PRIVACY COMPLIANCE ASSURANCE PROGRAM AND PRIVACY/FREEDOM OF INFORMATION ACT (FOIA) CONTINUOUS READINESS REVIEW AND REMEDIATION

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive establishes the Privacy Compliance Assurance Program and the required activities and procedures to conduct C3R and validate VHA compliance with Federal privacy laws, Department of Veterans Affairs (VA) and VHA privacy policies, the Freedom of Information Act (FOIA), and National Archives and Records Administration (NARA) regulations at Title 36 Code of Federal Regulations (CFR) Chapter XII Subchapter B.

2. SUMMARY OF CONTENTS: This directive includes changes to procedures necessary to conduct auditing and C3R to ensure compliance with all applicable Federal privacy laws, and to evaluate VHA's implementation of its privacy, FOIA, and records management practices. This directive also includes a terminology change from "monitoring" to "continuous readiness review and remediation" (C3R) or "review", to better align with the National Institute of Standards and Technology (NIST) language as applied to NIST privacy standards.

3. RELATED ISSUES: VHA Directive 1605, VHA Privacy Program, dated September 1, 2017; VHA Directive 6300, Records Management, dated October 22, 2018; VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016; VHA Directive 6300.01, Records Management Compliance Monitoring, dated August 17, 2017; VHA Directive 1605.02, Minimum Necessary Standard for Protected Health Information, dated April 4, 2019; VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015; VHA Handbook 1605.05, Business Associate Agreements, dated July 22, 2014; VHA Directive 1935, VHA Freedom of Information Act Program, dated February 5, 2018.

4. RESPONSIBLE OFFICE: The VHA Office of Health Informatics (OHI), Health Information Governance (HIG), Office of Information Access and Privacy (IAP) (10A7B) is responsible for the contents of this directive. Questions may be referred to the VHA Privacy Compliance Assurance Officer at 202-360-1475 or the Notice of Privacy Practices hotline at 1-877-461-5038.

5. RESCISSION: VHA Handbook 1605.03, Privacy Compliance Assurance Program and Privacy Compliance Monitoring, dated April 13, 2009, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of September 2024. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

BY THE DIRECTION OF THE UNDER SECRETARY FOR HEALTH:

/s/ Steven L. Lieberman, M.D.
Acting Principal Deputy Under Secretary
for Health

DISTRIBUTION: Emailed to the VHA Publications Distribution List on September 20, 2019.

NOTE: *All references herein to VA and VHA documents incorporate by reference subsequent VA and VHA documents on the same or similar subject matter.*

CONTENTS

PRIVACY COMPLIANCE ASSURANCE PROGRAM AND PRIVACY/FREEDOM OF INFORMATION ACT (FOIA) CONTINUOUS READNIESS REVIEW AND REMEDIATION

PRIVACY COMPLIANCE ASSURANCE PROGRAM AND PRIVACY/FREEDOM OF INFORMATION ACT CONTINUOUS READINESS REVIEW AND REMEDIATION

1. PURPOSE

a. This Veterans Health Administration (VHA) directive establishes the Privacy Compliance Assurance Program and the auditing and continuous readiness review and remediation (C3R) activities required within VHA for validating compliance with Federal privacy, research privacy, Freedom of Information Act (FOIA) and records management laws, regulations, and Department of Veterans Affairs (VA) and VHA privacy, FOIA and records management policies, the Health Insurance Portability and Accountability Act (HIPAA); Title 45 Code of Federal Regulations (CFR) 160-164, the Privacy Act of 1974; Title 5 United States Code (U.S.C.) 552a, the Freedom of Information Act (FOIA); Title 5 U.S.C. 552, the FOIA Improvement Act of 2016; Pub. L. 114–185, and National Archives and Records Administration (NARA) regulations at Title 36 CFR Chapter XII Subchapter B.

b. This directive also designates the VHA Privacy Compliance Assurance Office (PCA), within the Office of Information Access and Privacy (IAP), as the office responsible for defining and implementing these auditing and C3R activities. Additional auditing, C3R, and oversight requirements under IAP's responsibility and authority are defined for records management in VHA Directive 6300.01, Records Management Compliance Monitoring, dated August 17, 2017. ***NOTE:*** *For more information on a sustainable Records Management program, please see Appendix A, figure 3.*
AUTHORITY: Title 38 U.S.C. 7301(b).

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 statutes and regulations most commonly encountered are listed below and are the basis for the privacy policies issued by VHA. VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016, is VHA's overarching privacy policy. That directive applies the privacy statutes and regulations simultaneously to govern the collection, maintenance, and release of information from VHA records. The FOIA statutes are covered in the VHA FOIA policies. The Privacy and FOIA statutes and regulations are:

(1) **The Freedom of Information Act.** Title 5 U.S.C. section 552, implemented by 38 CFR 1.550-1.562. 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 a foreign citizen of a foreign country), partnership, corporation, association, and foreign, State, or local government. 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 VHA Directive 1935, VHA Freedom of Information Act Program, dated February 5, 2018.

(2) **The FOIA Improvement Act of 2016.** Pub. L. 114-185, sets forth amendments to FOIA addressing a range of procedural issues, including requirements that agencies establish a minimum of 90 days for requesters to file an administrative appeal and that they provide dispute resolution services at various times throughout the FOIA process. The Act also codifies the Department of Justice's "foreseeable harm" standard, amends Exemption 5, creates a new "FOIA Council," and adds two new elements to agency Annual FOIA Reports. The Act also specifically adds responsibilities to Chief FOIA Officers who are now required to "review, not less frequently than annually, all aspects" of their agency's administration of the FOIA "to ensure compliance" with the FOIA's requirements. As required, reviews include: agency regulations, disclosure of records under paragraphs (a)(2) [proactive disclosure provision] and (a)(8) [foreseeable harm standard], assessment of fees and fee waivers, timely processing of requests, use of exemptions, and dispute resolution services with the Office of Government Information Services or the FOIA Public Liaison.

(3) **The Privacy Act, 5 U.S.C. 552a, implemented by 38 CFR 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. The Privacy Act requires that all information be maintained in a manner that precludes unwarranted intrusion upon individual privacy. Information is collected directly from the subject individual to the extent possible. As required 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 (Title 44 U.S.C. Chapter 35) must be met, where applicable.*

(4) **The VA Claims Confidentiality Statute, Title 38 U.S.C. 5701, implemented by 38 CFR 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. The statute addresses disclosures from all files, records, reports, and other papers and documents pertaining to any claim under any of the laws administered by VA, and the names and addresses of present or former members of the Armed Forces, and their dependents, in the possession of VA. Title 38 CFR 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.

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

(6) **Health Insurance Portability and Accountability Act of 1996 (HIPAA) (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 complies with the Privacy Rule of this Act when creating, maintaining, using, and disclosing individually-identifiable health information.

(7) **Confidentiality of Healthcare Quality Assurance Review Records, Title 38 U.S.C. 5705, implemented by Title 38 CFR 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. As a component of a government agency, VHA must comply with all applicable Federal records management statutes and regulations. The regulation most commonly encountered is the basis for the records management policies issued by VHA. It is NARA Regulations, 36 CFR Chapter XII, Subchapter B. This regulation outlines agency requirements for establishing and maintaining a Records Management program.

3. POLICY

It is VHA policy to comply with all applicable Federal privacy, research privacy, FOIA and records management laws, regulations, and policies. The Privacy Compliance Assurance (PCA) Program Office serves as the consolidated VHA office for independent compliance auditing, reporting, and oversight on all aforementioned Federal laws, regulations, and policies.

4. OVERSIGHT OF HEALTH CARE FACILITIES

a. **Use of "VA Health Care Facility" versus "VA Medical Facility."** This directive uses the broader term "VA Health Care Facility," instead the more commonly used "VA medical facility." This directive uses this broader term to include all locations within VHA where privacy, research privacy, FOIA and records management must be implemented. In contrast, "VA medical facility" is only encompassing of locations where direct medical care is delivered.

b. **Scope of VA Health Care Facilities.** For the purpose of this directive, the term "VA Health Care Facility" also includes each office and operation under the jurisdiction of VHA, including, but not limited to: VHA program offices, 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 Innovation (COIN). The use of the term "facility" in this directive is synonymous with this definition.

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health, or designee, is responsible for ensuring overall VHA compliance with this directive and:

(1) Ensuring a safe and functional environment for patients, employees, visitors, and contractors and the appropriate administering of privacy and confidentiality rights to Veterans, employees, and other individuals whose information is maintained by VHA.

(2) Ensuring that PCA remains independent of the programs or functions it audits and is not subordinate to any audited program or office.

(3) Ensuring that PCA is sufficiently funded and resourced to complete the auditing, C3R and oversight functions outlined in this directive.

b. **Deputy Under Secretary for Health for Operations and Management.** The Deputy Under Secretary for Health for Operations and Management, or designee, is responsible for:

(1) Communicating the contents of this directive to each of the VISNs.

(2) Ensuring that each VISN Director has sufficient resources to fulfill the terms of this directive in all VA Health Care Facilities within that VISN.

(3) Providing oversight of VISNs to ensure compliance with this directive, relevant standards, and applicable regulations.

(4) Ensuring the development and successful implementation of VHA's privacy, FOIA, and records management functions.

c. **Director, VHA Office of Human Resources.** To ensure sufficient and appropriate resourcing to the privacy, FOIA, and records management programs, the Director of Human Resources in VHA is responsible for ensuring compliance with the United States Office of Personnel Management (OPM) "Position Classification Flysheet for Government Information Series, 0306" dated March 2012 and "Position Classification Flysheet for Government Information Series, 0308" dated March 2015. This responsibility includes:

(1) Classifying Privacy and FOIA Officers within the GS-0306 job series and prohibiting the assignment of collateral duties other than FOIA.

(2) Classifying Records Managers within the GS-0308 job series and prohibiting assignment of collateral duties not directly compatible with Records Management.

d. **VHA Privacy Officer/Director, VHA Information Access and Privacy.** The VHA Privacy Officer serves as the Director of the VHA Information Access and Privacy (IAP) Office and is responsible for:

(1) The administration of the VHA Privacy Program (see VHA Directive 1605, VHA Privacy Program, dated September 1, 2017; VHA Directive 1605.01; and VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015).

(2) The administration of the VHA PCA Program.

(3) The administration of the VHA FOIA Program (see VHA Directive 1935).

(4) Providing regular and ad hoc reports about VA Health Care Facilities' implementation of the privacy, FOIA and records management programs and compliance with legal and policy requirements to the Office of the Under Secretary for Health.

e. **VHA Records Officer.** With respect to this directive, the VHA Records Officer is responsible for:

(1) Collaborating with PCA on the criteria for how VA Health Care Facilities will be audited, what level of auditing will be conducted, the content of audit criteria and C3R activities, and other operational decisions which impact the auditing and C3R functions outlined in this policy.

(2) Collaborating with PCA to remediate high-risk non-compliance within VA Health Care Facilities, as determined by the VHA PCA Officer, VHA Records Officer, or VHA Senior Leadership.

(3) Assisting PCA in conducting an annual review of all auditing and C3R criteria, and advising PCA of any necessary updates that impact PCA's audit processes.

f. **Manager, VHA Privacy Office.** The Manager of the VHA Privacy Office is responsible for:

(1) Implementing the VHA Privacy Program (see VHA Directive 1605, VHA Directive 1605.01, and VHA Handbook 1605.04).

(2) Developing and interpreting all VHA privacy policy provisions including Business Associate policies with the exception of this directive.

(3) Providing guidance to PCA on official interpretations of policies and procedures in a manner that ensures that PCA can accurately audit against specific policy requirements.

(4) Cooperating with PCA in audits related to activities that may violate Federal or VA Privacy statutes or regulations, or VA or VHA Privacy policies and responding to VISN or national complaints in collaboration with PCA.

(5) Promptly investigating and resolving all allegations and complaints submitted to the VHA Privacy Office.

(6) Adequately documenting each received complaint, as well as the investigation, and resolution thereof, in the Privacy and Security Event Tracking System (PSETS) at https://vaww.psets.va.gov, and documenting its findings concerning a complaint in PSETS. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

g. **Director, National Data Systems Health Information Access.** The Deputy Director of National Data Systems (NDS), Health Information Access (HIA) Office is responsible for:

(1) Implementing the VHA HIA Program and interpreting all VHA HIA policy provisions.

(2) Implementing the Business Associate Program in collaboration with the VHA Privacy Office.

(3) Identifying Business Associates who are candidates for PCA Audits based on a risk-based model.

(4) Collaborating with PCA on auditing activities associated with Business Associates as requested by PCA.

(5) Collaborating with PCA and the VHA Privacy Office on resolution of non-compliance found in Business Associate organizations.

h. **Director, Health Care Security Requirements.** The Director of the Health Care Security Requirements (HCSR) Office is responsible for:

(1) Implementing the VHA HCSR Program.

(2) Developing and interpreting all national VHA HCSR policy provisions.

(3) Ensuring VHA's security program supports compliance with the Security Rule contained in HIPAA in conjunction with PCA as appropriate.

(4) Collaborating with PCA on auditing activities associated with Business Associates as appropriate.

i. **VHA Privacy Compliance Assurance Officer.** The VHA PCA Officer is responsible for:

(1) Conducting independent performance audits of one-third of VA Health Care Facilities per year utilizing on-site methods, including interviews of Privacy and FOIA Officer(s) and Records Managers, interviews of a sampling of workforce members or other applicable individuals and review of operations of VA Health Care Facilities in order to evaluate those facilities' compliance with applicable Federal privacy, research

privacy, FOIA, and records management laws and regulations, and VA and VHA privacy, FOIA and records management policies. The frequency of the cycle, audit sample size and data-collection methods may be changed at the discretion of the PCA Officer based on business need.

(2) Collaborating with the VHA Privacy, FOIA, and Records Management offices and the VHA Office of Research Oversight (ORO) or other applicable offices as necessary in PCA's development of audit criteria for the evaluation of the respective programs.

(3) Administering Facility Self-Assessments (FSAs) for the purpose of gaining facility self-reported compliance status on a quarterly basis within VA Health Care Facilities as defined in this directive.

(4) Gathering, maintaining, and analyzing information about VA Health Care Facilities' compliance with applicable Federal privacy, research privacy, FOIA, and records management laws and regulations, and applicable VA and VHA policies.

(5) Providing an executive summary report of PCA findings to VA Health Care Facility leadership including findings for privacy, research privacy, FOIA, and Records Management, providing a Prioritized Action Plan to facilities at the conclusion of a PCA Audit and making a detailed report available to oversight bodies and VHA leadership at the PCA Officer's discretion.

(6) Providing reports of PCA findings and FSAs to VHA leadership including findings for privacy, research privacy, FOIA and records management.

(7) Conducting periodic independent performance audits of the operations of VA's national Business Associates for compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act and the terms of the Business Associate Agreement (BAA), as determined necessary by the VHA PCA Officer, in collaboration with applicable program offices (see paragraphs 5.d. and 5.f.(2) above).

(8) Conducting independent performance audits or re-audits, as appropriate, in any VA Health Care Facility at any time if the VHA PCA Officer determines that the facility is non-compliant to the degree that such non-compliance creates or presents a high risk of harm or injury to Veterans, employees or other individuals, or to the VHA organization.

(9) Auditing or re-auditing any VA Health Care Facility upon request from Office of Inspector General (OIG), White House Office of Special Counsel, Congressional Oversight Committees or other oversight organizations.

(10) Conducting independent performance audits or re-audits, as appropriate, of any VHA Business Associate at any time if the VHA PCA Officer determines that the Business Associate is non-compliant to the degree that such non-compliance creates or presents a high risk of harm or injury to Veterans, Employees or other individuals or to the VHA organization.

(11) Auditing or re-auditing any VA Business Associates upon request from Office of Inspector General (OIG), White House Office of Special Counsel, Congressional Oversight Committees or other oversight organizations.

(12) Ensuring PCA audits are coordinated with all applicable individuals in accordance with the PCA Communication Plan approved by the Office of the Under Secretary for Health.

(13) Ensuring PCA audits of Business Associates are coordinated with the Business Associate's designated point-of-contact (POC).

(14) Auditing the C3R activities of VA Health Care Facility Privacy and FOIA Officers and Records Managers to determine if they appropriately review, analyze, report, and remediate facility privacy, research privacy, FOIA and records management programs to ensure that the privacy of individuals is protected and VHA records are maintained in accordance with applicable laws, regulations and policies.

(15) Reviewing and annually updating all audit criteria and Compliance Auditing Tools (CAT, formerly Compliance Monitoring Tool (CMT)), as necessary, in conjunction with the program offices responsible for each audited program and maintaining a comprehensive, objective auditing methodology.

(16) Reviewing, maintaining and updating the PCA intranet Web site to ensure the information is relevant and provides the needed assistance to the Privacy and FOIA Officers and Records Managers to achieve the requirements of this directive. This Web site can be accessed at https://vaww.vets.vaco.portal.va.gov/sites/privacy/pca/Pages/default.aspx. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

(17) Establishing and maintaining an open line of communication with VISN/Regional Leadership concerning PCA audits and encouraging VISN involvement in the PCA audit process.

(18) Providing results of PCA audits, facility risk mitigation activities, and information concerning the FSAs for facilities within their VISN per the PCA Communications Plan, as a tool to be transparent, engage, and facilitate needed change.

(19) To the extent feasible, conducting all PCA audits in compliance with the Generally Accepted Government Audit Standards (GAGAS) for Performance Audits and maintaining the operations of the PCA Office in compliance with the administrative requirements of GAGAS for government audit organizations.

(20) Initiating Post-Audit Oversight after a PCA audit to ensure that facilities take prompt action to mitigate and/or remediate deficiencies identified that pose the highest risk to the effectiveness of the privacy, research privacy, FOIA, and records management programs (defined in paragraph nine of this directive).

(21) Requiring facility leadership (e.g., Directors, Program Officers, etc.) to complete corrective actions for high-risk findings identified; defining mitigation and remediation actions based on risk priorities; establishing a prioritized action plan for identified non-compliance; and providing oversight to the facility program managers and leadership during Post-Audit Oversight. (defined in paragraph nine of this directive).

(22) Communicating with appropriate officials throughout Post-Audit Oversight to ensure all facilities are held accountable for completing the prioritized action plan in the electronic Post-Audit Tool (ePAT) and executing and documenting corrective actions in risk order.

(23) Performing responsibilities (21) and (22) of this paragraph for any high-risk instance(s) of non-compliance in VA Health Care Facilities at the Privacy Compliance Assurance Officer's (PCAO's) discretion, regardless of how PCA becomes aware of it.

(24) Determining reasonableness standard for completing remediation actions based on VHA leadership guidance, harm to the organization or to individuals or severity of non-compliance.

(25) Resolving any discrepancies between this directive and VHA Directive 6300.01, related to implementation of these two policies.

j. **Chief Program Officers.** Chief Program Officers, including those designated as Executive Directors, are responsible for:

(1) Ensuring that all privacy, FOIA and records management functions within their program office are assigned and performed in compliance with all Federal laws and regulations, VA regulations and policies, and VHA policies that address these functions. Program offices are not required to conduct regular self-assessments unless otherwise instructed by the PCA Officer to do so. Program offices may also be subjected to a PCA audit at the discretion of the PCA Officer. ***NOTE:*** *If the PCA Officer gives instruction to complete a self-assessment, the program office may request a waiver for conducting assessments if the Chief Officer certifies that the function of the office does not involve the direct use or disclosure of Individually Identified Information (III). Program offices may choose to conduct self-assessments voluntarily as a means of reviewing their own compliance proactively. Program offices may not request a waiver for any FOIA audits administered by PCA in compliance with the FOIA Improvement Act.*

(2) Ensuring that the privacy programs for their respective program office are appropriately supported with resources, management support, and operational integration.

(3) Ensuring that the designated Privacy Officer(s)/Liaison(s) for their respective programs are included in discussions regarding strategic initiatives, to ensure that the program office addresses any significant privacy concerns which may be raised by such initiatives.

(4) Ensuring any requested facility staff or area of the program office is available to the VHA PCA Office for audit within 30 calendar days of the requested audit date, unless a later date is negotiated with the VHA PCA Officer. PCA must be granted immediate access to a facility if the PCA Officer determines that the circumstances warrant an urgent audit.

(5) Ensuring completion of all post-audit risk mitigation activities required by the PCA Office are conducted by the facility within the time frame specified by PCA, unless otherwise approved by the PCA Officer.

(6) Cooperating with the PCA Office in all matters concerning C3R activities.

k. **Veteran Integrated Service Network Directors.** VISN Directors are responsible for:

(1) Ensuring that all privacy, FOIA and records management functions within their VISN are assigned and performed in compliance with all Federal laws and regulations, VA regulations and policies, and VHA policies that address these functions. VISNs are not required to conduct regular self-assessments unless otherwise instructed by the PCA Officer to do so. VISNs may also be subjected to a PCA audit at the discretion of the PCA Officer. ***NOTE:*** *If the PCA Officer gives instruction to complete a self-assessment, the VISN may request a waiver for conducting assessments if the VISN Director certifies that the function of the office does not involve the direct use or disclosure of III. VISNs may choose to conduct self-assessments voluntarily as a means of reviewing their own compliance proactively. VISNs may not request a waiver for any FOIA audits administered by PCA in compliance with the FOIA Improvement Act.*

(2) Appointing individuals to serve as the VISN Privacy and FOIA Officers and Records Manager; delegating authority to these individuals to administer the VISN privacy, research privacy, FOIA, and records management programs and C3R activities; and provide VISN oversight to these programs within the facilities subordinate to the VISN.

(3) Ensuring that the privacy, research privacy, FOIA, and records management programs in their VISN are appropriately supported with resources, management support, and operational integration.

(4) Ensuring that the VISN Privacy and FOIA Officers and Records Manager serve as liaisons between the VHA PCA Office, the VISN, and the VA Health Care Facilities within the VISN.

(5) Ensuring the VISN Privacy and FOIA Officers and Records Manager and/or their alternates are included in discussions regarding strategic initiatives, to guarantee that VISN leadership can address any privacy, FOIA, and records management concerns raised by such strategic initiatives.

(6) Ensuring that the VISN Privacy and FOIA Officers and Records Manager consolidate all data requests from PCA and provide responses within requested timeframes.

(7) Ensuring any requested VISN staff or area of the VISN Office are available to PCA for audit within 30 calendar days of the requested audit date, unless a later date is negotiated with the VHA PCA Officer. PCA must be granted immediate access to a facility if the PCA Officer determines that the circumstances warrant an urgent audit.

(8) Ensuring completion of all post-audit risk mitigation activities required by PCA are conducted by the facility within the time frame specified by that office, unless otherwise approved by the PCA Officer.

l. **Veterans Integrated Service Network Privacy and FOIA Officers and Records Manager.** VISN Privacy and FOIA Officers and Records Managers are responsible for:

(1) Ensuring a C3R program is implemented in each facility within the VISN in accordance with this directive.

(2) Assisting facilities within the VISN with meeting logistical or staffing requirements for PCA audits, if requested by the facility.

(3) Assisting facilities within the VISN with risk mitigation and remediation activities as requested. In instances of unsatisfactory progress with the ePAT reporting or ongoing non-compliance, assisting PCA with facility failure to mitigate risks, lack of cooperation or other non-responsiveness.

(4) Ensuring all facilities within the VISN comply with the completion and submission of the quarterly FSAs, including FSAs for off-site clinics, by the last day of each quarter.

(5) Facilitating facility Privacy/FOIA Officer(s) and Records Manager access to information when required to fulfill the C3R responsibilities established by this directive (e.g., access to contracts generated by a regional contracting office in order for the Privacy Officer to review the facility's compliance with VA Handbook 6500.6, Contract Security, dated March 12, 2010).

(6) Reviewing the duties and activities at the VISN level, that are consistent with the duties of facility Privacy/FOIA Officer(s) and Records Managers as outlined in this directive when specifically requested by PCA.

(7) Reviewing PCA compliance reports for facilities within the VISN and develop strategies and remediation actions to deploy VISN-wide solutions addressing trends of non-compliance.

(8) Collaborating with the assigned PCA Lead Compliance Specialist to promote an effective relationship that facilitates C3R in their VISN.

m. **VA Health Care Facility Director.** The VA Health Care Facility Director is responsible for:

(1) Ensuring that all Privacy, FOIA, and Records Management functions within the facility are assigned and performed in compliance with all Federal laws and regulations, VA regulations and policies, and VHA policies that address these functions. This includes formal delegation of competent Privacy and FOIA Officers and Records Manager and at least one competent alternate for each of these positions.

(2) Being knowledgeable about the content and operation of the Privacy program; and ensuring that all operations and practices are being conducted in continuing compliance with the laws, regulations and standards which govern these activities and the highest standards of ethical conduct related to privacy rights and responsibilities of the individuals whose data VA collects, uses, maintains and discloses.

(3) Employing at least one dedicated, full time, senior-level Privacy Officer, charged with responsibility of day-to-day operations, implementation and effectiveness of the Privacy Program.

(a) The dedicated, full time, senior-level Privacy Officer must report directly to and be supervised by the VA Health Care Facility Director, the VA Health Care Facility Associate Director, or a senior individual who reports directly to and is supervised by the VA Health Care Facility Director and whose primary responsibilities at the facility include privacy program compliance.

(b) Regardless of to whom the individual reports at the facility, the facility Privacy Officer must have a dotted line reporting relationship to the VISN Privacy Officer who shall assist the VA Health Care Facility Director in the recruitment, onboarding, and ongoing management and performance review.

(c) The VISN Privacy Officer will provide input into the performance review.

(d) The VA Health Care Facility Director will not remove a VA Health Care Facility Privacy Officer without first discussing the circumstances with the VISN Privacy Officer. If there is an irreconcilable difference of opinion, the removal issue shall be raised with the VISN Director and adequate time shall be provided for a neutral adjudication if necessary. Working collaboratively with the VISN Privacy Officer, an Acting VA Health Care Facility Privacy Officer will be appointed in the absence of the incumbent.

(4) Ensuring that the Privacy Officer is not encumbered with collateral duties that impair their independence or otherwise prevent the operation of an effective Privacy Program.

(a) If collateral duties are assigned, the Director is responsible for ensuring that these duties do not create a conflict of interest with respect to the Privacy Officer's Continuous Readiness Review and Remediation responsibilities as set forth in this Directive, associated Guidebooks, and other VHA operational guidance.

(b) Collateral duties should also not create excess burden on the Privacy Officer and prevent the support and maintenance of an effective Privacy program.

(c) ***NOTE:*** *The Privacy Officer position is not conducive to virtual or remote coverage due to the C3R responsibilities contained in this directive. Teleworking should also not be allowed for more than one to two days per month.*

(5) Ensuring that the designated Privacy Officer has access to the Director as needed for privacy issues that need the directors attention or at a minimum of once per quarter for a face-to-face meeting to discuss the status of the Privacy Program. If the program is found to be failing to meet policy and regulatory compliance, these meetings should be more frequent until compliance is obtained and maintained; and must have direct access to the Director with regard to any issues of significance at any time.

(6) Ensuring that the PCA Office has access to appropriate areas of the facility and facility staff in order to conduct an audit within 30 calendar days of the requested audit date, unless a later date is negotiated with the PCA Officer. PCA must be granted immediate access to a facility if the PCA Officer determines that the circumstances warrant an urgent audit.

(7) Promoting a facility culture that enables staff to meet the requirements of all applicable Federal, VA, and VHA privacy, research privacy, FOIA, and records management statutes, regulations, and policies.

(8) Implementing business processes, providing adequate staffing, and taking other actions necessary to create and maintain privacy, research privacy, FOIA, and records management programs that comply with all Federal laws and regulations, VA regulations and policies, and VHA policies.

(9) Ensuring that documentation of all C3R activities is created and maintained consistent with VHA Record Control Schedule (RCS) 10-1 and the NARA General Records Schedule (GRS) requirements.

(10) Conducting operations in a manner that ensures patient safety, while also enabling compliance through the use of local policy and sound standard operating procedures (SOPs), based on national VHA privacy, FOIA, and records management policies.

(11) Ensuring use of C3R tools provided by the PCA Office to assess the facility's compliance with Federal privacy laws, Federal regulations, and VA and VHA privacy, FOIA, and records management policies.

(12) Ensuring the facility Privacy and FOIA Officers and Records Manager are involved in operational and strategic planning to provide the privacy, FOIA, and records management perspectives for facility decision-making.

(13) Providing the facility Privacy and FOIA Officers and Records Manager the needed support and resources to develop their respective roles and the awareness of

those roles within the facility and delegating appropriate authority in writing for them to exercise their privacy, FOIA, and records management duties.

(14) Upon PCA's request, certifying annual training completion to PCA, the VHA Privacy Office, or the VHA Records Management Office for all workforce members. ***NOTE:*** *This is based on the reports generated by the facility Privacy Officer(s), Records Manager, and Education Coordinator or Education Office.*

(15) Ensuring all complaints, incidents, and/or breaches of an individual's privacy are documented by the facility Privacy Officer(s) in the PSETS.

(16) Ensuring prompt reporting of any privacy complaint, allegation, or activity that has the potential of VISN-level or national-level impact to the VHA Privacy Office.

(17) Responding to facility-specific allegations or complaints of activities that violate Federal laws and regulations, VA regulations and policies, and VHA policies regarding privacy, FOIA, or records management.

(18) Ensuring prompt investigation of each allegation or complaint and complete documentation of the investigation and resolution thereof.

(19) Cooperating fully with the VHA Privacy Office in any investigation, mediation strategies, or correspondence that is required in order to investigate and resolve a complaint or allegation.

(20) Ensuring that privacy training records for all workforce members (employees, volunteers, students, and contractors) are readily available to the Privacy Officer(s) to review as defined in this directive, to ensure that training requirements defined in VHA Directive 1605.01 are continuously met.

(21) Ensuring completion of all post-audit risk mitigation activities required by PCA are conducted by the facility within the time frame specified by that office, unless otherwise approved by the PCA Officer.

(22) Cooperating fully with PCA during Post-Audit Oversight to ensure the facility promptly remediates non-compliance identified by PCA as defined in paragraph nine of this directive. ***NOTE:*** *Facilities must continue their remediation activities until all non-compliance identified during a PCA Audit have been resolved.*

(23) Ensuring that the Privacy Officer and Records Manager (or their alternates) are active participants in the facility Environment of Care (EoC) Rounds, in order to evaluate the physical environment related to Privacy and Records Management with facility leadership present, and that all deficiencies identified during these EoC Rounds are addressed in a satisfactory manner according to facility policy.

(24) Cooperating with PCA in all matters concerning PCA audits and C3R.

n. **VA Health Care Facility Privacy Officer.** The VA Health Care Facility Privacy Officer is responsible for:

(1) Managing and conducting C3R of the facility Privacy Program in accordance with all applicable VA and VHA privacy policies, rules and regulations.

(2) Serving as the facility POC and privacy Subject-Matter Expert (SME) for all privacy matters in the facility.

(3) Reporting directly to the facility Director or Associate Director for activities of the facility Privacy Program.

(4) Regularly participating in new-employee orientation to introduce themselves as the facility Privacy Officer, provide a basic overview of the privacy program, and inform new employees of their privacy responsibilities.

(5) Ensuring that all workforce members (employees, volunteers, students and contractors) complete mandatory privacy training, in conjunction with the facility Education Coordinator or other staff/office, per facility policy, and review training records as per Appendix D in this directive.

(6) Providing training and information to facility workforce members on how to contact the facility Privacy Officer(s) in the event of a complaint, incident or breach, or to ask questions concerning the privacy program.

(7) Conducting continuous privacy awareness activities in the facility for workforce members and Veterans, including participation in VA's annual Privacy and Information Protection weeks.

(8) Administering facility C3R activities, documenting the findings of these activities, remediating non-compliance, recording actions taken and making the documentation of these actions available to PCA upon request. ***NOTE*****:** *This requires that all C3R activities are appropriately documented. C3R tools and checklists on the PCA intranet site or other tools generated by the facility may be used to ensure documentation.*

(9) Developing and implementing a formalized and documented privacy C3R program as outlined in Appendix D of this directive and conducting C3R activities at the frequencies required by the program.

(10) Conducting a monthly physical evaluation of a reasonable cross-section of facility operations in order to review operational compliance with privacy requirements. This may be accomplished by ongoing C3R throughout the month. These evaluations must include:

(a) A review of a reasonable cross-section of the parent facility and associated buildings and all subordinate clinics to evaluate reasonable physical safeguards. ***NOTE*****:** *EoC Rounds may supplement this process as a means of showing facility*

leadership non-compliant areas of the operation and only satisfies this requirement for monthly physical evaluation for a review of reasonable physical safeguards.

(b) Interviewing staff to assess awareness of the privacy program and staffs' specific roles in privacy.

(c) Observing workforce behaviors and actions.

(11) Working with the Contracting Officer and Contracting Officer's Representative to ensure that contracts, purchase orders, or other acquisition documents include all the clauses needed to safeguard sensitive information, when appropriate, and reviewing to ensure that the Privacy Officer is kept involved in the contracting process. This includes coordination with the facility Information System Security Officer (ISSO) and other personnel to complete the review checklist, as required by VA Handbook 6500.6.

(12) Completing and submitting the Privacy FSA, to include all off-site clinic locations, within established timeframes specified by PCA.

(13) Reviewing and updating the facility privacy policy and all other policies and procedures that have privacy implications at least annually for consistency and compliance with legislative and policy changes.

(14) Developing, in coordination with the facility Education Coordinator/Education Office or other designated office, a local level privacy training strategy that outlines the facility procedures for ensuring compliance with the annual privacy training requirement established by current VHA policy.

(15) Conducting C3R to ensure that facility workforce members are aware that III contained in VHA records may only be used in the performance of their official job duties for treatment, payment, or health care operations.

(16) Conducting C3R to ensure that supervisors are assigning functional categories and are explaining minimum necessary access to their employees, that this assignment and explanation is documented, and the assignment of functional categories is completed in accordance with VHA Directive 1605.02, Minimum Necessary Standard for Protected Health Information, published April 4, 2019.

(17) Conducting C3R to ensure that the facility's PSETS files are maintained in accordance with VHA Directive 1605.01.

(18) As applicable, conducting a review of human study research protocols to ensure the privacy requirements are met prior to allowing the Principal Investigator to begin collecting and using protected health information (PHI), maintaining appropriate documentation of this process, and providing the documentation to PCA upon request.

(19) Fully cooperating with PCA during Post-Audit Oversight as defined in paragraph nine of this directive.

o. **VA Health Care Facility Records Manager.** The VA Health Care Facility Records Manager is responsible for:

(1) Managing and reviewing the facility records management program in accordance with this directive, VHA Directive 6300.01, and all other applicable Federal, VA, and VHA records management laws, regulations, and policies.

(2) Collaborating with the facility Privacy Officer to ensure that Federal records that contain sensitive or protected information are managed and maintained with reasonable physical safeguards sufficient to protect them from unauthorized access.

p. **VA Health Care Facility FOIA Officer.** The Health Care Facility FOIA Officer(s) acts as the SME and is the POC for the FOIA. The facility FOIA Officer is responsible for completing all FOIA-related C3R activities designated by the PCA Officer for the purpose of complying with the FOIA Improvement Act of 2016. For further details, see paragraph 15 of this directive.

q. **VHA Contracting Officers and Contracting Officer Representatives.** VHA Contracting Officers and Contracting Officer Representatives are responsible for:

(1) Reviewing contractor compliance with privacy and records management clauses in contracts and providing documented evidence to facility Privacy Officers, facility Records Managers, VISN Privacy Officer and Records Managers, and PCA upon request.

(2) Reviewing contractor compliance with BAAs and providing documented evidence to facility Privacy Officers, VISN Privacy Officer, and PCA upon request.

(3) Taking appropriate actions against contractors and Business Associates who fail to mitigate non-compliance with privacy and/or records management clauses in contracts and terms of BAAs.

r. **VHA Workforce.** The VHA workforce is responsible for:

(1) Using, disclosing, and protecting III in accordance with the facility privacy program and Federal, VA, and VHA laws and policies.

(2) Cooperating with the facility Privacy Officer to ensure that they:

(a) Know the name and location of the facility's Privacy Officer(s) and how to report misuse or breaches of information to the Privacy Officer(s).

(b) Respond to investigations regarding data breaches as necessary.

(c) Being aware of their assigned functional category(ies) and that they only access the minimum information necessary to conduct their official duties.

(d) Practice auditory privacy when discussing an individual's private information and protect their work areas from unauthorized access.

(e) Protect information in their possession according to VHA and facility privacy policies and procedures.

6. KEY ELEMENTS OF THE PRIVACY COMPLIANCE ASSURANCE PROGRAM

The PCA Program was established in order to establish and maintain a culture within VHA that promotes Federal privacy, research privacy, FOIA, and records management compliance. The key elements of the program include:

a. Conducting independent performance audits and reviewing overall program(s) compliance at VA Health Care Facilities.

b. Development and management of PCA operations, tools and activities specific to audits, C3R, and FSA processes and tools for use by VA Health Care Facilities.

c. The establishment of baseline performance auditing and C3R requirements for PCA and VA Health Care Facilities specific to Privacy, Research Privacy, and FOIA. The baseline compliance requirements for records management are defined in VHA Directive 6300.01, established by the VHA Records Management Office, which delegates C3R responsibilities for Records Management to PCA. PCA supports an enterprise-wide auditing, analysis, reporting, oversight, and C3R program within VA by collaborating with Department-level compliance programs for enterprise-wide reporting and risk mitigation. PCA conducts audit activities in compliance with the GAGAS as defined by the Government Accountability Office (GAO) where feasible.

d. Emphasis on the most stringent provisions of privacy, research privacy, FOIA, and records management compliance. VHA facilities must apply this directive such 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 are provided. ***NOTE:*** *VA Health Care Facilities must also adhere to other VA and VHA directives implementing privacy and records management policies to be in compliance with privacy and records management requirements.*

7. PCA COMPLIANCE AUDITING AND C3R TOOLS

PCA uses several distinct tools for gathering data in order to audit compliance within VHA. PCA staff, facility Privacy and FOIA Officers, and facility Records Managers use these tools to evaluate and review the activities of their respective programs. PCA may develop and deploy other tools as necessary for auditing and reviewing Privacy, FOIA, Records Management, Business Associates and other applicable programs' compliance.

a. **PCA Compliance Auditing Tools and Electronic Compliance Auditing Tool.** Compliance Auditing Tools (CAT) and the electronic Compliance Auditing Tool (eCAT) are PCA's primary tools for conducting and documenting audits of VA Health Care

Facilities. Access to these tools will be granted to all PCA staff for conducting audits. The questions that define the audit criteria are accessed within the eCAT and used by the audit team to systematically evaluate each program and document the findings for each audit criteria. ***NOTE:*** *these tools were formerly known as Compliance Monitoring Tools (CMT) and the electronic Compliance Monitoring Tool (eCMT).*

b. **Business Associate Compliance Auditing Tool.** PCA uses these tools to conduct and document Privacy and Records Management audits of National Business Associates as deemed necessary by the VHA PCA Officer. At its discretion, PCA may conduct these audits electronically. The Business Associate Compliance Auditing Tool (BA-CAT) is utilized in the same manner as the CAT and eCAT above.

c. **Facility Self-Assessment Tools.** Facilities have FSA tools available to conduct self-assessment activities for their programs as defined in this directive. PCA at its discretion may develop, edit or suspend the use of any of these tools to manage the FSA process. The VA Health Care Facility must use the appropriate tools to conduct and document its annual FSA and submit the FSA to PCA as required in this directive. Individuals who are responsible for completing an FSA are provided access to these tools when necessary. Other FSA tools may be developed and deployed to Business Associates or other applicable programs as deemed necessary by the VHA PCA Officer.

d. In collaboration with the VHA Privacy, FOIA, and Records Management Offices, the VHA PCA Officer must review and update the content of these auditing and C3R tools annually.

8. PCA AUDITS OF HEALTH CARE FACILITY

a. PCA Audits are conducted by the VHA PCA Office and are coordinated with the audited VA Health Care Facility's leadership as well as the facility Privacy and FOIA Officers or privacy and FOIA POCs. ***NOTE:*** *If the facility does not have a Privacy or FOIA Officer or POC at the time of the PCA Audit, the alternate or acting for the respective program must be prepared to coordinate the audit with the PCA Audit Coordinator.* The VHA PCA Office may conduct audits in conjunction with or on behalf of other VA or VHA programs or other agencies. These audits are administered on a fixed three-year cycle with each facility being assigned to a specific cycle-year. The frequency of the cycle or number of audits conducted may be changed at the discretion of the PCA Officer based on business needs. ***NOTE:*** *The process discussed in this paragraph will also be followed for applicable VHA Business Associate audits.*

b. When PCA has identified a facility to be audited, VHA leadership will be notified of the audit via the method outlined in the PCA Communication Plan.

c. Once VHA leadership has been notified, the facility Director or Program Officer is contacted. The Director or Program Officer must make the facility and personnel available for the audit in accordance with this directive.

d. PCA will provide the facility with general audit information prior to the audit to assist in the facility's preparation. The facility Privacy Officer may conduct a pre-audit of the facility using the PCA audit tools in order to identify and mitigate any deficiencies prior to the audit. Information on how to prepare for an audit is available on the PCA intranet Web site (VHA Privacy Compliance Assurance Visits Page at http://vaww.vhaco.va.gov/privacy/PCA-visits.htm. ***NOTE:*** *This is an internal VA Web site that is not available to the public.)*

e. PCA will conduct a pre-audit review of all necessary documentation as outlined in the Audit Preparation Guide, which will be provided to the Facility Director/Program Officer at least 30-days prior to the audit. ***NOTE:*** *If an emergent audit is determined to be warranted by the PCA Officer, a 30-day notice may not be provided.*

f. The Audit Preparation Guide contains the Document Review List that must be followed for submitting documents to PCA prior to an audit. Failure to follow this list will result in a finding of non-compliance for all documents not provided. This Guide is available on the PCA Intranet site. The guide also includes specific instructions for how to prepare for an audit and how to provide documentation to the audit team using the PCA Audit Portal located at https://vaww.vashare.vha.va.gov/sites/PCAAuditPortal/SitePages/Home.aspx. ***NOTE:*** *This an internal VA Web site and is not available to the public.*

g. The facility must provide documentation as instructed in the Audit Preparation Guide and PCA Audit Portal including the types of documents to be provided, security of the documents, naming conventions and readable formats. Documents will be uploaded into the PCA Audit Portal according to instructions provided on the Portal and during the audit preparation call conducted approximately 30 days prior to the audit. All required documents must be uploaded by the deadline established by the PCA Officer.

h. PCA will conduct records management audits in accordance with VHA Directive 6300.01 and this directive. VA Health Care Facilities being audited by PCA for Records Management compliance must adhere to the requirements related to records management and any applicable general C3R requirements in this directive as well as the requirements for compliance-monitoring defined in VHA Directive 6300.01.

i. The PCA Audit Team conducting performance audits must:

(1) **Provide an Entrance Briefing (In-Briefing).** The PCA Audit Team must provide an entrance briefing to the VA Health Care Facility leadership including, but not limited to: facility Director or program office Director and their associates, Chief of Staff, Privacy Officer, FOIA Officer, Records Manager and other officers or personnel deemed appropriate by the facility. This briefing will address the scope of the audit, the protocols and agenda that the PCA Audit Team will follow, the methods used, the PCA Audit Team membership, the facility staff expected to participate, and what to expect during the exit-briefing. ***NOTE:*** *Findings of significant risk during a PCA audit will be reported to the facility leadership immediately for corrective action and will not be withheld until the end of the audit.*

(2) **Conduct Focused Workforce Interviews.** The PCA Audit Team interviews key facility personnel, including the Privacy Officer, FOIA Officer, Records Manager, Health Information Management (HIM), Occupational Health professional, VA Police, selected Contracting Officer Representatives, and other personnel identified by the PCA Audit Team. These focused interviews will target individuals with unique or specific job duties related to the programs being audited. Interview topics include, but are not limited to:

(a) Privacy and FOIA Officer assignments, duties, and skills related to privacy and FOIA, including a review of privacy research protocols.

(b) Privacy Officer's involvement in the contracting and BAA processes.

(c) Processes for investigating and resolving privacy complaints, incidents, and breaches.

(d) Focused knowledge about their program specific responsibilities directly impacting the programs being audited.

(e) Other topics pertinent to the programs being audited.

(3) **Conduct General Workforce Interviews.** The PCA Audit Team will conduct interviews of a random sampling of the general workforce members of the audited facility. PCA will utilize a standardized methodology in order to minimize the time it takes to conduct these interviews so as to minimize the impact on workforce productivity. The audit team will utilize the most suitable interview method necessary to interview a statistically-significant sample of the general workforce. If the method used is face-to-face, the audit team will read prescribed interview questions to the interviewee, which will ensure that there is no personality conflict between the interviewer and interviewee or miscommunication that could lead to an unfair interview process. PCA may, at its discretion, conduct workforce interviews online or using other technology to obtain its interview sample. The interview findings will remain confidential, voluntary and anonymous. The interview questions must be directly related to the facility's practices and activities for the programs being audited. Interview topics include, but are not limited to:

(a) Employee knowledge about their specific job duties related to protecting Veterans' and employees' privacy.

(b) Veterans' Rights to privacy and employees' duties in the provision of these rights.

(c) Their role in the processes for investigating and resolving privacy complaints, incidents, and breaches.

(d) Other topics pertinent to the programs being audited.

(4) The team must also interview a random selection of supervisors and other pertinent workforce members (e.g., human resources personnel, occupational health, etc.). These interviews will include, but are not limited to:

(a) Individual responsibilities to follow privacy-related laws and policies.

(b) Assignment of functional categories.

(c) Knowledge of the minimum necessary access to information standard in the performance of their official duties.

(d) Accessibility of privacy policies and procedures.

(e) Knowledge of the privacy and records management programs and how to report privacy or records management issues or gain information on these programs.

(5) **Review of Documentation (Policies, Procedures, C3R Data, etc.).** The PCA Audit Team reviews:

(a) The facility's policies and procedures for privacy, FOIA, research, and records management.

(b) Other facility policies and procedures that impact the privacy, FOIA, research, and records management programs.

(c) SOPs and facility memoranda addressing guidance or requirements related to the audited programs.

(d) Reports requested by the Audit Team (e.g., training status report) and other official documentation (e.g., C3R data, delegations of authority, and complaint investigation correspondence) that provide evidence of the facility's compliance with Federal privacy statutes and regulations, and VA and VHA policies and procedures. ***NOTE:*** *All policies and procedures must be documented and in force. PCA will not recognize undocumented customs or practices as evidence of C3R data or policies and procedures for purposes of the compliance audit.*

(6) **Conduct a VA Health Care Facility Physical Evaluation.** The PCA Audit Team performs a physical evaluation of a reasonable cross-section of all facility operations including any remote locations used by the facility. This evaluation assesses the physical environment to include reasonable physical safeguards, workforce responsiveness, auditory privacy, records storage and accessibility, placement of equipment generating or containing PHI/III and the overall protection of documents and systems containing PHI/III as well as other factors related to physical operations impacting privacy, FOIA, and records management. An after-hours evalution may also be conducted at PCA's discretion to assess the physical environment after business operations have ceased for the day. During the physical evaluation, the PCA Audit Team will note all general instances of non-compliance. Facility staff accompanying the PCA Audit Team is responsible for documenting any specific findings during the physical evaluation, and for implementing appropriate corrective actions.

(a) The physical evaluation includes visual observations of the grounds, buildings, operations, and services, including a sample of Offsite Clinic locations and other offsite

buildings, which may house facility or contracted staff, facility operations or VHA information in any form.

(b) Facility personnel must not interfere with or influence the physical evaluation or its outcomes. As a general practice, the PCA Audit Team may be escorted by facility personnel. However, the PCA Audit Team must be allowed to walk through areas of the facility separate from, but still in visual contact with, the facility escort to ensure that the privacy culture observed is representative of day-to-day operations.

(c) The PCA Audit Team may, at its discretion, interview any workforce member to inquire about their knowledge of privacy, research privacy, FOIA, or records management responsibilities or practices. PCA will utilize a standardized methodology of interviewing in order to ensure consistency and efficiency. Interviews of general workforce members will be kept confidential, anonymous, and voluntary. The information gathered in workforce interviews will be aggregated to reflect overall knowledge and skills, and not depict the performance of any individual employee.

(d) The PCA Audit Team will take necessary measures to minimize any impacts to normal operations and patient care and may decide to abbreviate the physical evaluation in areas where operations are complex or the workforce is significantly busy. PCA may impact normal operations during the physical evaluation where the negative impact of the non-compliant issue to VHA outweighs a disturbance in facility operations. ***NOTE:*** *If the PCA Audit team conducts a physical evaluation virtually due to special circumstances, the audit team will require the facility to provide evidence of compliance sufficient to evaluate the physical environment for compliance. Evidence may include, but is not limited to: photographs, attestations from key personnel, use of technology such as Skype or FaceTime, etc.*

(7) **Provide an Exit Briefing.** Upon completion of the audit, the PCA Audit Team must provide an exit briefing to the facility Director or Program Office Director and their associates, Chief of Staff, Privacy Officer, FOIA Officer, Records Manager, and other officers or personnel deemed appropriate by the facility. During this briefing, the PCA Audit Team must:

(a) Present an Executive Summary that outlines the facility's overall program compliance in the form of performance scores for each overall program that was evaluated (e.g., Privacy, Research Privacy, FOIA, and Records Management). The Executive Summary will also provide scores for each of the elements comprising each of these overall programs. (Example: The facility will receive an overall score for the Privacy Program, as well as scores for the individual Privacy Program components, such as policy, reasonable safeguards, program C3R activities, etc.) The compliance scoring methodology will be determined by the PCA Officer in collaboration with VHA senior leadership and may be changed at the PCA Officer's discretion.

(b) Identify and explain any specific findings that significantly impacted the facility's overall performance scores. In addition, the PCA Audit Team may highlight areas in which the facility's programs demonstrated exceptional strength or best practices.

(c) Introduce the PCA Post-Audit Oversight process for how the facility will be expected to conduct remediation actions. The Post-Audit Oversight Coordinator assigned to the facility may participate in the Exit Briefing.

(8) **Use of PCA Audit Findings.** PCA Performance Audit findings are primarily for the purpose of identifying program non-compliance in order to remediate weaknesses and improve overall program effectiveness. The findings reflect non-compliant business processes and the cumulative performance of facility leadership, supervisory staff, program officers (e.g., Privacy and FOIA officers and Records Manager) and the general workforce. These findings must not be used as a means of evaluating the success of the Privacy, FOIA Officer(s), and Records Manager. The audit results are cumulative of the actions, knowledge and skills of all facility leadership, supervisory staff, program officers, and the general workforce.

9. PCA POST-AUDIT OVERSIGHT

PCA will maintain a Post-Audit Oversight process to follow-up on the audited facilities' responsiveness to non-compliance identified during a PCA Audit. The required components of this oversight process are described in Appendix C, Required Components of PCA Post-Audit Oversight. ***NOTE:*** *All of the material in Appendix C constitutes mandatory policy material.*

10. PROGRAM COMPONENTS AUDITED UNDER THIS DIRECTIVE

a. **Auditing and C3R of All Privacy Program Components.** "Figure 1" in Appendix A depicts all of the major components of a Privacy Program. The auditing and C3R activities required in this directive are divided into these components. Some of the components address basic regulatory or policy compliance, while other components address the sustainability of the program over time and varying circumstances. These components will be audited and reviewed by various means determined by PCA to include, but are not limited to, PCA on-site audits, quarterly administration of FSAs, special component-specific audits and special audits of VISNs or VHA program offices.

b. **Auditing and C3R of All FOIA Program Components.** "Figure 2" in Appendix A depicts all of the major components of a FOIA Program. The anditing and C3R activities required in this directive are divided into these components. Some of the components address basic regulatory or policy compliance, while other components address the sustainability of the program over time and circumstances. These components will be audited and reviewed by various means determined by PCA to include, but are not limited to, PCA on-site audits, quarterly administration of FSAs, special component-specific audits and special audits of VISNs or VHA program offices.

c. **Auditing and C3R of All Records Management Program Components.** "Figure 3" in Appendix A depicts all of the major components of a Records Management Program. Records Management components audited by PCA are defined in VHA Directive 6300.01 along with other C3R requirements administered by PCA and completed by VA Health Care Facilities.

11. REPORTING OF CONTINOUS READINESS REVIEW AND REMEDIATION

a. PCA will develop various regular and ad hoc reports that depict the compliance performance of the privacy, research privacy, FOIA, and records management programs in VHA. PCA will generate reports in an objective, statistically-significant manner. If PCA is unable to collect a sufficient sample to reflect a minimum of one-third of the overall VA Health Care Facilities, only the performance of each individual facility audited will be reported and a VHA overall average cannot be reflected from a sample size smaller than one-third of the facilities. These reports include, but are not limited to:

(1) **Executive Summary Report.** Outlines the specific findings, by program components, of a VA Health Care Facility and is provided to facility leadership at the close of a PCA Audit. This report may also be provided to VHA leadership and other oversight organizations as determined by the PCA Officer.

(2) **Detailed Report.** Provides the status of all audit criteria used to evaluate the program. This report is generated using the electronic Post-Audit Tool (ePAT). This report and the prioritized action plan include the findings for each individual element audited by PCA. This report may be provided to VHA leadership or external oversight bodies to report detailed findings of a PCA Audit.

(3) **Post-Audit Oversight Report.** Provides a general status of VHA's or a specific VA Health Care Facility's remediation actions based a review of the actions and supporting documentation provided in the ePAT during Post-Audit Oversight. This report may be provided to VHA leadership or external oversight bodies to report detailed findings of a PCA Audit.

(4) **Privacy, FOIA, and Records Management Audit and C3R Report.** Provides the overall results of the audits and other C3R activities conducted on VHA facilities and the average performance, basic compliance and sustainability scores for the facilities within a fiscal year. The report is updated on a regular basis as audits are completed throughout the fiscal year and available through the electronic Compliance Auditing Database (eCAD, formerly electronic Compliance Monitoring Database (eCMD)) – Reports menu. This report is available to VHA program offices and VHA central office (VHACO) leadership as needed.

(5) **PCA Quarterly Audit and C3R Report.** Provides a high-level overview of the current audit and C3R activities conducted by PCA on VHA facilities within the given quarter of the fiscal year. This may include, but is not limited to, Facility Self-Assessment (FSA) completion status, audits conducted with the average performance score, and the top five high-risk non-compliant findings. The report is provided to VHA senior leadership and managers for the programs audited each quarter based on the completion of audits and other C3R activities.

(6) **PCA Annual Report.** Provides a combination of the results of PCA onsite audits, FSAs, and other progress reports specific to audits and C3R activities conducted or administered by PCA for the fiscal year. ***NOTE:*** *In the event that the PCA audit*

sample-size is less than the statistically-significant one-third of all VHA facilities, the Annual Report will reflect only the specific performance of the facilities audited and should not be interpreted as a VHA overall performance average.

(7) **Ad Hoc Reports.** Reports generated based on responses from oversight bodies, Congress, or other requestors for the compliance performance status of the programs audited by PCA. These reports may be provided in the form of the other reports listed in this paragraph or may be generated specific to the request for reporting from the oversight bodies. They include, but are not limited to:

(a) Department of Health and Human Services, Office for Civil Rights. Requests for any and all audit and C3R data related to Privacy as required by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

(b) National Archives and Records Administration. Requests for any and all audit and C3R data related to Records Management as required by the Federal Records Act.

(c) White House Office of Special Counsel. Requests for any and all audit and C3R data as required by the oversight authority of this Counsel.

(d) House and Senate Veterans Affairs Committees. Requests for any and all audit and C3R data as required by the oversight authority of these Committees.

(e) PCA may provide any of the above reports to the VHA Network Office representative for the VISN in which the facility falls, the VISN Privacy Officer, the VHA Chief of Staff or other appropriate VHA leadership as deemed necessary. PCA may request assistance from VISNs and VHA leadership in ensuring facilities fully remediate all findings from PCA audits reflected in these reports.

12. VA HEALTH CARE FACILITY PRIVACY OFFICER CONTINUOUS READINESS REVIEW AND REMEDIATION PROGRAM

The VA Health Care Facility Privacy Officer must develop documented C3R processes for each of the C3R requirements in Appendix D, Required Components of the VA Health Care Facility Privacy Officer Continuous Readiness Review and Remediation Program, according to the requirements set forth in this directive. ***NOTE:*** *All of the material in Appendix D constitutes mandatory policy material.* The Privacy Officer must maintain documentation of all required C3R activities in a manner that clearly defines the C3R activity, frequency of the activity, observations, and findings and remediation actions taken. This documentation must be maintained in accordance with VA Records Control Schedule 10-1, section 1008.

13. BUSINESS ASSOCIATE AGREEMENTS, CONTRACTS, AND DATA USE AGREEMENTS

a. **Business Associates.** The facility Privacy Officer must work in conjunction with the facility Information System Security Officer (ISSO), contracting personnel and/or Contracting Officer Representatives, VISN contracting personnel, and others as

necessary to engage in Business Associate Agreements (BAAs) according to VHA Handbook 1605.05, Business Associate Agreements, dated July 22, 2014, and VA Handbook 6500.6. The facility Privacy Officer must develop local facility policy (and standard operating procedures if necessary) that comply with these national requirements. The Privacy Officer must also establish a documented process for C3R of the facility's compliance with these requirements and must review BAA activities within the facility at least annually to include, but not limited to:

(1) C3R of the overall BAA development process to include:

(a) Reviewing the national BAA list maintained by the VHA National Data Systems Office at the Health Information Access BAA Web site (see http://vaww.vhadataportal.med.va.gov/PolicyAdmin/BusinessAssociateAgreements.aspx) to determine if a national BAA is already signed with the contractor prior to engaging them in signing a new local BAA. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

1. If a national agreement is in place, reviewing to determine whether the agreement covers the services the facility is receiving from the vendor.

2. If a national BAA is in place, and the services received by the facility are covered in the national BAA, the Privacy Officer must review to determine that:

a. A local BAA is not processed.

b. The contractor is aware that the terms of the national BAA also apply to the relationship with the facility.

c. The national BAA is relied upon and that the facility holds the Business Associate accountable to the terms of the national BAA.

3. If a national BAA is in place and the services received by the facility are not covered in the national BAA, the Privacy Officer must conduct C3R to determine that:

a. No Protected Health Information is disclosed to the Business Associate until the national agreement is modified and finalized.

b. A local BAA is not processed.

c. The national BAA with the vendor is modified by VHA National Data Systems (NDS), Health Information Access (HIA) as necessary to cover services received by the local facility prior to the facility relying on the national agreement.

(2) Once modified, the national BAA is relied-upon and that the facility holds the Business Associate accountable to the terms of the national BAA.

4. If a national agreement is not in place, the Privacy Officer must conduct C3R to determine that:

a. No Protected Health Information is disclosed to the Business Associate until a local Business Associate Agreement is finalized.

b. The most recent BAA template is utilized by Contracting Officers or other individuals responsible for initiating local BAAs.

c. The preamble language of the BAA accurately reflects the services provided by the contractor.

d. The appropriate parties are listed on the BAA and that all parties have signed it and it is fully completed and enforceable.

e. All contractors that have access to sensitive information are up to date with the appropriate training requirements.

f. The signatory for the facility is duly delegated to sign BAAs by the facility Director.

g. All local BAAs are loaded promptly to the VHA National Data Systems Office at the Health Information Access BAA Web site (see http://vaww.vhadataportal.med.va.gov/PolicyAdmin/BusinessAssociateAgreements.aspx). ***NOTE:*** *This is an internal VA Web site that is not available to the public*.

h. Conducting C3R, in conjunction with Contracting Officers and their representatives, local Business Associates with whom the facility has entered into local BAAs to ensure the Business Associates complies with the terms of the agreements. ***NOTE:*** *Conducting C3R of contractor performance may only be done by a warranted Contracting Officer or authorized Representative. The Contracting Officer or authorized Representative must provide sufficient feedback to the Privacy Officer to allow for this monitoring to take place.*

(3) Develop a documented process to conduct C3R of the facility's response to a discovery that a Business Associate is non-compliant with the terms of the BAA. The process must include steps that the facility will take to mitigate the non-compliance. The Privacy Officer must review at least annually to determine if the facility is appropriately responding to BAA non-compliance.

(a) When non-compliance is identified, the Privacy Officer or facility Director must inform the VHA Privacy Office and the Office of HIA of the situation to gain guidance on how to proceed with the contractor/vendor relationship to resolve the non-compliance. If the vendor does not comply, the vendor relationship must be terminated.

(b) If the relationship with the Business Associate cannot be terminated (e.g., VHA is required to use the Business Associate by regulation or for other reasons that the relationship cannot be severed), and the vendor is unable or unwilling to comply, the facility must obtain guidance from the VHA Privacy Office on how to report the vendor to the Department of Health and Human Services, Office for Civil Rights (HHS-OCR). ***NOTE:*** *The Facility Privacy Officer, in conjunction with the Contracting Officer or their*

Representative is responsible for conducting C3R of all local Business Associates. If a national BAA is used, the PCA Office is responsible for auditing national Business Associates. If the facility becomes aware of non-compliance of a Business Associate under a national BAA, the Facility Privacy Officer must inform the PCA Officer, the VHA Privacy Officer and HIA immediately.

b. **Contracts.** The facility Privacy Officer must conduct C3R of all contracts in accordance with VA Handbook 6500.6 to determine whether there are privacy implications, and whether privacy provisions are included in contracts when necessary. This review must be conducted in conjunction with Contracting Officers and their representatives. Contracts, purchase orders, and other agreements that have privacy-related components must adequately address privacy implications of creating, using, releasing, or dispositioning VHA information. This should also include a review to determine if the contractor or vendor is implementing safeguards and adhering to appropriate uses and disclosures of VHA information throughout the life of the contract. ***NOTE:*** *This C3R is satisfied by completing the Checklist for Information Security in the Initiation Phase of Acquisitions, as required in Appendix A of VA Handbook 6500.6.*

c. **Data Use Agreements.** Data Use Agreements (DUAs) define the specific arrangements that multiple parties must follow when exchanging or sharing VA information. The Privacy Officer must develop a local policy for entering into data use agreements that ensure that the Privacy Officer and Information System Security Officer (ISSO) are included in the creation of data use agreements related sharing or obtaining information from sources outside of the facility or when internal data-exchanges require a DUA by policy (e.g., use of Centers for Medicare and Medicaid Services (CMS) data). These policies must be in compliance with VHA Handbook 1080.01, Data Use Agreements, dated November 20, 2013, except as noted in that handbook. The Privacy Officer must review at least annually to ensure that the local policy contains elements requiring DUAs to include terms that:

(1) Govern the sharing of data between a Data Owner and Requestor.

(2) Define ownership as related to the data exchange.

(3) Establish the specific terms of use and disclosure for the Requestor.

(4) Provide a means to transfer liability for the protection of the data to the Requestor (if applicable).

(5) Serve as a means to establish criteria for using, disclosing, storing, processing, and disposing of data.

(6) Satisfy HIPAA requirements when providing information within Limited Data Sets for research.

(7) Reviewing existing DUAs at least annually to determine whether DUAs:

(a) Contain a privacy legal authority for sharing VHA data.

(b) Are fully executed and signed by all required parties.

(c) Are kept current and have not expired.

(d) Specifically address minimum-necessary access requirements appropriate with the approved use of the data.

(e) Have been uploaded to the VHA HIA DUA repository.

(8) Reviewing at least annually (and more frequently as necessary) to determine if the facility and its data-sharing partners are consistently following the terms of all DUAs entered into by the facility. This review must include, but is not limited to:

(a) Establishing a documented process to review DUA activities through random spot checks that address the requirements defined in this directive and VHA Handbook 1080.01.

(b) Reviewing the practices of the research or administrative uses of the data to determine if the terms of the DUA are being followed (e.g., storage or access requirements, scope of the use of the data, etc.).

(c) Collaborating with researchers and administrative users of national data sets (e.g., CMS data) and applicable program offices to evaluate compliance with the terms of DUAs related to these high-risk data sets.

14. HEALTH CARE FACILITY PRIVACY SELF-ASSESSMENT

a. The facility Privacy Officer(s) must conduct an FSA each quarter utilizing the Privacy FSA tool provided by PCA (see VHA Privacy Compliance Assurance – FSA at http://vaww.vhaco.va.gov/privacy/PCA-FSA.htm. ***NOTE:*** *This is an internal VA Web site that is not available to the public.)* The FSA will be administered in quarterly increments by program components as defined in this paragraph. The PCA Officer may change the specified components as necessary to ensure that the entire program is sufficiently evaluated over the course of a single fiscal year. Each VA Health Care Facility must submit its FSA as described in this paragraph. This assessment must be completed and submitted to PCA by the last day of each quarter of the fiscal year or as instructed by the PCA Officer.

b. VISN and program office Privacy Officers are only required to submit an FSA at the request of the PCA Officer. However, VISNs and program offices may conduct these assessments as local practice to review their program's compliance and submit them to PCA each quarter in the same manner as described in this paragraph.

c. PCA may report delinquent submissions to the VHA Network Office representative for the VISN in which the facility falls, the VISN Privacy Officer, the VHA Chief of Staff or other appropriate VHA leadership. PCA may request assistance from VISNs and VHA leadership in ensuring FSA submissions are completed timely.

d. In order to encourage ongoing C3R and to break the overall privacy program into more manageable increments, the annual FSA will be administered in quarterly submissions to PCA. The key components of the facility's privacy program must be assessed quarterly, in the following order unless otherwise determined by the PCA Officer:

(1) First quarter of the fiscal year:

(a) Program Support.

(b) Privacy Officer.

(c) Reasonable Safeguards.

(d) Date Destruction.

(e) Notice of Privacy Practices.

(f) Facility Complexity.

(2) Second quarter of the fiscal year:

(a) Program Support.

(b) Right of Access.

(c) Amendment of Records.

(d) Facility Directory.

(e) Confidential Communications.

(3) Third quarter of the Fiscal year:

(a) Program Support.

(b) Accounting of Disclosures.

(c) Release of Information.

(d) Research (Administered only to facilities with Research Programs).

(e) Information Access.

(4) Fourth quarter of the fiscal year:

(a) Program Support.

(b) Privacy Training.

(c) Complaints/Incidents.

(d) Contracting/BAAs/DUAs.

(e) Privacy Policies and Procedures.

(f) FSA submissions must be completed for each offsite clinic subordinate to the parent VA medical center or health system at least once each fiscal year. Facilities may submit the FSA for each offsite clinic in the quarter of their choosing based on what is convenient for them, but an FSA for all offsite clinics must be conducted and submitted to PCA sometime during the fiscal year. The offsite FSA covers all of the appropriate program components for the offsite clinic in one FSA and it is not broken into quarterly increments.

15. VA HEALTH CARE FACILITY FOIA OFFICER CONTINUOUS READINESS REVIEW AND REMEDIATION PROGRAM

The facility FOIA Officer must develop processes for each of the program requirements in Appendix E, Required Components of the VA Health Care Facility FOIA Continuous Readiness Review and Remediation Program. ***NOTE:*** *All of the material in Appendix E constitutes mandatory policy material.* The FOIA Officer must conduct these processes in a manner that ensures compliance with the FOIA, VA, and VHA FOIA policies and procedures. The FOIA Officer must demonstrate evidence of this compliance by completion of the FOIA FSA as outlined in paragraph 16 of this directive.

16. VA HEALTH CARE FACILITY FOIA FACILITY SELF-ASSESSMENT

a. The facility FOIA Officer(s) must conduct an FSA each quarter utilizing the FOIA FSA tool provided by PCA (See VHA Privacy Compliance Assurance – FSA at http://vaww.vhaco.va.gov/privacy/PCA-FSA.htm. ***NOTE:*** *This is an internal VA Web site that is not available to the public.)* The FSA will be administered in quarterly increments by program components as defined in this paragraph. The PCA Officer may change the specified components as necessary to ensure that the entire program is sufficiently evaluated over the course of a single fiscal year. Each VA Health Care Facility must submit its FSA by the last day of each quarter of the fiscal year unless otherwise directed by the PCA Officer.

b. VISN and program office FOIA Officers are only required to submit an FSA at the request of the PCA Officer. However, VISNs and program offices may conduct these assessments as a local practice in order to review their program's compliance and submit them to PCA each quarter in the same manner as described in this paragraph.

c. PCA may report delinquent submissions to the VHA Network Office representative for the VISN in which the facility falls, the VISN FOIA Officer, the VHA Chief of Staff or other appropriate VHA leadership. PCA may request assistance from VISNs, and VHA leadership in ensuring FSA submissions are completed on time.

d. In order to encourage ongoing C3R and to break the overall FOIA program into more manageable increments, the annual FSA will be administered in quarterly submissions to PCA. The key component of the facility's FOIA program must be assessed quarterly in the following order unless otherwise determined by the PCA Officer:

(1) First quarter of the fiscal year:

(a) Program Support.

(b) Delegation of FOIA Officer.

(c) Disclosure of Records.

(d) Assessment of Fees.

(e) Fee Waivers.

(2) Second quarter of the fiscal year:

(a) Program Support.

(b) Timely Processing.

(c) Use of Exemptions.

(d) Substantial Interest Request Processing.

(e) Facility Policies and Procedures.

(3) Third quarter of the fiscal year:

(a) Program Support.

(b) Correspondence.

(c) Administrative Files.

(d) Dispute Resolution*.

(4) Fourth quarter of the fiscal Year:

(a) Program Support.

(b) FOIA Electronic Tracking.

(c) Records Retention.

(d) FOIA Training.

(e) Agency Regulations*.

NOTE: *FOIA Program components denoted with an asterisk, "Dispute Resolution" and "Agency Regulations," are primarily related to VHA FOIA Office compliance and not to field FOIA programs*.

17. TRAINING

There are no formal training requirements associated with this directive.

18. RECORDS MANAGEMENT

All records regardless of format (paper, electronic, electronic systems) created in the requirements of this directive shall be managed per the National Archives and Records Administration (NARA) approved records schedules found in VHA Records Control Schedule 10-1. If you have any question regarding any aspect of records management you should contact your facility Records Manager or your Records Liaison.

19. REFERENCES

a. Pub. L. 114-185.

b. 5 U.S.C. 552 and 552a.

c. 38 U.S.C. 5701, 5705, and 7332.

d. 45 CFR 160 and 164.

e. VA Directive 6371, Destruction of Temporary Paper Records, dated April 8, 2014.

f. VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008.

g. VA Directive 6511, Presentations Displaying Personally Identifable Information, dated January 7, 2011.

h. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, dated August 19, 2013.

i. VA Handbook 6300.5, Procedures for Establishing and Maintaining Privacy Act Systems of Records, dated August 3, 2017.

j. VA Handbook 6500.6, Contract Security, dated March 12, 2010.

k. VA Handbook 6502.1, Privacy Event Tracking, dated February 18, 2011.

l. VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment, dated July 30, 2015.

m. VHA Directive 1078(1), Privacy Of Persons Regarding Photographs, Digital Images, And Video Or Audio Recordings, dated November 4, 2014.

n. VHA Directive 1200.05, Requirements for the Protection of Human Subjects in Research, dated January 7, 2019.

o. VHA Directive 1605, VHA Privacy Program, dated September 1, 2017.

p. VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.

q. VHA Directive 1605.02, Minimum Necessary Standard for Protected Health Information, dated April 4, 2019.

r. VHA Directive 1935, VHA Freedom of Information Act Program, dated February 5, 2018.

s. VHA Directive 6300, Records Management, dated October 22, 2018.

t. VHA Directive 6300.01, Records Management Compliance Monitoring, dated August 17, 2017.

u. VHA Handbook 1080.01, Data Use Agreements, dated November 20, 2013.

v. VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015.

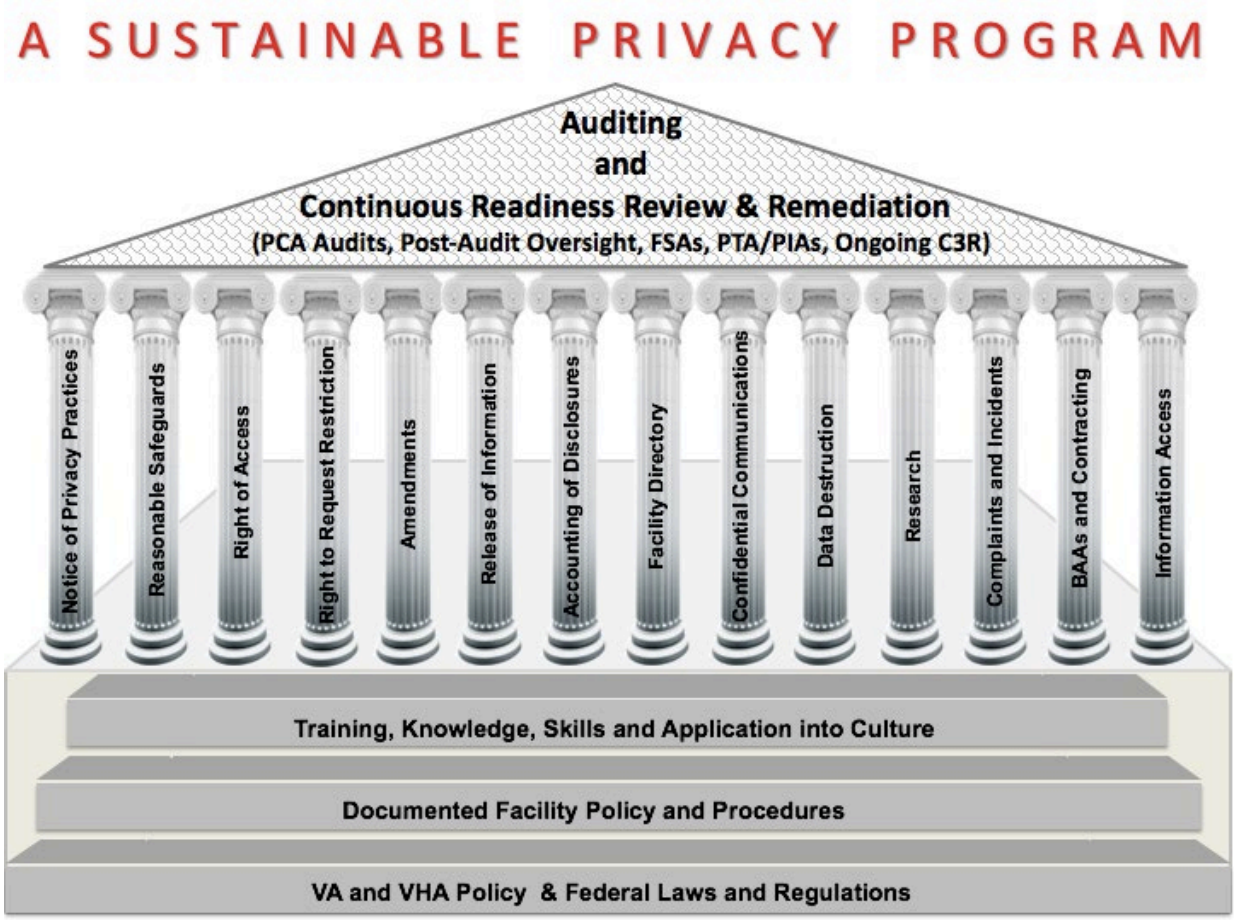
w. VHA Handbook 1605.05, Business Associate Agreements, dated July 22, 2014.

x. VHA Handbook 1907.01, Health Information Management and Health Records, dated March 19, 2015.

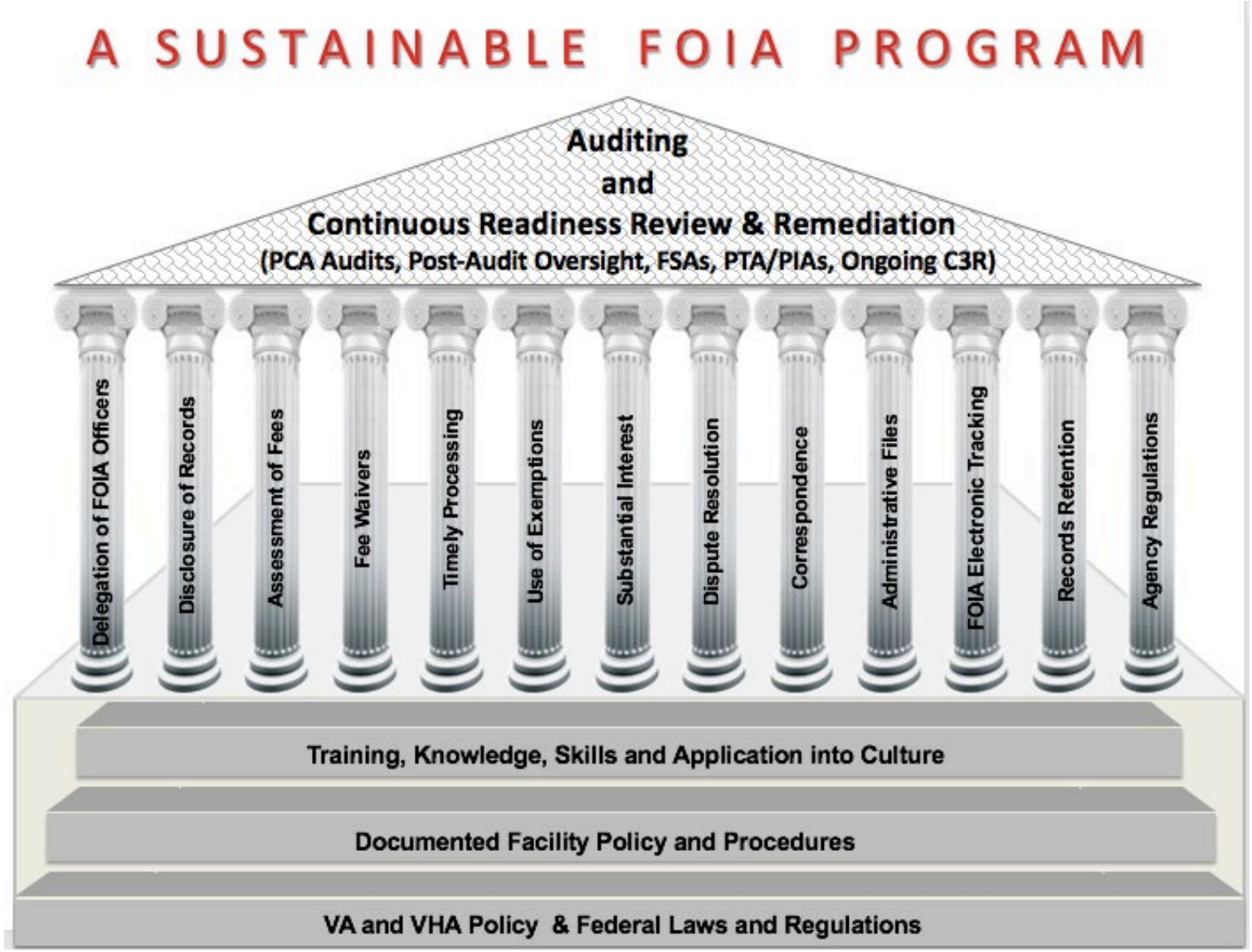
y. United States Office of Personnel Management, Position Classification Flysheet for Government Information Series, 0306, issued March 2012. https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/standards/0300/gs0306.pdf. ***NOTE:*** *This linked document is outside of VA control and may not be conformant with Section 508 of the Rehabilitation Act of 1973.*

z. United States Office of Personnel Management, Position Classification Flysheet for Government Information Series, 0308, issued March 2012. https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/standards/0300/gs0308.pdf. ***NOTE:*** *This linked document is outside of VA control and may not be conformant with Section 508 of the Rehabilitation Act of 1973.*

SUSTAINABLE PRIVACY, FOIA AND RECORDS MANAGEMENT PROGRAMS



(Figure 1)


A SUSTAINABLE FOIA PROGRAM
Auditing
and
Continuous Readiness Review & Remediation
(PCA Audits, Post-Audit Oversight, FSAs, PTA/PIAs, Ongoing C3R)
Delegation of FOIA Officers
Disclosure of Records
Assessment of Fees
Fee Waivers
Timely Processing
Use of Exemptions
Substantial Interest
Dispute Resolution
Correspondence
Administrative Files
FOIA Electronic Tracking
Records Retention
Agency Regulations
Training, Knowledge, Skills and Application into Culture
Documented Facility Policy and Procedures
VA and VHA Policy & Federal Laws and Regulations

(Figure 2)

(Figure 3). ***NOTE:*** *CUI stands for Controlled Unclassified Information.*

CROSS-FUNCTIONAL DEFINITIONS

The following list contains common terms used across the Privacy, Freedom of Information Act (FOIA), and Records Management Programs. It is intended to serve as a non-exhaustive reference tool.

a. **Access.** The viewing, inspecting, or obtaining a copy of Veterans Health Administration (VHA) Personally Identifiable Information (PII) or Protected Health Information (PHI) electronically, on paper or in any other medium.

b. **Audit.** A process by which a compliance performance value is assigned to a program using an objective, pre-established set of questions, evaluations, and observations. This is accomplished by conducting periodic reviews of operations of Department of Veterans Affairs (VA) Health Care Facilities to evaluate those facilities' compliance with applicable Federal privacy, research privacy, FOIA, and records management laws and regulations, and VA and VHA privacy, FOIA and records management policies. Audits may be conducted onsite or by other means identified by PCA. Where feasible, PCA audits will be conducted in accordance with the Generally Accepted Government Audit Standards (GAGAS) Performance Audit requirements as defined by the Government Accountability Office (GAO).

c. **Audit Coordinator.** The Privacy Compliance Assurance (PCA) staff member assigned to be the primary point of contact (POC) for a particular audit. The audit coordinator completes all logistical arrangements with the facility and the PCA Audit Team, coordinates the activities of the PCA Audit Team, and provides the facility with the findings of the PCA audit upon completion of the audit process.

d. **Business Associate.** A business associate is an entity, including an individual, company, or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receiving, maintenance or transmission of PHI, or that provides to or for VHA certain services as specified in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule that involve the disclosure of PHI by VHA. Subcontractors of business associates are also considered business associates.

e. **Chief, Health Information Management.** The Chief of Health Information Management (HIM) is the individual responsible for the functions and management of the HIM Department in a VA Health Care Facility.

f. **Compliance.** For the purposes of this directive, compliance is the full adherence to all statutes, regulations and VA and VHA policies, related to privacy, research privacy, FOIA and records management.

g. **Continuous Readiness Review and Remediation (or C3R).** Continuous Readiness Review and Remediation is an evaluative ongoing oversight process whereby the program is audited for overall adherence with regulatory and policy requirements with an outcome that is most likely to ensure that employee actions and

facility processes are consistent with those applicable laws and policies at all times and that non-compliant findings are promptly remediated. As used in this directive, Continuous Readiness Review and Remediation (or C3R) is the process by which an evaluator (facility privacy or FOIA officer, records manager or designee) evaluates program performance to include; reviews of facility policies, procedures and practices, and workforce performance to ensure that relevant Federal laws, regulations and policies are being followed. This C3R process must be documented and the documentation maintained and made available for review by PCA and other Federal oversight agencies, upon request. Incident-specific privacy investigations and complaint responses do not constitute C3R. ***NOTE:*** *Continous Readiness Review was formerly known as Compliance Monitoring.*

h. **Compliance Auditing Tool.** The Compliance Auditing Tool (CAT, formerly known as Compliance Monitoring Tool (CMT)) is an objective-methodology monitoring tool developed by PCA to evaluate targeted programs within VA Health Care Facilities. The CAT is used to objectively evaluate major components of programs and assign a performance score to each component of a program based on an established10-point performance scale.

i. **De-identified Information.** De-identified information is heath information that is presumed not to identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual because the 18 Patient Identifiers described in the HIPAA Privacy Rule have been removed. De-identified information is no longer covered by the Privacy Act, Title 38 United States Code (U.S.C.) 5701, 38 U.S.C. 7332, or the HIPAA Privacy Rule 45 Code of Federal Regulations (CFR) 164.514(b) (2) (i).

j. **Detailed Report.** The Detailed Report is a report, generated from the electronic Post-Audit Tool (ePAT), that includes the results for each audited criterion. This report may be used to provide detailed findings of individual audit criteria to VHA leadership or external oversight bodies.

k. **Document Review List.** The document review list is a listing of all documents to be provided to the PCA Audit Team prior to and/or at the time of a PCA Audit for the Team's review to determine documented compliance. This list will be provided by the PCA Audit Team to the facility Privacy and FOIA Officers, Records Manager or other facility personnel as necessary in order for the facility to have all required documentation ready for the PCA Audit Team's review. This list may include both documents to be provided prior to a PCA Audit and documents to be provided at the time the audit takes place. The audited facility must produce pre-audit documents by a specific deadline prior to the audit and on-site documents upon the PCA Audit Team's arrival to the audited facility.

l. **Documentation.** Documentation is the printed or electronic material, which contains instructions, comments, processes, policies and procedures, monitoring logs and other information substantiating that certain processes have been implemented, or specific activities or actions have taken place in order to manage and monitor a

program. Monitoring documentation, whether in printed or electronic format, must be created, maintained and available for review by PCA or other designated members of the VHA workforce or outside oversight agencies upon request and must be maintained in accordance with VHA Records Control Schedule (RCS) 10-1.

m. **Electronic Compliance Auditing Database.** The electronic Compliance Auditing Database (eCAD, formerly electronic Compliance Monitoring Database (eCMD)) is an electronic database and reporting tool used to collect and analyze information gathered during various audits conducted and monitored by PCA. This includes data from PCA Audits and Post-Audit Oversight activities, FSAs, and other data deemed necessary to analyze program compliance.

n. **Electronic Compliance Auditing Tool.** The electronic Compliance Auditing Tool (eCAT) is a web-based CAT (see definition of CAT above) used to capture information during PCA Audits. The eCAT is used to enter data directly into the eCAD during PCA Audits. This is the commonly used term used to describe the electronic version of the CAT defined above.

o. **Electronic Post-Audit Tool.** The electronic Post-Audit Tool (ePAT) is a web-based tool used to communicate a prioritized action plan developed by PCA that includes all non-compliant findings in risk-priority order to be used by the audited facility for completing remediation activities. The plan includes the non-compliant findings and placeholders for the facility to enter the resources needed, the individual(s) responsible for remediation, the timelines for completion, actions to be taken. The ePAT also provides a mechanism for the facility to demonstrate corrective actions during Post-Audit Oversight by uploading supporting documentation for each action item remediated and to communicate with the Post-Audit Oversight Coordinator.

p. **Facility Self-Assessment.** The Facility Self-Assessment (FSA) is a self-monitoring process consisting of established questions designed to evaluate all pertinent aspects of the program being self-evaluated. The FSA is divided into sections, with all sections being completed by each VA Health Care Facility Privacy or FOIA Officer, Records Manager or designees, during a specified quarter of the fiscal year (FY) and submitted to PCA. The FSA provides VA Health Care Facilities and PCA with a secondary method of monitoring compliance with Federal regulatory requirements and VA/VHA policies on an annual basis. The FSA provides PCA with monitoring data during the periods of time between PCA Audits completed on PCA's fixed audit cycle (see paragraphs eight and nine). The FSA is created and administered by PCA.

q. **Freedom of Information Officer.** The Freedom of Information (FOIA) Officer is the VA Health Care Facility official responsible for handling FOIA requests sent to the facility. The facility Privacy Officer may also be designated as the facility FOIA Officer.

r. **High-Risk Health Care Facility**. A VHA Health Care Facility that has been audited by PCA in response to an external oversight body's non-compliant findings (e.g., VA Office of Inspector General (OIG); White House Office of Special Counsel (OSC); Department of Health and Human Services, Office for Civil Rights (HHS-OCR);

Office of Medical Inspector (OMI); Congressional Oversight Committees (House Committee on Veterans Affairs, Senate Committee on Veterans Affairs)). A facility may also be identified as high-risk at the discretion of the Privacy Compliance Assurance Officer (PCAO) or VHA central office leadership. This is an internally-identified designation that is determined by the PCA Officer, not by as defined by the GAO.

s. **Individually-Identifiable Information.** Individually-identifiable information (III) is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as Individually Identifiable Health Information, regardless of how it is retrieved. III is a subset of Personally Identifiable Information and is protected by the Privacy Act (5 U.S.C. 552a).

t. **Individually-Identifiable Health Information.** Individually-Identifiable Health Information (IIHI) 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 (e.g., a HIPAA-covered entity, such as VHA).

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

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

u. **Limited Data Set.** A Limited Data Set is PHI from which certain specified direct identifiers of the individuals and their relatives, household members, and employers have been removed. These identifiers include name, address (other than town or city, state, or zip code), phone number, fax number, e-mail address, Social Security Number (SSN), medical record number, health plan number, account number, certificate and/or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers, and full-face photographic images. The two patient identifiers that can be used are dates and postal address information that is limited to town or city, State or zip code. Thus, a Limited Data Set is not de-identified information, and it is covered by the HIPAA Privacy Rule. A Limited Data Set may be used and disclosed for research, health care operations, and public health purposes pursuant to a Data Use Agreement. See 45 CFR 164.514(e) (2).

v. **Non-Identifiable Information.** Non-identifiable Information is information from which all Unique Identifiers have been removed so that the information is no longer protected under the Privacy Act, 38 U.S.C. 5701, or 38 U.S.C. 7332. However, Non-identifiable Information has not necessarily been de-identified and may still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the Rule's de-identification standards are removed.

w. **Patient Identifiers.** Patient Identifiers are the 18 data elements attributed to an individual under the HIPAA Privacy Rule that must be removed from health information for it to be de-identified and no longer covered by the Rule.

x. **PCA Audit Team.** The PCA Audit Team is a specific group of PCA staff assigned to a given audit to facilitate the audit process, gather data, and report findings. A PCA Audit Team may consist of two to six individuals depending on the size and complexity of the program being audited**.** Larger teams may be deployed at the PCA Officer's discretion depending on circumstances that warrant increased personnel support to the audit.

y. **PCA Communication Plan.** PCA Communication Plan is a comprehensive communications strategy outlining permissible and required communications between PCA and VA Health Care Facilities, VISNs, program offices, and VHA leadership. The Deputy Under Secretary for Health approved this plan in April 2013. PCA will adhere to this signed plan or subsequent versions for all applicable communications.

z. **Personally Identifiable Information.** Personally Identifiable Information is any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be personally identifiable information. ***NOTE:*** *The term "Personally Identifiable Information" is synonymous and interchangeable with "Sensitive Personal Information."*

aa. **Post-Audit Oversight.** Post-Audit Oversight is the formal and ongoing review by PCA to track facility remediation actions taken to correct non-compliance identified during a PCA Audit. This process commences at the close of a PCA Audit and will continue until PCA determines that full remediation has been accomplished or until the next PCA Audit. Post-Audit Oversight includes the development of a prioritized action plan for the facility to follow in conducting its post-audit remediation actions and random oversight and review of supporting documentation to evaluate the effectiveness of the facility's remediation actions.

bb. **Post-Audit Oversight Coordinator (Oversight Coordinator).** The Oversight Coordinator (OC) is a PCA staff member assigned to provide strategic oversight to a facility's Privacy and FOIA Officers and/or Records Manager after a PCA Audit in order to coordinate and facilitate the development of a prioritized action plan and to randomly review a facility's remediation actions during Post-Audit Oversight.

cc. **Post-Audit Oversight Report.** A Post-Audit Oversight Report is an executive-level report that provides a general status of a given facility's remediation actions, effectiveness of their remediation efforts and supporting documentation. This report will be provided to VHA leadership on a periodic basis, determined by whether the facility is a High-Risk Health Care Facility or by the risks associated with the areas of non-

compliance. This report may be generated as a facility-specific report or as a general overview of all facilities currently undergoing Post-Audit Oversight.

dd. **Privacy Officer.** The Privacy Officer is the VA Health Care Facility official responsible for ensuring that PII, collected by VA, is limited to that which is legally authorized and necessary and is maintained in a manner that precludes unwarranted intrusion upon individual privacy thereby minimizing privacy events. The Privacy Officer implements the facility privacy program and monitors compliance with VHA privacy policies in accordance with this directive. To ensure consistency in the Privacy program, a fully competent and trained Alternate Privacy Officer must be appointed who will perform the privacy duties in the absence of the Privacy Officer.

ee. **Privacy Liaison/Point-of-Contact.** The Privacy Liaison, or Point-of-Contact (POC), is the individual who serves as the privacy resource to a program office, VISN or other VHA program that does not have an official Privacy Officer because the program relies on the VHA Privacy Office as its Privacy Officer. ***NOTE:*** *VHA program offices are not required to have an assigned Privacy Officer, but must have a Liaison/POC if a Privacy Officer is not assigned.*

ff. **Protected Health Information.** Protected Health Information (PHI) is defined by the HIPAA Privacy Rule as IIHI transmitted or maintained in any form or medium by a covered entity, such as VHA. ***NOTE:*** *VHA uses this term to define information that is covered by HIPAA but, unlike IIHI, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer*.

gg. **Records Manager.** The Records Manager (RM) is the VA Health Care Facility official who has designated responsibility for managing and coordinating a records management program for a respective VA Health Care Facility. The head of the VA Health Care Facility must appoint this position in writing. To ensure consistency in the Records Management program, a fully competent and trained Alternate Records Manager must be appointed who will perform the records management duties in the absence of the Records Manager.

hh. **Research Privacy.** Research Privacy as used in this directive consists of the activities completed by the facility Privacy Officer to ensure that research programs meet all HIPAA and other privacy requirements for use and disclosure of PHI and PII as per VHA Directive 1605.01, Privacy and Release of Information, published August 31, 2016.

ii. **Unique Identifier.** A unique identifier is an individual's name, address, social security number, or some other identifying number, symbol, or code assigned only to that individual (e.g., medical record number and claim number). If these identifiers are removed, then the information is no longer III and is no longer covered by the Privacy Act, 38 U.S.C. 5701, or 38 U.S.C. 7332. However, if the information was originally IIHI, then it would still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the de-identification standard have been removed. ***NOTE:*** *The VA Office of*

General Counsel has indicated that the first initial of last name and last four of the Social Security Number (e.g., A2222) is generally not a unique identifier; therefore, inclusion of this combination of letter and numbers is not likely to make the information identifiable or sensitive absent other data or circumstances that could lead to the reidentification of individuals.

jj. **VA Health Care Facility.** For the purpose of this directive, the term "VA Health Care Facility" means each office and operation under the jurisdiction of VHA, including, but not limited to: VHA program offices, 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 Innovation (COIN). ***NOTE:*** *The use of the term "facility" in this directive is synonymous with this definition.*

kk. **VA Sensitive Information/Data.** VA Sensitive Information/Data is all Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions (38 U.S.C. 5727).

ll. **VHA Privacy Compliance Assurance Officer.** The VHA Privacy Compliance Assurance Officer (PCAO) is the individual with direct authority and responsibility for ensuring the efficient and appropriate management of the VHA Privacy Compliance Assurance Office and C3R programs for Privacy, Research Privacy, FOIA, and Records Management. Also referred to in this directive as PCA Officer.

mm. **VHA Records Officer.** The VHA Records Officer is the direct manager of the VHA Records Management Office and is the individual with direct responsibility for ensuring the efficient and appropriate management of the VHA records program and compliance with all applicable records management statutes, regulations, NARA policy and the requirements of related handbooks and directives.

nn. **VHA Workforce.** The VHA Workforce includes all employees, contractors, students, Without Compensation (WOC), volunteers, and any other appointed workforce members regardless of their work location.

REQUIRED COMPONENTS OF PRIVACY COMPLIANCE ASSURANCE POST-AUDIT OVERSIGHT

The Privacy Compliance Assurance (PCA) Officer will assign a Post-Audit Oversight Coordinator (OC) for each audit. In effort to mitigate and remediate high-risk deficiencies, the OC will contact the facility within two weeks of the close of the PCA audit, unless otherwise approved by the PCA Officer, and will provide training on the use of the electronic Post-Audit Tool (ePAT). The PCA Officer will provide a prioritized action plan in the ePAT, which will contain each of the non-compliant findings in risk-priority order in a format conducive to assigning resources, timelines for completion and actions to be taken. The prioritized action plan will be created using a pre-defined risk model that uses factors such as program sustainability, likelihood and frequency of harm to the organization and implementation factors as to which action items must be in place before others can be accomplished. The OC will review the facility's remediation progress in the ePAT at any time up to the next scheduled audit of the facility. Facility leadership will receive updates via automatic emails generated by the ePAT. This email will outline high-level remediation progress as documented by the facility and the concurrence or non-concurrence of the OC. In the event of oversight for High-Risk Health Care Facilities (see Appendix B), the OC will oversee remediation actions for each program audited on a more frequent basis. The oversight of High-Risk Health Care Facilities will continue until the investigations of external oversight bodies are closed or unless otherwise directed by the PCA Officer to continue oversight for a longer period of time due to the level of risk associated with the non-compliance.

d. **Scope of Post-Audit Oversight (Oversight).** Post-Audit Oversight includes PCA's creation of a prioritized action plan within the ePAT and training for the facility POCs on how to complete the necessary sections of the ePAT to make it a viable project management tool for completing non-compliant action items. The facility must continue to update their plan in the ePAT in real time. The ePAT documentation completed by an audited facility is subject to review from the OC at any time after the facility is provided access and training on the ePAT. This random review by PCA includes evaluation of the remediation actions of the facility and documented evidence of the actions taken.

e. **Duration of the Post-Audit Oversight.** PCA will determine the duration of Post-Audit Oversight. The duration of the oversight will be impacted by whether the facility meets the definition of a High-Risk Health Care Facility. PCA, at its discretion, may randomly review the prioritized action plan and documented evidence of remediation actions at any time up to the next scheduled audit of the facility.

f. **Facility Activities during Post-Audit Oversight.** During Post-Audit Oversight, facilities must follow the steps necessary to ensure they plan and execute corrective actions in a manner that minimizes the risks of ongoing non-compliance by:

(1) Completing all resource and timeline elements of each action item in the ePAT in risk order immediately following the audit and ePAT training.

(2) Completing remediation actions in the risk-priority order and submitting documentary evidence of corrective actions into the ePAT on an ongoing basis as they are completed. The required documentation must be submitted using the ePAT, unless otherwise directed by the OC.

(a) The specific type of evidence that must be submitted by the facility for each audit finding should reflect the actions taken, should contain program documentation that defines policy, process and should show how risks have been mitigated or remediated.

(b) Any questions as to what evidence must be provided must be referred to the OC for clarification. Questions must be submitted using the ePAT communications function.

g. **PCA Feedback on Risk Mitigation and Remediation Actions.** The PCA Oversight Coordinator will review a random sample of the updates submitted by program managers. Feedback regarding the effectiveness of the remediation actions and the sufficiency of the supporting documentation will be provided by the OC at the time of their review of facility submissions into ePAT.

(1) If the evidence submitted demonstrates that the VA Health Care Facility has taken sufficient corrective action for an audit finding, the OC will indicate their concurrence with the actions and documentation in the ePAT after review of supporting documentation.

(2) If the evidence submitted by the VA Health Care Facility does not demonstrate sufficient risk mitigation or remediation action or the facility is failing to respond or responding insufficiently, the OC will non-concur in the ePAT and comment on what additional action or evidence is necessary.

(3) The feedback outlined above will be provided by auto-generated email from the ePAT to the facility leadership and program officers conducting the remediation actions. This email will be sent each time remediation actions are posted to the ePAT or at a frequency determined by PCA to ensure that facility leadership is kept apprised of their facility's progress.

(4) In the event of High-Risk Health Care Facilities, the frequency of the random reviews conducted by the OC will be greater based on the requirements of the oversight body investigating the facility, the level of risk associated with the non-compliance or on the instruction of the PCA Officer to provide more frequent oversight and reporting.

h. **Post-Audit Oversight Report.** The Lead Compliance Specialist for Post-Audit Oversight will develop a Post-Audit Oversight Report utilizing the data gathered in the ePAT. This Lead Compliance Specialist will develop a standard operating procedure that ensures standardized reporting of this information to VHA leadership and defines the information provided. The Post-Audit Oversight Report will be provided to the PCA Officer at least quarterly and may also be provided to VISN leadership, Network Office Health System Specialists, VHA program offices and to VHA senior leadership as

necessary to ensure remediation actions are being completed and leadership is kept apprised of the status of remediation actions.

i. **Notification of Other VHA Entities.** If one or more program managers does not commence completion of corrective action activities or does not cooperate with PCA oversight efforts, the OC will inform the facility leadership of this failure or lack of cooperation. If the facility does not commence or resume remediation to an acceptable level within a reasonable time frame defined by the Lead Compliance Specialist for PCA Oversight, the Lead will inform the PCA Officer. The Lead or the PCA Officer may also inform one or more of the following entities of the facility's failure to engage in remediation actions:

(1) VHA Program Office(s) (VHA Privacy Office, VHA FOIA Office, VHA HIM/Records Management Office).

(2) Applicable VISN Director.

(3) Health System Specialist from the VHA Network Office responsible for the VISN to whom the facility reports.

(4) Deputy Under Secretary for Health for Operations and Management.

(5) VHA Chief of Staff.

j. **Provision of Post-Audit Oversight.** The PCA Officer in collaboration with VHA leadership may increase or decrease the levels of oversight provided during Post-Audit Oversight or may cease providing oversight if business needs or organization resources change.

REQUIRED COMPONENTS OF THE VA HEALTH CARE FACILITY PRIVACY OFFICER CONTINUOUS READINESS REVIEW AND REMEDIATION PROGRAM

1. PROGRAM COMPONENTS THAT ADDRESS BASIC COMPLIANCE

a. **Veterans Health Administration Notice of Privacy Practices.** The facility Privacy Officer(s) acts as the facility subject matter expert (SME) for the VHA Notice of Privacy Practices (NOPP), Information Bulletin (IB) 10-163, and is the facility point-of-contact (POC) for any questions regarding the NOPP. As such, the Privacy Officer must conduct C3R activities to evaluate facility operations to ensure that the NOPP is distributed in accordance with VHA Directive 1605.01, Privacy and Release of Information, published August 31, 2016, and VHA Handbook 1605.04, Notice of Privacy Practices, published October 7, 2015. This component must be reviewed at least quarterly and in a manner that sufficiently reflects the facility's compliance. The facility Privacy Officer(s) must conduct C3R activities to determine:

(1) Whether administrative personnel responsible for the admission of non-Veterans, personnel treating employees in occupational health, and principal investigators engaging non-Veterans in research studies are providing these individuals with the NOPP as appropriate.

(2) If general workforce members are aware of and understand their individual responsibilities for providing non-Veterans the NOPP and where to refer questions concerning the NOPP.

(3) If the facility has developed local policies and/or standard operating procedures (SOPs) concerning the NOPP, which include the steps the facility must take to provide a copy of the NOPP to Veterans, if requested, or non-Veteran patients (e.g., humanitarian, non-VA research subjects, caregivers, facility employees, and active duty personnel).

(4) If the distribution and posting of the NOPP is being done in accordance with VHA Handbook 1605.04.

(5) If the NOPP was provided to non-Veterans or the non-Veteran was given the opportunity to review the NOPP at the initial point-of-care.

(6) If the written acknowledgement form for receipt of the NOPP was obtained and entered (scanned) into Computerized Patient Record System (CPRS), or if the acknowledgement was not received, whether the reason(s) for why it was not received was documented in CPRS.

(7) If the Privacy Officer was notified of the signed acknowledgment form and the method of notification.

(8) If the acknowledgement form has been entered (scanned) into the non-Veteran's CPRS under the administrative tab or in the case of research, a copy is maintained in

the subject's research record or in the case of Employee Health, maintained in the Employee Health Office.

(9) If the NOPP is posted in locations where it would be reasonably seen by individuals seeking services and would be able to read the notice (i. e., Release of Information Office, Eligibility Office, etc.) ***NOTE:*** *If the facility is not required to provide the NOPP because it does not, under any circumstance, treat non-Veteran patients, the Privacy Officer must document that their monitoring identified that non-Veterans are not treated. It is likely that this will only apply to VHA program offices or other VHA services that do not provide patient care.*

b. **Reasonable Physical Safeguards.** Wrongful access and/or loss of VA sensitive information may result in substantial harm, embarrassment, inconvenience, or unfairness to individuals on whom information is maintained. This paragraph outlines the methods by which the facility Privacy Officer reviews to ensure reasonable safeguards are deployed to protect VA Sensitive Information within facility operations. The facility Privacy Officer is responsible for ensuring that the facility has implemented reasonable physical safeguards to ensure the privacy and confidentiality of VA Sensitive Information. The safeguards must be sufficient to protect the integrity of information, limit its access to only those individuals with legal authority to access it and ensure that the facility uses and discloses the VA Sensitive Information only as permitted under privacy statutes and regulations and VA/VHA policies. The Privacy Officer must conduct C3R of the reasonable safeguards within the facility and subordinate locations at least monthly unless otherwise specified in this paragraph. C3R must take place in the following manner:

(1) **VA Facility Physical Assessment.** The facility Privacy Officer or a trained designee must conduct a physical assessment of the facility to review compliance with the facility's privacy program and ensure reasonable safeguards are in place to protect VA Sensitive Information. EoC Rounds may be used as a means of conducting this monthly assessment only if all the following criteria outlined are addressed. Criteria for the physical assessment must include:

(a) Visual observation of a reasonable cross-section of the grounds, buildings, operations, and services, including a sample of Offsite Clinic locations and other offsite buildings, which may house facility or contract staff, facility operations or VHA information in any form.

(b) Asking employees with various job functions about their understanding, training and actions concerning VHA privacy policies, practices, and procedures to include accessing information.

(c) Interviews of individuals whose job duties have specific privacy responsibilities inherent to their position to ensure that these responsibilities are understood and are being completed appropriately (e.g., Administrator of the Day (AOD), Admissions staff, Eligibility staff, Release of Information, Mailroom staff, Information Desk, etc.).

(d) A review of activities such as looking for unauthorized access to VA Sensitive Information (e.g., open computers, access to restricted areas, shred material not secure, unsecured documents, inappropriate auditory disclosures and staff not practicing auditory safeguards processes, and unsecured printed VA Sensitive Information (e.g., appointment lists, progress notes, etc.)).

(e) Other actions and activities deemed necessary to ensure accurate and thorough evaluation of the physical safeguards provisions of the privacy program.

(2) **Offsite Clinic and Alternate Work Location Physical Assessments.** The facility Privacy Officer must conduct a physical assessment of all Offsite Clinics or other alternate work locations at least annually. If the facility Privacy Officer is unable to perform the assessment for any reason, the review must be performed by the Offsite Clinic Coordinator or other trained designee. When the physical assessment is performed by someone other than the Privacy Officer, the individual must be knowledgeable and properly trained by the Privacy Officer to evaluate the components of the program required in this directive and must provide in writing, and in a timely manner, documentation of the findings of the physical assessment to the Privacy Officer. The individual conducting the physical assessment on the Privacy Officer's behalf must not be in conflict-of-interest or have a bias toward the outcome of the physical assessment. If the Privacy Officer is unsure as to whether a bias exists, they should consult their facility leadership for guidance. ***NOTE:*** *The physical assessment may be conducted in conjunction with the Information System Security Officer (ISSO) or Safety Office.*

(3) **Logbooks.** Due to the nature and levels of risks associated with maintaining logbooks within the facility, the Privacy Officer must review their use, storage and protection to ensure that they are not accessed inappropriately or are lost or stolen. A review of logbooks must be ongoing, but at least monthly. Reviewing logbooks may be completed during the physical assessment outlined above and must include a review of logbooks in any format. This C3R activity must include:

(a) A review to determine that the facility has established a facility-level policy on the approval, use and protection of logbooks that is in compliance with VHA Directive 1605.01 and VA/VHA guidance. The policy must also contain approval, use and protection processes for both physical and electronic logbooks.

(b) A review of the activities required in the facility logbook policy to ensure that the facility is in compliance with the policy. This review of logbooks may be done using random monthly spot checks.

(c) A review to determine whether the facility maintains a logbook inventory.

(d) A review to determine whether programs or services are using logbooks, and if they are being used, if the logbook has been approved per the facility logbook policy.

(e) A review to determine whether logbooks contain only the minimum necessary information to satisfy the compelling business need for the logbook.

(f) A review to determine whether reasonable safeguards are in place to protect logbooks from inappropriate use, disclosure, loss or theft.

c. **Right Of Access (First-Party).** VA Health Care Facilities must process an individual's request to obtain a copy of or to review information maintained by VHA related to them in accordance with VHA Directive 1605.01. The Privacy Officer must review the facility's processing of right of access requests at least quarterly. The facility Privacy Officer(s) must:

(1) Conduct C3R activities of right-of-access requests (whether they are for receiving copies or viewing information in its original format) to ensure the request is handled in accordance with VHA Directive 1605.01 and facility policy. C3R must include requests processed by the Release of Information (ROI) staff, as well as requests processed outside the ROI Office (e.g., Offsite Clinics, Employee Health, etc.).

(2) Review a sampling of requests from the VHA release of information software (e.g., ROI Plus software) report that includes a cross-section of all types of requests (including cancelled, denied, closed-partial, and closed-granted) and a sampling of releases made by staff outside of the ROI Department, if applicable, to determine if the first-party right of access process is compliant.

(3) Review requests to ensure they were made in writing by the individual or a personal representative.

(4) Ensure there is evidence of verifying the identity of the requestor.

(5) Review the request for the date stamp upon receipt or that it was entered into the ROI Plus software within one day of receipt.

(6) Review the request to ensure that it reasonably states the records sought by the requestor.

(7) Review to determine if only the requested information was provided and in the format requested.

(8) Review the request to ensure that it was granted or denied appropriately and if denied, whether the denial process was followed as outlined in VHA Directive 1605.01 and the FOIA guidance was followed.

(9) Review the request to ensure it was processed within required timeframes and if not whether the requestor was notified of the delay.

(10) Verify that all correspondence with the requestor is maintained within the ROI Plus software and is signed appropriately.

(11) The Privacy Officer must conduct C3R activities of first-party right-of-access requests to review records in their original format to determine if individuals are allowed to view their information in its original format and whether the facility has a documented process for allowing review of information that follows VHA Directive 1605.01. The C3R must include a review of whether the facility follows its documented policy and standard operating procedures. The Privacy Officer must review to ensure that the individuals' privacy and confidentiality is protected when granting access to view their information in its original format (e.g., allowing viewing in a secure and private location). ***NOTE:*** *If no first-party right-of-access requests are received at the time of the review, the Privacy Officer must indicate in their C3R documentation that no requests were received. In these instances, it is acceptable for the review to be limited to determining if a process is in place should a request be made.*

(12) The Privacy Officer must relay all C3R results related to ROI to the Chief HIM/ROI Supervisor for review and corrective action, as necessary.

d. **Amendments.** VA Health Care Facilities are required to process an individuals' request to amend any information or records retrieved by the individual's name contained in a VA system of records in accordance with applicable Federal laws and regulations and VHA policies, including VHA Directive 1605.01. The facility Privacy Officer must conduct C3R activities of the facility amendment process at least quarterly and must:

(1) Create a process for reviewing amendments that includes:

(a) The steps to take when the Privacy Officer is the individual responsible for processing amendments (self-review).

(b) The steps to take when the Chief of Health Information or other delegated individual is responsible for processing amendments.

(c) Include processes for documenting that no amendment requests were received during the time frame reviewed.

(2) Review the amendment request file to ensure that the following elements are contained in the file:

(a) Original (initial) amendment request.

(b) Copy of the health records subject to the amendment request.

(c) All correspondence with the requestor (acknowledgement letter, clarifying information letters, initial agency decision letter, etc.).

(d) All internal correspondence with other individuals involved in the amendment process (e.g., health care providers, other authors of the disputed record, etc.).

(e) Statement of disagreement, if applicable. This includes whether a statement of disagreement has been included in the record regardless of an appeal.

(f) Facility rebuttal of requestor's statement of disagreement, if applicable.

(g) Documentation of search for accounting of disclosures to determine if other parties have received the records subject to the amendment request.

(h) Copy of the amended record.

(3) Review to ensure that the amendment request file on all amendments is maintained in accordance with VA Records Control Schedule 10-1.

(4) Review the overall amendment process through random spot checks. C3R activities must include:

(a) Reviewing the amendment request to ensure that it was made in writing and that it adequately described the specific information believed to be inaccurate, incomplete, irrelevant or untimely and the reason for this belief.

(b) Ensuring the request was date stamped upon receipt by the Privacy Officer or the office designated to receive the request.

(c) Ensuring the request was sent to the VHA staff member who authored the note in question or the applicable appropriate-level staff member if the original author is no longer available, for determination whether to approve or deny the amendment request.

(d) Determining if the amendment request required an acknowledgment letter and if so, was the process in VHA Directive 1605.01 followed for notifying the requestor of the delay and when the facility expects to take action on the request.

(e) If the amendment request was denied, determining if the written notification of the denial included: the reason for denial; advisement of appeal rights; a description of how the requestor may complain to VHA or to the Secretary, Department of Health and Human Services (HHS); notice that they may submit a statement of disagreement; notice that they may request that a copy of the amendment request and subsequent documentation as defined in VHA Directive 1605.01 be included with all future disclosure of the information; and the signature of the VA Health Care Facility Director or designee.

(f) If the amendment was approved, determining whether the disputed information was made illegible in the paper record and for electronic records, whether the Text Integration Utility (TIU) menu was used; whether the requestor was provided a copy of the amended note; whether there was documentation indicating if previous recipients who received the disputed note were provided copies of the amended note (to in include Business Associates); and whether the requestor was informed that they could request to have notification sent to any relevant persons or organization(s) to whom they gave copies of their disputed record.

e. **Release of Information (Third-Party).** VA Health Care Facilities can only disclose individually-identifiable information (III) in accordance with applicable Federal laws. The facility Privacy Officer must conduct C3R of the release of information activities of the facility at least quarterly, to ensure that disclosures are only made pursuant to legal authority to do so. The Privacy Officer must:

(1) Review a sample of third-party disclosure requests. This C3R must include samples of disclosures documented in ROI Plus software (or any future software released by the VHA Privacy Office) as well as any other means of tracking disclosures used by the facility. The sample must include a cross-section of all types of requests (e.g., cancelled, denied, closed-partial, and closed-granted) and encompass disclosures made by the facility including those made by staff outside the ROI department. These C3R activities must include but are not limited to:

(a) Verifying the legal authority for disclosures (e.g., authorization, written request, standing written request letter, Power of Attorney, routine use, etc.).

(b) Reviewing authorizations to ensure authorizations that were relied-upon for disclosures were valid Health Insurance Portability and Accountability Act (HIPAA) authorizations and that they met the content requirements outlined in VHA Directive 1605.01. ***NOTE:*** *If in the course of C3R, it is determined that disclosures were made pursuant to an invalid authorization, they must be entered into the Privacy and Security Event Tracking System (PSETS) as an incident and appropriate actions should be taken to investigate the wrongful disclosures and take corrective actions as per VA Handbook 6502.1, Privacy Event Tracking, dated February 18, 2011.*

(c) Verifying the disclosures were processed in accordance with VHA Directive 1605.01:

1. Processed timely.

2. Made in writing.

3. Identity of requestor verified.

4. Requested information was sent to the appropriate requestor.

5. Provided in the form that it was requested (i.e., paper, compact disc, etc.)

(d) Assist in remediating any deficiencies found by providing additional training to the department/service responsible for the specific disclosure and ensure compliance for future disclosures.

(e) Ensure that the VHA release of information software (e.g., ROI Plus software) is being fully utilized by the ROI section to ensure accurate accounting of disclosures and productivity reporting.

f. **Right to Request Restriction**.

(1) An individual has the right to request a restriction of the use or disclosure of the information pertaining to them.

(2) The Facility Privacy Officer must maintain a documented process for conducting C3R activities for an individual's right to request a restriction to the use and or disclosure of their information.

(3) This C3R must be conducted at least annually to determine if the facility has a documented process for allowing an individual to request a restriction and to review whether the facility adheres to the request if granted.

g. **Accounting of Disclosures.**

(1) An individual has the right to request a list of all disclosures of information that VHA has made, from records pertaining to them, subject to the provisions of Title 38 Code of Federal Regulations (CFR) 1.576(c) and 45 CFR 164.528. The Privacy Officer(s) must conduct C3R to determine if the facility's accounting of disclosures practices is compliant with VHA Directive 1605.01 regardless of who in the facility is keeping the accountings and regardless of whether the accountings are documented in the release of information software (e.g., ROI Plus software) or by other means permitted by the facility. C3R accounting of disclosures must include two distinct aspects of the accounting process: 1) whether a documented accounting of disclosures is being maintained or can be generated; and 2) whether requests for an accounting of disclosures is processed in a manner that affords individuals with their right to know where information about them is being disclosed. The facility Privacy Officer must review both of these aspects of accounting of disclosures practices at least quarterly. The C3R must include but is not limited to:

(a) Reviewing the creation and maintenance of or capability to generate an accounting of disclosures by:

1. Ensuring that an accounting of disclosures is created or able to be generated in the ROI department for all disclosures made by the ROI department in accordance with VHA Directive 1605.01 and facility policy.

2. Ensuring accountings of disclosures that are maintained by other offices or services (e.g., Human Resources, Research, VA Police, Infectious Diseases Reporting, etc.) other than the ROI department meet the requirements of VHA Directive 1605.01 and facility policy. If the facility has other methods to track disclosures of information that are not tracked in the ROI Plus software, the facility Privacy Officer must review to ensure that an accounting of disclosures is created or able to be generated by each office or service making disclosures outside of ROI and that the accounting contains:

a. Name of the individual to whom the information pertains.

b. Date of Disclosure.

c. Description of what was disclosed.

d. Purpose of the disclosure.

e. Name of the person or organization to whom the disclosure was made.

f. Address of the person or organization to whom the disclosure was made (if known).

3. Conducting C3R of a representative sample of actual requests for an accounting of disclosures received by the facility by:

a. Reviewing accounting of disclosure requests to ensure that the requests were made in writing and that they adequately identify the VHA system of records or designated record sets for which the accounting is requested.

b. Reviewing to determine if all areas where accountings of disclosures are kept have been included in the response to an accounting of disclosures request.

c. Reviewing the accounting provided to the requestor to determine if the following information was included:

(1) Date of Disclosure.

(2) Description of what was disclosed.

(3) Purpose of the disclosure.

(4) Name of the person or organization to whom the disclosure was made.

(5) Address of the person or organization to whom the disclosure was made (if known).

d. Verifying that the accounting of disclosures was provided within 60 calendar days after receipt of the request. If the accounting was not provided within the specified timeframe, also verifying that:

(1) The facility did not extend the timeframe longer than 30 calendar days.

(2) The facility provided the individual with a written statement of the reasons for the delay and the date by which the accounting will be provided to them.

e. Determine whether a copy of the accounting of disclosure response was maintained for the record.

h. **Facility Directory Opt-Out.** The Veteran has a right to choose to be included or not included in the Facility Directory. The facility Privacy Officer will conduct C3R of this process at least quarterly to ensure that the opportunity to opt-out of the facility directory is offered and that this right is being afforded to Veterans when they chose to opt-out of the facility directory. The facility Privacy Officer(s) will:

(1) Coordinate with the local Education Office and Supervisors to ensure that all applicable workforce receive appropriate training on the steps involved in the Facility Directory Opt-Out process.

(2) Establish a documented C3R process for Facility Directory Opt-Out which includes all aspects of the process.

(3) Conduct C3R activities to include but are not limited to:

(a) Observation of intake areas to determine if appropriate opt-out choices are being provided to the Veteran.

(b) Calling into the VA Health Care Facility to ask about patients known to be "opted-out" of the facility directory to determine if the workforce provides the correct Glomar response regarding those patients. ***NOTE:*** *The specific Glomar response approved by the VA Office of General Counsel is "I am sorry, but I do not have any information I can give you on whether <patient name> is a patient"*.

(c) Talking with information desk and mailroom personnel to ensure they are aware of how to handle requests for information on patients who have opted out of the facility directory and how to handle floral and mail deliveries and whether this process is consistent with local policy for opted-out patients.

(4) In the event of incapacitated or unconscious patients who were unable to make the opt-out decision themselves, reviewing physician-determined opt-out decisions to ensure that appropriate documentation of the opt-out decision was made and documented in the patient's electronic medical record. Also reviewing whether the patient was given an opportunity to change opt-out status once they were no longer incapacitated or unconscious and were able to make the decision for themselves.

i. **Confidential Communications.** The Veteran has a right to request to receive their communications from VHA by a confidential alternative means or at an alternative location other than their official permanent address. When these requests are received, the facility is required to consider the request and process it if it is a reasonable request. If the request is granted, VHA must communicate with the Veteran using the agreed-upon confidential means. The facility Privacy Officer must conduct C3R of this process at least quarterly to ensure these requests are processed and used appropriately. The facility Privacy Officer(s) must:

(1) Provide, in coordination with the Education Office and supervisors, all applicable workforce with appropriate training on the process of handling Veterans' questions and requests for confidential communications (correspondence) according to VHA Directive 1605.01.

(2) Establish a documented process for C3R of the Confidential Communications process to include instructions on running the report for Veterans who have a confidential communications (correspondence) in place.

(3) Conduct C3R activities to verify that the facility is processing Veterans' requests for confidential communication and that the confidential communications process is being followed throughout the facility. These activities include but are not limited to:

(a) Reviewing intake areas (Eligibility, AOD) to determine if the workforce in these areas is knowledgeable in the process to follow when confidential communications is requested.

(b) Interviewing a sample of the general workforce to determine if they know where to refer a Veteran who is requesting confidential communications for their correspondence with VHA.

(c) Reviewing areas of the facility where communications with Veterans take place (e.g., Billing, ROI, Pharmacy, Outpatient Clinics, etc.), to determine if confidential communications address or phone numbers are being used by the facility appropriately.

j. **Data Destruction.** The Privacy Officer must be knowledgeable of the facility's process for destroying temporary paper records containing sensitive information and implement processes to ensure they are destroyed according to the contractual agreement and /or facility policy and in accordance with VA Directive 6371, Destruction of Temporary Paper Records, dated April 8, 2014. This requires the facility to determine and document when final destruction occurs and whether reasonable safeguards are in place until final destruction is accomplished. If interim destruction processes are used (e.g., shredding before final pulping), the Privacy Officer's C3R activities will include C3R throughout the whole data-destruction life-cycle and not just through interim processes. The facility Privacy Officer will review this process at least quarterly, unless otherwise specified in this paragraph, to ensure that these processes are followed. C3R of data destruction is the responsibility of the Privacy Officer and not the facility Records Manager as the documents are no longer Federal Records once they have entered the data destruction process. However, although the documents are no longer Federal Records, they are still considered VA sensitive or individually identifiable information requiring reasonable physical safeguards until they are no longer a risk to individuals' privacy or are a potential injury to the organization. It is the Privacy Officer's responsibility to conduct C3R activities that ensure the safe storage, handling and destruction of these documents. The Privacy Officer must:

(1) Establish a documented C3R process to ensure the facility is meeting the requirements outlined in VA Directive 6371.

(2) Conduct C3R activities to verify the data destruction process is a thorough, safe and compliant process. These activities must include but are not limited to:

(a) Staff awareness of and adherence to the facility processes.

(b) Reviewing data destruction contract(s) to ensure the appropriate clauses are included for safeguarding material and to ensure the facility is in the chain-of-custody to safeguard temporary paper records until final destruction is achieved.

(c) If shredding is the means of final destruction used by the facility and the shredding takes place on-site, observing the shred process at least quarterly to ensure the contractor is shredding the material as outlined in the data destruction contract.

(d) If shredding is the final means of destruction used by the facility and the shredding takes place off-site, observing the process at least annually to ensure the contractor is shredding the material as outlined in the data destruction contract. ***NOTE:*** *In addition to a Privacy Officer review of the process annually, the Privacy Officer must coordinate with the Contracting Officer or their Contracting Officer's Representative (COR) responsible for the data-destruction contract to review the efficacy of the off-site process at least quarterly (the Privacy Officer should obtain some assurance in writing from the COR that the process is still compliant).*

(e) Requesting a sampling of the shredded material from the contractor at least quarterly regardless of whether the shredding takes place on-site or off-site to determine if shred outputs meet the terms of the contract and constitute the level of destruction required in VA Directive 6371.

(f) Reviewing the certificates of destruction to ensure they meet the requirements of VA Directive 6371 and that the facility is receiving these as confirmation that final destruction has taken place. ***NOTE:*** *The facility must not accept promissory notes from the shredding vendor indicating that the data "will be destroyed". The certificate must reflect assurance that final destruction has already taken place.*

(g) If the facility conducts its own data destruction, reviewing to determine that it is following its local policy and process and that the process renders the material no longer readable or re-constructible.

(h) Ensuring the collection/storage bins for shred material have reasonable physical safeguards in place regardless of whether they are located throughout the facility or in storage areas awaiting shredding.

NOTE: *Some vendors may provide a certificate for interim destruction or certificates of receipt of material, which is permissible, but the vendor must also provide a certificate of final destruction once final destruction has been completed.*

k. **Research Privacy.** The facility Privacy Officer(s) will be involved in the human studies research study submission process to ensure the privacy rights of individuals participating in studies are protected appropriately. The privacy rights of VA research subjects are addressed at 38 CFR 16.104 and 16.111. The facility Privacy Officer must:

(1) Establish a documented process to ensure that a privacy review of all human subject protocols (full board, expedited and exempt) is conducted. The purpose of this process is to guarantee that proposed research complies with all applicable local, VA, and other Federal requirements for privacy and confidentiality. This process must include the steps to take to address and mitigate potential privacy concerns about proposed research studies. ***NOTE:*** *If a study includes information protected under Title*

38 United States Code (U.S.C.) 7332 and will be disclosed outside of VA, the study must include written assurance from the researcher that the purpose of the data collection is to conduct scientific research and that the information will not be identified, directly or indirectly, by individual patient or subject in any report of the research, e.g., manuscript or publication.

(2) Document the Privacy Officer's review of the protocol in such a manner that it shows a thorough evaluation of how the study has addressed the privacy implications and correspondence with applicable parties (e.g., Institutional Review Board (IRB), Research and Development Committee, Principal Investigator (PI), ISSO, etc.). The VHA PCA research checklist must be used to conduct this review and will serve as sufficient documentation of the review of research privacy processes.

(3) Ensure that documentation of the privacy review remains with the research protocol and available to the PCA Office or other agencies upon request.

(4) Identify deficiencies in the provisions for privacy and confidentiality of the proposed research and make recommendations to the PI and/or IRB or Research and Development Committee of options available to correct the deficiencies as defined in the facility policy. Follow up with the PI and/or IRB or Research and Development Committee to ensure what must be done so that the proposed research is in compliance with relevant privacy and confidentiality requirements before the investigator initiates the study as per facility policy. This correspondence and resolution of deficiencies must be documented in writing.

(5) Conduct the preliminary research privacy review. The preliminary research privacy review is required for any human subjects study submitted for approval prior to approval being granted, in order to address any privacy concerns before the review. If the human subjects study requires IRB review, including a limited IRB review for the applicable exempt human subject research study as described in VHA Directive 1200.05, Requirements for the Protection of Human Subjects in Research, dated January 7, 2019, the review is conducted prior to IRB review. If the exempt human subjects research study does not require a limited IRB review, the review is conducted prior to VA Research and Development Committee review. This review process is intended to ensure that legal authorities exist for the use and disclosure of protected identifiable information, to protect VA research programs from inadvertent mis-uses or wrongful disclosures of data collected during a research study, and to ensure that the minimum-necessary standards of the HIPAA Privacy Rule and the Privacy Act are followed. The following areas must be reviewed during the preliminary review:

(a) HIPAA Waiver of Authorization Process. The facility Privacy Officer(s) reviews requests for waiver of HIPAA authorization have the following required elements:

1. Statement that waiver is justified because the use of the information poses no more than minimal risk to the privacy of the subjects.

2. Adequate assurance that the requested information will be appropriately used, disclosed, and protected.

3. An adequate plan for protecting the identifiers from improper use and disclosure.

4. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers (or otherwise required by law).

5. Validation of the statement that the research could not practicably be conducted without the waiver of authorization.

6. Validation of the statement that the research could not practicably be conducted without access to Protected Health Information.

7. Description of Protected Health Information accessed and/or collected. ***NOTE:*** *This should be more than just the identifiers being accessed and should be specific (i.e., "access to the medical record", "progress notes", etc.).*

8. Validation that the waiver is not being used to authorize a disclosure. If the waiver is being used as the authority to make a disclosure under the HIPAA Privacy Rule, additional disclosure authority is required under the Privacy Act, 38 U.S.C. 7332 and 38 U.S.C. 5701.

(b) Authorizations. The facility Privacy Officer(s) must:

1. Ensure that VA Form 10-0493 is used as the authorization form, unless the authorization is combined with the informed consent document in accordance with VHA Directive 1200.05.

2. Ensure that if VA Form 10-0493 is used as the authorization, review HIPAA authorization for the following required elements:

a. Completion of the purpose of the study, which cannot conflict with the purpose in the informed consent.

b. Appropriate selections of the information to be used and/or disclosed.

c. Appropriate selections and identification of the people and organizations authorized to use and/or disclose the information.

d. Expiration date or specific event that indicates when the authorization expires. ***NOTE:*** *The "Not Expire" box should not be used unless a specific justification is provided*.

e. Completion of the address of the individual(s) to whom a subject may submit a revocation of the authorization.

f. Determine if data-banking or tissue-banking is part of the protocol (if the banking involves identifiable data or identifiable tissue). Depending on whether the banking is optional or mandatory, ensure authorization is completed correctly.

3. Ensure that if informed consent and authorization are combined, the form meets the HIPAA requirements for authorization in VHA Directive 1605.01.

(c) Research Protocol and Other Research Study Documents. The facility Privacy Officer reviews the research protocol and other research study documents to ensure that:

1. Requirements for implementation of reasonable safeguards to protect and safeguard protected identifiable information are described.

2. A description is included regarding how data will be used by each VA and non-VA entity that will have access to the research data.

3. If non-Veterans are participating in the study, there is a mechanism for how they will be provided with a copy of the VA Notice of Privacy Practices.

4. If research data are collected, that they are consistent with the scope of the study (e.g., adherence to the minimum-necessary standard).

(6) Conduct a final review prior to VA Research and Development approval to ensure that no further changes were made, which may impact the privacy and confidentiality of the study. This final review must be documented in accordance with VHA Directive 1605.

(7) Review IRB approval memos or other approval documentation for HIPAA waivers to ensure they contain all required elements:

(a) A statement that the waiver of authorization has been reviewed and approved under either normal or expedited review procedures.

(b) Signature by the IRB, Privacy Board Chair, or other voting member of the IRB.

(c) IRB or Privacy Board is identified in the approval memo or letter or other documentation.

(d) The date and approval of the waiver of HIPAA authorization.

(e) Statement that the IRB or Privacy Board has determined that the waiver of HIPAA authorization satisfies all required criteria (see VHA Directive 1605.01, paragraph 13).

(f) A brief description of the Protected Health Information determined by either the IRB or Privacy Board to be necessary to conduct the research.

(8) Review Physical Environment Elements:

(a) Areas where research is conducted to determine if reasonable safeguards are deployed to protect and safeguard protected identifiable information.

(b) Data destruction for research to determine if it meets requirements of VA Directive 6371.

(9) Review National Data and Centers for Medicaid and Medicare (CMS) Data by:

(a) Ensuring that if data have been requested from a National Data Set (i.e., CMS, Corporate Data Warehouse (CDW), National Data Systems (NDS), etc.) that the PI receives only the information that was requested; that only those individuals approved to use the information have access to the data; if a Data Use Agreement is required, that it is in place and is in compliance with VHA Handbook 1080.01, Data Use Agreements, dated November 20, 2013; that the data are stored where agreed upon in the Data Use Agreement; that reasonable safeguards are implemented for the data; and that there is a defined plan for protection of the data until it reaches its disposition date according to VHA RCS 10-1.

(b) If the facility has CMS data, that the data are being used, managed, accessed, stored, and protected in accordance with the terms of the data use agreement with the VA Information Resource Center (VIReC).

(c) Reviewing to determine that only the studies approved by VIReC and the individuals listed in the Data Use Agreement are using CMS data.

(10) Develop self-reviews to ensure that the above steps are completed accurately and timely for each human research study. This self-review will be conducted at least annually and must be documented.

l. **Information Access.** Access to VA sensitive information must be limited to the minimum amount of information necessary and to only those individuals who have an official business need to know. Information can be accessed through a variety of ways such as information systems (Veteran health record and Employee health record), paper documents, auditory disclosures, etc. To that end, the facility must institute processes to ensure access to VA sensitive information is limited to individuals with a business need to the information regardless of the form it takes. Activities ensuring appropriate access to VA sensitive information must be incorporated into facility policy. These processes must be reviewed by the facility Privacy Officer to ensure that the minimum necessary standard is met. This C3R must include, but is not limited to:

(1) **Assignment of Functional Category(ies).**

(a) The Facility Privacy Officer must review, at least annually, to determine the assignment of functional categories. C3R of functional categories must include, but is not limited to:

1. Establishing a documented C3R process for the assignment of functional categories that includes reviewing whether the assignment is documented and workforce has been explained their category(ies).

2. Conducting C3R of supervisors' assignments of functional categories to ensure workforce members have been assigned a functional category or categories consistent with VHA Directive 1605.02, Minimum Necessary Standard for Protected Health Information, dated April 4, 2019, by:

a. Checking a random sample of employee competency folders to ensure that the assignment of the functional category is documented according to VHA Directive 1605.02.

b. Checking to see if multiple categories have been assigned when appropriate.

c. Interviewing supervisors to determine whether they explained the functional category(ies) to their workforce when they assigned the category(ies).

d. Interviewing a representative sample of workforce members to determine whether they understand the category(ies) assigned to them and whether they understand the requirement to only access and use the minimum necessary amount of information in order to complete their official job functions. ***NOTE:*** *The functional category applies to information in any form or medium. It is not limited to electronic information accessible through Veterans Information Systems and Technology Architecture (VistA), CPRS, or subsequent electronic health record systems.*

3. Access to information. The Privacy Officer will conduct C3R at least quarterly to determine if the work environment and workforce activities are conducive to adherence to minimum necessary access requirements outlined in VHA Directive 1605.02 and this directive. This C3R must include, but is not limited to:

a. Establishing a documented process for reviewing general access to information (PHI, III) throughout the facility to ensure that it is not accessible by unauthorized individuals.

b. Reviewing a reasonable cross-section of the facility to determine whether information is accessible to unauthorized persons. C3R will include but is not limited to:

(1) Reviewing workforce behaviors that would make information accessible to unauthorized individuals.

(2) Reviewing auditory privacy practices such as conversations in public areas or discussions loud enough for bystanders to overhear information.

(3) Reviewing "authorized-only" areas of the facility to determine if workforce is sensitive to protecting these areas from intrusion by unauthorized individuals.

(4) Reviewing the use of Personal Identification Verification (PIV) badges and whether these are being used to identify individuals as appropriate for "authorized-only" areas.

(5) Reviewing high-risk areas and processes within the facility where protected or sensitive information is accessible such as the Mail Room, Medical Records storage, Employee Health, Release of Information, Research, charting and nursing stations, etc., to ensure that the facility has implemented reasonable safeguards so that access to information is limited to only those individuals with an official business need for the information.

c. Conducting C3R to ensure that if the facility receives national data sets for administrative purposes (e.g., CMS, Medicare Analysis Center, (MAC), and NDS) that Data Use Agreements or other agreements specifically and appropriately address access to the data and that legal authority exists for the access.

d. Access is limited to only those individuals who have been authorized.

e. Only the minimum-necessary data requested has been received by the administrative data user.

4. Conducting C3R the investigation of all complaints of inappropriate access. The Privacy Officer will also coordinate with Human Resources to ensure appropriate sanctions are applied consistently in the facility for access-related personnel actions.

5. Ensuring the facility marks all records as sensitive that are associated with a wrongful access complaint to alert workforce of their obligation to access records only for official business purposes and to track future access to these records. Review at least monthly to verify that these records are marked sensitive.

6. Ensuring the facility marks all records as sensitive that are associated with tort claims to alert workforce of their obligation to access records only for official business and to track any access or changes or modifications to the records once a tort claim has been filed. Conduct C3R at least quarterly to verify that these records are marked sensitive.

m. **Privacy Threshold Analysis and Privacy Impact Assessment.** The facility Privacy Officer(s) must develop a documented C3R process to ensure facility compliance with VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessments, dated July 30, 2015. This C3R must be conducted at least annually to include, but not limited to:

(1) Reviewing the facility process of identifying data systems and associated risks to ensure that the Privacy Officer and ISSO are included in these processes and that documented Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) submissions are being made timely.

(2) Reviewing to determine if a PTA was completed for all current PIAs and reviewing whether they have maintained a copy of all PTAs completed within the past three years.

(3) Reviewing whether a PTA was submitted to the VA Privacy Service for all expired PIAs.

(4) Reviewing to determine if a PIA was completed, when required according to the outcome of a PTA.

(5) Reviewing the PTA/PIA for each system of operation to ensure that it is of a quality that will reasonably ensure its approval by the VA Privacy Service PIA Support Team.

(6) Reviewing the facility process for completing PTAs and PIAs to ensure that PTAs are updated at least annually and that PIAs are updated at least every three years.

(7) Reviewing to ensure that all facility PIAs are included in the Governance Remediation and Compliance (GRC) Tool (or subsequent tools) and are current.

(8) Reviewing the forward-facing internet page of the VA Privacy Service to ensure that PTAs and PIAs are posted for public review and if they are not posted, contacting the VA Privacy Service to ensure posting takes place.

n. **Presentations Displaying Personally Identifiable Information.** The facility Privacy Officer(s) must develop a documented C3R process to ensure facility compliance with VA Directive 6511, Presentations Displaying Personally Identifiable Information (PII), dated January 7, 2011. This C3R must be conducted at least annually to include, but is not limited to:

(1) Reviewing the presentation clearance process to ensure that workforce members creating presentations are aware of and follow the redaction processes outlined in the directive.

(2) Reviewing a representative sample of presentations to determine if PII has been properly removed.

o. **Privacy Of Persons Regarding Photographs, Digital Images, And Video Or Audio Recordings.** The facility Privacy Officer(s) must develop a documented C3R process to ensure facility compliance with VHA Directive 1078(1), Privacy Of Persons Regarding Photographs, Digital Images, And Video Or Audio Recordings, dated November 4, 2014. This C3R must be conducted at least annually to include, but is not limited to, conducting a sample of interviews of workforce to determine if they understand the requirements regarding photographing and whether employees are aware of and follow the photography processes outlined in the directive.

2. PROGRAM COMPONENTS THAT ADDRESS PROGRAM SUSTAINABILITY OVER TIME

Basic compliance is only effective when it is sustained over time. In order to ensure that the privacy program is not only implemented and fully compliant as indicated in the C3R activities in paragraph 1.a. of this Appendix (D), but that the program must also contain components that ensure that the program is sustained over time. The facility Privacy Officer must conduct the following C3R activities to ensure program sustainability over time, particularly in their absence or unavailability. These sustainability components address methods by which the program is documented for repeatability as well as how the responsibilities of the workforce and specific individuals is incorporated into the facility's culture.

a. **C3R of Facility Policies and Procedures.** The facility Privacy Officer must have a documented C3R process to review at least annually to ensure that facility-specific privacy policies and procedures are consistent with the VHA Privacy Policy Template as required in VHA Directive 1605.01 and ensuring that the procedures are updated each time the Template is revised or VHA guidance requires an update to the facility procedures. The VHA Privacy Policy Template is located at: https://vaww.vets.vaco.portal.va.gov/sites/privacy/vhapo/Pages/templates.aspx. ***NOTE:*** *This is an internal VA Web site that is not available to the public.* This C3R must include, but is not limited to:

(1) Evaluating whether the local Privacy procedures cover all required Privacy Program components. ***NOTE:*** *The facility may rely on VISN or National-level Privacy policies for areas where the local practices are identical to those of VISN or National-level requirements. However, the local Privacy procedures must reflect this adherence to and reliance upon the VISN or National-level policy. Local procedures must provide citations as to where the VISN/National-level Privacy policy may be found in order for the workforce to be appraised of the policy requirements so they can adhere to them. If practices are not identical, local Privacy procedures must address the local expectations within the facility Privacy policy*.

(2) Ensuring that the Privacy policy is in-force and properly executed by the facility leadership.

(3) Ensuring that the Privacy policy has been disseminated to the workforce and that the workforce has ongoing access to the policy.

(4) Determining that all facility workforce is adhering to the requirements contained in the policy. This determination may include but is not limited to interviewing the workforce to identify if:

(a) They know where to find the facility policy when needed for reference.

(b) They are aware of their responsibilities outlined in the facility Privacy policy.

(c) They know to whom and how they report a privacy breach or compliant.

(5) Identifying necessary changes to the Privacy policy due to regulatory and VA and VHA policy changes.

(6) Reviewing and updating the Privacy policy upon expiration and ensuring that an updated policy is adopted and formalized.

(7) Ensuring that expired Privacy policies are retained for at least six years, in accordance with 45 CFR 164.530(j).

(8) Establishing a documented process for how the Privacy Officer will be consulted on other facility policies containing privacy implications (e.g., using, disclosing, protecting, transporting and destroying sensitive information, etc.) so that the Privacy Officer can review all facility policies that impact privacy.

(9) Conducting C3R of other facility policies containing privacy implications including, but not limited to:

(a) Reviewing local policies containing privacy implications to ensure they are not in conflict with the approved local facility Privacy policy.

(b) Working with the person(s) responsible for these policies to bring them into compliance with Federal privacy requirements and VA and VHA privacy policies as soon as possible. ***NOTE:*** *The Privacy Officer's review of local policies is limited to only those policies that have a direct or indirect privacy implication. This C3R activity does not require the Privacy Officer to review all facility policies.*

(c) The Privacy Officer must review facility privacy SOPs at least annually to ensure that they reflect the processes used by the facility and must make amendments as necessary to keep the SOPs current to business practices.

b. **Privacy Training, Education and Awareness Strategy Development.** The Facility Privacy Officer, in coordination with the facility Education Coordinator or Education Office, must develop a local-level privacy training strategy that outlines the facility procedures for ensuring compliance with the annual training requirement in VHA Directive 1605.01 and provides direction on how the facility will train, educate and make workforce and Veterans aware of privacy rights and responsibilities. ***NOTE:*** *This strategy must be documented in the facility privacy policy as required in the VHA Privacy Policy Template.* The Privacy Officer must review the comprehensiveness of the strategy at least annually by reviewing to determine if the strategy contains:

(1) Methods of tracking required VHA privacy training of the workforce.

(2) Methods of tracking contractors' training requirements.

(3) Privacy Officer participation in new employee orientation to provide new employees with an introduction to privacy concepts and requirements.

(4) Methods of specialized education when necessary to mitigate risks related to a lack of workforce understanding (e.g., in response to a data breach or other incident).

(5) Methods of educating Veterans and employees on their privacy rights.

(6) Methods of incorporating continuous privacy awareness into the facility culture as a means of ensuring compliant privacy responses by the workforce.

(7) Methods of training workforce involved in purchasing activities on when and how to engage in Business Associate Agreements (BAAs).

c. **Privacy Training, Education and Awareness Strategy Implementation.** The Facility Privacy Officer, in coordination with the facility Education Coordinator or Education Office, must implement the facility privacy training strategy. The Privacy Officer must conduct C3R of the implementation of the strategy at least annually by reviewing to determine if the facility training, education and awareness activities are effective. This C3R must include, but is not limited to:

(1) Reviewing the timeframes for completion of training to ensure compliance with current VA/VHA policies for workforce training and any other training requirements specific to the facility.

(2) Participation in New Employee Orientation to introduce new employees to their privacy obligations, inform them how to reach the Privacy Officer, and to provide introductory information on the facility privacy program.

(3) Developing and maintaining a documented process for compiling annual training records in order to report the facility privacy training completion status to facility leadership and PCA for auditing purposes upon request.

(4) Evaluating the methods for tracking workforce training to determine if these methods are sufficient to allow the facility Director to certify annual training completion to PCA. This evaluation must include, but is not limited to:

(a) Reviewing methods that allow the facility to determine compliance with training requirements for all workforce based on the reports generated within the Talent Management System (TMS) or by other means of tracking used by the facility Privacy Officer and/or Education Coordinator or Education Office.

(b) Utilizing the VA TMS to track the annual training status for all VA workforce (including Personnel and Accounting Integrated Data (PAID) and Contracted employees). ***NOTE:*** *If necessary, the facility Privacy Officer must establish an alternative method to track the annual training status for those members of the workforce not included in TMS. These workforce members may include volunteers, students, and those contractors not included in TMS.*

(c) Conducting activities that enhance workforce awareness and understanding of Federal, VA, and VHA privacy laws and policies that have a positive impact on the

overall privacy culture and posture of the facility. These activities may include, but are not limited to:

1. Participation in VA's annual Privacy Week activities.

2. Posting privacy posters and announcements throughout the facility.

3. Publishing articles in facility newsletters and email blasts to workforce.

4. Conducting one-on-one training with individual personnel, departments or services, as requested or deemed necessary.

(d) Providing training to personnel involved in purchasing services or external functions that may require a BAA as well as those responsible for the BAA process. The facility Privacy Officer must conduct C3R of the training provided to these individuals to ensure that they understand and follow the requirements of a fully implemented BAA (when appropriate). The C3R must include, but is not limited to whether the training covers:

1. The criteria for determining when it is necessary and appropriate to enter into a local BAA.

2. Information about who in the facility to contact to implement a BAA, if necessary.

3. The process for engaging in local BAAs and how to ensure a national BAA does not exist for the same services.

4. Ensuring that PHI is not disclosed to a vendor until a BAA is established.

5. Processes for addressing Business Associate non-compliance with the BAA.

d. **Veterans Privacy Rights and Awareness.** The Facility Privacy Officer(s) serves as the facility point-of-contact and privacy SME for all privacy matters throughout the facility. This includes helping Veterans understand and take part in ensuring their own privacy rights. The Privacy Officer must provide Veterans with information to educate them on their privacy rights and responsibilities to keep their own information confidential. To facilitate this education, the Privacy Officer must conduct C3R at least annually to ensure:

(1) That the facility develops and maintains policies and procedures addressing how the facility informs Veterans of their privacy rights including facility distribution of the Notice of Privacy Practices.

(2) Coordination 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 so they will partner with VHA to protect their own information.

(3) Serving as an advocate to Veterans for their privacy rights and conducting C3R of the facility for instances where Veterans are putting themselves at risk for data loss.

e. **Privacy Complaints and Incidents.** The facility is required to process all complaints and incidents according to VA and VHA policies, procedures and guidance. The facility Privacy Officer(s) must monitor conduct C3R of complaints and incidents at least quarterly. The C3R must include, but is not limited to:

(1) Ensuring that a documented C3R process is in place that requires all privacy complaints be processed and maintained in accordance with VHA Directive 1605.01, VA Handbook 6502.1 and RCS 10-1.

(2) Ensuring that the C3R process includes evidence that:

(a) The complaint has been entered into the PSETS within one hour of discovery regardless of validity.

(b) Complaints and incidents are managed and investigated to full resolution.

(c) Leadership is provided with timely information concerning facility privacy complaints/incidents according to facility policy.

(d) A written response has been provided to the complainant within the specified timeframe outlined in the facility's privacy policy.

(e) The appropriate notification and credit monitoring letters are sent and within the required time frame outlined in VA Handbook 6502.1.

(f) The Privacy Officer coordinates with stakeholders (i.e., Human Resources for sanctions or disciplinary actions, union representatives, department heads, and supervisors, etc.) as outlined in VHA Directive 1605.01.

(g) Privacy complaint files are maintained on all complaints and incidents and these files are kept in an accessible and organized manner that will allow the Alternate Privacy Officer to retrieve and use all documents related to the complaint or incident in the event the Privacy Officer is not available.

(h) The complaint files are retained and dispositioned according to RCS 10-1.

(i) A system is established to identify trends in the type and frequency of facility privacy complaints/incidents, and report these trends to the facility leadership on a regular basis and the VHA Privacy Office upon request.

(j) The facility coordinates with the VHA Privacy Office when it receives a Department of Health and Human Services (HHS), Office for Civil Rights (OCR) complaint.

(3) Reviewing a sample of privacy complaint files sufficient to ensure they contain all documentation to support the findings of the complaint as required by VHA Directive 1605.01.

REQUIRED COMPONENTS OF THE VA HEALTH CARE FACILITY FOIA OFFICER CONTINUOUS READINESS REVIEW AND REMEDIATION PROGRAM

The Freedom of Information Act (FOIA) program components are divided into those components that ensure basic compliance and those that sustain the program over time. They are as follows:

1. PROGRAM COMPONENTS THAT ADDRESS BASIC COMPLIANCE

a. **Designation of FOIA Officer.**

(1) Each VISN and VA Health Care Facility Director must formally designate by name and in writing, a FOIA Officer and an Alternate FOIA Officer for their respective component. Such designations must indicate whether the individual has signature authority for FOIA requests. Release of Information staff processing medical records requests under the FOIA must also be formally designated by the facility Director by name and in writing and indicate authority to sign the initial agency decision letter.

(2) The facility FOIA Officer must meet this requirement before processing FOIA requests, but is not required to conduct C3R of this component once compliance is met. However, the facility FOIA Officer is required to report compliance in the FOIA Facility Self-Assessment (FSA) as prescribed in this directive or as directed by the PCA Officer.

b. **Disclosures of Records.**

(1) The FOIA requires VA to proactively disclose to the public, records which have been determined to become or are likely to become subject to multiple FOIA requests or records that have been requested three times or more under the FOIA. Under the FOIA, information will only be withheld if the FOIA Officer can articulate a foreseeable harm in the disclosure or if the disclosure is prohibited by law. Whenever possible, the VHA FOIA Officer will disclose nonexempt information.

(2) The facility FOIA Officer must meet this requirement each time a FOIA request is processed, but is not required to conduct C3R of this component on an on-going basis. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

c. **Assessment of Fees.**

(1) FOIA processing fees will be assessed in accordance with the FOIA.

(2) The facility FOIA Officer must accurately assess processing fees each time they process a FOIA request, but is not required to conduct C3R of this component on-going. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

d. **Fee Waivers.**

(1) Requests for FOIA fee waivers will be assessed in accordance with the FOIA.

(2) The facility FOIA Officer must properly assess fee waivers each time they are requested as part of a FOIA request, but is not required to conduct C3R of this component on an on-going basis. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

e. **Timely Processing.**

(1) The FOIA provides that an agency has 20 business days to process a FOIA request. Under unusual circumstances, the FOIA provides for a 10-business-day extension.

(2) The facility FOIA Officer must adhere to the timeframes for processing FOIA requests each time they process a request, but is not required to conduct C3R of this component on-going. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

f. **Use of Exemptions.**

(1) FOIA exemptions should only be invoked in denying a request or portions of a request after careful review of the requested information.

(2) The facility FOIA Officer must properly invoke exemptions when denying a request each time they process a FOIA request, but is not required to conduct C3R of this component on-going. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

g. **Substantial Interest Requests.**

(1) The facility FOIA Officer is responsible for advising the appropriate facility leadership, VISN officials and the VHA FOIA Office of receipt of a substantial interest FOIA request. A substantial interest FOIA request is defined in VHA Directive 1935, VHA Freedom of Information Act Program, dated February 5, 2018.

(2) The facility FOIA Officer must advise appropriate personnel each time they process a substantial interest FOIA request, but is not required to conduct C3R of this component on-going. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

h. **Dispute Resolution.**

(1) The FOIA requester can contact the VHA FOIA Public Liaison and/or the Office of Government Information Services (OGIS) to seek assistance and/or dispute resolution services on any adverse determination.

(2) The facility FOIA Officer must fully cooperate with the VHA FOIA Public Liaison and OGIS in the event of a dispute, but is not required to conduct C3R of this component on-going. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

2. PROGRAM COMPONENTS THAT ADDRESS PROGRAM SUSTAINABILITY OVER TIME

a. **Correspondence.**

(1) The facility FOIA Officer(s) must ensure that all correspondence for each step in the FOIA process is sent to the requestor, that all required clauses and information are included and that the correspondence is signed by the correct facility official.

(2) The facility FOIA Officer must send all appropriate correspondence that includes all necessary information and ensure that it is signed by the correct official, but is not required to conduct C3R of this component on-going. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

b. **Administrative Files.**

(1) The facility FOIA Officer(s) must create and maintain an administrative case file for every request processed under the FOIA. The contents of the VHA FOIA administrative case file will be in compliance with VHA Directive 1935.

(2) The facility FOIA Officer must maintain a complete administrative file for each FOIA request processed, but is not required to conduct C3R of this component on an on-going basis. However, the facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

c. **FOIA Electronic Tracking.**

(1) All requests processed under the FOIA must be entered into VA's electronic FOIA tracking system in accordance with VHA Directive 1935.

(2) The facility FOIA Officer must enter all requests into VA's electronic FOIA system, but is not required to conduct C3R of this component on an on-going basis. However, the Facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

d. **Records Retention.**

(1) All FOIA administrative case files will be maintained in accordance with the NARA General Records Schedule (GRS) and VHA RCS 10-1.

(2) The facility FOIA Officer(s) must review their administrative case files at least annually to determine if the RCS 10-1 is being followed for the records created when processing FOIA requests. This review should also include a determination as to whether the FOIA files are maintained on a current file plan and inventory in order for them to be accessible to the agency when needed. The facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer.

e. **Agency Regulations and Policies.**

(1) The FOIA is implemented by VA FOIA regulations, 38 CFR 1.550-1.562.

(2) The facility FOIA Officer(s) must review the facility FOIA policies and practices at least annually to ensure the facility is managing the FOIA program consistent with Federal, VA, and VHA regulations and policies and that the facility adjusts its policies and practices when the regulations are changed. The facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Officer. ***NOTE:*** *The VHA FOIA Office is responsible for managing and updating VHA FOIA regulations and making necessary modifications based on changes to the FOIA and VA FOIA regulations. PCA will audit the VHA FOIA Office's compliance with this requirement.*

f. **FOIA Training.**

(1) The facility workforce must be aware of and follow FOIA requirements for appropriately releasing information under the FOIA. Specific areas of the facility that frequently make disclosures under the FOIA must be evaluated to determine that the workforce is aware of their responsibilities to follow FOIA and VA/VHA policies.

(2) The facility FOIA Officer(s) must conduct C3R of the following aspects of the workforce: Public Affairs, Privacy, Research and Release of Information departments, or other areas determined by PCA or the VHA FOIA Office, at least annually to determine if the workforce in these areas understand how FOIA requests are to be processed and that all FOIA requests must be processed by an official FOIA Officer. The Facility FOIA Officer is required to report compliance in the FOIA FSA as prescribed in this directive or as directed by the PCA Office.