for the electronic transmission, privacy, and security of certain health information. VHA must comply with the Privacy Rule of this Act when creating, maintaining, using, and disclosing individually-identifiable health information.

(6) **Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705, implemented by 38 CFR Section 17.500-17.511.** This statute provides that records and documents created by VHA as part of a designated medical quality-assurance program are confidential and privileged and may not be disclosed to any person or entity except when specifically authorized by statute.

b. VA facilities must comply with this policy in that the most stringent provision governing any use or disclosure of data is applied and the greatest rights to individuals under these statutes and regulations is provided ***NOTE:*** *Facilities must also adhere to other VA and VHA Handbooks implementing privacy policies to be in compliance with privacy requirements.*

3. DEFINITIONS

NOTE: *Terms defined in statutes or regulations have the same meaning when used in this Handbook. The definitions of the same statutory or regulatory terms in the Handbook are meant to be easy to understand and do not change the legal meaning of the statutory or regulatory definition of the term.*

a. **Compliance.** Compliance is the adherence to all VA and VHA policies, as well as the regulatory requirements set forth in the statutes VHA must follow. It is also an oversight process, supported by appropriate organizational resources, which is most likely to ensure that employee actions are consistent with applicable laws and policies. Compliance is used by all levels of the organization to identify high-risk areas, and to see that appropriate corrective actions are taken.

b. **Health Care Facility.** For the purpose of this Handbook, the term "health care facility" means each office and facility under the jurisdiction of VHA, including, but not limited to: VA Central Office, Veterans Integrated Service Network (VISN) offices, VA medical centers, VA Health Care Systems, Community-based Outpatient Clinics (CBOCs), Readjustment Counseling Centers (Vet Centers), and Research Centers of Excellence (CoE).

c. **Individually-identifiable Information.** Individually-identifiable information is any information about an individual that is maintained and retrieved by VHA using the individual's name or other unique identifier, and either directly identifies the record subject, or may be used with other information to identify the individual. Individually-identifiable information is also called personally-identifiable information. Individually-identifiable health information is included in this definition whether or not the information is retrieved by name.

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

(1) Is created or received by a health care provider, health plan, or health care clearinghouse;

(2) Relates to the past, present, or future condition of an individual and provision of, or payment for, health care; and

(3) Identifies the individual or a reasonable basis exists to believe the information can be used to identify the individual.

NOTE: *Individually-identifiable health information does not have to be retrieved by name or other unique identifier to be covered by this Handbook.*

e. **VA Personnel.** For the purpose of this Handbook, the term VA personnel includes: officers and employees of the Department, consultants and attendings, without compensation (WOC) employees, contractors, others employed on a fee basis, medical students and other trainees, and official, uncompensated volunteer workers. ***NOTE:*** *Compensated Work Therapy (CWT) workers are not VHA personnel; they are patients receiving active treatment or therapy.*

f. **Privacy Officer(s).** The Privacy Officer(s) is the employee(s) designated to implement and monitor compliance with VHA privacy policies at the health care facility. Any appropriately qualified and experienced employee may be assigned these responsibilities and must be so assigned in accordance with VHA policy or guidance (e.g., full-time, part-time, etc.).

g. **Protected Health Information (PHI).** PHI is individually-identifiable health information maintained in any form or medium. ***NOTE:*** *PHI excludes employment records held by VHA in its role as an employer.*

h. **Sensitive Personal Information (SPI).** SPI is defined in VA Handbook 6500 as any information about the individual maintained by an agency, including the following:

(1) Education, financial transactions, medical history, and criminal or employment history; and

(2) 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. ***NOTE:*** *For purposes of this Handbook, the term SPI is interchangeable with the term Personally-Identifiable Information (PII).*

4. SCOPE

The Privacy Compliance Assurance Program is designed to establish and maintain a culture within VHA that promotes compliance with all applicable Federal privacy laws, regulations, and policies. An active privacy-protection culture within VA assists all administration personnel in the prevention, detection, and resolution of conduct that would be contrary to maintaining the privacy of individuals' SPI or the sensitive information of the organization.

5. RESPONSIBILITIES OF THE VHA INFORMATION ACCESS AND PRIVACY OFFICE

The VHA Information Access and Privacy Office is responsible for:

a. The administration of the VHA Privacy Program; and

b. The administration of the VHA Privacy Compliance Assurance Program; and

c. Providing annual reports about VHA health care facilities' implementation of the privacy program and compliance with privacy, legal, and policy requirements to the Office of the Under Secretary for Health.

6. RESPONSIBILITIES OF THE VHA PRIVACY OFFICE

The VHA Privacy Office is responsible for:

a. Implementing the VHA Privacy Program and providing all VHA privacy policy interpretations.

b. Responding to VISN or national allegations or complaints of activities that violate Federal or VA privacy statutes or regulations or VA or VHA privacy policies.

c. Promptly investigating and resolving all allegations and complaints.

d. Adequately documenting each complaint, investigation, and resolution.

e. Documenting all complaints of violations of an individual's privacy reported directly to the Privacy Office in the Privacy Violation Tracking System (PVTS).

f. Documenting its findings concerning a complaint in PVTS.

7. RESPONSIBILITIES OF THE VHA PRIVACY COMPLIANCE ASSURANCE OFFICE

The VHA Privacy Compliance Assurance Office within the VHA Information Access and Privacy Office is responsible for:

a. Gathering, maintaining, and analyzing information about VHA health care facilities' compliance with applicable Federal privacy, research, records management, and Freedom of Information Act (FOIA) laws and regulations, and VA and VHA policies.

b. Conducting periodic reviews of operations of VHA health care facilities to assess those facilities' compliance with applicable Federal privacy laws, regulations and VA and VHA privacy policies.

c. Developing and utilizing objective criteria to select VHA facilities or offices to evaluate.

d. Conducting no fewer than six facility assessments per year.

e. Re-assessing, as appropriate, a facility at any time if the VHA Privacy Office or Privacy Compliance Assurance Office receives information that the facility is not complying with VA or VHA privacy policy or has violated a Federal privacy law, Federal regulation, or VA or VHA privacy policy.

f. Ensuring VHA health care facilities conduct annual self-assessments of their operations to determine levels of compliance with applicable Federal privacy laws, Federal regulations, and VA and VHA privacy policies.

g. Ensuring VHA health care facilities submit the annual self-assessment results to the VHA Privacy Compliance Assurance Office within the time period specified by the Information Access and Privacy Office.

h. Ensuring the health care facility Privacy Officer(s) monitors the rights of individuals in accordance with this Handbook.

i. Ensuring on-site privacy assessments conducted by the VHA Privacy Compliance Assurance Office are coordinated with the health care facility Privacy Officer(s) or privacy point-of-contact.

j. Reviewing and annually updating the Privacy Compliance Assessment Tool.

8. RESPONSIBILITIES OF CHIEF PROGRAM OFFICERS

Chief Program Officers are responsible for:

a. Conducting a privacy self-assessment of their respective VHA Program, when requested by the VHA Privacy Compliance Assurance Office to do so. ***NOTE:*** *VHA Program Offices may choose not to conduct annual assessments, if the function of the office does not involve the direct use or disclosure of individually-identifiable information or VA SPI, unless requested by the VHA Privacy Compliance Assurance Office.*

b. Ensuring compliance within their respective programs or VISNs with all Federal laws, regulations, VA regulation and policies, and VHA policies relating to privacy.

c. Ensuring that the Privacy Officer(s) in the respective programs is included in discussions and privacy concerns which are addressed in strategic initiatives.

d. Ensuring that the Privacy Program in their respective programs is appropriately supported with resources, management support, and operation activities.

9. RESPONSIBILITIES OF THE VISN DIRECTOR

Each VISN Director is responsible for:

a. Ensuring compliance within the VISN with all Federal laws, Federal regulations, VA regulations and policies, and VHA policies relating to privacy.

b. Ensuring that the Privacy Program in the VISN is appropriately supported with resources, management support, and operations activities.

c. Ensuring the VISN Privacy Officer(s) is the privacy liaison between the VHA Privacy Office and the VISN and its facilities.

d. Ensuring the VISN Privacy Officer is included in discussions and privacy concerns of the VHA health care facility which are addressed in strategic initiatives.

10. RESPONSIBILITIES OF THE FACILITY DIRECTOR

The facility Director is responsible for:

a. Ensuring any requested facility staff or area of the facility is available to the VHA Privacy Compliance Assurance Office for assessment within 30 days of the requested assessment date, unless a later date is negotiated with the VHA Privacy Compliance Assurance Office.

b. Maintaining a culture of privacy that meets the requirements of all applicable Federal privacy statutes and regulations, as well as VA and VHA policies.

c. Implementing business processes, staffing, and other actions needed to ensure privacy compliance.

d. Conducting operations in a manner that ensures patient safety, as well as, providing privacy compliance through the use of sound, standard operating procedures (SOPs) based on national VHA Privacy policy.

e. Ensuring use of the Privacy Compliance Assessment Tools provided by the VHA Information Access and Privacy Office to assess the facility's compliance with Federal Privacy laws, Federal regulations, and VA and VHA privacy policies.

f. Ensuring the facility Privacy Officer(s) is included in discussions and privacy concerns of the facility which are addressed in strategic initiatives.

g. Providing the facility Privacy Officer(s) the needed support to develop this role and the awareness of this role within the facility.

h. Ensuring that strategic planning and records disposal (privacy activities) are subject to compliance monitoring.

i. Upon request, certifying annual training completion to the VHA Privacy Office for all personnel. ***NOTE:*** *This is based on the reports generated by the facility Privacy Officer(s) and Education Coordinator or Education Office.*

j. Ensuring all complaints of violations of an individual's privacy are documented by the facility Privacy Officer(s) in PVTS.

k. Reporting promptly any privacy complaint, allegation, or activity that has the potential of VISN-level or national-level impact to the VHA Privacy Office.

l. Responding to facility-specific allegations or complaints of activities that violate Federal privacy statutes, Federal regulations, or VA or VHA privacy policies.

m. Promptly investigating, resolving, and adequately documenting each allegation, complaint, investigation, and resolution of the complaint.

n. Cooperating fully with the VHA Privacy Office in any investigations, mediation strategies, or correspondence that it requires in order to investigate and resolve a complaint or allegation.

o. Ensuring the annual records indicating completion of privacy training are to be kept for all employees, volunteers, students, and contractors. In order for reporting of facility privacy training completion numbers by each group, all records are to be forwarded to the Privacy Officer(s) on a monthly basis.

p. Ensuring completion of all remediation activities required by the VHA Privacy Compliance Assurance Office within the timeframes specified by that office, unless otherwise approved by the VHA Privacy Compliance Assurance Officer.

11. RESPONSIBILITIES OF THE FACILITY PRIVACY OFFICER(S)

The VHA health care facility Privacy Officer(s) is responsible for:

a. Managing and monitoring the facility Privacy Program in accordance with all VA and VHA privacy policies.

b. Reporting directly to the facility Director or Associate Director for responsibilities as the designated facility Privacy Officer(s) and for activities of the facility Privacy Program.

c. Participating in new-employee orientation concerning their privacy responsibilities.

d. Ensuring that all employees, including new employees, complete mandatory privacy training, in a timely manner in conjunction with the facility Education Coordinator.

e. Providing training and information to facility personnel on how to contact the facility Privacy Officer(s) in the event of an incident or to ask a question.

f. Conducting continuous employee privacy awareness activities in the facility, including participation in VA's annual Privacy Week. ***NOTE:*** *Privacy Awareness activities may include, but is not limited to, such activities as strategically posting flyers and distributing memos and reminders within the health care facility for visibility and privacy awareness.*

g. Maintaining facility assessments using the Privacy Compliance Assessment Tools and making the findings available to the VHA Privacy Compliance Assurance Office upon request.

h. Working with the Contracting Officer and Contracting Officer's Technical Representative to ensure that any contracts with disposal or recycling vendors have all the needed clauses to safeguard sensitive information being disposed of by the health care facility. This includes coordination with the facility Information Security Officer, Records Management Officer, and other personnel involved in the storage, maintenance, and destruction of media, including paper, containing individually-identifiable information.

i. Conducting a medical center walk-through on a monthly basis (see par. 13).

j. Conducting facility self-assessments (see par. 15).

k. Periodically reviewing all existing local-level privacy policies and procedures for consistency and compliance with legislative and policy changes in VHA privacy Directives and Handbooks (see par. 16).

l. Developing, in coordination with the facility Education Coordinator or Education Office, a local-level privacy training policy that outlines the facility procedures for ensuring compliance with the annual privacy training requirement according to current VHA policy (see par. 17 and VHA Handbook 1605.1).

m. Ensuring facility personnel are aware that individually-identifiable information contained in VHA records may only be used in the performance of their official duties for treatment, payment, or health care operations (see par.18).

n. Assisting the facility FOIA Officer with compiling the Annual FOIA Report (see par. 19).

o. Documenting all complaints of violations of an individual's privacy in PVTS and processing, investigating, and remediating all facility privacy complaints (see par. 27).

p. Acting as the facility subject-matter expert (SME) for the VA Notice of Privacy of Practices, Information Bulletin (IB) 10-163, and being the facility point-of-contact for any questions regarding the Notice (see par. 20).

q. Serving as the facility point-of-contact and privacy SME for all privacy matters in the facility (see par. 21).

r. Monitoring the facility's compliance with VHA Handbook 1600.01, Business Associate Agreements (see par. 28).

s. Monitoring uses of individually-identifiable information (see par. 18).

t. Monitoring the disclosures of individually-identifiable information through random spot-checks conducted quarterly (see par. 18).

u. Monitoring the right of access requests (see par. 22).

v. Monitoring amendment requests (see par. 23).

w. Monitoring the accounting of disclosure requests to ensure that the request was made in writing and processed within required timeframes (see par. 22).

x. Monitoring activities to verify that the medical center is providing appropriate Facility Directory Opt-Out options to veterans (see par. 25).

y. Monitoring activities to verify that the facility is providing appropriate confidential communications options to veterans who have requested confidential communications with VHA (see par. 26).

12. PRIVACY COMPLIANCE ASSESSMENT TOOLS

a. There are two Privacy Compliance Assessment Tools.

(1) One tool is for on-site privacy assessments of VHA heath care facilities by VHA personnel from outside the facility (see http://vaww.vhaco.va.gov/privacy/PCA.htm).

(2) The second tool is the self-assessment tool for facilities to conduct their annual assessments (see http://vaww.vhaco.va.gov/privacy/PCA.htm).

b. The content of the Privacy Compliance Assessment Tools is reviewed and updated annually by the VHA Information Access and Privacy Office.

13. PRIVACY WALK-THROUGH

a. A privacy walk-through of a VHA health care facility must include a reasonable cross-section of the grounds, buildings, operations, and services to observe for privacy compliance.

b. Conducted by the facility Privacy Officer(s) on a monthly basis, the walk-through needs to: ***NOTE:*** *The walk-through may be conducted in conjunction with the facility Information Security Office (ISO) or Safety Officer.*

(1) Include asking employees with various job functions about their understanding, training and actions concerning VHA privacy practices and procedures.

(2) Focus, using the VHA Privacy Compliance Assessment Tool as a guideline, on all aspects of privacy and the observation of daily business practices.

c. A walk-through of a CBOC must be conducted annually, at a minimum, by the facility Privacy Officer(s) or by the CBOC Director, or designee (if the facility Privacy Officer(s) is unable to perform the task for any reason). When the walk-through is performed by someone other than the facility Privacy Officer(s), the official performing the walk-through must provide, in writing and in a timely manner, documentation of the findings of the walk-through to the facility Privacy Officer(s).

14. HEALTH CARE FACILITY ON-SITE PRIVACY ASSESSMENTS

On-site privacy assessments are conducted by the VHA Privacy Compliance Assurance Office which coordinates with the health care facility Privacy Officer(s) or privacy point-of-contact. ***NOTE:*** *If the health care facility does not have a Privacy Officer(s) or privacy point-of-contact at the time of the assessment, the VHA Privacy Compliance Assurance Office coordinates the assessment with the Office of the Director.* The VHA Privacy Compliance Assurance Office may conduct assessments in conjunction with or on behalf of other VA or VHA programs.

a. When the VHA Privacy Compliance Assurance Office identifies a health care facility to be assessed, the facility Director must make any requested facility staff or the facility available to the VHA Privacy Compliance Assurance Office for assessment within 30 days of the requested assessment date, unless a later date is negotiated with the VHA Privacy Compliance Assurance Office.

b. The VHA Privacy Compliance Assurance Office provides the VHA health care facility with an agenda and the Privacy Compliance Assessment Tools prior to the on-site privacy assessment to allow the facility to prepare for the assessment. The health care facility Privacy

Officer(s) may conduct a pre-assessment of the facility using the assessment tools in order to identify and mitigate any deficiencies prior to the on-site privacy assessment.

c. The VHA Privacy Compliance Assurance Office assessment team conducting the on-site privacy assessment must:

(1) **Provide an Entrance Briefing.** The Assessment Team must provide an entrance briefing to the health care facility leadership including, but not limited to: Facility Director or Program Office Director and their associates, Privacy Officer(s), Compliance and Business Integrity Officer, Chief of Staff or other officers of the facility, ISO, VA Police, and other personnel, as requested.

(2) **Interview Key Personnel.** The Assessment Team interviews key health care facility personnel, including the Privacy, Security, Compliance and Business Integrity Officers, Health Information Management (HIM), VA Police, Contracting Officer, Information Technology (IT) or other personnel identified by the Assessment Team.

(3) **Review Policies and Procedures.** The Assessment Team reviews: the facility's policies and procedures for privacy and security, other facility or program office policies and procedures, SOPs, memoranda, or other official documentation that would support documentation of compliance with Federal privacy laws, Federal regulations, and VA and VHA policies and procedures.

(4) **Conduct a Health Care Facility Walk Through.** The Assessment Team performs a walk-through of the health care facility as part of its on-site assessment of the facility's compliance with privacy laws, regulations, policies, and procedures.

(a) The walk through must include visual observation of a reasonable cross-section of the grounds, buildings, operations, and services.

(b) Facility personnel are not to interfere with the assessment or the walk-through and must allow the assessment team to conduct the walk-through un-escorted or, at a minimum, escorted from a distance to ensure the privacy culture observed is that of day-to-day operations and not changed by the circumstances of the on-site privacy assessment.

(5) **Provide an Exit Briefing.** Immediately upon completion of the on-site assessment, the Assessment Team must provide an exit briefing to the health care facility leadership, including the Facility Director and associates, Privacy Officer(s), Compliance and Business Integrity Officer, Chief of Staff or other officers of the facility, ISO, VA Police, and any other identified personnel. During this briefing, the findings of the assessment are discussed, including observed best practices, compliance issues to be addressed, recommended actions, and timeframes for remediation.

15. HEALTH CARE FACILITY SELF-ASSESSMENTS

a. The facility self-assessment process must be conducted quarterly and a quarterly Privacy Performance Report sent by the health care facility Privacy Officer(s) to the VHA Privacy

Compliance Assurance Office. These self-assessments must be conducted by the health care facility Privacy Officer(s) using the Self-Assessment Tool (unless otherwise instructed by the VHA Privacy Compliance Assurance Office) and the findings submitted to the VHA Privacy Compliance Assurance Office by the last business day of each quarter. The key areas must be assessed quarterly, in the following order: ***NOTE:*** *This order for quarterly review does not preclude a health care facility from also completing other sections not included for performance during the specific quarterly self assessment.*

b. First Quarter of the Fiscal Year (Physical Safeguards Focus) includes:

(1) Reasonable Safeguards, and

(2) Privacy Officer Information.

c. Second Quarter of the Fiscal Year (Patient Rights Focus) includes:

(1) Right of Access,

(2) Amendment of Records,

(3) Facility Directory, and

(4) Confidential Communications.

d. Third Quarter of the Fiscal Year (Disclosures Focus) includes:

(1) Accounting of Disclosures,

(2) Research, and

(3) Release of Information (ROI).

e. Fourth Quarter of the Fiscal Year (Administrative Requirements Focus) includes:

(1) Privacy Training;

(2) Complaints;

(3) Business Associate Agreements, and

(4) Privacy Policies and Procedures.

16. DEVELOPMENT AND MAINTENANCE OF FACILITY POLICIES AND PROCEDURES

a. If the health care facility Privacy Officer(s) identifies any local policies or directives that, in the Privacy Officer's opinion, are non-compliant with VHA privacy Directives or

Handbooks, the Privacy Officer(s) must advise the local official responsible for the local policy document of how the document is non-compliant, and of the VHA requirement that the policy document must be immediately brought into compliance.

b. The local Privacy Officer(s) may consult with the VHA Privacy Officer before advising the local facility that one of its policies is non-compliant. The health care facility Privacy Officer(s) may use the VHA Privacy Policy template, which can be found on the VHA Privacy site at: http://vaww.vhaco.va.gov/privacy , to ensure that all areas of local-level privacy policies and procedures are in compliance. ***NOTE:*** *This is an internal VA link not available to the public.*

c. The health care facility Privacy Officer(s) must:

(1) Ensure that all local-level privacy policies and procedures are properly documented, signed by the health care facility Director, and appropriately distributed within the facility.

(2) Review and update local-level policies and procedures upon expiration and ensure that updated policies and procedures are adopted, formalized, and retained for at least 6 years in accordance with 45 CFR 164.530(j). ***NOTE:*** *For best practices, the recommended format for privacy policies is the use of the VHA Privacy Office Privacy Policy and Procedure Template*.

(3) Ensure that all facility personnel have access to local-level privacy policies and procedures, and facilitate activities that allow all personnel to be aware of the requirements of the policies and procedures.

(4) Promote a facility culture that reflects adherence to the documented policies and procedures. This may include, but is not limited to: posting the documented policies and procedures on the facility website, making electronic or paper copies available to personnel or supervisors upon request, or making privacy policies and procedures available and accessible to personnel through other means.

(5) Serve as the facility SME on all local-level policies and procedures relating to privacy, all VHA and VA privacy policies and procedures, and all applicable Federal privacy laws and regulations.

17. PRIVACY TRAINING, EDUCATION, AND AWARENESS

a. The health care facility Privacy Officer(s), in coordination with the facility Education Coordinator or Education Office, must develop 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. This policy must contain requirements for:

(1) Timeframes for completion of training, methods of tracking training participation, provisions for managing non-cooperation from personnel, and any other training requirements specific to the facility.

(2) The health care facility Privacy Officer(s) or other qualified personnel to conduct privacy awareness training at all facility New Employee Orientation programs.

(3) Ensuring all new personnel are trained in accordance with VHA Directive 1605 and VHA Handbook 1605.1, within the specified timeframe.

b. The health care facility Privacy Officer(s) must:

(1) Develop a local training strategy in conjunction with the facility Education Coordinator or Education Office. This strategy must:

(a) Document the overall training strategy for how the facility provides privacy training to personnel that heightens awareness of facility and personnel privacy requirements and patient privacy rights.

(b) Include activities that ensure a privacy culture and posture is maintained throughout the facility and that personnel are kept aware of how the privacy policies apply to their specific work duties. ***NOTE:*** *The health care facility Director makes the strategy available to the VHA Privacy Office upon request.*

(2) Maintain a process of compiling annual training records (in coordination with the facility Education Coordinator or Education Office, department heads, and supervisors), in order to report the facility privacy training completion status to the VHA Privacy Office monthly and to the health care facility Director upon request.

(a) The annual training records of completion of privacy training are to be kept for all employees, volunteers, students, and contractors in order for reporting of facility privacy training completion numbers by each group (see par. 10). ***NOTE:*** *Typically, the annual training records for employees are also kept as part of the employee's official personnel record.*

(b) The facility Director certifies annual training completion to the VHA Privacy Office for all personnel based on the reports generated by the health care facility Privacy Officer(s) and Education Coordinator or Education Office upon request.

(3) Conduct other activities within the facility to enhance employees' understanding of VA privacy policies and awareness of privacy and conduct other activities that have a positive impact on the overall privacy culture and posture of the facility. These activities need to 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, as requested.

(4) Train or develop an appropriate mechanism for other personnel to train all applicable personnel on the requirements of the business associate agreement, to include:

(a) All personnel who acquire services or external functions are aware of the business-associate-agreement requirement,

(b) The local process for engaging in business associate agreements, and

(c) The personnel responsible for the business-associate-agreement process.

18. MONITORING USES AND DISCLOSURES

a. **Use.** The health care facility Privacy Officer(s) must:

(1) Establish a process to make facility personnel aware that individually-identifiable information contained in VHA records may only be used in the performance of their official duties for treatment, payment, or health care operations.

(2) Work with the facility ISO and system Program Support Assistants (PSAs) to ensure that the facility uses appropriate access controls that limit access to individually-identifiable information based on job function in accordance with the minimum necessary requirements of VHA Handbook 1605.2. ***NOTE:*** *While assigning this access is not the responsibility of the Privacy Officer(s), the Privacy Officer(s) coordinates with the facility ISO and system PSAs to ensure this requirement is followed.* The facility Privacy Officer(s) must be included in any determination of instances of inappropriate use at the facility.

b. **Disclosures.** VHA health care facilities can only disclose individually-identifiable information in accordance with applicable Federal laws and regulations and VHA Handbook 1605.1. The health care facility Privacy Officer(s) must monitor the disclosure of individually-identifiable information to ensure proper legal authority for the disclosure was present, the processing of the disclosure was handled appropriately, and the disclosure was completed within required timeframes.

(1) The monitoring of disclosures of individually-identifiable information must be through random spot-checks conducted quarterly.

(2) The disclosures to be reviewed must be selected randomly using ROI Records Management software reports of all disclosures made by the facility during the quarter. ***NOTE:*** *If disclosures are made from areas other than the RIO Office, a random review of these areas must be conducted as well.*

(3) The following aspects of the disclosure must be reviewed by the facility Privacy Officer(s), or designee:

(a) There was legal authority for the disclosure (e.g., authorization, standing written request letter). If an authorization was obtained, the authorization must be reviewed to ensure it was valid and met content requirements as outlined in VHA Handbook 1605.1.

(b) There was an entry of the request in the ROI Records Management software to ensure appropriate accounting of the disclosure.

(c) The processing time was within the required timeframes in accordance with VHA Handbook 1605.1.

c. **Research.** The health care facility Privacy Officer(s), or designee, must ensure that:

(1) All applicable privacy requirements have been met before individually-identifiable information, including health information, is provided to a Research Investigator.

(2) Data Use Agreements for Limited Data Sets for Research are in place before a limited set of individually-identifiable information is disclosed from the facility. ***NOTE:*** *Appendix A contains the privacy requirements for research.*

d. **Access and Use of the Minimal Necessary Amount of Information.** The health care facility Privacy Officer(s) must:

(1) Establish a process for facility employees to be made aware of their functional category to ensure that they understand that they only access and use the minimal necessary amount of information in order to complete their job function.

(2) Monitor facility employees' awareness of their functional category quarterly through random checks to determine if employees understand their minimum necessary limits and that they are following them.

(3) Randomly check to see that the assignments of functional categories are documented by supervisors when they inform their personnel of the functional category assignment (see VHA Handbook 1605.2).

19. ANNUAL FREEDOM OF INFORMATION ACT (FOIA) REPORT

a. The health care facility Privacy Officer(s) must:

(1) Assist the facility FOIA Officer with compiling the Annual FOIA Report.

(2) Ensure that the FOIA Reports in the ROI Records Management software are generated and validated in order to provide the facility FOIA Officer with the information for the facility's Annual FOIA Report.

b. The facility Director must ensure, as applicable, other offices within the health care facility coordinate and provide input into the facility Annual FOIA Report. This ensures all FOIA requests processed by the facility during the year are included in the report.

20. VHA NOTICE OF PRIVACY OF PRACTICES, INFORMATION BULLETIN (IB) 10-163

a. The health care facility Privacy Officer(s) acts as the facility SME for the VA Notice of Privacy of Practices, Information Bulletin (IB) 10-163, and is the facility point-of-contact for any questions regarding the Notice.

b. As such, the health care facility Privacy Officer(s) must:

(1) Provide training to applicable staff on the VA Notice of Privacy Practices;

(2) Develop local policies regarding the distribution of the VA Notice for the facility, upon request; and

(3) Monitor activities of privacy practices to ensure the facility is in compliance with the VA Notice of Privacy Practices.

c. The facility Director, or designee, must ensure the facility participates in any future distributions of the VA Notice as directed by VA Central Office. This enables the facility to accommodate special needs of veterans or their families in understanding the VA Notice (i.e., reading it to veterans who cannot see or read well, translating to other languages, explaining the Notice to Veterans who do not understand it, etc.).

21. VETERANS PRIVACY RIGHTS AND EDUCATION

The health care facility Privacy Officer(s) serves as the facility point-of-contact and privacy SME for all privacy matters in the facility, and must:

a. Ensure that the facility develops and maintains policies and procedures addressing how the facility makes Veterans aware of their privacy rights.

b. Coordinate with education, volunteer, patient, advocacy, and other programs to develop methods to increase veterans' awareness of their privacy rights and to educate Veterans about their rights and responsibilities.

c. Ensure that veterans' privacy rights are being upheld within the facility by reviewing:

(1) Local-level policies and procedures implementing processes for handling veterans' requests to exercise their privacy rights to ensure compliance with VA and VHA policy, and

(2) The privacy file from the actual processing of veterans' requests to exercise their privacy rights (see pars. 16-21).

22. MONITORING RIGHT OF ACCESS REQUESTS

a. VHA health care facilities are to process individuals' right of access requests for copies of their information in accordance with current VHA policy (see VHA Handbook 1605.1).

b. Right of access requests are either granted, partially denied, or completely denied. For any randomly-selected right of access requests that were denied, a written notification providing appeals rights must be provided to the individual. The written notification needs to be reviewed to ensure compliance with this requirement.

c. The health care facility Privacy Officer(s) must:

(1) Monitor the right of access requests to ensure that the request was made in writing, granted or denied appropriately, and processed within required timeframes.

(2) Monitor the right of access requests through random spot-checks conducted quarterly.

(a) Within the VA health care facility the right of access requests to be reviewed is selected randomly using ROI Records Management software reports of all releases to the Requestor Type of Patient or Veteran made by the health care facility during the quarter.

(b) For the randomly selected right of access requests, the processing time must be reviewed to ensure compliance with requirements in current VHA policy (see VHA Handbook 1605.1), as follows:

1. VA health care facilities need to process all requests for review or copies of individually-identifiable information within 20 working days (excludes weekends and Federal holidays) of receipt whenever possible. If it is determined that the right of access request can not be processed within the 20-day time frame, the system manager for the concerned VHA system of records, the Privacy Officer(s), or the designee, must forward an acknowledgment letter of the request to the requestor within the same 20 working days.

2. When, for good cause, a facility is unable to provide the requested information in a record within the 20 working-day period, the individual must be informed in writing as to the reasons why access cannot be provided within the required time frame. The facility must also state when it is anticipated that the record will be available, and this must not exceed 40 working days from receipt of request. VA Form Letter 70-17, Postal Card Acknowledgment of Request, may be used for this purpose except when circumstances in a particular case warrant a specially written letter.

23. MONITORING AMENDMENT REQUESTS

a. VHA health care facilities are required to process individuals' right to request an amendment to any information or records retrieved by the individual's name in accordance with applicable Federal laws and regulations and VHA policies.

b. The health care facility Privacy Officer(s) must:

(1) Monitor amendment requests through random reviews to ensure that the request was made in writing, granted or denied appropriately, processed within required timeframes, and written notification was provided as follows:

(a) A request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, or the facility Privacy Officer(s), or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request.

(b) The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

(2) Select through a turnaround report, or other random method, amendment requests for review on a quarterly basis.

c. Amendment requests are either granted, partially denied or completely denied. For any amendment requests that were denied, a written notification that: provides appeals rights, indicates a statement of disagreement may be filed at any time, indicates the original request and the denial letter may be filed with the disputed information, and provides contact information for filing a complaint must be provided to the individual. When conducting the review, the health care facility Privacy Officer(s) determines if the written notification letter to the veteran complied with the requirements.

24. ACCOUNTING OF DISCLOSURES

a. The ROI Records Management Software was developed to meet the requirements of the VHA Privacy Office in order for VA facilities to comply with the Privacy Act and HIPAA Privacy Rule accounting of disclosure requirements for health information. The ROI Records Management software has been approved and its use in the facilities mandated. It is the responsibility of the facility Privacy Officer(s) to ensure this application is being fully utilized by the ROI section to ensure accurate accounting of disclosures and productivity reporting.

b. Individuals' requests for a list of disclosures of information, both written and oral, from records pertaining to the individual in accordance with applicable Federal laws and regulations and VHA Handbook 1605.1, must be processed.

c. The health care facility Privacy Officer(s) must:

(1) Maintain an accurate accounting for each disclosure of a record to any person or agency.

(2) Monitor the accounting of disclosure requests to ensure that the request was made in writing and processed within required timeframes.

(3) Monitor the accounting of disclosure requests through random spot-checks conducted quarterly.

(a) The veteran requests to be reviewed are selected randomly using ROI Records Management software reports of all releases to the Requestor Type of Patient/Veteran made by the facility during the quarter.

(b) The health care facility Privacy Officer(s) monitors the accounting of disclosure requests to determine if requests are acknowledged and processed as outlined in current VHA

policy (see VHA Handbook 1605.1). ***NOTE:*** *Additional guidance may be found in the Privacy Fact Sheet, January 2005, Vol. 05, No. 1 - Accounting of Disclosures.*

(c) For the randomly selected accounting of disclosure requests, the processing time must be reviewed to ensure compliance with the following requirements:

1. The accounting records of disclosures must be made available upon request to the individual to whom the record pertains within 60 calendar days after receipt of such a request; except disclosures made for law enforcement purposes, which will not be made available except as provided by 38 CFR 1.576(b)(7) and 45 CFR 164.528(a)(2)(i).

2. If the accounting cannot be provided within the specified timeframe, the facility or program can extend the timeframe no longer than 30 calendar days, provided that the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided. ***NOTE:*** *Only one such extension of time for action on a request for an accounting is allowed.*

(4) Monitor other offices within the facility that make disclosures and do not use the ROI Records Management Software (e.g., Human Resources, VA Police, Infectious Diseases Reporting, etc.), to ensure that an accounting of disclosures is kept by other acceptable means.

25. FACILITY DIRECTORY

The facility Privacy Officer(s) must:

a. Ensure, in coordination with the Education Office and supervisors, that all applicable personnel receive the appropriate training along with procedures outlined in Privacy Fact Sheet, July 2003, Vol. 03, No. 2 – Facility Directory Opt Out on how to provide Veterans with their Facility Directory options. ***NOTE:*** *This is available on the Privacy Officer website at: http://vaww.vhaco.va.gov/privacy/PCA.htm . This is an internal VA link not available to the public.*

b. Conduct monitoring activities to verify that the health care facility is providing appropriate Facility Directory options to Veterans. This monitoring consists of spot-checks conducted on a regular basis and includes, but is not limited to:

(1) Observation of intakes to determine if appropriate options are being given;

(2) Calls by the Privacy Officer(s), or designee, into the medical center to ask about patients known to be “opted out” of the Facility Directory to determine if the facility personnel respond correctly to telephone inquiries regarding opted-out patients; and

(3) Reviews of documentation on physician-determined opt-out decisions to determine if appropriate documentation of the opt-out determination was made in the patient’s electronic medical record.

26. CONFIDENTIAL COMMUNICATIONS

The health care facility Privacy Officer(s) must:

a. Provide, in coordination with the Education Office and supervisors, all applicable personnel with appropriate training and effective SOPs on how to handle veterans' questions and requests for confidential communications.

b. Conduct monitoring activities to verify that the facility is providing appropriate confidential communications options to Veterans who have requested confidential communications with VHA. This monitoring consists of spot-checks conducted on a regular basis and includes, but is not limited to:

(1) Observation of intakes to determine if appropriate documentation is being completed when a confidential communications is requested; and

(2) Investigation to determine if confidential communications address or phone numbers is being used by the facility.

27. PRIVACY COMPLAINTS

The health care facility Privacy Officer(s), in a timely manner, must:

a. Process, investigate and remediate all facility privacy complaints, to include, but not limited to:

(1) Coordinating with stakeholders (i.e., Human Resources for sanctions or disciplinary actions, union representatives, department heads, and supervisors, etc.);

(2) Inputting all privacy complaints received by the facility into PVTS;

(3) Managing and investigating, as appropriate, depending on type of privacy complaint;

(4) Providing written response to complainant within the specified timeframe outlined in the facility's privacy policy;

(5) Communicating with leadership, as appropriate (VHA Privacy Office, VISN, Office of Inspector General, Office of General Counsel);

(6) Managing privacy complaints to full resolution; and

(7) Identifying and tracking resolution and best practices in relating to privacy complaints.

b. Trend the types and incidence of privacy complaints and report these trends to the facility leadership and VHA Privacy Office, upon request.

c. Coordinate with the VHA Privacy Office when the facility receives a Health and Human Services (HHS), Office for Civil Rights (OCR) Complaint.

28. REVIEW OF BUSINESS ASSOCIATE AGREEMENTS

The facility Privacy Officer(s) must:

a. Monitor the facility's compliance with VHA Handbook 1600.01, and develop local-level policy(ies) and procedures that comply with this national guidance.

b. Coordinate with the appropriate facility officials, as appropriate, to restore or maintain compliance with the execution and administration of the business associate agreement process and VHA Handbook 1600.01.

c. Monitor the facility's business associates to determine if the business associate meets the terms of their business associate agreement with the facility.

29. PRIVACY IMPACT ASSESSMENTS (PIA)

The health care facility Privacy Officer(s) must:

a. Assist the Systems Manager with identifying privacy risks.

b. Review the PIA and the System of Records notice.

c. Obtain clarification from the system owner and system developer, as needed.

d. Endorse the PIA and submit it to the Chief ISO.

30. REFERENCES

a. The Freedom of Information Act (FOIA), 5 U.S.C. 552, implemented by 38 CFR §§ 1.550-1.559.

b. The Privacy Act, 5 U.S.C. 552a, implemented by 38 CFR §§ 1.575-1.584.

c. Standards for Privacy of Individually Identifiable Health Information, HIPAA Privacy Rule, (45 CFR Parts 160 and 164*).*

d. The VA Claims Confidentiality Statute, 38 U.S.C. 5701, implemented by 38 CFR §§ 1.500-1.527.

e. Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332, implemented by 38 CFR §§ 1.460-1.496.

f. Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705, implemented by 38 CFR §§ 17.500-17.511.

g. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act.

h. VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act System of Records.

i. VA Directive 6502, VA Enterprise Privacy Program.

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

k. VA Handbook 6502.2, Privacy Impact Assessments (PIA).

l. VHA Handbook 1600.01.

m. VHA Directive 1605.

n. VHA Handbook 1605.1.

o. VHA Handbook 1605.2.

p. VHA Handbook 1907.1.

q. Privacy Fact Sheet, January 2005, Vol. 05, No. 1, Accounting of Disclosures.

r. Privacy Fact Sheet, July 2003, Vol. 03, No. 2, Facility Directory Opt-Out.

PRIVACY REQUIREMENTS FOR RESEARCH

NOTE: *More then one of the following statutes may be applicable to any one specific research protocol.*

Laws and Regulations	Department of Veterans Affairs (VA) Researcher	Non-VA Federal Researcher	Non-Federal Researcher
Title 38 United States Code (U.S.C.) 5702	Not Applicable.	Written request dated and signed by the Researcher.	Written request dated and signed by the Researcher.
Title 38 U.S.C. 5701 (Applicable to Names and Addresses)	VA Researcher may be provided name and address under 38 U.S.C. 5701(b)(3).	No special requirement. Researcher may be provided name and address under 38 U.S.C. 5701(b)(3).	Researcher must provide the names and addresses of the research subject in order to obtain identifiable information on individuals.
Title 38 U.S.C. 7332 (Applicable to Drug Abuse, Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Records)	Assurance from the VA Researcher that the purpose of the data is to conduct scientific research and that no personnel involved in the study may identify, directly or indirectly, any individual patient or subject in any report of such research or otherwise disclose patient or subject identities in any manner.	Assurance from the Researcher that the purpose of the data is to conduct scientific research and that no personnel involved in the study may identify, directly or indirectly, any individual patient or subject in any report of such research or otherwise disclose patient or subject identities in any manner.	Assurance from the Researcher that the purpose of the data is to conduct scientific research and that no personnel involved in the study may identify, directly or indirectly, any individual patient or subject in any report of such research or otherwise disclose patient or subject identities in any manner.
Title 38 Code of Federal Regulations (CFR) §1.488 (Applicable to Drug Abuse, Alcohol Abuse, HIV Infection, and Sickle Cell Anemia Records)		The Under Secretary for Health, or designee, determines that the recipient of the patient identifying information: (1) Is qualified to conduct the research. (2) Has a research protocol under which the information will be maintained in accordance with the security requirements of 38 CFR Sec. 1.466; and will not be re-disclosed except back to VA. (3) Has furnished a written statement that the research protocol has been reviewed by an Internal Review Board (IRB) who found that the rights of patients would be adequately protected and that the potential benefits of the research outweigh any potential risks to patient confidentiality posed by the disclosure of records.	The Under Secretary for Health, or designee, determines that the recipient of the patient identifying information: (1) Is qualified to conduct the research. (2) Has a research protocol under which the information will be maintained in accordance with the security requirements of 38 CFR Sec. 1.466; and will not be re-disclosed except back to VA. (3) Has furnished a written statement that the research protocol has been reviewed by an IRB who found that the rights of patients would be adequately protected and that the potential benefits of the research outweigh any potential risks to patient confidentiality posed by the disclosure of records.

Privacy Act of 1974 (Applicable to Individually Identifiable Information)	VA Researcher may be provided VHA individually-identifiable information (III) as needed in the performance of his/her official VA duties under 5 U.S.C. 552a(b)(1).	With a routine use in the applicable system of records, approval of VHA's participation in the research study by appropriate leadership.	With a routine use in the applicable system of records, approval of VHA's participation in the research study by appropriate leadership.
Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (Applicable to Health Information)	a. Documented approval of waiver of authorization from an IRB or Privacy Board that includes the following elements: (1) A statement identifying the IRB or privacy board and the date on which the waiver of authorization was approved. (2) A statement that the IRB or privacy board has determined that the waiver of authorization satisfies the following criteria: (a) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals; and (b) The research could not practicably be conducted without access to and use of the protected health information. (3) A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy. (4) A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures. b. The documentation must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.	a. Documented approval of waiver of authorization from an IRB or Privacy Board that includes the following elements: (1) A statement identifying the IRB or privacy board and the date on which the waiver of authorization was approved. (2) A statement that the IRB or privacy board has determined that the waiver of authorization satisfies the following criteria: (a) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals; and (b) The research could not practicably be conducted without access to and use of the protected health information. (3) A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy. (4) A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures. b. The documentation must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.	a. Documented approval of waiver of authorization from an IRB or Privacy Board that includes the following elements: (1) A statement identifying the IRB or privacy board and the date on which the waiver of authorization was approved. (2) A statement that the IRB or privacy board has determined that the waiver of authorization satisfies the following criteria: (a) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals; and (b) The research could not practicably be conducted without access to and use of the protected health information. (3) A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy. (4) A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures. b. The documentation must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.