DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH VA 22042

BUMEDINST 5263.1C
BUMED-N6
26 May 2026

BUMED INSTRUCTION 5263.1C

From: Chief, Bureau of Medicine and Surgery

Subj: PRIVACY AND CIVIL LIBERTIES PROGRAM

Ref: (a) 10 U.S.C. §8077
(b) OPNAVINST 5450.215G
(c) DoD Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Healthcare Programs, 13 March 2019
(d) DoD Instruction 8580.02 of 12 August 2015
(e) DoD Instruction 5400.11 of 29 January 2019
(f) SECNAVINST 5211.5F
(g) DHA-PM 6025.02, DoD Health Record Lifecycle Management, Volume 1: General Principles, Custody and Control, and Inpatient Records, 23 November 2021
(h) DHA-PM 6025.02, DoD Health Record Lifecycle Management, Volume 2: Outpatient Record Components and Dental Records, 16 December 2021
(i) DoD Instruction 5400.16 of 11 August 2017
(j) OMB Circular No. A-130, Managing Information as a Strategic Resource, 28 July 2016
(k) OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, 23 December 2016
(l) 45 CFR Part 160 and Subparts A and E of Part 164
(m) SECNAVINST 5510.35D
(n) 5 U.S.C. §552a
(o) DoD Instruction 6025.18 of 13 March 2019
(p) DoD Instruction 8510.01 of 19 July 2022
(q) DoD 5400.11-R, Department of Defense Privacy Program, May 2007
(r) Public Law 107-347
(s) DoD Manual 5400.11, Volume 2, DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan, 6 May 2021
(t) DoD Instruction 5000.90 of 31 December 2020

1. Purpose

a. This Bureau of Medicine and Surgery (BUMED) instruction, based on authority of references (a) and (b) and per references (c) through (t) establishes policy, assigns responsibilities, and establishes the BUMED Privacy and Civil Liberties Program procedures for achieving and sustaining compliance within BUMED for the following functions:

Privacy and civil liberties regulatory compliance program and initiatives; Health Insurance Portability and Accountability Act (HIPAA) policy development and guidance; E-Government Act implementation; civil liberties policy and training; complaint resolution; and privacy risk management. This publication does not address implementation of religious freedoms under the civil liberties program as prescribed in Department of Defense (DoD) Instruction 1300.17, Religious Liberty in the Military Services, 1 September 2020.

b. This policy revision consolidates privacy policy, establishes a civil liberties complaint resolution process, updates privacy requirements, and establishes roles and responsibilities for covered entities and business associates organized under the authority of the Surgeon General of the Navy. The policy enhances Navy Medicine alignment and grouping of privacy functions and tasks in support of the Department of the Navy (DON) and the Defense Health Agency (DHA) Military Health System (MHS) privacy frameworks.

2. Cancellation. BUMEDINST 5263.1B and BUMEDINST 5211.4.

3. Scope and Applicability

a. This instruction is applicable to all military, civilian, and contractor and subcontractor personnel assigned or supporting Budget Submitting Office (BSO) 18 commands and detachments as well as non-BSO-18 medical personnel subject to the authorities of the Navy Surgeon General, who also performs the duties of Chief of BUMED.

b. Navy expeditionary medical forces subject to the authorities of the Surgeon General of the Navy are considered part of the MHS hybrid designation as covered entities under the HIPAA Privacy Rule as defined in reference (c) section 3.3.c.3 and are subject to the Privacy, Security, and Breach Notification Rule requirements outlined in references (c) and (d). Navy personnel assigned or attached to the DHA are subject to comply with DHA AI 5400.01, Privacy and Civil Liberties Compliance policy as amended. The following BUMED Headquarters (HQ) N-Codes are designated covered entity functions and subject to the HIPAA Privacy Rule: Surgeon General of the Navy/Chief, BUMED (BUMED-N00); Deputy Surgeon General of the Navy/Deputy Chief, BUMED (BUMED-N01); Director, HQ Operations (BUMED-N02B); Director, Maritime Headquarters (BUMED-N03); Director, Maritime Operations (BUMED-N04); Public Health and Safety (BUMED-N44); Director, Communication and Information Systems (BUMED-N6); Director, Medical Information and Research & Development (BUMED-N2), (DON Veterinary Research (BUMED-N24) exempt); Director, Operations, Plans, and Policy (BUMED-N3N5); and Director, Clinical Operations, Policy, and Standards (BUMED-N10). Echelon 3 and below commands will designate which of their Region N-Codes and below are subject to the HIPAA Privacy Rule based on their assessments and consultation with their legal staff or Privacy, Integration, and Capability Management (BUMED-N61). Commands will publish their respective policies and amend as required to reflect these designations.

c. The Department of War (DOW) drug laboratories and echelon 3 and below commands that are not designated as a covered entity or subject to a business associate agreement (BAA)

are exempt from complying with the HIPAA Privacy Rule, however, may have responsibilities to adhere to the HIPAA Security Rule if required by authorization to operate local network issued by DHA PEO Medical Systems and Chief Information Officer (J-6).

4. Background. As an essential element in managing organizational privacy risks, it is BUMED policy to use the Fair Information Practice Principles (FIPP) as the foundation of its privacy policies. It promotes compliance with the Privacy Act of 1974 as amended, E-Government Act section 208, and the Office of Management and Budget (OMB) privacy policies applicable to all Federal information systems (IS) and organizations. The BUMED privacy framework is predicated on the following elements: leadership engagement and strategic planning, privacy risk management, information security, incident response, complaint redress, training, and accountability, which are prescribed in references (c) through (e). The policy prescribes the proper handling of personally identifiable information (PII) and protected health information (PHI) to include access, dissemination, disclosure, processing, or transmission of such information in the performance of the Navy Medicine mission and official duties. PHI is a subset of PII and requires additional safeguards based on the HIPAA Privacy, Security, Breach Response, and Notification Rules. References to PII in this instruction includes the subset of PHI, unless otherwise specified.

5. Roles and Responsibilities

a. BUMED-N00. BUMED-N00 will maintain overall responsibility for the implementation of this publication to safeguard the privacy and security of PII entrusted to the Navy Medicine workforce and to ensure reasonable and adequate safeguards are maintained for all such PII created, maintained, received, or transmitted through electronic or non-electronic media.

b. BUMED-N6

(1) Exercise oversight over BUMED privacy and civil liberties functions to ensure compliance with this instruction, Federal statutory laws, and higher authority directives.

(2) Ensures coordination between BUMED N-Codes, DHA, DON, other uniformed medical departments, Federal agencies, and subordinate commands on privacy policy and compliance requirements.

(3) Provide strategic program direction, budget support, and ensure staffing for enterprise and HQ privacy and civil liberties program execution.

c. BUMED-N61. BUMED-N61 serves as the enterprise and HQ BUMED privacy officer and has responsibility for the implementation, development, and execution of privacy compliance and risk management functions and per applicable higher authority guidance and statutory laws listed in subparagraphs 5c(1) through 5c(7).

(1) Coordinate and liaison across BUMED N-Codes; Navy Medicine region commanders and subordinate commands; DON Chief Information Officer (DONCIO); Chief of Naval Operations Freedom of Information Act (FOIA)/Privacy Act (PA) Program Office (DNS-36); U.S. Fleet Forces Surgeon; the Medical Officer of the Marine Corps (TMO); and the DHA Privacy and Civil Liberties Office (PCLO) to ensure implementation of privacy policies and reporting requirements subject to the authorities of BUMED-N00 and DOW directives.

(2) Establish policies and procedures within the organization for receiving, documenting, tracking, investigating, and acting on all complaints, breaches, redress, and conflicts with DOW and DON privacy policy.

(3) Perform compliance activities, privacy risk assessments, mitigation, and implementation of best business practices across BSO-18. BUMED-N61 reviews and provides input to the Component privacy plan, policies, and procedures.

(4) Serve as a BUMED coordinating office for data sharing agreement (DSA) application reviews, privacy impact assessments (PIA), Navy Medicine System of Records Notices (SORN), and breaches of PII and PHI. Facilitates privacy reviews for Navy Medicine and Tri-Service data with appropriate BUMED N-Codes and DHA data sharing compliance manager.

(5) Support implementation of privacy controls and safeguards and ensures privacy requirements are incorporated into each stage of the information life cycle as required by references (e) and (f) as amended.

(6) BUMED-N61 supports BUMED readiness, force health protection, training, and research functions by balancing its need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and dissemination of their PII.

(7) Facilitate training of personnel involved with collecting, using, maintaining, safeguarding, accessing, amending, and disseminating PII within BUMED to ensure compliance with references (d) and (e).

d. Staff Judge Advocate (BUMED-N01J) and Office of General Counsel (BUMED-N01L). Serves as the BUMED HQ and Navy Medicine senior legal advisors. Advises, interprets, reviews, and coordinates on privacy legal matters related to Privacy Act of 1974 as amended, FOIA, E-Government of 2002, HIPAA, and other legal authorities; reviews for legal sufficiency reports, SORNs, proposed rules, and other related matters that BUMED establishes in the Federal Register, posts on the BUMED Web site, and submits to Congress, OMB, or other parties; ensures BUMED directives, BAA, DSAs, memorandums of understanding, and memorandums of agreement meet statutory requirements stipulated in Federal laws and governing directives.

e. BUMED Forms Manager (BUMED-N02B2). Serves as the forms, survey, and records manager for BUMED enterprise. Ensures all surveys, forms, and information collections received for processing, which are subject to the Privacy Act of 1974 as amended, are coordinated for appropriate privacy compliance and legal reviews; additionally, BUMED-N02B2 is responsible for managing BUMED's compliance with the Paperwork Reduction Act and serves as the Information Management Control Office (IMCO) for submitting BUMED's SORNs, forms, and surveys to DNS-36 and the OMB. Ensures BUMED IS portfolio records have appropriate life cycle and retention schedules applied to them as the records manager signature authority for Navy Medicine privacy impact assessments.

f. Navy Medicine Commanders, Commanding Officers, and Officers in Charge. Commanders and commanding officers are responsible for appointing a privacy officer and implementing privacy and civil liberties compliance oversight of all subordinate command activities under their respective authority. Region commanders are to provide HIPAA Privacy consultation and support to the operational medical forces within their respective areas of responsibility by providing guidance, coordination support, and assistance with PHI breach complaints and investigations. Commander and commanding officers are to exercise accountability and develop local privacy policies and procedures to support the BSO-18 mission.

g. Navy Operational Healthcare Personnel. The Medical Officer of the Marine Corps, U.S. Fleet Forces Command Surgeon, and other DON operational healthcare personnel and related assets including Fleet and Fleet Marine Force operational medical platforms, units, and deployed medical personnel under the control of the DON are included in a DOW covered entity under the Surgeon General of the Navy. These personnel are responsible for adhering to the uses, disclosures, safeguarding, and breach notifications of PHI outlined in references (c), (d), (g), and (h).

h. Program Managers (PM). Designated BUMED PMs are responsible for ensuring the appropriate collection, use, maintenance, and dissemination of that program's PII assets as required by applicable directives. Refer to references (e) and (f) as amended for a comprehensive listing of PM responsibilities to include implementing administrative, technical, and physical safeguards for PII assets.

i. BUMED Workforce. Supervisors are responsible for ensuring that staff receive instruction and training on safeguarding PII prior to their access to or maintenance of systems protected under the Privacy Act of 1974 as amended. Staff may be subject to disciplinary action for failure to take appropriate action upon discovering a breach or failure to take required steps to appropriately safeguard PII. The workforce is responsible for complying with the requirements of the HIPAA Privacy, Security, and Breach Notification Rules; Privacy Act of 1974 as amended; and other Federal privacy authorities as applicable.

6. Policy. It is BUMED policy to use the FIPP as the foundation for complying with the Privacy Act, the E-Government Act Section 208, and the OMB privacy policies. The FIPPs frame the privacy risks and the mitigation strategies required to protect and ensure the proper

handling of PII. Examples of PII include but are not limited to: name, address, social security number (SSN) or other identifying number or code, mother's maiden name, individually identifiable health information, date of birth, place of birth, driver's license number, medical records or medical record number, telephone number, and email address. PII can also consist of a combination of indirect data elements such as gender, race, birthdate, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. The BUMED Privacy Program uses the FIPPs elements outlined in subparagraphs 6a through 6h as a framework for organizing and addressing privacy protections when considering privacy in BUMED programs throughout the information lifecycle.

a. Authority and Purpose. BUMED should articulate specifically the authority that permits the collection of PII and articulate specifically the purpose(s) for which the PII is intended for use.

b. Accountability, Audit, and Risk Management. Provide accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern collection, use, maintenance, and dissemination of PII, and audit for the actual use of PII to demonstrate compliance with established privacy controls.

c. Data Quality and Integrity. Ensure, to the greatest extent possible, that PII use is accurate, relevant, timely, and complete, as identified in the public notice and applicable privacy impact assessments.

d. Data Minimization and Retention. Collect only PII that is directly relevant and necessary to accomplish the specified purposes authorized by statute, directive, or policy. Only retain PII for as long as necessary to fulfill the specified purposes and per the appropriate DON and National Archives and Records Administration-approved record retention schedules referenced in SECNAV Manual 5210.1 of September 2019 and located at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

e. Individual Participation and Redress. BUMED should involve the individual in the decision-making process regarding the collection and use of his or her PII and seek individual consent for the collection, use, maintenance, and dissemination of PII as required by the Privacy Act of 1974 as amended, and provide a mechanism for appropriate access, redress, and amendment of the PII.

f. Security. BUMED should protect PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or unauthorized disclosure.

g. Transparency. BUMED should be transparent and provide notice to individuals regarding its collection, use, maintenance, and dissemination of PII.

h. Use Limitation. Use PII solely for the purposes specified in the public notice and share information compatible with PII intent and objectives.

7. Privacy Controls. Per reference (i), BUMED uses the PIA to evaluate the application of required privacy controls in BUMED IS, electronic data collections, and business intelligence projects. In adherence with DOW policies, privacy controls are based on the FIPPs and the guidance provided by the National Institute for Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020, as amended. The privacy control catalog provides a structured set of controls based on best practices to facilitate compliance with Federal privacy authorities and to manage privacy risks.

8. Federal Privacy Compliance. Pursuant to references (c), (e), and (j), BUMED must comply with Federal privacy legislation and the implementing DOW regulations and OMB policy guidance.

a. SORN. BUMED must publish a notice in the Federal Register for systems of records where records are retrieved, per references (j) and (k), by an individual's name or other PII that uniquely identifies or links to an individual.

(1) Requests to publish a new SORN or modify, amend, or rescind an existing SORN for any BUMED system of record must be submitted by information technology managers and owners to BUMED-N61 for review via e-mail to usn.ncr.bumedfchva.list.bumed-privacy@health.mil. BUMED-N61 will coordinate with the IMCO to submit the request to Defense Privacy, Civil Liberties, and Freedom of Information Act Directorate (DPCLFD) via Director Secretary of the Navy, Freedom of Information and Privacy Act and Privacy Program Office (DNS-36) for approval and publication in the Federal Register.

(2) Any request to claim a Privacy Act Exemption for a system of record must be reviewed by BUMED-N01J or BUMED-N01L prior to submission to BUMED-N61 for review and further coordination.

(3) Compliance with surveys, forms, and collections is under the purview of the IMCO. BUMED-N61 will facilitate privacy compliance reviews with the IMCO for SORNs, forms, surveys, and electronic collections.

(4) BUMED components are required to ensure SORNs submitted to BUMED-N61 for review and submission to Director of Navy Staff are compliant with references (e) and (j) by coordinating with their respective records manager and local privacy officer.

b. SSN Justification Memorandums. The collection, use, or retention of the SSN in any form, system, application, shared drive, web portal, or other repository (e.g., full, truncated,

masked, partially masked, encrypted, or disguised SSNs) pursuant to the DOW acceptable use criteria must be documented in an SSN Justification Memorandum and approved by DPCLFD as directed in reference (e).

(1) Memoranda must be submitted to BUMED-N61 for review via e-mail to usn.ncr.bumedfchva.list.bumed-privacy@health.mil. BUMED-N61 will work with the PM or action officer to ensure the justification package is complete and ensure there is a plan to eliminate the SSN (if possible), prior to submission to DPCLFD for approval and signature.

(2) Memoranda are effective for 2 years and unless there are significant changes to the associated IS, form, or other information collection that would make the information contained in the original memorandum outdated or inaccurate. In such instances, stakeholders should consult with BUMED-N61 to determine whether a new memorandum is required. BUMED-N61 will additionally consult with DHA PCLO and Director of Navy Staff on these matters as appropriate.

c. Information Collections. Requests to implement a new BUMED information collection (i.e., forms and surveys) or modify an existing collection must be routed through the forms management officer and IMCO as appropriate.

d. Privacy Act Statement and Advisories. A Privacy Act Statement must be provided when PII is collected directly from an individual, placed into a system of record, and retrieved by a personal identifier. The statement provides the individual with information necessary to make an informed decision about whether to provide that information. A privacy advisory is required whenever accessing a system which may contain PII.

(1) BUMED-N61 will advise on the requirement for a Privacy Act Statement or advisory.

(2) Privacy Act Statements and privacy advisories must be submitted to BUMED-N61 for review via e-mail to usn.ncr.bumedfchva.list.bumed-privacy@health.mil.

e. PIA. A PIA must be performed on DOW IS and electronic collections, including those supported through contracts with external sources, that collect, maintain, or disseminate PII. PIAs must be updated by the system owner or manager, per references (j) and (i).

(1) Use of the DD Form 2930 Privacy Impact Assessment (PIA) is mandatory for all PIA submissions. The DD Form 2930 should be coordinated with BUMED-N61 using MED365-BUMED PCLO Resource Hub Channel or via e-mail at usn.ncr.bumedfchva.list.bumed-privacy@health.mil. After review and signature coordination within BUMED, BUMED-N61 will coordinate with DHA PCLO for additional coordination and approval. For Navy Medicine managed systems that are hosted in a DONCIO authorized network boundary, those PIAs will be coordinated with the DONCIO for review and approval.

(2) Once signed by the DHA CIO or designee, the PIA is considered fully executed and will remain valid for a period of 3 years. If a system or collection with a completed PIA is significantly changed and creates new privacy risks, the privacy risk posture must be reassessed with a new PIA. Significant modification examples may include system management changes, hosting environment migrations, significant merging, new interagency uses, alteration in character of data (e.g., when new PII is added to a collection), or if there are changes in a system's actual retrieval of records subject to the Privacy Act.

(3) Once the fully executed PIA is approved, a section 508 compliant version of section 1 of the PIA will be posted for the public on the DHA Web site at: https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Impact-Assessments, per reference (i).

(4) A copy of the fully executed PIA will be provided to the Office of the DOW CIO by DHA PCLO.

(5) BUMED-N61 will update the DOW Information Technology Portfolio Repository (DITPR) to ensure the privacy modules reflect the current privacy status for Navy Medicine managed IS and applications.

f. Privacy Act Amendments, Complaints, and Redress. Requests for amendments of records subject to the Privacy Act of 1974 as amended are to be coordinated and redressed following the procedures outlined in references (e) and (f).

(1) All requests should be labeled "Privacy Act Amendment Request," or a similar designation. A request should identify each particular record in question, state the amendment or correction that the requestor wishes to make, and state why the requestor believes that the record is not accurate, relevant, timely, or complete. The requestor may submit any documentation that they think would be helpful. If the requestor believes that the same record is in more than one system of records, the requestor should state that and address their request to each component that maintains the record.

(2) Within 10 working days of receiving a request for amendment or correction of records, the BUMED Program Office or designee that received the request should send the requestor a written acknowledgment of its receipt of the request, notifying the requestor whether the request is granted or denied.

(3) Privacy Act complaints will be forwarded to BUMED-N61 or local command privacy officer for review, coordination, and final determination in consultation with BUMED-N01J or BUMED-N01L as appropriate and the program office responsible for the system of record. Amendment requests and complaints may be submitted to BUMED-N61 at usn.ncr.bumedfchva.list.bumed-privacy@health.mil.

9. DSAs. DSAs are administrative controls used by Navy Medicine to document the requested use of data managed by the organization to ensure compliance with Federal law and DOW and DON implementing policies. DSA is an umbrella term utilized to refer to various agreements (i.e., memorandums of agreement, BAAs, and memorandums of understanding) concerning data transfers or those involving controlled unclassified information subject to access, use, transfer, maintenance, and disclosure requirements. BUMED-N61 does not provide data extractions or grant system access to requestors seeking PII for research, business associate functions, or health care operations. The system managers or PMs who control access to systems containing PII are responsible for providing data extractions to requestors once a DSA or other applicable agreement has been approved.

a. Navy Medicine has adopted a data sharing review process using templates to help facilitate and streamline the process. To ensure compliance, stakeholders should initiate appropriate DSAs when requests for use or disclosure of PII in Navy Medicine managed IS or systems of record occur. Data sharing requests should be submitted to the Assessments and Analytics (Consolidated Information Center) (BUMED-N58) for chief data officer oversight and coordination.

b. Data stakeholders requesting PII managed by or under the custodial care of Navy Medicine will be forwarded by BUMED-N58 to BUMED-N61 for privacy and cybersecurity compliance review, approval, and additional coordination using usn.ncr.bumedfchva.list.bumed-privacy@health.mil.

c. Stakeholders may refer to the business associate agreement contract template and the BUMED procedure, guidance, and information for standardized contract language and procurement responsibilities when sharing PII with contractors also referred to as business associates when PHI is shared. Contractors who provide services to the DON and receive or create PHI in performance of the service must have a BAA incorporated into their contract as required by reference (c), where appropriate. BUMED privacy standard operating procedures (SOP), guidance, and templates may be located on the BUMED SharePoint site and MED365-BUMED PCLO Resource Hub Channel.

10. Breach Response and Prevention. Commanders and commanding officers must designate a privacy officer or other designated official for incident reporting, investigations, follow-up actions, and individual notifications. References (e) and (h) provide the procedures for reporting, responding, and mitigating any potential or confirmed breaches of PII or PHI within BUMED areas of responsibility. Organizational leadership must ensure a prompt and coordinated response is initiated when PII is lost, stolen, or compromised within the respective Navy Medicine areas of responsibility.

a. Reference (h) defines a breach as a loss of control (i.e., missing or lost service treatment records, misdirected emails, compromised network, etc.), compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access to or potential access to PII, whether physical or

ensure all mandatory reporting and notification requirements are executed. Refer to the BUMED Breach Incident Reporting and Mitigation SOPs for additional response and prevention guidance. BUMED Privacy SOPs may be located on the BUMED SharePoint site and MED365-BUMED PCLO Resource Hub Channel.

b. All BUMED workforce members will report suspected or confirmed compromise of PII or PHI to the local privacy officer or IS security manager within 1 hour upon discovery. In coordination with the privacy officer, workforce members will verify with the local information technology department and upon confirmation report a confirmed or suspected cybersecurity incident to DHA Cyber Operations Center within 1 hour at usn.jbcharleston.niwcatlanticsc.mbx.cssp-watch@health.mil. The information technology department or IS security manager will make courtesy notification to the DON Fleet Cyber Command for their situational awareness when Navy equities, including records, data, mission, or controlled unclassified information are potentially compromised.

c. DHA Cyber Operations Center is responsible for executing required reporting to U.S. Cyber Command within 48 hours as required by reference (h).

d. Business associates who create, receive, maintain, or transmit PII or PHI will report all cybersecurity incidents that occur outside of DOW's network directly to Cybersecurity and Infrastructure Security Agency and U.S. Computer Emergency Readiness Team within 48 hours. Additionally, business associates will report all breaches to BUMED-N61 within 24 hours of discovery using DD Form 2959 Breach of Personally Identifiable Information (PII) Report via e-mail: usn.ncr.bumedfchva.list.bumed-pii-rpt@health.mil.

e. U.S. Cyber Command will report to Cybersecurity and Infrastructure Security Agency and U.S. Computer Emergency Readiness Team within 1 hour if the incident involves a confirmed cybersecurity incident.

f. BUMED-N61 or the reporting DOW stakeholder will submit the breach report in the Defense Privacy Information Management System (DPIMS) located at https://dpims.disa.mil/eCasePortal/Home.aspx (any DOW CAC holder), or use DD Form 2959 when DPIMS is unavailable. Report all PHI breaches to the DHA PCLO and ensure the chain of command and the supporting privacy office is made aware of the breach.

g. BUMED-N61 will make an initial risk notification determination on whether a PII breach subject to the Privacy Act of 1974 as amended is required on a case-by-case basis and will document a breach risk analysis for each reported breach in DPIMS. All PHI related breaches must be coordinated and reported to the DHA PCLO for risk and notification determination. If notification is required, the command responsible for the breach must submit a notification letter within 10 days of receiving a breach risk analysis determination.

h. The DHA PCLO will make the determination regarding whether a PHI breach is reportable to the U.S. Department of Health and Human Services (HHS), Office of Civil Rights.

11. Use and Disclosures of PHI Subject to the HIPAA Privacy Rule. With the exception of those BUMED N-Codes or commands that have been granted a HIPAA waiver, the BUMED workforce and expeditionary medical forces under the authority of the Surgeon General of the Navy are subject to the requirements of the HIPAA Privacy, Security, and Breach Notification rules pursuant to references (c) and (l) as either part of the MHS covered entity (a hybrid organization) or as a business associate based on DSAs, policies, or condition of access to systems and networks containing PHI under the authority of the DHA. All PHI released will be limited to the minimum necessary to accomplish the intended purpose of the disclosure, to an identified requester, and in support of a valid requirement for the information.

a. Disclosure, Amendment, and Restriction Guidance. In general, PHI of individuals both living and deceased must not be used or disclosed except for specifically permitted purposes. According to HIPAA Privacy Rule, DOW regulations, and the MHS Notice of Privacy Practices, individuals have a right to request (in writing) amendments or restrictions of uses and disclosures of their PHI; however, covered entities are not required to agree to the amendment or restriction request.

(1) Reference (c) authorizes the use of DD Form 2870 Authorization for Disclosure of Medical or Dental Information when authorizations are required for disclosure (Please Note: Not authorized for drug and alcohol abuse medical records). DD Form 2871 Request to Restrict Medical or Dental Information is used for beneficiaries requesting restrictions on the disclosure of their PHI.

(2) Substance Use Disorder (SUD) Records. Beneficiaries requesting a copy of their substance use disorders records or requesting disclosure to a third party must submit their request to the appropriate treatment site. The confidentiality of medical records associated with counseling, treatment, or rehabilitation of beneficiaries who received treatment in a substance abuse rehabilitation program must be made utilizing DD Form 3130 Consent for the Disclosure of Confidential Substance Use Information.

b. Disclosure of PHI to Military Command Authorities. Per reference (c), PHI may be disclosed for determination of a Service member's fitness for duty, including but not limited to, the member's compliance with standards and all other activities carried out under the authority of DOW Physical Fitness and Body Fat Program, DOW Physical Evaluation Board Programs, Nuclear Weapons Personnel Reliability Program (PRP), and other similar requirements.

(1) PHI that is disclosed to an appropriate command authority is on a need-to-know basis and only the minimum necessary information will be released to accomplish the purpose for which the request is made. These disclosures require an accounting of disclosure as outlined in subparagraph 11e.

(2) Appropriate military command authorities include commanders, commanding officers, and designated representatives who have oversight of the Service member. Designations should be received in writing and made available to the individual(s) responsible for disclosing PHI.

(3) Disclosures of mental health PHI to command authorities must be disclosed per section 3.1 of DoD Instruction 6490.08, which requires disclosures based on nine conditions or circumstances warranting command notification.

(4) Competent medical authorities and medical personnel assigned to support PRP may access and disclose PHI to PRP administrators and military command authorities per references (c) and (m). DON policy requires authorizations for PRP civilians, contractors, and Service members to acknowledge their understanding of routine disclosures outlined on the OPNAV 5510/419 Nuclear Weapons Personnel Reliability Program.

(5) When in doubt, contact the local privacy officer or consult with the legal staff for clarification on any disclosure or release of information requests.

c. Disclosures to Law Enforcement. DOW investigative agency personnel (e.g., Naval Criminal Investigative Service) are granted access to records containing PII or PHI when proper identification is provided, and the request conforms with the requirements of references (c) and (d). All law enforcement requests for records will be coordinated with BUMED-N01J, BUMED-N01L, or the local command legal office as appropriate. DOW agents will be requested to sign a dated statement, which contains the identity of the record to be examined, the identity (file number) of the investigation for which the record is being examined, and a certification by the examiner that the examination is required as part of the official investigation. Obtain a signed receipt for any material or record copies furnished to the agent. Please Note: Do not file the statement, document receipt in a system of record, or account for the disclosure when releasing information to law enforcement. Maintain the statement in a separate correspondence file until the investigation is concluded or authorized by command legal office.

(1) Requests must be specific and limited in scope to the extent reasonably practicable considering the purpose for which the information is sought (i.e., application of minimum necessary standard).

(2) Command representatives may not disclose an entire system of record pertaining to an individual, except when the entire record is specifically justified as the amount that is necessary to accomplish the purpose of the disclosure.

(3) DOW investigative agencies have the authority to request a delay in disclosure reporting. The individual right to receive an accounting of disclosures to law enforcement may be temporarily suspended if the agency or official indicates that such an accounting would impede the agency's activities.

(4) The request may be verbal; however, suspension for accounting must not exceed 30 days unless a written request is submitted.

d. Disclosures Requiring Authorization. Except as otherwise permitted or required by reference (d), a covered entity may not use or disclose PHI without authorization. Third party authorization forms can be used if they meet the criteria and include the required statements as outlined in reference (d), to include the name or organization authorized to make the disclosure, the name or organization to whom the command is making the disclosure (the third party), the purpose of the disclosure, an expiration date or an expiration event, the signature of the individual, and signature date. If a personal representative of the individual signs the authorization, a description of such representative authority to act for the individual must also be provided. Otherwise, authorizations are invalid per reference (d).

e. Accounting of Disclosures. Accounting of disclosures subject to the HIPAA Privacy Rule must be made utilizing MHS GENESIS, MHS Protected Health Information Management Tool (PHIMT) system and any designated successor system identified by DHA PCLO or the DON for Privacy Act accounting of disclosures. Alternative methods for accounting of disclosure subject to HIPAA Privacy Rule must be approved by DHA PCLO. Workforce members performing release of information function may request access to PHIMT through the MHS identity Authentication Services Web site managed by the DHA. Contact the local privacy officer for assistance in obtaining access. When a beneficiary or workforce member requests an accounting of disclosures, the command will provide a report of the disclosures made during the period requested by the requestor, for up to 6 years preceding the request. Request for accounting of disclosures do not include request for copies of audits performed on electronic systems containing the records. System cybersecurity audit records are exempt from disclosure.

f. De-Identified Information. There are 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. To comply with the Privacy Rule, Navy Medicine workforce members may choose either the safe harbor or expert determination model to comply, which is stipulated in reference (c). De-identifying PHI eliminates the ability to identify the individual(s) when the information is presented. This can be accomplished by removing all or some of the individual's demographic information, such as SSN, address, birthdate, or other identifiable information. References (c), (d), and (n), provide a complete listing of identifiers.

12. Workforce Training. This policy establishes requirements for initial and annual privacy training per references (c) and (e) and applies to all workforce members. The Waypoints Learning Management System is the primary method for delivering initial and core HIPAA Privacy, Security, Breach Notification and Privacy Act of 1974 as amended training to Navy Medicine civilian employees. Civilian employees will complete course number 18-BUMED HIPAA and Privacy Act Training, via Waypoints, when required. Active duty and contract personnel will complete their training via the Joint Knowledge Online (JKO) Learning Management System until such a time as the Waypoints Learning Management System has been implemented for use by active duty and contract personnel. Commands must ensure new

employees complete the initial training during orientation for personnel working with Privacy Act covered records or prior to granting access to IS containing PII or PHI. Refresher training must be completed per the annual BUMED Fiscal Year Training Plan. Specialized training must be completed as necessary depending on workforce assignment and responsibilities to include but not limited to personnel performing the following: managing Privacy Act systems; performing release of information functions; contracting officers, personnel performing disposition of equipment containing PII, legal officers, and personnel who are government sponsors for data sharing and data custodian responsibilities.

13. Complaints. Commands must establish a standard procedure to receive and investigate privacy related complaints and allegations of non-compliance. Privacy complaints should be forwarded to the command appointed privacy officer, legal officer, or local compliance official for resolution. A written response should be executed within 10 days for Privacy Act related complaints and within 30 days receipt for those subject to HIPAA Privacy and Security Rules. All BUMED HQ privacy complaints will be executed through BUMED-N61. Employees or beneficiaries who need to file a complaint about privacy practices may submit their complaint to the local privacy officer, the Navy Medicine region privacy officer, DNS-36, or DHA PCLO. Complaints should state which command or business associate is believed to have violated the Privacy Act or HIPAA Rules; should include as much detail as possible surrounding the violation (e.g., what happened, when it occurred, identify the potential violator(s), etc.); is filed within 180 days after the complainant was made aware of the violation; and is in written form. When appropriate, commands should initiate formal investigations to address serious violations of privacy practice, regulations, and statutes.

a. Complaints filed to the DON or HHS Office of Civil Rights may result in civil and criminal penalties. Workforce members or beneficiaries wishing to file a complaint with HHS may do so utilizing the Office of Civil Rights complaint portal at https://ocrportal.hhs.gov or in writing to U.S. Department of Health and Human Services, 200 Independence Avenue Southwest, Room 509F, HHH Building, Washington, District of Colombia 20201.

b. Complaints filed with DHA PCLO should be forwarded to DHA Privacy and Civil Liberties Office, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22041-5101.

c. Complaints filed with BUMED should be forwarded to BUMED Detachment Jacksonville, Attention: Privacy Office Code N61, H2005 Knight Lane, P.O. Box 140, Naval Air Station Jacksonville, Florida 32212-0140.

14. Sanctions. Commands must apply appropriate sanctions against members of their workforce who fail to comply with DOW, DON, or DHA policies and procedures as applicable. Violations of DOW privacy and security regulations may result in severe penalties. All workforce members can face misdemeanor criminal charges and fines for knowingly and willfully disclosing protected PII to any person not entitled. Penalties are always dependent upon the facts and the situation related to the mishandling, failure to protect, compromise, or suspected compromise of an individual's PII or PHI.

a. All application of sanctions must comply with Uniform Code of Military Justice for Service members, Federal acquisition regulations for contractors, and SECNAVINST 12752.1A for civilian employees.

b. For contractor personnel subject to this policy, sanctions may include actions permissible under applicable procurement regulations and BAAs or other agreements when required by contract, including complete or partial termination; liquidated damages to which the Government is entitled under the contract; administrative costs; or removal of contract employee responsible for the damage.

c. At a minimum, Navy Medicine workforce members who mishandled, failed to protect, or compromised PII should be counseled and directed to complete remedial privacy and security training for violations using the JKO remedial training module or other designated training system reflected in the command annual training plan (e.g. Waypoint).

15. Contacts. Contact BUMED-N61 via e-mail at usn.ncr.bumedfchva.list.bumed-privacy@health.mil or commercial (904) 542-3559 to report a privacy complaint or to seek guidance.

16. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules found on Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager or the Office of the Chief of Naval Operations (OPNAV) Records Management Program (DNS-16).

17. Review and Effective Date. Per OPNAVINST 5215.17A, BUMED-N6 will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DOW, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

18. Forms and Information Management Control

a. Forms. The forms listed in subparagraphs 18a(1) through 18a(6) are available at https://forms.documentservices.dla.mil/order/ and http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.html.

(1) DD Form 2870 Authorization for Disclosure of Medical or Dental Information

(2) DD Form 2871 Request to Restrict Medical or Dental Information

(3) DD Form 3130 Consent for the Disclosure of Confidential Substance Use Information

(4) DD Form 2930 Privacy Impact Assessment (PIA)

(5) DD Form 2959 Breach of Personally Identifiable Information (PII) Report

(6) OPNAV 5510/419 Form Nuclear Weapons Personnel Reliability Program

b. Information Management Control. Reports required of this notice are exempt from reports control per SECNAV Manual 5214.1 of December 2005, part IV, subparagraph 7k.

R. FREEDMAN
Acting

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Navy Medicine Web site, https://www.med.navy.mil/Directives/