



## DEPARTMENT OF THE NAVY

NAVY MEDICINE EAST  
620 JOHN PAUL JONES CIRCLE  
PORTSMOUTH, VIRGINIA 23708-2106

NAVMEDEASTINST 6025.1  
M3C4  
8 Jun 07

### NAVMEDEAST INSTRUCTION 6025.1

From: Commander, Navy Medicine East

Subj: PRIVACY AND SECURITY STANDARD OPERATING PROCEDURES

Ref: (a) DoD Directive 6025.18R (DoD Privacy Regulation)  
(b) MHS Information Assurance Policy Guidance, Mar 04  
(c) SECNAVINST 5212.5D  
(d) Public Law 104-191  
(e) Manual of the Medical Department, Chapter 16  
(f) NAVCOMPTMAN, Volume 3, Articles 035875 and 035887  
(g) DoD Directive 6490.2 (Joint Medical Surveillance)  
(h) DoD Directive 8500.1  
(i) DoD Instruction 8500.2

Encl: (1) Definitions

1. Purpose. To ensure protected health information (PHI) is maintained in accordance with federal law and higher authority guidance and that references (a) through (f) are adhered to.

2. Applicability. This instruction applies to all Navy Medicine East (NME) personnel having access to M2 (MHS Data Repository), Composite Health Care System (CHCS), Coding Compliance Editor (CCE) or other systems which provide access to PHI. All staff members who have access to or are responsible for the management of health information (electronic, paper, or oral medium) shall implement and perform necessary precautions to minimize access to or unauthorized disclosure of PHI.

3. Scope. This instruction pertains to access, use, and disclosure of PHI. NME is an Echelon 3 staff command and as such has limited vulnerability to unauthorized disclosure to outside sources, however, access to various information systems containing sensitive information present some security and unauthorized disclosure risks.

4. Responsibility. The Command's designated Health Portability & Accountability Action (HIPAA)/Privacy Officer shall be

NAVMEDEASTINST 6025.1  
M3C4  
8 Jun 07

responsible for the management, development, and implementation of both privacy and security policies, standards, and procedures to ensure ongoing compliance. Each staff member shall make concerted efforts to minimize potential vulnerability.

a. The HIPAA/Privacy Officer shall:

(1) Ensure access to patient level medical information is restricted to persons with need-to-know.

(2) Ensure procedures are in place to properly dispose of PHI.

(3) Mitigate high risk areas through audit assessments and corrective action plans.

(4) Monitor initial staff orientation and annual privacy/security training.

(5) Monitor current and new instructions for HIPAA applicability and compliance.

(6) Monitor and review all new Memorandum of Understanding's (MOUs) as well as renewal of existing MOUs for HIPAA compliance.

b. NME Information Technology Administrator shall:

(1) Ensure detaching personnel are removed from access to legacy systems.

(3) Conduct audit assessments in conjunction with Naval Medical Center Portsmouth Management Information Department (MID) personnel to determine security risks.

(4) Assist Privacy Officer with conducting audits of share drive network if PHI is unprotected.

(6) Ensure computer systems are scrubbed of all PHI prior to Defense Reutilization Management Organization (DRMO) or disposal in accordance with DoD and Navy Information Assurance protocols.

(7) Ensure systems are audited in accordance with references (h) and (i).

5. Information Management Systems. NME staff members have access to several systems which allow drill down capability to patient specific healthcare data. The following systems have been identified as potential risks for unauthorized disclosure and use: M2, Armed Forces Health Longitudinal Technology Application (AHLTA), CHCS, CCE, and TRICARE network applications. Staff having access to these various systems and other data repositories must adhere to guidelines for handling individually identifiable data in accordance with training provided during the granting of access privileges process and higher authority. Computer systems shall be locked when left unattended for extended periods of time and reports generated from them shall be secured appropriately in secure file folders (electronic or mechanical).

6. Standards of Conduct

a. Patient Privacy. In general, personally identifiable health information of individuals, both living and deceased, shall not be used or disclosed except for specifically permitted purposes. Healthcare operations activities are generally permitted, consistent with Chapter 4 of reference (a) without the need for authorization from the subject of the PHI being used or disclosed.

b. Minimum Necessary. All staff members shall make every reasonable effort to limit PHI dissemination to only those in a need to know capacity and within their scope of responsibilities. The privacy rule generally requires covered entities (i.e., Military Treatment Facilities (MTFs), dental treatment facilities, TRICARE) to take reasonable steps to limit the use or disclosure of and request for PHI to the minimum necessary for intended purposes. NME's mission does not routinely require disclosing PHI to outside sources, however, NME routinely communicates with MTF staff about data discrepancies or program issues. Sometimes this communications requires drill down to specific patient identifiable data or the

NAVMEDEASTINST 6025.1  
M3C4  
8 Jun 07

transmittal of PHI data via electronic means (e.g. facsimile (fax), email).

c. Disclosures. The following valid disclosures are those most likely to occur at NME:

- (1) Uses or disclosures that are required by law.
- (2) Disclosure of PHI to military command authorities in accordance with reference (a)
- (3) Disclosures to the Department of Health and Human Services when disclosure of information is required for enforcement 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, credentialing approval, or by direction authority are permitted access to PHI.

e. Military Exemptions. Commands may disclose PHI for determination of a 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 (PRP), and similar requirements. The PHI that is released to a command authority is on a "need to know" basis. The Chief of Staff (COS) 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 should be released in order to accomplish the purpose for which the request is made. When in doubt, contact the Privacy/HIPAA Officer or Staff Judge Advocate for clarification on any release of information issues. Additional purposes for which PHI may be disclosed under the Military Exemption Clause include:

- (1) To determine the member's fitness to perform any particular mission, assignment, order, or duty, including compliance with any actions required as a precondition to performance of such mission, assignment, order, or duty.

(2) To carry out activities under the authority of reference (g).

(3) To report on casualties in any military operation or activity in accordance with applicable military regulations or procedures.

(4) To carry out any other activity necessary to the proper execution of the mission of the Armed Forces.

f. Public Need. Information may be disclosed for public need without the patient's authorization for purposes including public health activities, research, and fraud investigations. Additionally, 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 Assistant Chief of Staff (ACOS) prior to the release of any information to media sources. The ACOS or designee shall coordinate communication efforts in release of PHI to public health or law enforcement agencies when it is determined there is the possibility of an imminent threat to the safety of an individual or the public.

h. De-Identified Information. Generally, most reports generated at NME 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 patient with the information presented. This can be accomplished by removing all or some of the patient's demographic information, such as social security number, address, phone number, or other identifiable information. Reference (a) provides a complete listing of identifiers.

i. Media Disclosures. Although inquiries from the media to NME may be minimal, all inquiries are to be referred to the ACOS and through the chain of command. The ACOS shall provide direction on the extent to which information shall be disclosed. At no time shall a staff member relay information to the media without expressed approval.

8 Jun 07

j. Disposal of Patient Information. PHI contained in reports and adhocs are to be shredded or archived in accordance with higher authority directives [see reference (d)]. Department Heads are responsible for ensuring that procedures are in place to ensure proper disposal of PHI when determined it is no longer needed. Patient information should not be disposed of in trash receptacles without prior shredding or filed in unlocked cabinets/file drawers and unsecured spaces.

## 7. PHI Transmission

a. Transporting PHI. PHI data will be stored on encrypted government furnished equipment. All mobile devices (e.g. BlackBerrys, laptops, CD-ROMs, and mobile USB mini drives) should be secured properly and PHI removed when not needed for official business. Approval to transport PHI/Privacy Act data must be granted by supervisors. In the event a mobile device is lost, stolen, or compromised, the Privacy Officer and the Command Security Officer will be notified immediately. Mobile USB mini drives will be checked out from the Information Technology Administrator.

b. Mailing PHI. If mailing of PHI is required, it shall be forwarded via "Return Receipt" mail only and stamped with a confidentiality statement in accordance with references (a) and (e). PHI shall not be forwarded utilizing guardmail or unsecured mail.

c. Electronic Transmission of PHI. Health information must be protected while it is being processed or accessed. To decrease the chance for breach of patient confidentiality, PHI shall be transmitted by facsimile or email only when the original record or mail-delivered copies will not meet the needs of the command or supported MTF operations. Sensitive information may be transmitted via facsimile or email unless an authorization is required prior to transmission. The information transmitted must be limited to that necessary to meet the requestor's needs. The following guidelines apply:

(1) All electronic transmissions (i.e. email, fax, etc.) containing PHI, shall contain the following confidentiality statement:

*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. Healthcare information is personal and sensitive and must be treated accordingly. If this correspondence contains healthcare information it is being provided to you after appropriate authorization from the patient or under circumstances that don't require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Redisclosure without additional patient consent or as permitted by law is prohibited. Unauthorized redisclosure or failure to maintain confidentiality subjects you to application of appropriate sanction. If you have received this correspondence in error, please notify the sender at once and destroy any copies you have made.*

(2) Fax machines used for the transmission of PHI shall be located in secure areas and monitored for immediate removal of incoming and outgoing documents. Verify receipt and legibility of all incoming facsimiles.

(3) If a misdirected facsimile or email is received, notify the sender immediately for further instructions or for proper disposal of information.

(4) Emails containing PHI shall be forwarded utilizing either password protection, encryption, or use of Common Access Card (CAC) system when possible.

f. Record of Disclosure. The HIPAA/Privacy Officer shall ensure all accounting of disclosures are tracked utilizing PHI tool.

g. Disposal of PHI. Disposal of PHI shall be in accordance with reference (a), section 16-20 and reference (d).

h. Readiness Reports Access. Access to readiness reports shall only be given to those with a need to know, (i.e. COS, ACOS, Deputy COS, and Department Heads).

NAVMEDEASTINST 6025.1

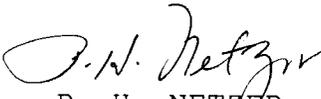
M3C4

8 Jun 07

8. Mitigation of Unauthorized Release of PHI. If a staff member inadvertently or deliberately releases PHI to an unauthorized recipient, the Command will attempt to mitigate the disclosure. In most cases, the mitigation will involve limiting future unauthorized disclosures and advising individuals whose information may have been compromised. The HIPAA Privacy Officer shall direct, monitor, and document any necessary mitigating actions.

9. Sanctions for Non-Compliance. All staff members who have contact with PHI in any official capacity are required to comply with the provisions of this instruction and reference (a). Deliberate or repeated violations may lead to Uniform Code of Military Justice disciplinary action and/or administrative action against military service members; adverse personnel actions against civil service staff; contract termination for contractors; or denial of continued services for volunteers. Non-compliance with training requirements may result in suspension of computer access to systems containing PHI or other appropriate measures as determined by command leadership.

10. Action. The Command HIPAA/Privacy Officer shall monitor this instruction for compliance and effectiveness.

  
P. H. NETZER  
Chief of Staff

Distribution: (See NAVMEDEASTINST 5215.1A)  
List C

DEFINITIONS

Protected Health Information (PHI): Individually identifiable health information including demographics in electronic paper or oral medium held by this Command, other Command, civilian facility, insurance company, law offices or courts.

De-Identified Information: Process by which all identifiers to Protected Health Information (PHI) with a particular patient is removed. An example would be disclosing a limited data set of city, state and zip code of the patient; all other demographic information to identify the patient shall be removed.

Treatment, Payment and Healthcare Operations (TPO):

(1) Treatment - Provision, coordination, consultation and referral.

(2) Payment - Billing, reimbursement, eligibility and utilization review.

(3) Healthcare Operations - Quality assurance, credentialing, legal, medical or dental review, auditing and regular business management.

Enclosure (1)