



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

IN REPLY REFER TO
BUMEDINST 5211.4
BUMED-M3B1
JUL 24 2015

BUMED INSTRUCTION 5211.4

From: Chief, Bureau of Medicine and Surgery

Subj: BUREAU OF MEDICINE AND SURGERY HEADQUARTERS PRIVACY PROGRAM

Ref: (a) DoD Instruction 6025.18 of 2 December 2009
(b) DoD 8580.02-R of 12 July 2007
(c) DoD 5400.11-R of 14 May 2007
(d) DoD Instruction 5400.16 of 12 February 2009
(e) DoD Manual 5200.01, Vol.4 of 24 February 2012
(f) Public Law 104-191
(g) Public Law 111-5
(h) 5 United States Code § 552a
(i) SECNAVINST 5211.5E
(j) SECNAVINST M-5210.1
(k) JAGMAN Chapter 5
(l) DoD Instruction 8500.01 of 14 March 2014
(m) DoD Instruction 8510.01 of 12 March 2014
(n) DoD Instruction 6490.08 of 17 August 2011
(o) BUMEDINST 5239 Ser M09B6/09UMOB6121 6 Jul 09
(p) BUMED Policy 08-005 of 28 Jan 08
(q) 5 U.S.C, Chapter 75

1. Purpose. This instruction establishes responsibilities and procedures per privacy and security directives and requirements outlined in references (a) through (q), and any successor references, as applicable, and establishes Health Insurance Portability and Accountability Act (HIPPA) privacy, security and Breach Notification Rules for the use, disclosure, and safeguarding of Personally Identifiable Information (PII), and Protected Health Information (PHI).

2. Scope. This instruction applies to all Bureau of Medicine and Surgery (BUMED) Headquarters (HQ) staff and detachment personnel to include: military personnel, federal civilians, contractors, and other personnel assigned temporary or permanent duty to BUMED HQ and Detachments.

3. Responsibilities

a. Deputy Director, Healthcare Delivery (BUMED-M3) shall:

(1) Execute oversight of BUMED HIPAA Privacy functions to ensure compliance with this instruction.

(2) Delegate authority to the BUMED Privacy Program Office (BUMED-M3B16) to develop, implement and update supporting guidance and initiatives as needed for HIPAA Privacy and Security.

(3) Oversee coordination between BUMED-M3B16, Cybersecurity (HIPAA Security Officer) (BUMED-M62) and BUMED Legal (Privacy Act Coordinator).

b. Program Manager, BUMED HIPAA Privacy Office. BUMED-M3B16 executes privacy program management functions and has the responsibility and authority for the implementation, maintenance, development and reporting of privacy reporting requirements for privacy compliance. BUMED-M3B16 shall:

(1) Serve as the HIPAA Privacy Officer and coordinate across BUMED Directorates, BUMED Special Advisors, and other staff assigned privacy and security responsibilities to ensure requirements are appropriately addressed and safeguards are consistent across BUMED HQ, detachments, and mission specific commands.

(2) Establish mechanisms within the organization for receiving, documenting, tracking, investigating and taking action on all complaints concerning the organization's privacy policies and procedures.

(3) Ensure BUMED HQ's policies and procedures comply with Department of Defense (DoD) and Department of Navy (DON) privacy regulations. Perform compliance activities to include reporting requirements, performing risk assessments, mitigating risks, and implementing best business practices.

(4) Coordinate with BUMED Training Officer to ensure staff members receive initial orientation, refresher and ad-hoc training as needed on best practices, privacy and security policies and procedures per regulations.

(5) Serve as a point of contact for the Defense Health Agency (DHA) Privacy and Civil Liberties Office for compliance concerns, issues and policy implementation.

(6) Serve as an Alternate Data Sharing Agreement Representative to help ensure requests for Tri-Service data are reviewed for type and amount of data, and the proposed analysis are appropriate.

JUL 24 2015

c. HIPAA Security Officer. The Deputy Director, Information Manager/Technology, (BUMED-M6) serves as the Service HQ's HIPAA Security Officer and is responsible for performing functions to implement and maintain compliance with the HIPAA Security rule and DoD/DON cybersecurity directives that govern the protection of controlled unclassified information, including PII/PHI. BUMED M6 shall:

(1) Ensure security policies and procedures comply with the HIPAA Security Rule and related DoD/DON regulations.

(2) Facilitate and perform map and gap analysis of organizational policies and practices to meet compliance objectives with the HIPAA Security Rule and DoD/DON regulations.

(3) Ensure periodic organizational risk assessments are conducted, and related ongoing compliance activities are coordinated with applicable service directives and DHA. Serve as a point of contact for Service compliance concerns, issues and policy implementation. Compliance activities may include reporting requirements, conducting annual risk assessments, auditing, mitigating risks, and implementing best business practices as it relates to electronic PHI.

(4) Initiate, facilitate and promote activities to foster information security awareness within the organization.

(5) Serve as the primary Data Sharing Agreement Representative to review, approve or disapprove requests for sensitive service or Tri-Service data.

4. Policy. BUMED shall employ privacy and security management practices and procedures that evaluate risk, mitigate non-compliance, and ensure Systems of Record containing PHI, and PII are not lost, stolen or inappropriately disclosed to the public or those without a need to know. It is the policy of BUMED to:

a. Ensure all personnel comply fully with references (a) through (q) to ensure protection of individuals from unwarranted invasions of privacy and to minimize unauthorized disclosures.

b. Collect, maintain and use only personal information needed to support a Navy function or program as authorized by law or Executive Order and disclose this information only as authorized by references (a) through (i).

c. Ensure the confidentiality, integrity and availability of all PHI the organization creates, receives, maintains or transmits against anticipated threats or hazards.

d. Ensure adequate administrative, technical and physical safeguards are in place to prevent misuse, unauthorized disclosure, alteration or destruction of PHI/PII.

e. Ensure all personnel complete HIPAA and Privacy Act orientation and refresher training utilizing approved Military Health System training tools (i.e., Joint Knowledge Online, Navy Knowledge Online, etc.), and properly document in Defense Medical Human Resource internet.

5. Breaches. Reference (c) defines a breach as any lost, stolen or compromised information. It is the actual or possible loss of control, unauthorized disclosure or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected. Breaches should be reported to higher authority utilizing OPNAV 5211/13, DON Loss or Compromise of PII Breach Reporting Form per references (c) and (i). The following guidelines should be followed to ensure appropriate reporting in accordance with DHA policies:

a. Notify Cybersecurity Support, local Privacy Officer (BUMED-M3B16) and supervisor of any breach or possible breach of PII/PHI (immediately, upon discovery).

b. The Privacy Officer or other designated official will notify United States Computer Emergency Readiness Team (US-CERT) of breach (paper or electronic) within 1 hour using the following Web site: <https://forms.us-cert.gov/report/>. Once the report is submitted, the US-CERT will provide a response with an incident number attached to it, which should be used as reference on all future correspondence concerning the reported incident.

c. After receiving US-CERT response, submit the initial report using OPNAV 5211/13 to the DON Chief Information Office (CIO) Privacy Office, BUMED, your chain of command, and the DHA Privacy and Civil Liberties Office (Notification should occur within 24 hours of event or awareness). Follow-up communication to DON CIO Privacy Office will occur as needed utilizing OPNAV 5211/14, DON Loss or Compromise of PII After Action Reporting Form. See reference (j) for e-mail contact information.

d. The DON CIO Privacy Office and/or DHA Privacy and Civil Liberties Office, will provide guidance on notification to affected individuals. Notification typically must occur within 10 working days after the loss, theft or compromise is discovered and the identities of the individuals determined.

e. If a crime is suspected, notify the local Naval Criminal Investigative Service Office to conduct an investigation. Consultation with Regional staff judge advocate or BUMED Legal is highly advised.

f. If appropriate, BUMED will issue Operations Report 3 Situation Report, per reporting procedures.

g. Notify issuing banks if government issued credit cards are involved.

h. If PHI is involved, refer to the DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 2003 and reference (b) for mitigation requirements.

6. Information Management Systems. BUMED employees may have access to several systems that allow drill down capability to specific PII data. Staff having access to these various systems, and other data repositories, must adhere to guidelines from higher authority for handling individually identifiable data per training provided during the granting of access privileges. Computer systems shall be locked when left unattended, and reports generated from them shall be secured appropriately in secure file folders, restricted share drive and SharePoint folders, cabinets or safes (electronic or mechanical) as outlined in references (a) through (l).

7. Use and Disclosures. In general, personally identifiable health information of individuals, both living and deceased shall not be used or disclosed except for specifically permitted purposes. BUMED workforce members are permitted to use and disclose PHI for treatment, payment or healthcare operations activities. Healthcare operations are generally permitted, consistent with Chapter 4 of reference (a) without the need for authorization from the subject of the PHI/PII being used or disclosed. Accounting of disclosures shall be made per references (a) and (i). Accounting of disclosures shall be made utilizing the Military Health System's Protected Health Information Management Tool (PHIMT). Workforce members requiring access to PHIMT may contact the HIPAA Privacy Office for assistance. Privacy Act disclosures may be documented using the OPNAV 5211/9, Disclosure Accounting Form. All HIPAA accounting of disclosures are required to be maintained for a period of 6 years. Alternative forms for accounting of disclosure must be approved by Health Care Operations, BUMED-M3B1 for HIPAA or BUMED Legal for Privacy Act.

a. Disclosures. As required by references (a) and (d), the BUMED HIPAA Privacy Office ensures the dissemination of the Military Health System (MHS) Notice of Privacy Practices (NoPP) which is readily available to MHS beneficiaries and prominently displayed on all Navy Medicine Web sites. The following disclosures are those most likely to occur at BUMED, Mission Specific Commands and Detachments:

- (1) Uses or disclosures required by law.
- (2) Disclosure of PHI to military command authorities per reference (a).
- (3) Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required for enforcement purposes.
- (4) Disclosure to government oversight agencies for purposes of quality assurance, research, public health reporting, and occupational safety and health requirements.

b. Exceptions to accounting. BUMED activities must account for all disclosures made, except for the following:

(1) To carry out treatment, payment, or health care operations (pursuant to changes forthcoming from HHS).

(2) Pursuant to a valid authorization.

(3) To the beneficiary.

(4) To Federal officials for national security or intelligence purposes.

(5) For facility directories or to persons involved in the beneficiaries care or other notification purposes.

(6) To correctional institutions or law enforcement officials that have custody of the individual.

(7) That are part of a limited data set.

(8) Incident to a use or disclosure otherwise permitted or required by the HIPAA Privacy Rule.

c. Minimum Necessary. All staff members shall make every reasonable effort to limit PHI/PII dissemination to only those in a need to know capacity and within their scope of responsibilities. The privacy rule generally requires covered entities to take reasonable steps to limit the use of disclosure and request for PHI/PII to the minimum necessary for intended purposes.

d. Need to Know. Only those personnel who have a need to know based on scope and responsibilities established in writing via appointment letter(s), position description(s), directive or instruction, credentialing approval, or by direction authority are permitted access to PHI/PII.

e. Disseminating Privacy Protected Data. The following practices should be adhered to:

(1) PHI/PII data shall be stored on encrypted government furnished equipment. All mobile devices (e.g., BlackBerrys, Ipads, laptops, storage devices, and DoD approved Universal Serial Bus mini drives) shall be secured properly and PHI/PII removed when not needed for official business. Approval to transport PHI/PII data must be granted by supervisors and documented. In the event a mobile device is lost, stolen, or compromised, the Privacy Officer and the HIPAA Security Officer will be notified immediately. Make sure all privacy information is properly marked (e.g., "For Official Use Only) per references (i) and (l) when disseminating. Correspondence mail containing PII/PHI should be mailed using certified mail and tracking options. If a commercial carrier is used, ensure tracking and confirmation delivery receipts are utilized.

(2) Electronic Transmission of PHI/PII. Per reference (p), when PHI or PII is to be transmitted by e-mail, BUMED personnel shall only use government furnished equipment and software, and encrypt the sensitive information with DoD approved encryption methods prior to transmission. This requires authorized, non-DoD recipients to use a DoD approved digital certificate to encrypt and decrypt sensitive e-mail. Such information must be protected while it is being processed or accessed. Alternative forms of e-mail (i.e., password protected emails utilizing WINZIP, ARMDEC SAFE and other DoD approved encryption methods) are sometimes utilized for operational purposes to meet mission requirements; however, these type of transmissions should be minimal and with appropriate risk analysis conducted.

(3) Although faxes are currently permitted, the DoN CIO has issued a directive restricting the use of faxes to transmit sensitive PII. As of the date of this instruction, Navy Medicine has been granted an exemption from the DoN CIO, but precaution should be exercised to ensure faxes are either encrypted, fax numbers verified, and other necessary safeguards are in place. The information transmitted must be limited to that necessary to meet the requestor's needs. Mark e-mail and other electronic messages with proper warnings and encrypt all e-mails containing PII/PHI. All electronic transmissions (i.e., e-mail, fax, etc.) containing PHI/PII shall contain a confidentiality statement:

"For Official Use Only" This document may contain information covered under the Privacy Act, 5 USC 552(a), and/or the Health Insurance Portability and Accountability Act (PL 104-191) and its various implementing regulations and must be protected in accordance with those provisions. If you have received this correspondence in error, please notify the sender at once and destroy any copies you received in error.

f. Military Exemptions. Per reference (a), PHI may be disclosed for determination of an active duty 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 DoD Physical Fitness and Body Fat Program, DoD Physical Evaluation Board Programs, Nuclear Weapons Personnel Reliability Program, and similar requirements. The PHI that is released to a command authority is on a need-to-know basis. The commanding officer or his/her designated representative requesting a member's PHI, must be in the individual's chain of command and only the minimum necessary information will be released in order to accomplish the purpose for which the request is made. When in doubt, contact the local Privacy Officer or consult with the Legal staff for clarification on any release of information issues. Disclosures of mental health PHI to Command Authorities should be disclosed per reference (n), which restricts disclosures based on nine conditions or circumstances warranting command notification. Commands are recommended to review guidance provided by the BUMED Psychological Health Advisory Board's Information paper and training materials. Additional purposes for which PHI may be disclosed under the Military Exemption Clause are provided in reference (a).

g. Public Need. Information may be disclosed for public need without authorization for purposes including public health activities, research, and fraud investigations. Additionally,

JUL 24 2015

information can be released that may prevent or lessen a serious/imminent threat to the health/safety of a person/public presuming it is done in good faith. Contact the Public Affairs Officer and Staff Judge Advocate prior to the release of any information to media sources. Release of information to law enforcement officials shall be coordinated through Legal.

h. De-Identified Information. Generally, most reports generated at BUMED shall contain non-individually identifiable information. Reports that contain patient specific information shall be de-identified if transmitted to a third party and the transaction is not under the scope of healthcare operations. 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 social security number, address, phone number, or other identifiable information. References (a) and (e) provide a complete listing of identifiers.

i. Disposal of PHI/PII. PHI/PII contained in reports and adhoc are to be shredded or archived per local and higher authority directives. Supervisors are responsible for ensuring procedures are in place to ensure proper disposal of PHI/PII when determined it is no longer needed. At no time should PII/PHI information be disposed of in trash receptacles without prior shredding or filed in unlocked cabinets/file drawers and unsecured spaces.

j. Verification of Identity. An individual shall provide reasonable verification of identity before obtaining access to records. Disclosures shall be made when an individual seeks access in person or via written correspondence and identification can be verified.

8. Mitigation of Unauthorized Release of PHI/PII. If a staff member inadvertently or deliberately releases PHI/PII to an unauthorized recipient, the Command will attempt to mitigate the disclosure. In most cases, the mitigation will involve limited future unauthorized disclosures and advising individual(s) whose information may have been compromised. The HIPAA Privacy Officer shall direct, monitor, and document any necessary mitigating actions. These actions may include appropriate information system responses, public notices, investigations, and required reporting to appropriate authorities, media responses, and web content removal.

9. Complaints. Employees or beneficiaries who need to file a complaint about privacy practices may submit their complaint to the HIPAA Privacy Officer who is responsible for receiving and the disposition of the complaints per reference (a). Complaints filed with the HHS Office for Civil Rights may include civil and criminal penalties and are mitigated through BUMED Legal M09B9.

10. Sanctions. This instruction establishes policy and assigns responsibility for how sanctions should be determined and applied against workforce members of Navy Medicine who fail to follow appropriate standards for PII/PHI protection in accordance with applicable DoD and DON directives and guidelines.

JUL 24 2015

a. Sanction Scope. Military and civilian full-time and part-time employees, volunteers, trainees, students, and other persons whose conduct, in the performance of work for BUMED, is under the direct control of BUMED, whether or not they are paid by BUMED.

b. Policy. The Privacy Officer shall coordinate with the Human Resources and BUMED Legal to ensure HQ uses standard disciplinary process, when appropriate, to determine specific sanctions according to the severity and circumstances of violations. The type and severity of sanctions imposed, and the categories of "violation", are at the discretion of the commander or commanding officer for subordinate activities; however, BUMED will utilize a multifactor model to aid in the application of sanctions for standardization.

c. Model. The BUMED sanction model consists of four major risk areas to include organizational exposure, number of workforce/beneficiaries involved, purpose of action causing risk, and applicability of special protections PHI/PII (e.g., HIV results, psychiatric information, genetic data, or substance abuse records). The multifactor sanctioning model identifies three categories of severity across four areas of risk. BUMED shall take corrective action and base remediation on the highest level of category indicated. If a breach falls into one or more risk areas, the corrective action will be based on the highest category level of risk.

Category	Exposure Range	Number of Records Compromised	Purpose of Action	Special Protection Categories
1	Low external exposure to organization	Involves a single record of PHI/PII	Incidental negligence or lack of education and training	No additional state or federal protections
2	Medium external exposure to organization	Involves 2–99 workforce members or beneficiaries	Snooping, incidental, curiosity, and or technical misuse	Employees, Beneficiaries, Business Associates
3	High external exposure to organization	Involves 100+ patients	Malice, Repeat offender deliberate, sale, or personal gain	HIV, mental health, etc.

d. Penalties. BUMED must apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of references (a) through (q). Violations of DoD Privacy and Security Regulations may result in severe penalties. All members can face misdemeanor criminal charges and fines for knowingly and willfully disclosing protected data to any person not entitled. For members of the military, these penalties may include action under the Uniform Code of Military Justice, administrative, or other appropriate sanctions. For civilian employees, sanctions should be applied consistent with the provisions of Chapter 75 of Title 5, United States Code. For contractor personnel subject to this policy, sanctions may include actions permissible under applicable procurement regulations and Business Associate Agreements (BAA) and/or other agreements when required by contract, including termination. Non-compliance with training requirements (e.g., Information Assurance,

JUL 24 2015

HIPAA, Privacy Act, and PII Awareness) may result in suspension of computer access, or restriction from accessing Systems of Record or other appropriate measures as determined by command leadership. The command's Training Officer is responsible for reporting training deficiencies to leadership for appropriate action at least quarterly.

e. Responsibilities. Human Resources Office will document the sanctions and maintain written or electronic records on military and civilian employees only. Such documentation must be retained for 6 years per the provisions of reference (a) and appropriate DON regulations. The Privacy Officer will further assign tasks to mitigate, to the extent practicable, any harmful effect that is known as a result of a violation.

f. Mitigating and Aggravating Factors. The following factors may be utilized to help determine final application of sanctions:

- (1) Beneficiaries/workforce member(s) suffered no harm.
- (2) Offender voluntarily reported offense, cooperated with investigators, and took appropriate mitigation steps.
- (3) Employee was inadequately trained.
- (4) Multiple offenses.
- (5) Significant harm to victims assessed.
- (6) High volume of people or data affected.
- (7) Large organizational expenses occurred in mitigation efforts.
- (8) Loss of public trust.
- (9) Breach of specially protected information (e.g., HIV status, psychiatric diagnosis, substance abuse data, and genetic information).

g. When applying sanctions other than remedial training please consult with your Legal staff and Human Resource Officials for guidance.

11. Individual Rights. References (a) and (f) provide individual rights under the Privacy Rule, and it is the responsibility of the command to have policies and procedures that facilitate the following rights:

- a. Right to inspect and copy PHI in a designated record set.
- b. Right to request amendment to PHI in a designated record set.

JUL 24 2015

- c. Right to receive a notice of privacy practices that includes how health information may be used and shared.
- d. Right to request restrictions of PHI that is used or disclosed for certain purposes.
- e. Right to receive confidential communications by alternative means or at alternative locations.
- f. Right to request an accounting of certain disclosures of PHI.
- g. Right to file a HIPAA complaint directly with the local HIPAA Privacy Officer, BUMED Privacy Office, with DHA Privacy and Civil Liberties Office, and/or with HHS Office for Civil Rights.

12. Data Sharing Agreements. BUMED Directorates and Detachments are required to control the disclosure and/or use of PHI/PII that are owned and/or managed by the DON and the MHS to ensure compliance with applicable Privacy Act and HIPAA privacy and security requirements. In order to ensure compliance, BUMED Program Offices should initiate appropriate Data Sharing Agreements when requests for use, or disclosure of, PHI/PII in Navy or MHS owned data occur. All Data Sharing Agreement types shall be forwarded to Information Management and Technology (BUMED-M62) for review, approval, and/or additional routing to the DHA. Contractors who provide services to the DON and receive and/or create PHI in performance of the service must have a BAA incorporated into their contract as required by reference (a) where it's appropriate.

13. HIPAA Privacy and Security Risk Management. Per references (a) and (b), BUMED-M62 Cybersecurity performs routine risk assessments throughout the life cycle of information systems, and following significant changes to the organizational privacy or security posture. The HIPAA Privacy and Security Officers will submit risk analysis inputs and requirements to Financial Management BUMED-M8. Current Management Internal Control Auditable Units are utilized to facilitate oversight and mitigation of risks within HQ, and shall be reviewed at least annually for updates.

14. Contacts. Contact BUMED M3B16 Privacy Program Office via e-mail at (BUMEDPPI@mail.mil) or Commercial (904) 542-7200, ext. 8139 to report a privacy complaint or to seek guidance. If you wish to file a privacy complaint, you may also contact the following Privacy Offices: DHA Privacy and Civil Liberties Office at Commercial (703) 681-7500, or U.S. Office of Civil Rights.

15. Records. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

16. Report. The reporting requirements contained in this instruction are exempt from reports control per SECNAV M-5314.1 of Dec 2005, Part IV, paragraph 7k.

17. Forms

- a. The following OPNAV forms are available at:
<https://navalforms.documentservices.dla.mil/>:
- b. OPNAV 5211/9 (03-1992), Disclosure Accounting Form 4
- c. OPNAV 5211/13 (Rev. 03/2015), DON Loss or Compromise of Personally Identifiable Information (PII) Breach Reporting Form
- d. OPNAV 5211/14 (Rev. 03/2015), DON Loss or Compromise of Personally Identifiable Information (PII) Breach Reporting Form



P. B. COE
Executive Director
Acting

Distribution is electronic only via the Navy Medicine Web site at:
<http://www.med.navy.mil/directives/Pages/BUMEDHQInstructions.aspx>