

DEPARTMENT OF THE ARMY  
U.S. Army Medical Department Activity  
Fort Drum, New York 13602-5004

FD MEDDAC Reg 40-45

4 October 2007

Medical Services  
PROTECTED HEALTH INFORMATION AND PRIVACY

1. **HISTORY:** This is the second printing of this publication. All previous editions are obsolete.
2. **PURPOSE:** This policy is designed to give guidance and ensure compliance with all relevant laws and regulations when using or disclosing Protected Health Information (PHI).
3. **APPLICABILITY:** This document applies to all personnel (active duty, Reservists, civilian and contract personnel, American Red Cross volunteers, students and interns) who work in the U. S. Army Medical Department Activity (USA MEDDAC), Fort Drum, New York, and its satellite facilities.
4. **SCOPE:** The procedures outlined in this policy follow the specifications and actions required to comply with the laws and regulations governing the use and disclosure of PHI. This document does not reproduce a detailed explanation of the relevant standards, specifications, exclusions, or exceptions.
5. **REFERENCES:**
  - a. DoD 6025.18-R, DoD Health Information Privacy Regulation, January 2003
  - b. AR 40-66, Medical Record Administration and Health Care Documentation, 10 March 2003
  - c. AR 340-21, The Army Privacy Program, 5 July 1985
  - d. 45 CFR Part 164 Privacy, Final Rule, August 2002
  - e. DA Pam 340-6, Defense Privacy Board Decision Memoranda, 15 October 1983
  - f. AR 40-407, Nursing Records and Reports, 15 August 1991
  - g. AR 40-57, Armed Forces Medical Examiner System, 2 January 1991
  - h. AR 608-75, Exceptional Family Member Program, 20 December 2004

## FD MEDDAC Reg 40-45

i. AR 25-55, The Department of the Army Freedom of Information Act Program, 1 November 1997

j. AR 25-11, Record Communications and the Privacy Communications System, 4 September 1990

k. AR 40-400, Patient Administration, 12 March 2001

l. FD MEDDAC Pam 40-16, Medical Record Administration and Health Care Documentation, 23 March 2004

m. MEDCOM/OTSG Policy Memorandum 05-015, dated 6 October 2005, Subject: Release of Protected Health Information (PHI) to Unit Command Officials.

n. MEDCOM Reg 190-1, US Army Medical Command Key and Lock Control and Physical Security Standards

o. MEDCOM/OTSG Policy Memorandum 04-08, dated 18 June 2004, Subject: Transmission of Protected Health Information (PHI) Via Electronic-mail (Email)

p. MEDCOM Suppl 1 to AR 40-66, Medical Record Administration and Health Care Documentation

6. DEFINITIONS: A detailed explanation of terms used in this publication are found in Chapter DL1.1 in DoD 6025.18-R, DoD Health Information Privacy Regulation.

7. POLICY: MEDDAC is committed to:

a. protecting patient confidentiality and maintaining integrity and security during the collection, aggregation, analysis, storage, and destruction of PHI.

b. establishing systems and mechanisms to safeguard patient privacy without disrupting the provision or quality of health care.

c. enforcing the rights of patients with respect to health information privacy.

d. designating appropriate representatives to carry out privacy functions in accordance with applicable federal and state laws and regulations.

e. incorporating parameters to monitor and improve compliance with health information privacy standards in the design of the organizational compliance program.

## 8. PROCEDURES:

a. Notice of Privacy Practice. All patients will be provided a copy of, or have ready access to the Military Health System's (MHS) official Notice of Privacy Practice (NOPP). The MHS NOPP provides a comprehensive description, in ten different languages, of MEDDAC's probable uses and disclosures of PHI, legal duties, and the patient's rights with respect to PHI. As patients access care and services at MEDDAC, designated staff will make every attempt to request patients written acknowledgement of receipt of the NOPP. Each medical record will have a NOPP sticker on the back side signed by the patient.

b. Workforce Training. The success of MEDDAC's commitment to meet all standards of health information privacy will depend on how well employees, contractors, volunteers, trainees, and business associates understand what they can and cannot do under the applicable rules. As required by law, all MEDDAC workforce members will follow the procedures outlined at Appendix A. Required training includes web-based program modules covering health information privacy laws and all applicable policies and procedures for using and or disclosing PHI as related to an employee's job function and other responsibilities. Newly assigned personnel will complete training within 30 working days of arrival. (Telephone PIN numbers will not be issued to personnel until they have completed HIPAA training.)

c. Use of PHI. All workforce members will be familiar with the type of information protected under the laws and regulations referenced in this document. When uncertain, personnel may consult with the Privacy Officer or Chief, Patient Administration Division (PAD) to determine whether the information in question is protected as PHI. The highest standards of confidentiality and security will be observed among colleagues or co-workers during the exchange, application, utilization, examination, or analysis of PHI. As governed by state and federal laws, the use of PHI among MEDDAC employees will be limited to accomplish medical Treatment, Payment, and, or health care Operations (TPO). In the course of accomplishing TPO, personnel will make reasonable efforts to limit use of PHI to the minimum necessary to accomplish the intended purpose as prescribed in Appendices B and C.

d. PHI Disclosure Procedures. MEDDAC staff will follow the more stringent standards under federal and state laws governing disclosure of PHI. In all cases and circumstances, the personnel disclosing and receiving PHI must have the required authority to disclose or receive the information with respect to the individual(s) whom the information pertains and the purpose for the disclosure. Personnel will make reasonable efforts to limit disclosure of PHI to the minimum necessary to accomplish the intended purpose and to the fewest people possible. When appropriate for accomplishing the intended purpose, limited data sets will be disclosed in lieu of complete record sets. PHI will be de-identified when appropriate to meet the intended purpose. All employees will comply with the procedures and requirements for disclosure of PHI.

e. Business Associate. The success of MEDDAC's commitment to meet all standards of health information privacy will also depend on the commitment of our external business agents to comply with our requirements to protect patient privacy. Personnel will establish in writing, (i.e., contract, MOU, MOA), all business affiliations involving the exposure to or use of PHI, except activities to accomplish TPO. All relevant business agreements involving PHI will include required terms to define MEDDAC's responsibilities for protecting patient privacy. The agreements must also establish satisfactory assurances that the business associate will:

(1) use the information only for the purposes for which it is intended.

(2) safeguard the information from misuse.

(3) help MEDDAC comply with its duties under the prevailing laws. The guidelines at Appendix F outline the requirements for establishing business associate agreements that involve contact, use, or disclosure of PHI.

f. Patient Rights. All personnel will adhere to the procedures established to facilitate the rights of individuals regarding their personal health information. These rights and corresponding procedures include:

(1) the right to adequate notice of the uses and disclosures of PHI made by MEDDAC personnel (see Appendix G).

(2) the right to request (but not necessarily be granted) restrictions on the use and disclosure of PHI (see Appendix G).

(3) the right to request, but not necessarily be granted, confidential communications by alternative means at an alternative location (see Appendix H).

(4) the right to access their PHI (see Appendix I).

(5) the right to amend PHI (see Appendix J).

(6) the right to an accounting of certain disclosures of PHI (see Appendix K).

(7) the right to complain to the MEDDAC Commander and to the Department of Health and Human Services (HHS) any violations of privacy rights (see Appendix L).

g. Safeguarding PHI. The procedures in Appendix R provide guidelines for appropriate administrative, technical, and physical safeguards of PHI from intentional or unintentional use/disclosure that are contrary to privacy standards.

h. Monitoring Compliance. Departments, sections, and offices will maintain required documentation and files to show compliance with the applicable privacy function. The goals of the MEDDAC health information privacy program are: to achieve 100% workforce training, and have no substantiated complaints related to health information privacy. All personnel are responsible in contributing to the successful achievements of these goals through diligent compliance with all standards and procedures.

i. Sanctions. Personnel who fail to comply with privacy policies and procedures are subject to appropriate sanctions and corrective actions. Appendix M, Mitigating the Effect of An Unauthorized Release of PHI, outlines the sanctions policy.

## 9. RESPONSIBILITIES:

a. Commander will establish and enforce policies and procedures that influence compliant behavior and a work environment consistent with privacy standards and all specifications.

b. Deputy Commanders will:

(1) ensure 100% of subordinate staff is trained on time and according to policy.

(2) ensure subordinate staff establish and execute health information privacy safeguards as directed in this policy and referenced documents.

(3) ensure due process of investigations for privacy violation complaints and application of sanctions.

c. Legal Counsel will:

(1) provide legal interpretation and guidance related to the contents and application of this policy with respect to federal and state laws governing health information privacy.

(2) provide guidance for due process related to investigations of privacy violation complaints and the application of sanctions.

d. Inspector General (IG) will conduct independent assessments on the status of compliance and effectiveness of MEDDAC's health information privacy program.

e. Public Affairs Officer will obtain, develop, distribute and post marketing and educational materials in the most strategic locations throughout the medical treatment facilities to maximize patient and community awareness of health information privacy standards.

f. All Department, Division, Branch, and Section Chiefs will:

(1) periodically, at least annually, conduct risk assessments and consistently monitor internal policies, procedures, mechanisms and behavior trends to ensure compliance with the provisions outlined in this policy, referenced laws and regulations.

(2) instill a conscious vigilance among employees to minimize PHI exposure risk during the course of daily operations. Disclose the minimum data possible, only that which is needed for job-critical purpose, to the fewest people possible.

(3) enforce the use of the PAD, Correspondence Section, as the sole authority and clearinghouse for release of PHI, except for TPO.

g. Chief, Human Resources Division, will:

(1) promulgate the duty requirements and personnel management implications of the DoD Health Information Privacy Regulation and governing laws to the local Labor Organizations/Bargaining Units/Union Officials.

(2) ensure due process of investigations for privacy violation complaints and application of sanctions.

h. Chief, Resource Management Division, will establish internal controls to ensure and monitor all business agreements, contracts, memoranda of understandings, and other affiliations involving the use of PHI are established in writing and incorporate appropriate terminology to ensure the protection of patient privacy.

i. Chief, PAD, will:

(1) persistently promulgate the mission and responsibility of the PAD as the sole authority and clearinghouse for release of PHI, except for accomplishment of TPO.

(2) execute assigned privacy functions as directed in this policy.

(3) backup the HIPAA Privacy Officer.

j. HIPAA Privacy Officer, will:

(1) serve as proponent to this policy, provide program oversight in accordance with duties and responsibilities, and conduct designated privacy functions as directed herein.

(2) oversee and ensure privacy training of all employees, volunteers, contractors, business associates and other appropriate third parties.

(3) participate in the development, implementation, and ongoing compliance monitoring of business associate agreements.

(4) enforce, track, and report status of workforce training on health information privacy standards; act as administrator of the Learning Management System (LMS) training tool; will review training statistics and report training statistics to the Commander and Deputy Commanders.

(5) provide developmental guidance and assist in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with the Medical Information Security Readiness Team (MISRT) and organization management and administration.

(6) act as administrator of the Protected Health Information Management Tool (PHIMT). Ensure all releases and complaints are logged into PHIMT for reporting and tracking purposes.

(7) develop and implement an ongoing inspections program of all MEDDAC areas to ensure compliance with the HIPAA laws and regulations.

k. HIPAA Security Officer, will:

(1) chair the MISRT Committee

(2) develop and maintain an electronic environment with respect to transfer of PHI to areas and providers outside Army Medical Department Activity

(3) conduct ongoing inspections of all MEDDAC areas with the HIPAA Privacy Officer

(4) provide program oversight for security issues and electronic storage, input, modification and transmission of PHI IAW duties and responsibilities as directed by MEDCOM, NARMC and DoD 6025.18-R

l. Users/Staff members will:

(1) complete all HIPAA required training within specified time parameters

(2) maintain the highest standards of confidentiality and security when dealing with PHI

(3) limit use of PHI to the minimum necessary to accomplish the intended purpose and to the fewest people possible

## APPENDIX A

### Employee Training Regarding Individual Rights to PHI

1. **PURPOSE:** MEDDAC recognizes that individual rights are a critical aspect of maintaining quality care and service and is committed to allowing individuals to exercise their rights under 45 C.F.R. §164.524 and other applicable federal, state, and/or local laws and regulations. To support this commitment, all employees of MEDDAC will receive appropriate training regarding employee and organizational responsibilities regarding rights of individuals to access their PHI.

2. **POLICY:**

a. All employees of MEDDAC will be trained within 30 working days of their initial employment on the policies and procedures regarding individual rights. These policies pertain to the use, disclosure of, and access to an individual's PHI.

b. All employees will complete HIPAA Privacy and Security refresher training and any additional training within the required suspense dates.

3. **PROCEDURES:** Employee training regarding individual rights on the use and disclosure of, and access to, PHI will include the following:

a. allowing individuals to file complaints concerning MEDDAC's policies and procedures required by the HIPAA privacy rule or its compliance with such policies and procedures;

b. allowing individuals to receive an accounting of instances when their PHI has been disclosed;

c. allowing individuals to access, inspect, and/or obtain a copy of their PHI that is maintained in a designated record set;

d. denying a request from an individual to access, inspect, and/or obtain a copy of their PHI;

e. providing an individual with a written statement for the reason of a denial to inspect and copy his/her PHI;

f. allowing individuals to request confidential communications of PHI;

g. allowing individuals to request restriction of the uses and disclosures of their PHI;

h. allowing individuals to request an amendment or correction to their PHI that is erroneous or incomplete;

i. denying a request from an individual to amend or correct their PHI that is erroneous or incomplete.

4. Training will be conducted using the TMA web-based training tool at <https://www.hipaatraining.tricare.osd.mil>.

## APPENDIX B

### Identifying When Health Information Becomes PHI

1. PURPOSE: The MEDDAC is committed to ensuring the privacy and security of patient health information (PHI). To support this commitment, the following policies and procedures for identifying and securing PHI are outlined.

2. POLICY:

a. As specified in reference documents, the Patient Administration Division, Correspondence Section, is the sole authority for release of PHI, except for treatment, payment and healthcare operations.

b. The following information will be designated as PHI:

(1) any health information, including demographic information collected from an individual, transmitted or maintained in any form or medium, that;

(a) is created or received by a health care provider, health plan, employer, or health care clearinghouse.

(b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual and either identifies the individual or there is reasonable basis to believe the information can be used to identify the individual.

(2) Routine health information meeting the above definition will be automatically designated as PHI immediately upon its creation or receipt by MEDDAC.

(3) Full face photographic images and any comparable images are considered Individual Identifiable Health Information (IIHI), therefore appropriate safeguards must be in place to ensure that HIPAA standards are met.

3. PROCEDURES:

a. In the event of a discrepancy, the Chief, PAD or Privacy Officer make the decision as to whether health information has become PHI.

b. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer or Chief, PAD.

## APPENDIX C

### Disclosing and Requesting Only The Minimum Amount of PHI Necessary

1. **PURPOSE:** To outline the policy and procedures for disclosing and requesting only the minimum amount of PHI necessary. The MEDDAC is committed to ensuring the privacy and security of patient health information. While patient information must be available to health care professionals in the process of ensuring proper care, we should avoid disclosing more patient information than needed to perform our respective duties. To support our commitment to patient confidentiality, MEDDAC will ensure that the appropriate steps are taken to disclose only the minimum amount of PHI necessary to accomplish the particular use or disclosure, as required under 45 C.F.R. §164.502(b), and other applicable federal, state, and/or local laws and regulations.

#### 2. **POLICY:**

a. All employees will follow proper procedures to ensure that only the minimum amount of patient health information necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed.

b. All employees will request only the minimum amount of patient health information necessary to accomplish the specific purpose of the request.

c. This policy does not apply to the following uses or disclosures:

(1) disclosure to or request by a provider for treatment;

(2) uses or disclosure made to the individual who is the subject of the information;

(3) uses or disclosure pursuant to an authorization;

(4) disclosure made to the Department of Health and Human Services;

(5) uses or disclosures required by law; and

(6) uses or disclosure required for compliance with applicable laws and regulations.

#### 3. **PROCEDURES:**

a. All proposed uses or disclosures of patient health information will be reviewed by the appropriate personnel having an understanding of MEDDAC's privacy policies and practices and sufficient expertise to understand and weigh the necessary factors.

b. The MEDDAC will only use, disclose, or request an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.

c. Within the MEDDAC, the following classes of personnel require and will maintain the indicated levels of access to PHI on a routine basis to appropriately accomplish their duties and responsibilities to include treatment, payment and health care operations (TPO):

- (1) Medical Records Personnel:
  - (a) complete access to clinical operation record set
  - (b) complete access to case management record set
  - (c) Partial Access to Patient account record set.
- (2) Business Office Personnel:
  - (a) partial access to clinical operation record set
  - (b) partial access to case management record set
  - (c) complete access to patient accounts record set.
- (3) Case Management Personnel – Partial Access
- (4) Medical/Clinical Personnel – Selective Access
- (5) Dietary/Nutrition Personnel – Partial Access

d. Access to PHI will be reasonably limited to that described in paragraph 3 by utilizing access control systems. These may be physical controls and/or security controls preventing unauthorized access. Any person who, without proper authorization, discloses a patient's PHI or medical record may be subject to adverse administrative action or disciplinary proceedings.

e. The following criteria will be used in limiting the amount of PHI requested (disclosed) by MEDDAC personnel:

- (1) Does the individual who is requesting (disclosing) the PHI have complete understanding of the purpose for the use or disclosure of the PHI?
- (2) Are all of the individuals identified for whom the requested use or disclosure of the PHI is required?

f. Requests for disclosures of PHI will be reviewed on an individual basis in accordance with criteria listed in the policy and regulations.

g. MEDDAC personnel may reasonably reply on requests by:

(1) public health and law enforcement agencies in determining the minimum necessary information for certain disclosures;

(2) other covered entities in determining the minimum necessary information for certain disclosures; or

(3) a professional who is a member of its workforce or is a business associate of MEDDAC for the purpose of providing professional services to MEDDAC, if the professional represents that the information requested is the minimum necessary for the stated purpose.

h. In the event of disclosures for research purposes, the MTF Commander will approve all requests from personnel under their command whose research projects involve medical records at that facility. The Surgeon General is the approval authority for all other requests. Any approval letter from the Surgeon General allowing access to records will be shown to the Chief, PAD, when requesting access to records at the MTF level.

i. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer or the Chief, PAD.

## APPENDIX D

### Creating and Using a Limited Data Set

1. **PURPOSE:** The MEDDAC is committed to ensuring the privacy and security of patient health information. Federal law allows health care organizations to create and use a limited data set under certain conditions. A limited data set contains information from which all direct identifiers, such as name, have been removed, but which may contain some indirect identifiers. From time to time, MEDDAC will use or disclose limited data sets for the purposes of public health and health care operations. In doing so, the following policies and procedures for creating and using limited data sets will be observed.

2. **POLICY:**

a. As specified in reference documents, the PAD, Correspondence Section, is the sole authority for release of PHI, except for treatment, payment and healthcare operations.

b. The MEDDAC may use PHI to create, use and disclose a limited data set for the purposes of research, public health and health care operations, as long as the facility enters into a proper data use agreement with the recipient of the limited data set.

c. If MEDDAC is the recipient of a limited data set, MEDDAC will enter into and comply with the terms of a data-use agreement consistent with the requirements of such agreement.

3. **PROCEDURES/RESPONSIBILITY:**

a. The PAD Officer will make decisions as to whether a limited data set should be created and/or disclosed.

b. The reason for creating and/or disclosing information in a limited data set will be documented and maintained.

c. The following identifying elements of an individual, relatives, employers and household members will be removed or otherwise excluded from PHI in order to create a limited data set:

(1) names

(2) postal address information, other than town or city, State, and zip code

(3) telephone numbers

- (4) fax numbers
- (5) electronic mail addresses
- (6) social security numbers
- (7) medical record numbers
- (8) health plan beneficiary numbers
- (9) account numbers
- (10) certificate/license numbers
- (11) vehicle identifiers and serial numbers, including license plate numbers
- (12) device identifiers and serial numbers
- (13) web universal resource locators (URLs)
- (14) internet protocol (IP) address numbers
- (15) biometric identifiers, including finger and voice prints
- (16) full face photographic images and any comparable images

d. The MEDDAC will use only the minimum amount of PHI necessary to create and use the limited data sets.

e. The following process will be used for purposes of removing identifying elements from PHI:

- (1) physical removal by means of cutting out the information
- (2) electronic removal (deletion) of elements from an electronic document
- (3) black-out or white-out the elements by using a dark black ink or correction fluid or tape which fully covers the information, and then photocopying the page. Only the photocopy will be used in the limited data set. The original document is NOT considered a limited data set, as the information is typically still somewhat visible despite efforts to conceal it in these manners.

(4) Creating electronic queries that exclude all elements of identifying information.

f. The data-use agreement, which may be in the form of a formal contract, will not authorize the limited data set recipient to use or further disclose the information in a manner that is inconsistent with the requirements of this document, if done by a covered entity.

g. The data-use agreement between the MEDDAC and the limited data set recipient will establish:

(1) who is permitted to use or receive the limited data set

(2) the permitted uses and disclosures of such information by the recipient consistent with the limited purposes of research, public health or health care operations.

h. The data-use agreement between the MEDDAC and the limited data set recipient will provide MEDDAC with adequate assurances that the recipient of the limited data set will:

(1) not attempt to re-identify or contact the individuals whose information is contained in the limited data set

(2) use appropriate safeguards to prevent uses or disclosures outside the terms of the data use agreement

(3) ensure that any subcontractors or other recipients of the data agree to and abide by the terms of the data-use agreement

(4) report any breaches of the information or agreement to the covered entity in a timely manner.

i. Knowledge of a violation or potential violation of this policy must be reported directly to the HIPAA Privacy Officer or Chief, PAD.

j. Limited data sets will be forwarded to the PAD, Correspondence Section, for release.

(1) The PAD, Correspondence Section, will:

(a) examine the information to determine that it is prepared in accordance with the guidelines set forth in this policy and resource documents.

(b) document all requests and releases of the limited data set to the appropriate recipient into the official disclosure tool at <https://phimt.tricare.osd.mil/hipaax/logon.do>.

**APPENDIX E****Creating and Using De-Identified Health Information**

1. **PURPOSE:** The MEDDAC is committed to ensuring the privacy and security of patient health information. Federal law allows health care organizations to use or disclose PHI for the purpose of creating de-identified information. That is information which has been stripped of any elements that may identify the patient, such as name, birth date, or social security number. The policies and procedures for creating and using de-identified health information will ensure that the appropriate administrative and technical processes are in place to properly de-identify PHI, as well as to secure any methods of re-identification, as required by federal, state and/or local laws and regulations.

2. **POLICY:**

a. As specified in reference documents, the PAD, Correspondence Section, is the sole authority for release of PHI, except for treatment, payment and healthcare operations.

b. Health care organizations are permitted to create and use de-identified health information under certain conditions. De-identified health information contains information from which all direct identifiers, such as name and date of birth, have been removed, but which may contain some indirect identifiers. MEDDAC will, from time to time, use or disclose de-identified health information for utilization and data quality review and research. In doing so, we will ensure that the appropriate administrative and technical processes are in place to properly de-identify PHI, as well as to secure any methods of re-identification.

c. MEDDAC may create de-identified information for the following purposes:

- (1) utilization review
- (2) research
- (3) data quality review
- (4) other uses, as determined by the Chief, PAD, or releasing official.

d. The MEDDAC will not use or disclose the code or other means of record identification or mechanism used to re-identify health information for any other purpose than the following within MEDDAC internal operations:

- (1) facility directories

FD MEDDAC Reg 40-45

- (2) utilization review
- (3) research
- (4) auditing
- (5) other uses, as determined by the Chief, PAD, or releasing official.

e. De-identified information will not be disclosed if the employees creating or disclosing the information, or any other employee of the organization, have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

3. PROCEDURES:

a. The PAD Officer or Privacy Officer will make decisions as to whether PHI should be de-identified.

b. The reason for de-identification will be documented and maintained.

c. The following individually identifying elements will be removed or otherwise concealed from PHI in order to create de-identified information:

- (1) names
- (2) all elements of dates (except year) for dates directly related to an individual, including:
  - (a) birth date
  - (b) admission date
  - (c) discharge date
  - (d) date of death
  - (e) all ages over 89, except that such ages and elements may be aggregated into a single category of age 90 or older
- (3) telephone numbers
- (4) fax numbers
- (5) electronic mail addresses
- (6) social security numbers

- (7) medical record numbers
  - (8) health plan beneficiary numbers
  - (9) account numbers
  - (10) certificate/license numbers
  - (11) vehicle identifiers and serial numbers, including license plate numbers
  - (12) device identifiers and serial numbers
  - (13) web universal resource locators (URLs)
  - (14) internet protocol (IP) address numbers
  - (15) biometric identifiers, including finger and voice prints
  - (16) full face photographic images and any comparable images
  - (17) all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes
  - (18) any other unique identifying number, characteristic, or code other than a code assigned to a record to permit MEDDAC to re-identify the information
  - (19) the initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census:
    - (a) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
    - (b) the initial three digits of the zip code for all such geographic units containing 20,000 or fewer people is changed to 000
- d. the following process will be used for purposes of removing identifying elements from PHI:
- (1) physical removal by means of cutting out the information
  - (2) electronic removal (deletion) of elements from an electronic document
  - (3) black-out or white-out the elements by using a dark black ink or correction fluid or tape which fully covers the information, and then photocopying the page. Only the photocopy will be de-identified health information. The original document is NOT

de-identified. Simply blacking out or whitening out information does not de-identify it, as information is typically still somewhat visible despite efforts to conceal it in these manners.

(4) creating electronic queries that exclude all elements of identifying information.

e. If any of the listed identifiers are not removed, then the information will only be disclosed when approved by the Chief, PAD, or a designated releasing official. The releasing official will first examine the information and the recipient's intended use of the information before authorizing disclosure of the information. The releasing official, before authorizing disclosure shall:

(1) determine that the risk is very small that an anticipated recipient of the information could use the information provided to identify an individual alone or in combination with other reasonably available information

(2) document the methods and results of the analysis that justify such determination.

f. The code or other means of record identification used to re-identify information will not be derived from or related to information about the individual and should not otherwise be capable of being translated so as to identify the individual.

g. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer or Chief, PAD, or to the employee compliance hotline.

h. The PAD, Correspondence Section, will:

(1) examine the information to determine that it is prepared in accordance with the guidelines set forth in this policy and resource documents.

(2) document the request and the release of the de-identified health information to the appropriate recipient in the official disclosure database at <https://phimt.tricare.osd.mil/hipaax/logon.do>.

## APPENDIX F

### Assuring Business Associates Safeguard PHI

1. **PURPOSE:** To establish policy, assign responsibility, and provide procedures for obtaining assurances that business associates will appropriately safeguard PHI.

2. **REFERENCES:**

- a. DoD 6025.18-R, DoD Health Information Privacy Regulation, January 2003
- b. DoD 5400.11-R, DoD Privacy Program, August 83
- c. AR 11-2, Management Control, August 94
- d. AR 25-55, DA Freedom of Information Act Program

3. **RESPONSIBILITY:**

a. Personnel who write statements of work (SOW), contracts, or agreements with agencies external to MEDDAC and that involves PHI, will ensure that appropriate Health Insurance Portability and Accountability Act (HIPAA) language is included in these documents.

b. The Privacy Officer will review these documents to ensure compliance with HIPAA standards.

4. **PROCEDURES:**

a. All contracts and memorandums of agreements (MOA) will be reviewed for the contents of information that will be generated as a result of the services rendered. The clause in Para 6b below will be included in contracts/MOAs/agreements modified or initiated after 14 April 2003 that involve the handling or generation of PHI by military healthcare system (MHS) business associates.

b. Clause for inclusion in qualifying contracts/MOAs/agreements (see attached pages).

5. **Privacy of PHI:**

a. **Definitions:** As used in this clause:

(1) Individual has the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(2) Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

(3) PHI has the same meaning as the term "PHI" in 45 CFR 164.501, limited to the information created or received by the Contractor from or on behalf of the Government.

(4) Required by law has the same meaning as the term "required by law" in 45 CFR 164.501.

(5) Secretary means the Secretary of the Department of Health and Human Services or his/her designee.

b. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501.

c. The Contractor agrees to not use or further disclose PHI other than as permitted or required by the contract or as required by law.

d. The Contractor agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this contract.

e. The Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of PHI by the Contractor in violation of the requirements of this Contract.

f. The Contractor agrees to report to the government any use or disclosure of the PHI not provided for by this contract.

g. The Contractor agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by the Contractor on behalf of the government agrees to the same restrictions and conditions that apply through this contract to the Contractor with respect to such information.

h. The Contractor agrees to provide access, at the request of the government, and in the time and manner designated by the government to PHI in a designated record set, to the government or, as directed by the government, to an individual in order to meet the requirements under 45 CFR 164.524.

i. The Contractor agrees to make any amendment(s) to PHI in a designated record set that the government directs or agrees to pursuant to 45 CFR 164.526 at the request of the government or an individual, and in the time and manner designated by the government.

j. The Contractor agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Contractor on behalf of, the government, available to the government, or at the request of the government to the secretary, in a time and manner designated by the government or the secretary, for purposes of the secretary determining the government's compliance with the privacy rule.

k. The Contractor agrees to document such disclosures of PHI and information related to such disclosures as would be required for the government to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

l. The Contractor agrees to provide to the government or an individual, in time and manner designated by the government, information collected in accordance with this Clause of the contract, to permit the government to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

6. General Use and Disclosure Provisions. Except as otherwise limited in this Agreement, the Contractor may use or disclose PHI on behalf of, or to provide services to, the government if such use or disclosure of PHI would not violate the privacy rule or the Department of Defense Health Information Privacy Regulation.

7. Specific Use and Disclosure Provisions.

a. Except as otherwise limited in this Agreement, the Contractor may use PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

b. Except as otherwise limited in this Agreement, the Contractor may disclose PHI for the proper management and administration of the Contractor, provided that disclosures are required by law or the Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, the Contractor may use PHI to provide data aggregation services to the government as permitted by 45 CFR 164.504(e)(2)(i)(B).

d. Contractor may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR 164.502(j)(1).

8. Obligations of the government:

a. Provisions for the government to inform the Contractor of privacy practices and restrictions.

b. Upon request the government shall provide the Contractor with the notice of privacy practices that the government produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

c. The government shall provide the Contractor with any changes in, or revocation of, permission by individual to use or disclose PHI, if such changes affect the Contractor's permitted or required uses and disclosures.

d. The government shall notify the Contractor of any restriction to the use or disclosure of PHI that the government has agreed to in accordance with 45 CFR 164.522.

9. Permissible requests by the government: The government shall not request the Contractor to use or disclose PHI in any manner that would not be permissible under the privacy rule if done by the government, except for providing data aggregation services to the government and for management and administrative activities of the Contractor as otherwise permitted by this clause.

10. Termination:

a. Termination. A breach by the Contractor of this clause may subject the Contractor to termination under any applicable default or termination provision of this contract.

b. Effect of Termination:

(1) If this contract has records management requirements, the records subject to the clause should be handled in accordance with the records management requirements. If this contract does not have records management requirements, the records should be handled in accordance with paragraphs (2) and (3) below.

(2) If this contract does not have records management requirements, except as provided in paragraph (3) of this section, upon termination of this contract, for any reason, the Contractor shall return or destroy all PHI received from the government or created or received by the Contractor on behalf of the government. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Contractor. The Contractor shall retain no copies of PHI.

(3) If this contract does not have records management provisions and the Contractor determines that returning or destroying the PHI is infeasible, the Contractor shall provide to the government notification of the conditions that make return or

destruction not feasible. Upon mutual agreement of the government and the Contractor that return or destruction of PHI is infeasible, the Contractor shall extend the protections of this contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Contractor maintains such PHI.

11. Miscellaneous:

a. Regulatory References: A reference in this clause to a section in the privacy rule means the section as in effect or as amended, and for which compliance is required.

b. Survival: The respective rights and obligations of Business Associate under the "Effect of Termination" provision of this clause shall survive the termination of this Contract.

c. Interpretation: Any ambiguity in this clause shall be resolved in favor of a meaning that permits the government to comply with the privacy rule.

d. All records, notes, meeting minutes, etc., generated during the life of contact/agreement will be filed and maintained for 6 years.

## APPENDIX G

### Individual Rights to PHI Requesting Restrictions on Uses and Disclosures

1. **PURPOSE:** HIPAA requirements provide an individual with the right to request restrictions to the use and disclosure of his or her PHI. While covered entities are not required to permit the requested restrictions, they are required to permit the request. If the covered entity agrees to the requested restrictions, the covered entity may not make uses or disclosures that are inconsistent with such restrictions, unless such uses or disclosures are mandated by law. This provision does not apply to health care provided to an individual on an emergency basis.

2. **POLICY:** MEDDAC will allow an individual to request that uses and disclosures of his or her PHI be restricted.

3. **PROCEDURES:**

a. MEDDAC will allow an individual to request a restriction on the use and disclosure of PHI.

b. Upon agreeing to such a restriction, MEDDAC will not violate such restriction, unless as specified within this policy and procedure.

c. MEDDAC is not required to honor an individual's request in the following situation(s):

(1) when the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment;

(2) if restricted PHI is disclosed to a health care provider for emergency treatment, MEDDAC will request that such health care provider not further use or disclose the information.

d. If MEDDAC agrees to an individual's requested restriction, the restriction does not apply to the following uses and disclosures:

(1) to an individual accessing their own PHI (see policy, individual rights regarding PHI granting access to inspect and obtain a copy);

(2) to an individual requesting an accounting of their own PHI (see policy, individual rights to PHI - accounting and individual rights to PHI - suspension);

(3) facility directories (see policy, using PHI for facility directories);

(4) instances for which an authorization, or opportunity to agree or object is not required (see policies, disclosing PHI for judicial and administration release; disclosing PHI for health oversight release; disclosing PHI for research release; disclosing PHI for law enforcement release; disclosing PHI for public health release; disclosing PHI to avert a serious threat to health and safety; disclosing PHI for cadaveric organ, eye, or tissue donation; disclosing PHI about decedents; disclosing PHI for worker's compensation; disclosing PHI about victims of abuse, neglect, or domestic violence; disclosing PHI for specialized government functions; disclosing PHI as required by law).

e. MEDDAC may terminate its agreement to a restriction in the following situations:

(1) the individual agrees to or requests the termination in writing;

(2) the individual orally agrees to the termination and the oral agreement is documented;

(3) MEDDAC informs the individual that it is terminating its agreement to a restriction. Such termination is only effective with respect to PHI created or received after it has so informed the individual.

f. MEDDAC will document in the Protected Health Information Management Tool (PHIMT) tracking system and retain the restriction for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

## APPENDIX H

### Confidential Communications for PHI

1. **PURPOSE:** It is important to ensure that individuals can receive communications regarding their PHI in a means and location that the individual feels is safe from unauthorized use or disclosure. A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the covered health care provider by alternative means or at alternative locations.

2. **POLICY:**

a. MEDDAC will take necessary steps to accommodate reasonable requests by individuals to receive confidential communications of PHI.

b. In complying with policy, MEDDAC will provide confidential communications by alternative means or at alternative locations.

3. **PROCEDURES:**

a. MEDDAC may require individuals to make a request for a confidential communication in writing.

b. MEDDAC will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

c. When appropriate, MEDDAC may condition the provision of a reasonable accommodation on information as to how payment, if any, will be handled, and specification of an alternative address or other method of contact.

d. An alternative means or location will be designated on a case-by-case basis, that is satisfactory to both MEDDAC and the individual, before communication of PHI is made.

e. The Privacy Officer, using professional judgment and considering all relevant factors, will be responsible for deciding the alternative means or location to communicate PHI to an individual.

f. Once it is determined that use or disclosure is appropriate, Medical Records personnel with appropriate access clearance will access the individual's PHI using proper access and authorization procedures.

g. The requested PHI will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.

h. Medical Records personnel will appropriately document the request and delivery of the PHI.

i. In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.

j. Knowledge of a violation or potential violation of this policy must be reported directly to the Chief, Patient Administration Division, and/or Privacy Officer.

## APPENDIX I

### Allowing Individuals Access to Their Own PHI

1. **PURPOSE:** MEDDAC recognizes that individual rights are a critical aspect of maintaining quality care and service and is committed to allowing individuals to exercise their rights under 45 C.F.R. §164.524 and other applicable federal, state, and/or local laws and regulations. To support this commitment, MEDDAC will maintain and update, as appropriate, written policies and procedures to provide guidance on employee and organizational responsibilities to the rights of individuals regarding their PHI. However, situations may arise when the requested information is not readily available for access; and therefore, the time period for responding to the request may be extended. The policies and procedures herein have been established to assist personnel in the provision of such an extension. Personnel should also refer to Army Regulation 40-66 when responding to an individual's request for access to PHI.

#### 2. **POLICY:**

a. MEDDAC will take necessary steps to address individual requests to access, inspect, and/or obtain a copy of their PHI that is maintained in a designated record set in a timely and professional manner.

b. MEDDAC will adhere to Army Regulation 40-66 in providing individuals access, inspection, and/or copies of their PHI.

c. In the event that MEDDAC must extend the time period for responding to a request, we will adhere to the procedures herein.

#### 3. **PROCEDURES:**

a. Once MEDDAC receives a request, Patient Administration Division, Correspondence Clerk, will act on the request within 30 days after receipt of the request by:

(1) informing the individual of the acceptance and providing the access requested; or

(2) providing the individual with a written denial.

b. In the event that the request for access to PHI is not maintained or accessible to the facility on-site, then MEDDAC will act on the individual's request for an accounting no later than 60 days from the receipt of such a request.

c. In the event that the time period for the action must be extended, then Patient Administration Correspondence Clerk will provide the individual with a written statement of the reasons for the delay, and the date by which the action on the request will be completed.

d. If necessary, MEDDAC may extend the time period for the action, but for no more than 30 additional days.

e. The time period cannot be extended more than once.

f. Medical Records personnel with appropriate access clearance will access the individual's PHI using proper access and authorization procedures.

g. This policy and procedure will be documented in the PHIMT disclosure tool and retained for a period of at least 6 years from the date of its creation or the date when it last was in effect, whichever is later.

h. Knowledge of a violation or potential violation of this policy must be reported directly to the Chief, PAD, and/or Privacy Officer.

## APPENDIX J

### Policy for Amendment of Medical Records

#### 1. REFERENCES:

- a. AR 15-158, Army Board for Correction of Military Records, 29 February 2000.
- b. DoD 5400.11-R, Department of Defense Privacy Program, 31 August 1983.

2. PURPOSE: The purpose of this appendix is to offer the following steps as the necessary procedure to amend a medical record.

#### 3. POLICY:

a. Patients can request in writing amendments to their medical records. A letter detailing their complaint and request for an amendment will be sent to the Patient Administration Division (PAD). The patient should address why they want the information expunged.

b. The medical treatment facility's (MTF) PAD will endorse the patient's letter and forward to U.S. Army Medical Command (MEDCOM), PAD (MCHO-CL-P, Medical Records Consultant). The PAD will include their recommendation and address any reluctance of the physician to remove information because it is factual; i.e., the events actually happened as recorded. The patient administrator will include copies from the medical record of the appropriate pages included in the controversy.

c. The Medical Records Consultant, MEDCOM, will then forward the complaint to the MEDCOM Freedom of Information (FOIA) and Privacy Act (PA) Office (MCFP, Access and Amendment Refusal Authority (AARA).

d. The AARA makes the initial decision after coordination with the appropriate physician consultants and PAD. The decision will be returned to the MTF PAD.

e. Once a patient receives a denial, they have 60 days to appeal the decision in writing. The appeal should be addressed to: HQ, USAMEDCOM (MCFP-AARA), 2050 Worth Road, Suite 21, Fort Sam Houston, TX 78234-6021.

f. The AARA prepares a package for the Army Board for Correction of Medical Records. The Review Board meets on an ad hoc basis. This board will review the case and make a final decision. They will notify the individual directly (with coordination copies sent to MEDCOM FOIA/PA and MTF PAD).

g. If the patient continues to disagree, the patient can obtain a lawyer and pursue legal actions in the court system.

## APPENDIX K

### **Right To Receive Instances When PHI Has Been Disclosed Including Suspending and Individual's Right to Receive Such Accounting**

1. **PURPOSE:** Outline the policies and procedures for documenting, tracking and notifying individuals regarding disclosure of PHI.

2. **REFERENCES:**

a. DoD 6025.18-R Health Information Privacy Regulation, January 2003

b. AR 340-21, The Army Privacy Program, 5 July 1985

c. AR 40-66, Medical Record Administration and Health Care Documentation, 10 March 2003

3. **POLICY:**

a. As specified in reference documents, the Chief, PAD, or Correspondence Section, and Privacy Officer is the sole authority for release of PHI, except for treatment, payment and health care operations.

b. Individuals have the right to receive an accounting of all instances where PHI about them is disclosed by MEDDAC except for the following disclosures:

(1) to carry out treatment, payment and health care operations

(2) to individuals of PHI about themselves under their right to inspect and copy their PHI.

(3) a use or disclosure otherwise permitted or required under the Privacy rule.

(4) pursuant to a valid authorization given by the individual.

(5) for the facility's directory or to persons involved in the individual's care or other notification purposes.

(6) for national security or intelligence purposes.

(7) to correctional institutions or law enforcement officials.

(8) as part of a limited data set in accordance with requirements.

(9) occurred prior to the 14 April 2003 regulatory compliance date of the HIPAA Privacy Rule.

(10) for the facility's directory or to person involved in the individual's care or other notification purposes.

(11) as part of a limited data set

(12) disclosure made incidentally when another use was made, provided that MEDDAC used only the minimum amount of PHI necessary, and had safe guards in place to prevent unauthorized uses and disclosure.

c. When requested by a health oversight agency or law enforcement official, MEDDAC must suspend an individual's right to an accounting of their PHI for uses and disclosures to that agency.

#### 4. PROCEDURES:

a. Accounting of disclosure provided to the individual will include:

(1) accounting of disclosure for up to 6 years prior to the date on which the request is filed.

(2) the accounting will be in writing.

(3) disclosures to or by business associates of MEDDAC.

(4) for each disclosure the date of the disclosure.

(5) the name of the entity or person who received the PHI, and if available, the address of such entity or person.

(6) a brief description of the PHI disclosed.

(7) a brief statement of the purpose of the disclosure that provides a basis for the disclosure, or a copy of a written request for the disclosure.

(8) the individual's request is to be completed no later than 60 days after receipt of request by:

(a) providing the individual with the accounting requested.

(b) extending the time to provide the accounting by no more than 30 days.

(c) only one 30-day extension is to be applied to each request.

(9) If the 30-day extension is applied, the individual will be provided a written statement of the reasons for the delay and the date by which MEDDAC will provide the accounting.

(10) Each individual will receive, without charge, their first accounting within any 12 month period.

(11) Any fee applied to subsequent requests by an individual within a 12 month period will be reasonable and cost-based, the individual must be notified in advance of the fee and have the opportunity to withdraw or modify their request.

(12) MEDDAC must document and retain the information required to be included in an accounting for a period of at least 6 years from the date of its creation or the date when it was last in effect, including the titles of the persons or offices responsible for receiving and processing requests.

(13) The PAD, Correspondence Section, will be responsible for responding to a request from an individual for an audit trail of instances when their PHI has been disclosed for purposes other than treatment, payment or healthcare operations.

b. MEDDAC must temporarily suspend an individual's right to receive an accounting of disclosure to a health oversight agency or law enforcement official for the time specified by such agency or official, if the agency provided a written statement that an accounting to the individual would impede the agency's activities. The statement must specify the time for which the suspension is required.

c. If the request to temporarily suspend an individual's right to receive an accounting of disclosure is made orally, MEDDAC must document the statement, including the identity of the agency or official making the statement, temporarily suspend the individual's right to an accounting of disclosure subject to the statement, and limit the duration to no longer than 30 days from the date of the oral statement, unless an official written request is received within that time period.

d. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer or Chief, PAD, or to the employee compliance hotline.

e. The PAD, Correspondence Section, will:

(1) examine the information to determine that it is prepared in accordance with the guidelines set forth in this policy and resource documents.

(2) document in the request and the release of PHI to the appropriate recipient in the PHIMT disclosure tool.

## APPENDIX L

### Individual Rights To PHI Filing Complaints

1. **PURPOSE:** HIPAA requires covered plans and providers to have a mechanism for receiving complaints from individuals regarding the covered entity's compliance with the requirement of the privacy standards. The covered entity is required to accept complaints about any aspect of their practices regarding PHI. For example, individuals would be able to file a complaint when they believe that PHI relating to them has been used or disclosed improperly; that an employee of the entity has improperly handled the information; that they have wrongfully been denied access to or opportunity to amend the information; or, that the entity's notice does not accurately reflect its information practices.

2. **POLICY:**

a. As specified in 45 C.F.R. §164.530(d), MEDDAC will provide a process for individuals to make complaints concerning policies and procedures regarding the use or disclosure of PHI or its compliance with such policies and procedures.

(1) All patient complaints are to be in writing.

(2) Must be filed within 180 days of when suspected violation occurred.

(3) MCID-IM Form 836-R, Health Information Privacy Complaint Form, will be used to file complaint. This form will be available on the internet to be printed off for patients to complete and return to the HIPAA Privacy Officer.

b. The Privacy Officer will be MEDDAC's designated contact for individuals to file complaints pursuant to this policy.

c. Individuals will not be required to waive their rights to file a complaint with the Department of Health and Human Services as a condition of the provision of treatment or eligibility for benefits.

3. **PROCEDURES:**

a. All complaints received, and their disposition will be documented into the PHIMT by the Privacy Officer where it will be maintained for a period of at least 6 years from the date of its creation or the disposition date, whichever is later.

b. The Privacy Officer should be contacted in order to file a complaint concerning MEDDAC's policies and procedures required by the HIPAA privacy rule or its compliance with such policies and procedures.

c. The telephone number of the Privacy Officer will be posted throughout the medical facility, its satellite facilities, and the GAHC website homepage.

d. HIPAA complaints on medical facilities that are not MEDDAC, i.e., Samaritan Medical Center and Carthage Area Hospital. Any HIPAA complaints received by beneficiaries about these facilities will be filed and maintained. The Privacy Officer will contact the other medical facility for a copy of their investigation for record and information purposes only.

## APPENDIX M

### Mitigating the Effect of An Unauthorized Release of PHI

1. **PURPOSE:** A covered entity must take steps to mitigate any harmful effect that is known to it by a use or disclosure of PHI in violation of its policies and procedures by the covered entity itself or its business associates. This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to mitigating the effect of the unauthorized release of information.
2. **POLICY:** Pursuant to 45 C.F.R. §164.530(f), MEDDAC will take all necessary steps to mitigate any harmful effect that is known of a use or disclosure of PHI in violation of approved policies and procedures.
3. **REFERENCES:**
  - a. DoD 6025.18-R, DoD Health Information Privacy Regulation, January 2003
  - b. Uniform Code of Military Justice
  - c. United States Code Title 5, Chapter 75
  - d. AR 40-66, Medical Record Administration and Health Care Documentation, 10 March 2003
4. **PROCEDURES:** The following process will be utilized to mitigate the effect of an unauthorized release of PHI by an employee, contractor and/or business associate:
  - a. Any unauthorized release of PHI will be immediately reported to Privacy Officer and/or Chief, PAD, upon discovery of the release.
  - b. The Privacy Officer will investigate the release to determine how the information was released and whom the information was released to.
  - c. After the initial investigation, the Privacy Officer must notify any patients whose information may have been released as well as the MEDDAC's Deputy Commander for Administration.
5. **REGULATORY AUTHORITY 45 C.F.R. §164.530(f):** A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

6. ANALYSIS, BACKGROUND, AND IMPLICATIONS: The final rule imposes a duty on covered entities to mitigate any harmful effect of a use or disclosure of PHI that is known to the covered entity. The duty to mitigate is applied to a violation of the covered entity's policies and procedures.

7. FAILURE TO COMPLY WITH HIPAA POLICIES AND PROCEDURES:

a. Applicable sanctions for failure to comply with MEDDAC's HIPAA policies and procedures will be UCMJ action for military personnel, and Chapter 75, Title 5, for civilian personnel. Applicable procurement regulations will be utilized for contract personnel.

b. All personnel whether military, civilian, volunteers, students and contract that work in any MEDDAC facility are subject to sanctions if found in violation of above policies and procedures.

c. All violations of policies and procedures will be considered on an individual basis in order to determine severity of violation. Determining factors of severity include but are not limited to, intentional versus unintentional disclosure, pattern or practice of improper use of PHI.

e. Documentation of the sanctions will be forwarded to appropriate personnel office to be maintained for a minimum of 6 years in the individual's personnel file.

## APPENDIX N

### Disclosure Tool For Release Of PHI

1. **PURPOSE:** The MEDDAC is required to record and provide for a period of six years all PHI releases and HIPAA complaints. For this purpose a web-based disclosure tool has been designed.

2. **POLICY:**

a. In order to accomplish this requirement all information requested and released on an individual is recorded in the official Military Health System Protected Health Information Management Tool (PHIMT) <https://phimt.tricare.osd.mil/hipaax/logon.do>.

b. The Privacy Officer is the administrator of the tool. The administrator can add/modify users and assign roles.

c. The assigned roles are privacy specialist and regular user.

(1) Privacy specialist role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amendments to requests, restrictions to disclosures, disclosure suspensions and generate associated letters.

(2) Regular user can create disclosures and authorization requests that can be routed to the privacy specialist.

3. **PROCEDURES:**

a. Disclosures to unit commanders, Preventive Medicine Activity disclosures, and Occupational Health disclosures must be accounted for in the PHIMT.

b. Individuals have a right to request an accounting of disclosures made by MEDDAC in the 6 years prior to the date that the accounting is requested, except for disclosures:

(1) to carry out treatment, payment, and health care operations.

(2) to individuals of protected health information about them.

(3) pursuant to a valid authorization to release information to a third party.

(4) for the facility's directory or to persons involved in the individual's care, or for other notification purposes.

(5) for national security or intelligence purposes.

(6) to correctional institutions or law enforcement officials.

(7) as part of a limited data set.

(8) that were incidental to treatment, payment, and health care operations, such as calling a patient's name out in a waiting room.

(9) That occurred prior to 14 April 2003.

c. Chief, PAD will:

(1) Ensure each accounting of a disclosure will include the following:

(a) the date of disclosure;

(b) the name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(c) a brief description of the protected health information disclosed;

(d) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or in lieu of such statement;

(e) a copy of the individual's written authorization to use or disclosure the protected health information; or

(f) a copy of a written request for a disclosure required by HHS secretary to investigate or determine the covered entity's compliance with applicable laws and regulations.

(2) Within 60 days of request date, provide a written accounting of instances when the requester's PHI has been disclosed in the 6 years prior to the date on which the accounting is requested.

d. Privacy Officer will:

(1) document all complaints into the PHIMT tool.

(2) monitor and review the PHIMT tool to ensure compliance with documentation of disclosures and to analyze data for reporting to higher headquarters and Command Group.

## APPENDIX O

### Security Of PHI

1. **PURPOSE:** The final Security Rule was published on 20 February 2003. The overall goal of the security standards is to protect data against reasonably anticipated threats or hazards and improper use or disclosure. At the heart of the rule is the necessity for a covered entity to conduct a risk assessment that evaluates its systems and processes for potential risks and vulnerabilities to the health information and to develop, implement, and maintain appropriate measures. In order to be HIPAA compliant, information security must involve all the ways that people handle and access electronic PHI. The responsibility to implement HIPAA security standards extends to all members of an organization's workforce.

2. **POLICY:**

a. As a first step the MEDDAC has formed a Medical Information Security Readiness Team (MISRT). The MISRT will have responsibility for coordinating MTF HIPAA compliance efforts by establishing effective programs for protecting confidentiality, integrity and availability of healthcare information. This team will:

- (1) coordinate HIPAA data security and privacy programs.
- (2) oversee policy, procedure and practice compliance program.
- (3) supervise information security risk assessment and risk management.
- (4) coordinate training in health information assurance and medical privacy.
- (5) coordinate development of technical security infrastructure for health issues.
- (6) oversee certification and accreditation of medical information systems.

b. As a security measure all users are required to either log off or lock their computer systems when they leave their work site.

## **APPENDIX P**

### **Release of PHI to Commanders**

1. **PURPOSE:** Appropriate military command authorities that exercise authority over an individual or have been designated by a commander to receive PHI on behalf of the commander can obtain limited patient PHI on their Soldiers.
2. **POLICY:** Only the minimum necessary information should be released to accomplish the purpose of release. PHI may be disclosed to unit Commanders to:
  - a. determine Soldier's fitness to perform mission, assignment order or duty including compliance with any actions required as a precondition to performance of such mission, assignment, order or duty.
  - b. to carry out any other activity necessary to the proper execution of the mission of the army forces.
  - c. under no circumstances will a Soldier's entire medical record be provided to a commander or his authorized representative.
3. **PROCEDURES:** DA Form 4254, Request for Private Medical Information, will be used by unit Commanders or their designated representative to obtain PHI on their Soldiers. The form will be submitted to PAD for processing.

## APPENDIX Q

### Camera Use For Personal Photos and Videos

1. **PURPOSE:** This section will clarify “use of camera for personal photos and videos” within MEDDAC. MEDDAC is responsible for applying appropriate safeguards of PHI in their facilities.

2. **POLICY:** Generally, an authorization is required for the release of PHI, which involves photos and videos for purposes other than treatment, payment and healthcare operations. According to DoD 6025.18-R full face photographic images and any comparable images are considered Individually Identifiable Health Information (IIHI), therefore, appropriate safeguards must be in place to ensure the HIPAA privacy and security standards are met.

3. **PROCEDURES:**

a. Camera phones and other photographic devices should be regarded the same as cameras. The release of photographic PHI to anyone other than the individual himself is prohibited without prior authorization.

b. The use of cameras in authorized areas where patients or personnel can be caught on tape, film or other media should be prohibited without authorization of the individual(s).

c. Although patient consent is not required for personal photos taken by the patient's family and friends, camera usage should only be allowed to the extent that it medically consistent with the patient's best interests and is not disruptive to the overall care of that patient or other patients.

d. An individual can be asked to discontinue taping or photographing if deemed necessary by the staff or the patient.

## APPENDIX R

### Administrative, Physical and Technical Safeguards

1. PURPOSE: Outline the procedures and mechanisms for administrative, physical and technical safeguards to protect the privacy of protected health information.

2. POLICY:

a. MEDDAC shall reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of Section C14.3 of DoD 6025.18-R, DoD Health Information Privacy Regulation.

b. MEDDAC shall reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

3. PROCEDURES:

a. Administrative Safeguards.

(1) Role based access to PHI. Personnel will be granted access to PHI based upon their role in the care of a patient. Access to electronic PHI will be commensurate with their role.

(a) Health care providers are granted access to all PHI needed in order to provide treatment to patients.

(b) Nursing personnel are granted access to the PHI necessary to support health care providers in treating patients.

(c) Ancillary personnel (lab, x-ray, pharmacy etc.) are granted access to the PHI necessary to perform their function.

(d) Clerical and administrative personnel, such as secretaries, transcriptionists, and medical records personnel are authorized access to PHI necessary for MEDDAC to properly process and maintain information and records.

(e) Medical services account and uniform billing office personnel are granted access to the PHI necessary to perform their duties in obtaining payment for healthcare services delivered.

(f) Case managers, quality assurance personnel, credentialing personnel and resource management personnel are granted access to perform their health care operation duties.

(2) Minimum necessary standard. When using PHI in any form, release only the minimum amount of PHI necessary to accomplish the intended purpose of the use.

(3) Documents containing PHI. Documents containing PHI should be filed in medical records on a timely basis, convenience records, or authorized files. Copies of documents containing PHI should be shredded when no longer needed.

(4) Incidental disclosures. Some minimal PHI may be used or disclosed in the course of health care delivery. Examples of these uses or disclosures include: confidential conversations among health care providers or with patients when there is a possibility they may be overheard, using sign-in sheets in waiting rooms or calling patients in waiting rooms by name, using x-ray light boards. Personnel should be reminded to disclose only the minimum necessary information in circumstances such as these.

b. Physical Safeguards.

(1) Medical Records Room. Medical records rooms are designated as controlled access areas. Limit the number of personnel having combinations to the minimum necessary for efficient operations.

(2) Storage of PHI in Common Areas. File cabinets and containers should be locked when not in use. Limit the number of personnel having keys to the minimum necessary for efficient operations.

(3) Storage of PHI at reception desks and nursing stations. Medical records should not be left out and unattended. Medical records in clinics should be returned to the medical records room at the close of business each day. Convenience files in clinics should be secured in locked filing cabinets and containers when not in use.

(4) Storage of PHI in offices and examination rooms. Medical records should be returned to the medical records room at the close of business each business day. Convenience files and other PHI should be secured in locked filing cabinets and containers when not in use.

(5) Record holders outside examination rooms should be opaque and records should be placed in the holder so that the PHI may not be observed by persons walking by the examination room.

c. Technical Safeguards.

(1) Encryption of e-mail containing PHI. Email containing PHI will be transmitted within the Department of Defense only when encrypted by Common Access Card (CAC) in accordance with MEDCOM/OTSG Policy Memorandum 04-08, dated 18 June 2004, Subject: Transmission of Protected Health Information (PHI) Via Electronic-Mail (Email).

(2) Email communications with patients. Due to incompatibility of available email encryption programs between MEDDAC and the patients it serves, email will only be transmitted between health care providers and patients only after the patient has consented in writing using MEDCOM Form 756-R, Authorization to Send and Receive Medical Information by Electronic Mail. In accordance with MEDCOM Suppl 1 to AR 40-66, Medical Record Administration and Health Care Documentation, all MEDCOM Forms 756-R will be filled in the patient's medical record. No patient will be compelled to use email communications. A patient may decide to opt out of the use of clinical email at any time by informing the MEDDAC.

(3) Facsimile (FAX) Transmittal of PHI. The use of Fax machines poses certain risks of improper disclosure of PHI. Personnel are encouraged to send and receive PHI by mail whenever practical. Transmission of PHI by fax should be limited to urgent or non-urgent situations when mail or other delivery is not feasible.

(a) All fax machines shall be physically located so that it is not in an open public area, its use can be monitored, and only authorized staff can have direct access to it.

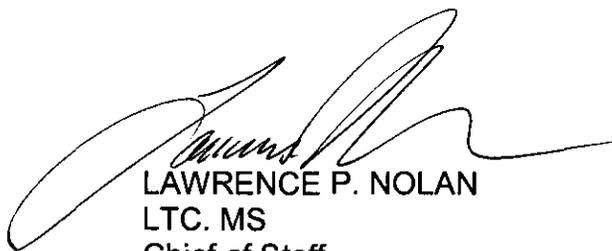
(b) Before transmitting PHI, the sender must fill out a PHI fax cover page containing the clinic identification, date and time of transmission, number of pages being transmitted (including cover page), the authorized receiver's name, address, telephone number, and fax machine number; the sender's name, provider's name, address, telephone number, and fax number, remarks or special instructions, information instructing the receiver to verify receipt of the fax, and a confidentiality statement.

(4) Control of PHI on workstations. Patient clinics are busy places, be mindful of those around the workstation and tilt screens away from prying eyes. When personnel leave their workstation unattended, they should lock the computer or log off to preserve confidentiality. Laptops and PDAs should be safeguarded to prevent theft of PHI.

(5) Password management. Sharing a password with forgetful or new personnel does no one any favors. Although they may get their work done, personnel and patients risk harm from damaged data or unauthorized disclosure. Do not write passwords down and leave them where they can be found and used by others. DoD regulations require passwords of eight or more characters that have a mixture of upper and lower case letters, numbers, and special characters. Passwords should be changed frequently.

The proponent for this publication is the HIPAA Privacy Officer. Users are invited to send comments/suggested improvements on DA Form 2028, Recommended Changes to Publications and Blank Forms, to Commander, USA MEDDAC, ATTN: MCID-IM, (HIPAA Privacy Officer), 11050 Mt Belvedere Blvd, Fort Drum, NY 13602-5004

FOR THE COMMANDER:



LAWRENCE P. NOLAN  
LTC. MS  
Chief of Staff

DISTRIBUTION:  
A