Department of Veterans Affairs
National Cemetery Administration
Washington, DC 20420

NCA DIRECTIVE 6509
Transmittal Sheet
November 14, 2023

NATIONAL CEMETERY ADMINISTRATION PRIVACY PROGRAM

1. REASON FOR ISSUE: To establish policy and responsibilities for the National Cemetery Administration (NCA) wide Privacy Program, a program to ensure the protection of the personally identifiable information (PII) of Veterans, their dependents, and beneficiaries in accordance with Federal privacy statutes and regulations.

2. SUMMARY OF CONTENTS: This new directive establishes:

a. Policies for implementing, managing, and monitoring the NCA Privacy Program in accordance with applicable federal privacy laws, regulations, Executive Orders, and VA policies.

b. A framework for general duties performed by the NCA Privacy Officer and specific responsibilities for District and Facility Level Privacy Officers.

3. RESPONSIBLE OFFICE: NCA, Business Transformation and Requirements Service (43E), 810 Vermont Ave NW, Washington, DC 20420 is responsible for the contents of this directive. Questions may be referred to the NCA Privacy Officer, within the Business Transformation and Requirements Service (BTRS).

4. RELATED PUBLICATIONS:

a. VA Directive 6509, Duties of Privacy Officers (July 30, 2015).

b. VA Directive 6502, VA Enterprise Privacy Program (May 5, 2008).

5. RESCISSION: This publication rescinds NCA Notice 2013-06 (October 31, 2013).

6. RECERTIFICATION: This publication is scheduled for recertification in November 2028.

/s/
Matthew T. Quinn
Under Secretary for Memorial Affairs

Distribution: Electronic Only

NATIONAL CEMETERY ADMINISTRATION PRIVACY PROGRAM

1. PURPOSE/AUTHORITY:

a. This directive defines the roles of National Cemetery Administration (NCA) Privacy Officers in accordance with Department of Veterans Affairs (VA) Directive 6502, VA Enterprise Privacy Program (May 5, 2008) and VA Directive 6509, Duties of Privacy Officers (July 30, 2015).

b. This directive establishes general duties for NCA employees to maintain data stewardship principles to manage data for all individuals on whom data is collected or maintained. This directive defines responsibilities to protect the confidentiality of Personally Identifiable Information (PII).

c. The statutory authorities for the policies contained in this document are found in sections 552 and 552a of title 5, United States Code (U.S.C.), 38 U.S.C. § 5701, 38 U.S.C § 7332 and other applicable Federal privacy regulations and guidance.

2. BACKGROUND:

a. The NCA Privacy Program establishes and implements privacy policies and practices that comply with the requirements of applicable Federal privacy statutes, regulations, Office of Management and Budget (OMB) guidance and VA privacy policies.

b. The NCA Privacy Program addresses privacy policies, privacy training, Use and disclosure of information, individuals' privacy rights, privacy complaints, and privacy compliance monitoring.

c. The NCA Privacy Program applies to PII that is collected, created, transmitted, used, disclosed, processed, stored, or disposed of by, or for, NCA and that is maintained in any medium, including hard copy, electronic format, and by information systems administrated by, or otherwise under the authority or control of, the VA. Personally Identifiable Information (PII) is a subset of Sensitive Personal Information (SPI).

3. POLICY: It is NCA policy to ensure employees apply all privacy laws, regulations, OMB guidance, and VA policies and procedures.

4. RESPONSIBILITIES:

a. **Principal Deputy Under Secretary for Memorial Affairs** will:

(1) Initiate investigations of any allegation of noncompliance with the Federal Records Act (FRA), Freedom of Information Act (FOIA), Privacy Act (PA), or any VA confidentiality statute; and contact the VA Office of General Counsel (OGC) for such violations; and

(2) Report certain substantiated allegations, i.e., willful, and intentional violations, to the Inspector General pursuant to 38 Code of Federal Regulations (CFR) §§ 1.200 - 1.203.

b. **Deputy Under Secretary for Management** will:

(1) Establish and maintain the NCA Privacy Program, in accordance with applicable laws, regulations, and policies;

(2) Designate in writing a dedicated NCA-level Privacy Officer (or officers) based on organizational needs and legal requirements and notifies the VA Privacy Service (005R1A) of this designation; and,

(3) Periodically reassess the need for additional Privacy Officers as well as the requisite skills and staffing levels for all NCA facilities including, but not limited to: NCA Central Office, Field Offices, District Offices, and Cemetery locations.

c. **Deputy Under Secretaries, Senior Executives, District Executive Directors, Cemetery Directors, Central Office Service Directors, and Equivalent Level Managers and Supervisors** will:

(1) Ensure employees under their respective level of control are aware of and comply with the requirements of applicable Federal privacy statutes, regulations, OMB guidance, VA privacy policies, and required training within their operations;

(2) Designate in writing one facility primary Privacy Officer and one facility alternate Privacy Officer to manage and coordinate the privacy program activities for their respective office, cemetery, or organization. Provide copies of the written designation to the NCA Privacy Officer (see paragraph g.(3) of this directive) and to each designated employee. NOTE: NCA Central Office (NCACO) collocated offices may designate one primary Privacy Officer and one alternate Privacy Officer to manage and coordinate the Privacy program activities for those within 810 Vermont N.W. and 1575 I Street N.W. offices, and other assigned NCACO offices, in coordination with the Chief of Staff;

(3) Ensure the Privacy Officers' reporting structure is aligned under the Office of the facility or program office Director;

(4) Periodically reassess the necessity for additional Privacy Officers;

(5) Require designated Privacy Officers under their supervision timely complete Talent Management System (TMS) courses, 10176: VA Privacy and Information Security Awareness and Rules of Behavior, 4564136: Privacy Webinar Series: Getting Started in Your Role as a Privacy Officer, 4559869: Completing the Facility Self-Assessment (FSA), and other applicable privacy related training, as assigned; and

(6) Coordinate with the Business Transformation and Requirements Service Director and the NCA Privacy Officer to complete quarterly facility self-assessments, as developed by VA's Office of Information Technology, Privacy and Records Assessment

Directorate (PRAD), by the last workday of each quarter, and other requirements as specified on the NCA "BTRS: Privacy and Records Management Assessment Directorate (PRAD)" intranet page (for internal VA employees only).

d. The **Director, Business Transformation and Requirements Service (BTRS Director)** will:

(1) Establish the NCA Privacy Program for NCA in accordance with applicable laws, regulations, and policies;

(2) Monitor the NCA compliance with privacy requirements and report Administration-Level performance to the VA Chief Information Officer, or designee;

(3) Notify the Director, VA Privacy Service of the names and contact information for NCA designated Privacy Officers (PO) and alternates;

(4) Consult the Senior Agency Official for VA, Privacy (SAOP) concerning problems or questions of an administrative nature that arise during implementation of VA Directive 6509;

(5) Seek legal guidance from the VA Office of the General Counsel (OGC), including District Counsel Offices, to ensure legal compliance with the provisions of the laws affecting matters of privacy and related responsibilities; and

(6) Review instances where the disclosure, loan or exchange of records or information with other Government agencies and the National Personnel Records Center (NPRC) requires development of a Memorandum of Agreement or Understanding that meets a specific purpose.

e. The **NCA Privacy Officer** will:

(1) Implement the NCA Privacy Program in accordance with applicable laws, regulations, and policies;

(2) Promote employee awareness of this directive, and related regulations, and laws governing the collection, use and disclosure of information;

(3) Maintain a current and complete list of District and Facility-Level Privacy Officers and Alternates, as designated under paragraph c.(2) above;

(4) Provide guidance, information, and training and promote awareness of general privacy requirements, VA National Rules of Behavior, and other focused subjects;

(5) Provide input to Director, BTRS for the development of privacy policies, initiatives, program effectiveness;

(6) Work with the VA Privacy Service and VA Enterprise Risk Management (ERM) to ensure District and Facility-Level Privacy Officers are available to assist in compliance monitoring assessments;

(7) Collaborate with the NCA Records Management Officer to ensure proper disposal of files and records which contain SPI;

(8) Respond to all privacy complaints and immediately enter all actual or suspected privacy events into the designated data breach reporting system within one hour of discovery;

(9) Collaborate with Administration-Level Privacy Officers, Information System Security Officers (ISSO), and System Managers to ensure that all NCA data and associated risks are identified and documented in Privacy Threshold Analysis (PTA) and Privacy Impact Assessments (PIA) submissions to the VA Privacy Service;

(10) Assist District and Facility-Level Privacy Officers responsible for completion of the quarterly PRAD facility self-assessments by the last workday of each quarter;

(11) Support the PRAD pre-assessment, assessment, and post-assessment corrective action planning activities to review, manage, and improve the Privacy Program;

(12) Collaborate with the VA Privacy Service, Administration-Level, District-Level, and Facility-Level Privacy Officers assess VA's compliance with all privacy policy requirements; and

(13) Identify Privacy Act System of Records (SORs) and work with the appropriate parties to publish current system of records notices (SORNs) for all NCA SORs.

f. **Designated District-Level Privacy Officers** and **Facility-Level Privacy Officers** will:

(1) Within 30-days of designation as a Privacy Officer, complete required Talent Management System (TMS) courses, including but not limited to: 10176: VA Privacy and Information Security Awareness and Rules of Behavior, 4564136: Privacy Webinar Series: Getting Started in your role as a Privacy Officer, 4559869: Completing the Facility Self-Assessment (FSA) and other applicable privacy related training, or as assigned;

(2) Coordinate with the NCA Privacy Officer to ensure compliance with privacy practices and consistent application of sanctions for failure to comply with VA privacy policies for all NCA Personnel within their program areas;

(3) Establish and implement facility policies and standard operating procedures (SOP) that implement this directive;

(4) Administer privacy awareness programs within their area of responsibility;

(5) Collaborate with the NCA Records Management Officer or designated Facility-Level Records Liaison Officers to retain and dispose of records, especially those that contain PII, in accordance with VA Directive 6509;

(6) Understand and apply federal laws, regulations, guidance, and VA policy related to privacy;

(7) Monitor completion of VA Privacy and Information Security and National Rules of Behavior annual training for all facility employees, volunteers, contractors, and other third parties, as appropriate;

(8) Respond immediately to all privacy incidents or complaints within one (1) hour of discovery as stipulated in VA Directive 6502, and VA Handbook 6500.2;

(9) All privacy incidents or complaints received by a District-Level Privacy Officer are for the purposes of gathering all background information needed to submit a PSET, and to forward the PSET ticket to NCA's Privacy Officer for tracking. All Cemetery Facility Privacy Officers are to contact their District Privacy Officers with all privacy incidents or complaints. If the District-Level Privacy Officer is unavailable the Cemetery Facility Privacy Officer should contact the NCA Privacy Officer at cemncaprivacy@va.gov. If the NCA Privacy Officer is unavailable or it is after normal business hours (e.g., weekends or holidays) contact the National Service Desk (NSD) by calling 1 (855) 673-4357 (Option 6, Option 1) or send an email to NSD/VPNSecurity@va.gov. The NSD will open a ticket and route to the NSOC Network Defense Center (NDC), who will then open a PSET ticket for the Privacy Officer;

(10) All other Facility-Level Privacy Officers will send all privacy incidents or complaints to cemncaprivacy@va.gov. If the NCA Privacy Officer is unavailable or it is after normal business hours (e.g., weekends or holidays) contact the National Service Desk (NSD) by calling 1 (855) 673-4357 (Option 6, Option 1) or send an email to NSD/VPNSecurity@va.gov. The NSD will open a ticket and route to the NSOC Network Defense Center (NDC), who will then open a PSET ticket for the Privacy Officer;

(11) Provide the findings of privacy investigations regarding confirmed privacy incidents (i.e., data breaches and policy violations) to stakeholders – such as the NCA Privacy Officer, NCA Human Capital Management Employee Relations/Labor Relations (ER/LR), and the NCA employee's supervisor – so that stakeholders can determine next steps;

(12) Promote activities sponsored by the enterprise or Administration-Level that foster privacy awareness within the facilities and promote a proactive privacy environment within their organizations;

(13) Conduct and document walkthroughs of all areas of the facility to ensure that privacy-related policies are being followed and provide guidance, and training as needed, to employees on proper procedures for the handling of PII at least quarterly;

(14) Work with facility personnel involved with any aspect of the collection, maintenance, protection, and disposal of PII to ensure full compliance with privacy laws, regulations, OMB guidance, VA policy and procedures;

(15) Complete quarterly PRAD Facility Self-Assessment (FSA) no later than the last workday of each quarter; see guidance on the NCA "BTRS: Privacy and Records Assessment Directorate (PRAD)" intranet page;

(16) Participate in contract acquisition reviews related to inclusion of privacy language in VA Performance Work Statements and approval of Privacy and Security checklist in accordance with VA Handbook 6500.6, Contract Security; (Contracting Officer's Representative, Information Security Officer, or Contracting Officer only if contract involves PII/SPI) Procurement Requestor/Program Manager, site Program Office or other Team Members participating in acquisitions, as applicable; and

(17) NCA site Privacy Officers should know the process to provide review and oversight for the facility Release of Information functions to comply with the Privacy Act of 1974, and the procedures for processing requests outlined in VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act. NCA FOIA Officer handles all Release for Information requests send to vacovancaf@va.gov.

g. **NCA Personnel** will:

(1) Complete all applicable VA and NCA required privacy training at the time of employment, annually thereafter, or as directed;

(2) Comply with all Federal laws and regulations, VA regulations and policies, NCA policies and local (program office and/or facility) procedures relating to privacy;

(3) Immediately report all actual or suspected breaches of privacy to the District or Facility-Level Privacy Coordinator;

(4) Consult the District or Facility-Level Privacy Officer to address questions or concerns about privacy-related issues;

(5) Prior to sharing or disclosing PII outside VA, consult with District or Facility-Level Privacy Officers or the NCA Privacy Officer to confirm legal authority exists for the disclosure; and

(6) Use, disclose, or request the minimum amount of PII necessary to perform specific job functions in accordance with applicable System of Records Notice (SORN).

5. REFERENCES: The VA Privacy Program has its foundation in Federal statutes, Executive Orders, Office of Management and Budget directives, and VA guidance to include, but not limited to, the authorities described below.

a. E-Government Act of 2002, Pub. L. 107-347, 166 Stat. 2899 (2002).

b. Federal Information Security Modernization Act of 2014.

c. Freedom of Information Act (FOIA), 5 U.S.C. § 552.

d. Privacy Act of 1974, as amended, 5 U.S.C. § 552a (2018).

e. 38 U.S.C. § 5701, Confidential Nature of Claims; 38 CFR §§1.500-527, Release of Information from Department of Veterans Affairs Claimant Records.

f. 38 U.S.C. § 7332, Confidentiality of Certain Medical Records; 38 CFR §§ 1.460-496, Release of information from Department of Veterans Affairs Records Relating to Drug Abuse, Alcoholism or Alcohol Abuse, Infection with the Human Immunodeficiency Virus (HIV), or Sickle Cell Anemia.

g. Social Security Fraud Prevention Act of 2017, Pub. L. 115-59.

h. OMB Circular No. A-130, Managing Information as a Strategic Resource, July 28, 2016.

i. OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and publication under the Privacy Act, December 23, 2016.

j. OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

k. OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy, September 15, 2016.

l. OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017.

m. OMB M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements, November 19, 2019.

n. National Institute for Standards and Technology Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide, August 8, 2012.

o. National Institute for Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 23, 2020.

p. National Institute for Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.

q. VA Directive 6500, VA Cybersecurity Program, February 24, 2021.

r. VA Directive 6507, Reducing the Use of Social Security Numbers, November 20, 2008.

s. VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014.

t. VA Handbook 5021, Employee/Management Relations, December 28, 2017.

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

v. VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records, August 3, 2017.

w. VA Handbook 6500, Risk Management Framework for VA Information Systems – VA Information Security Program, February 24, 2021.

x. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), June 30, 2023.

y. VA Handbook 6500.5, Incorporating Security and Privacy into the System Development Life Cycle, March 22, 2010.

z. VA Handbook 6500.6, Contract Security, March 12, 2010.

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

6. DEFINITIONS:

a. **Personally Identifiable Information (PII):** For purposes of this Directive, PII is considered to be the equivalent of VA Sensitive Information/Data. PII is any information about an individual that can be used to distinguish or trace an individual's identity, alone, or when combined with other information which is linked or linkable to a specific individual, such as: name, social security number, date and place of birth, mother's maiden name, telephone number, driver's license number, credit card number, photograph, finger prints, biometric records, training, financial transactions, medical history, and criminal or employment history, etc. For purposes of this directive, the term PII is interchangeable with the term Sensitive Personal Information (SPI).

b. **Privacy Impact Assessment (PIA):** An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks (SOURCE: 44 U.S.C. § 3541-3549; NIST SP 800-53; NIST SP 800-18; NIST SP 800-122; CNSSI 4009; OMB Memorandum 03-22).

c. **Privacy Incident:** A privacy incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (SOURCE: FIPS PUB 200 (adapted)).

d. **Privacy Threshold Analysis (PTA):** A PTA is used to identify information technology (IT) systems, rulemakings, programs, or pilot projects that involve SPI and other activities that otherwise impact the privacy of individuals as determined by the Director, VA Privacy Service, and to assess whether there is a need for a PIA, whether a System of Records Notice is required, and if any other privacy requirements apply to the IT system. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what SPI is collected (and from whom) and how that information is used (SOURCE: VA Handbook 6508.1).

e. **Sensitive Personal Information (SPI):** SPI, as defined by 38 U.S.C. § 5727(19), is any information about the individual maintained by an agency, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. For purposes of this directive, the term SPI is interchangeable with the term PII.

f. **System of Records (SOR):** A System of Records is a group of any records under the control of any agency from which information is retrievable by the name of the individual or by some identifying number, symbol, or other identifying element assigned to the individual (SOURCE: 5 U.S.C. § 552a).

g. **System of records notice (SORN):** The notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a SOR describing the existence and character of the system. A SORN identifies the SOR, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system (SOURCE: OMB Circular A-108).