

MEDDAC/DENTAC Regulation 40-36

Medical Services

Health Information Privacy

**Headquarters
U.S. Army Medical Department Activity
Fort George G. Meade
2480 Llewellyn Avenue
Fort George G. Meade, MD 20755-5800
7 May 2004**

Unclassified

SUMMARY of CHANGE

MEDDAC/DENTAC REG 40-36
Health Information Privacy

Specifically, this revision—

- o Expands the applicability of the regulation to include all the MEDDAC's outlying clinics. For this reason, substantive changes have been made throughout.
- o Changes the Supplementation paragraph to allow outlying clinic commanders and chiefs to supplement the regulation in accordance with paragraph 1-5.
- o Adds new paragraph 1-5 which adds instructions for outlying clinic commanders and chiefs to modify certain portions of the regulation as required to make the instructions consistent with their own organizational structures. Old paragraph 1-5 was changed to 1-6.

Medical Services

Health Information Privacy

FOR THE COMMANDER:

PATRICK J. SAUER
LTC, MS
Deputy Commander for
Administration

Official:



JOHN SCHNEIDER
Adjutant

History. This is the first revision of this regulation, which was originally published on 14 April 2004.

Summary. This regulation prescribes responsibilities, policies and procedures to ensure compliance with all relevant laws and regulations when using or disclosing protected health information (PHI), in accord-

ance with Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Applicability. This regulation applies to the MEDDAC headquarters; e.g., Kimbrough Ambulatory Care Center (KACC), all of the MEDDAC's outlying clinics, the US Army Dental Activity, Fort George G. Meade Dental Clinic No. 3 and the National Security Agency's Occupational Health, Environmental Health, and Safety Service Satellite Clinic. Specifically, this regulation applies to the following groups of personnel within the organizations mentioned above: all Active Component and Reserve Component military personnel, all Department of the Army general schedule and wage grade civilians, all contract civilians, American Red Cross volunteers, and students.

Proponent. The proponent of this

regulation is the HIPAA Privacy Officer.

Supplementation. Supplementation of this regulation is not authorized only as stated in paragraph 1-5.

Suggested improvements. Users of this publication are invited to send comments and suggested improvements, by memorandum, to Commander, U.S. Army Medical Department Activity, ATTN: MCXR-PAD, Fort George G. Meade, MD 20755-5800, or to the MEDDAC's Command Editor by fax to (301) 677-8088 or e-mail to john.schneider@na.amedd.army.mil.

Distribution. Distribution of this publication is by electronic medium only.

Contents (listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Use of pronouns • 1-4, page 1

* This regulation supersedes MEDDAC/DENTAC Reg 40-36, dated 14 April 2004.

Contents–continued

Special instructions for using this regulation at the MEDDAC’s outlying MTFs • 1-5, *page 1*
Responsibilities • 1-6, *page 1*

Chapter 2

Health Information Policy and Procedures, *page 3*

Health information policy • 2-1, *page 2*
Notice of Privacy Practices (NOPP) • 2-2, *page 3*
Workforce training • 2-3, *page 3*
Use of PHI • 2-4, *page 4*
PHI disclosure procedure • 2-5, *page 4*
Business associates • 2-6, *page 4*
Patient rights • 2-7, *page 5*
Safeguarding PHI • 2-8, *page 5*
Monitoring compliance • 2-9, *page 5*
Sanctions • 2-10, *page 5*

Appendixes

- A.** References, *page 6*
- B.** Employee Training Regarding Individual Rights to PHI, *page 8*
- C.** Procedures for Assurances that Business Associates Appropriately Safeguard PHI, *page 10*
- D.** Business Associate Privacy Clause Example Template, *page 12*
- E.** Individual Rights to PHI – Request for Confidential Communication, *page 13*
- F.** Allowing Individuals Access to their PHI, *page 16*
- G.** Amendment of Medical Records, *page 18*
- H.** Individual Rights to PHI – Accounting of Disclosures, *page 19*
- I.** Individual Rights to PHI – Filing Complaints, *page 21*
- J.** Safeguards to Protecting Protected Health Information, *page 23*
- K.** Allowing Use and Disclosure of PHI Without Patient Authorization, *page 33*

Contents—continued

Figure List

Figure D-1: Business Associate Privacy Clause Example Template, *page 12*

Glossary

-R Forms

Chapter 1 Introduction

1-1. Purpose

This regulation establishes responsibilities, policies and procedures to ensure compliance with all relevant laws and regulations when using or disclosing PHI, in accordance with (IAW) Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The procedures outlined in this regulation provide the general specifications and actions required to comply with the laws and regulations governing the use and disclosure of protected health information. This document does not replicate detailed explanations of relevant standards, specifications, exclusions, or exceptions published elsewhere.

1-2. References

Required publications, related publications and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this publication are listed in the glossary.

1-4. Use of pronouns

The pronouns he, his, him and himself include she, hers, her and herself.

1-5. Special instructions for using this regulation at the MEDDAC's outlying MTFs

The complexity involved in making each paragraph within this regulation precisely applicable to the organizational structure of each of the MEDDAC's outlying medical treatment facilities (MTFs) is not practical. Outlying MTF commanders and chiefs, and their personnel utilizing the regulation, must utilize the following guidance to make this regulation applicable within their MTF:

a. *Assignment of responsibilities.*

(1) All position titles in paragraph 1-6, below, are at KACC. If an outlying MTF has a position on its staff that performs the same functions as a position title listed below, but has a different title, individual assigned to that like position will assume the responsibilities and the MTF commander or chief will ensure that that person has done so.

(2) In a case where an outlying MTF has no position on its staff that is the similar to a position title listed below (which is probably the case at the smaller MTFs), the MTF commander or chief will assign those responsibilities as he deems best.

b. The policies and procedures in chapter 2 were written to be compatible with paragraph 1-6. Therefore, at outlying MTFs where individuals have been assigned responsibilities IAW paragraph a(1) or (2), above, the policies and procedures will be complied with by those individuals.

1-6. Responsibilities

a. *The medical treatment facility (MTF) commander or chief.*

(1) The MTF commander or chief will establish and enforce policies and procedures that influence the MTF's personnel behavior and work environment consistent with privacy standards.

(2) If an MTF commander or chief is required to assign responsibilities for a particular function of this regulation IAW paragraph 1-5a, above, he will ensure his staff is aware who those responsibilities have been assigned to so that the staff can comply with the procedural guidance.

b. *The deputy commanders.* The deputy commanders will—

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

(2) Ensure subordinate staff establish and execute health information privacy safeguards as directed by this regulation and the referenced publications.

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

c. *The supporting Staff Judge Advocate (SJA).* The supporting SJA will—

(1) Provide legal interpretation and guidance related to the contents and application of this regulation 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 application of sanctions.

d. *The Inspector General (IG), Walter Reed Army Medical Center (WRAMC).* The IG, WRAMC, will conduct independent assessments on the status of compliance and effectiveness of KACC's health information privacy program.

e. *Supervisors.* Supervisors will—

(1) Periodically, at least annually, conduct risk assessments.

(2) Consistently monitor internal policies, procedures, mechanisms and behavior trends to ensure compliance with the provisions of this regulation and the referenced laws and regulations.

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

(4) Enforce the use of the Patient Affairs Section, Patient Administration Division (PAD), as the sole authority and clearinghouse for release of PHI, except for treatment, payment, and health care operations (TPO).

f. *The Chief, PAD.* The Chief, PAD will persistently promulgate the mission and responsibility of the Patient Affairs Section as the sole authority and clearinghouse for release of PHI, except for accomplishment of TPO.

g. *The Chief, Plans, Training, Mobilization, Security and Education Division (PTMS&E).* The Chief, PTMS&E will enforce, track and report the status of workforce training on health information privacy standards.

h. *The Chief, Human Resources Division (HRD).* The Chief HRD will—

(1) Execute assigned privacy functions as directed in this regulation.

(2) Promulgate the duty requirements and personnel management implications of the Department of Defense (DoD) Health Information Privacy Regulation (DoD 6025.18-R) and governing laws to local labor organizations, bargaining units, union officials and other appropriate personnel or entities.

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

i. *The Chief, Resource Management Branch (RMB).* The Chief, RMB will establish in-

ternal controls to ensure and monitor all business agreements, contracts, memoranda of understanding, and other affiliations involving the use of PHI (except TPO) are established in writing and incorporate appropriate terminology to ensure the protection of patient privacy.

j. *The HIPAA Privacy Officer.* The HIPAA Privacy Officer will—

- (1) Serve as proponent of this regulation.
- (2) Provide program oversight IAW his assigned duties and responsibilities.
- (3) Conduct designated privacy functions as directed by this regulation.
- (4) Obtain, develop, distribute and post educational materials in the most strategic locations throughout the medical treatment facility to maximize patient and community awareness of health information privacy standards.

Chapter 2

Health Information Policy and Procedures

2-1. Health information policy

All staff will—

- a. Protect patient confidentiality and maintain integrity and security during the collection, aggregation, analysis, storage, and/or destruction of PHI.
- b. Establish systems and mechanisms to safeguard patient privacy without disrupting the provision or quality of health care.
- c. Enforce the rights of patients with respect to health information privacy.
- d. Designate appropriate representatives to carry out privacy functions IAW applicable Federal and State laws and regulations.
- e. Incorporate parameters to monitor and improve compliance with health information privacy standards in the design and execution of KACC's organizational compliance program.

2-2. Notice of Privacy Practices (NOPP)

All patients will be provided a copy of, or have ready access to, the Military Health System's (MHS's) official NOPP. The MHS NOPP provides a comprehensive description of the MTF's probable uses and disclosures of PHI, legal duties, and patients' rights with respect to PHI. As patients access care and services at the MTF, designated staff will make every attempt to request patients' written acknowledgement to receipt of the NOPP. The NOPP statement is available in ten different languages and can be made available in any of these upon request.

2-3. Workforce training

The success of the 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 for protection of health information. All MEDDAC workforce members will follow the procedures outlined in appendix B to complete initial and annual refresher health information privacy standards training. In accordance with the HIPAA law, additional training may be required periodically, as may be necessitated by changes to either the HIPAA law or the DoD regulation. Required training includes web-based program modules covering health information privacy laws and all applicable MEDDAC policies and procedures for using and/or disclosing PHI, as related to employees' job

functions and other responsibilities.

2-4. Use of PHI

All workforce members will be familiar with the type of information protected under the laws and regulations referenced in this regulation. 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 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.

2-5. PHI disclosure procedure

MEDDAC employees will follow the more stringent standards, under either Federal or State laws, governing disclosure of PHI. In all cases and circumstances, personnel disclosing and receiving PHI must have the authority to disclose or receive the information with respect to the individual(s) to whom the information pertains *and* for the purpose of the disclosure. Personnel will make reasonable efforts to limit disclosure of PHI to the absolute minimum necessary to accomplish the intended purpose. Disclose the least amount of data possible, only that which is needed for job-critical purposes, to the fewest people possible. When appropriate for accomplishing the intended purpose, limited data sets will be disclosed in lieu of complete record sets. When appropriate, PHI will be de-identified to meet the intended purpose.

2-6. Business associates

The success of the 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 requirements to protect patient privacy. MEDDAC personnel will establish, in writing (that is, by contract, memorandum of understanding (MOU), or memorandum of agreement (MOA)), an acknowledgement with all business associates involving the exposure to or use of PHI, except for activities qualifying as TPO, of the requirement to adhere to the principles and processes for ensuring the protection of health information. All relevant business agreements involving PHI will include required terms to define the MTF's responsibilities for protecting patient privacy and the obligation of the MTF's business associates to accept and execute the same responsibilities in the handling of PHI. The agreements will 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; and (3) help the MTF comply with its duties under the prevailing laws. The guidelines at appendix C outline the requirements for establishing business associate agreements that involve contact, use, or disclosure of PHI. All MTF activities will provide the RMB (or equivalent office), and/or the contracting office, copies of any external agreements, such as contracts, MOUs and MOAs, for their review. RMB (or equivalent) and contracting agents will ensure that all of the respective documents include language similar to that provided at appendix C. This requirement is effective immediately and applies to all agreements executed subsequent to 1 October 2003. All agreements made prior to 1 October 2003 must include the required language at the time of the next renewal, but not later than 14 April 2004. Agreements made before 1 October 2003 should either be re-accomplished early with the

appropriate language or should be amended to include acknowledgement of the business associate requirements for PHI.

2-7. Patient rights

All personnel will adhere to the procedures established to facilitate the rights of individuals regarding their PHI. These rights and corresponding procedures include—

- a. The right to adequate notice of the uses and disclosures of PHI made by MEDDAC personnel. (See appendix C.)
- b. The right to request, but not necessarily to be granted, restrictions on the use and disclosure of PHI. (See appendix D.)
- c. The right to request, but not necessarily to be granted, confidential communications by alternative means or at an alternative location. (See appendix E.)
- d. The right to access their PHI. (See appendix F.)
- e. The right to amend their PHI. (See appendix G.)
- f. The right to an accounting of certain disclosures of PHI. (See appendix H.)
- g. The right to complain to the MTF commander and to the Department of Health and Human Services (HHS) of any violations of privacy rights. (See appendix I.)

2-8. Safeguarding PHI

The procedures at appendix J provide guidelines for appropriate administrative, technical, and physical safeguards of PHI from intentional or unintentional use or disclosures that are contrary to privacy standards.

2-9. Monitoring compliance

The tasks and responsibilities of the privacy functions outlined in this regulation are incorporated in the Organizational Inspections Program. As outlined in the procedures, designated organizational elements will maintain required documentation and files to show compliance with applicable privacy functions. The goals of the MEDDAC's health information privacy program are to achieve 100 percent workforce training annually, and to have no substantiated complaints related to health information privacy. All MEDDAC employees are responsible to make individual contributions to the successful achievements of these goals through diligent compliance with all standards and procedures.

2-10. Sanctions

Personnel who fail to comply with KACC's privacy policies and procedures, as stated within this regulation, are subject to appropriate sanctions and corrective actions. Appendix K outlines the sanctions policy.

Appendix A References

Section I Required Publications

AR 40-66
Medical Record Administration and Health Care Documentation. (Cited in appendix F, para F-1 and appendix K, para K-3.)

AR 190-45
Law Enforcement Reporting. (Cited in appendix K, para K-3.)

Section II Referenced Publications

45 Code of Federal Regulations, Part 164
Privacy, Final Rule

AR 11-9
The Army Radiation Safety Program

AR 25-11
Record Communications and the Privacy Communications System

AR 25-55
The Department of the Army Freedom of Information Act Program

AR 27-20
Claims

AR 40-1
Composition, Mission, and Functions of the Army Medical Department

AR 40-2
Army Medical Treatment Facilities General Administration

AR 40-3
Medical, Dental, and Veterinary Care

AR 40-5
Preventive Medicine

AR 40-7
Use of Investigational Drugs and Devices in Humans and the Use of Schedule I Controlled Drug Substances

AR 40-13
Medical Support – Nuclear/Chemical Accidents and Incidents

AR 40-31
Armed Forces Institute of Pathology and Armed Forces Histopathology Centers

AR 40-38
Clinical Investigation Program

AR 40-48
Nonphysician Health Care Providers

AR 40-57
Armed Forces Medical Examiner System

AR 40-68
Quality Assurance Administration

AR 40-400
Patient Administration

AR 50-5
Nuclear Surety

AR 50-6
Chemical Surety

AR 321-1
Training of Military Personnel at Civilian Institutions

AR 340-21
The Army Privacy Program

AR 351-1
Individual Military Education and Training

AR 351-3
Professional Education and Training Programs of the Army Medical Department

AR 600-8-1
Army Casualty Operations/Assistance/Insurance

AR 600-85
Army Substance Abuse Program

AR 601-141
US Army Health Professions Scholarship Program

AR 601-210
Regular Army and Army Reserve Enlistment Program, 28 February 1995.

AR 608-18
The Army Family Advocacy Program, 1 September 1995.

AR 608-75
Exceptional Family Member Program, 29 May 2000.

DoD Directive 2310-1
DoD Program for Enemy Prisoners of War (POW) and other detainees

DoD 6025.18-R
DoD Health Information Privacy Regulation

Public Law 104-91
The Health Insurance Portability and Accountability Act of 1996

Section III
Prescribed Forms

MEDDAC Form 776-R
Record of Review of Request for Alternate Communication of Protected Health Information. (Prescribed in appendix E, para E-4.)

Section IV
Referenced Forms

DA Form 4254
Request for Private Medical Information

DA Form 7490
Exceptional Family Member Medical and Educational Summary

DD Form 1144
Support Agreement

MEDDAC Overprint 410
Quality Assurance/Risk Management Document for HIPAA Events

Appendix B

Employee Training Regarding Individual Rights to PHI

B-1. Purpose

The MEDDAC recognizes that individual rights are a critical aspect of maintaining quality health 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 MEDDAC employees will receive appropriate training regarding employee and organizational responsibilities to the rights of individuals to access their PHI.

B-2. Policy

a. All MEDDAC employees will be trained on the policies and procedures regarding individual rights. These policies pertain to the use of, disclosure of, and access to individuals PHI.

b. Training will occur upon initial employment and thereafter during annual Computer-Based Annual Training (CBAT), if required (or other method of training out outlying MTFs where CBAT is not available).

B-3. Procedure

a. All employees, regardless of grade, position, or whether they are civilian or military, will meet with the HIPAA Privacy Officer during in-processing and out-processing.

b. HIPAA compliance training.

(1) At KACC, the HIPAA Privacy Officer will advise new personnel that HIPAA compliance training will be conducted using the Tricare Management Agency's web-based training tool, which can be accessed from KACC's intranet home page by clicking on the button labeled "Training," then clicking on "Web Computer-Based Training." If necessary, the HIPAA Privacy Officer will provide personnel with assistance and/or a place (and computer) to obtain the necessary training.

(2) At each outlying MTF, the HIPAA Privacy Officer will establish a similar system to KACC's, as stated in paragraph (1) above.

d. Contract employees will be required to provide proof of HIPAA compliance training, through their contract employers, prior to reporting for duty at the MTF, or arrange to obtain the required training through the MTF's HIPAA Privacy Officer as soon as possible after beginning work at the MTF.

e. Employee training regarding individuals rights to the use of, disclosure of, and access to their PHI will include the following:

(1) Allowing individuals to file complaints concerning the MTF's policies and procedures required by the HIPAA privacy rule, or its compliance with such policies and procedures.

(2) Allowing individuals to receive accountings of instances when their PHI have been disclosed.

(3) Allowing individuals to access, inspect, and/or obtain copies of their PHI that are maintained in designated record sets.

(4) Denying requests from individuals to access, inspect, and/or obtain copies of their PHI.

(5) Providing individuals with a written statement for the reasons of denial to inspect and copy their PHI.

(6) Allowing individuals to request confidential communications of PHI.

(7) Allowing individuals to request restriction of the uses and disclosures of their PHI.

(8) Allowing individuals to request amendment or correction of their PHI, if they believe it is erroneous or incomplete.

(9) Denying requests from individuals to amend or correct their PHI that they believe is erroneous or incomplete.

f. New employees will complete initial training within 30 days of arrival; this training may be completed as part of the newcomers' orientation training or online at the departmental level. Annual refresher training will be accomplished as part of the KACC CBAT (or CBAT equivalent at outlying MTFs). Failure to accomplish the prescribed training within the required timeframe may result in suspension of practice privileges, delay of leave or funded training, or other administrative action as appropriate and authorized by either military or civilian personnel guidelines.

Appendix C

Procedures for Assurances that Business Associates Appropriately Safeguard PHI

C-1. References

- a. DoD Regulation 6025-18-R, DoD Health Information Privacy Regulation.
- b. U.S. Army Medical Department (AMEDD) HIPAA Implementation Guide (Version 1), 6 January 2003.

C-2. Policy

a. The HIPAA Privacy Rule requires organizations that generate or maintain protected patient information to establish written privacy assurances with business associates who may be exposed to this information. The requirement for privacy assurances extends to arrangements between the MTF and other parties that are formalized as affiliation agreements, gratuitous agreements, support agreements, MOA and MOU.

(1) If all parties in the agreement are components of DoD, the agreement must annotate reference F-1a, above, as the regulatory guide for the privacy standards.

(2) If any part in the agreement is non-DoD (either intra-governmental or nongovernmental), the agreement must include explicit language assuring protection of patient information in accordance with the HIPAA Privacy Rule.

b. Implementation instructions and a sample business associate privacy clause template are provided below in paragraphs F-3 and F-4, respectively. All MEDDAC MTF agreements that require privacy assurance must be compliant no later than 14 April 2004. However, any agreement in place before 15 October 2002, but renewed or modified between 15 October 2002 and 14 April 2003, must be made compliant immediately.

C-3. Instructions for establishing agreements in compliance with the HIPAA Privacy Rule

a. The following guidelines apply *only* to agreements that involve the use or disclosure of PHI.

b. There are two essential elements of compliance for this requirement, as follows:

(1) If the agreement entails the use or disclosure of PHI, it must be in writing.

(2) The agreement must incorporate language that describes the responsibility of each party to safeguard the medical information as related to the business endeavor. That language must be provided by the party maintaining the PHI.

c. Following are examples of agreements that require a privacy clause IAW the HIPAA Privacy Rule:

(1) *Training agreements.*

(a) Gratuitous agreements, medical training agreements, and educational service agreements (that is, for AMEDD personnel who train at civilian institutions). In these types of agreements, the AMEDD organization is the business associate who must provide assurance, as directed by the civilian institution, to protect patient information generated or maintained at the civilian institution. It is therefore incumbent upon the civilian institution to provide its own approved privacy clause for incorporation in the agreement.

(b) Affiliation agreements (that is, non-DoD personnel from civilian institutions

who train at AMEDD organizations). All affiliation agreements will be developed by the sponsoring AMEDD organization and must include a privacy clause, assuring that trainees from affiliated civilian institutions who train in AMEDD facilities will comply with privacy standards.

(2) *MOU, MOA, interservice support agreements, interagency agreements, and support agreements on DD Form 1144 (Support Agreement)*. Specifically, when these agreements include a non-DoD party, the party that maintains the PHI is responsible for incorporating language in the agreement assuring that all parties will comply with privacy standards, as required by law.

d. The privacy template language contained in appendix G may be used in the agreements listed above. (The recommended and preferred way to meet the requirement is by inserting the specified privacy clause in any new or revised agreement. An alternate but less preferred method is to add the privacy clause in a separate addendum to the agreement, should amending an existing agreement not be deemed in the best interest of the Army. If an addendum is added, annotate the original agreement to reflect establishment of the addendum.) All existing agreements that require privacy assurance must be compliant NLT 14 April 2004. Furthermore, any agreement in place before 15 October 2002, and renewed or modified before 14 April 2004, must be made privacy compliant immediately.

Appendix D

Business Associate Privacy Clause Example Template

1. The special terms used in this section shall have the same meaning as those terms in 45 C.F.R. 160 and/or DoD 6025-18-R.
2. **Obligations and activities of the Business Associate.** The Business Associate:
 - a. Will not use or disclose Protected Health Information other than as permitted or required by agreement or law.
 - b. Will use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this agreement (specify type of agreement such as Memorandum of Agreement, Affiliation Agreement, etc.).
 - c. Will report to the sponsoring Army Medical Department organization (Covered Entity) any use or disclosure of the Protected Health Information not provided for by this agreement.
 - d. Will mitigate, as practicable, any harmful effect known to the Business Associate of use or disclosure of Protected Health Information by the Business Associate in violation of the requirements of this agreement.
3. Except as otherwise limited in this agreement, the Business Associate:
 - a. May use or disclose Protected Health Information to perform functions or services for, or on behalf of, Covered Entity as specified in this agreement, provided that such use or disclosure would not violate the Privacy Rule if done by the Covered Entity.
 - b. May use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
 - c. May disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the other party to the agreement, 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 other party, and that the other party notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
4. **Obligations of the Covered Entity.** The Covered Entity:
 - a. Upon request shall provide the Business Associate with the notice of privacy practices that the Covered Entity produces, as well as any changes to such notice.
 - b. Shall provide the Business Associate with any changes in, or revocation of, permission by individual to use or disclose Protected Health Information, if such changes affect the Business Associate's permitted or required uses and disclosures.
 - c. Shall notify the Business Associate of any restriction to the use or disclosure of Protected Health Information that the Covered Entity has agreed to IAW 45 C.F.R. 164.522.

Figure D-1
Example template of a business associate privacy clause

Appendix E

Individual Rights to PHI – Request for Confidential Communication

E-1. Purpose

To outline procedures for processing patient requests to receive communication of their PHI by alternate means.

E-2. References

- a. AR 40-66, Medical Record Administration and Health Care Documentation
- b. DoD 6025.18-R, DoD Health Information Privacy Regulation.

E-3. Policy

a. The MEDDAC is committed to ensure that individuals can receive communications regarding their PHI by a means and in a location that they believe is safe will protect the PHI from unauthorized use or disclosure.

b. The MEDDAC will permit individuals to request to receive communication of their PHI at alternative locations or by a means that is different from normal or usual procedures. All such requests must be in writing. Similarly, a written response will be made to each request received.

c. The MEDDAC is not required to honor an individual's request for alternate communications. However, KACC will make every effort to accommodate reasonable requests for alternate means of communication or alternate locations, especially when the disclosure of all or part of the PHI could endanger the individual. If applicable, the request for confidential communication of PHI will clearly state that the disclosure of all or part of the PHI could endanger the individual.

d. Requests for a confidential or alternate communication that, in the opinion of the MTF's approving authority, presents no danger to the individual, is unreasonable, or will jeopardize the MTF's standard of health care, regulatory payment procedures, and health care operations will not be honored.

e. When appropriate, the MTF will 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.

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

g. Upon agreeing to a request for alternate communication, MTF staff will deliver the PHI as agreed. If an individual wishes to terminate the receipt of PHI by the alternate means before the requested end date, he must do so in writing.

h. The HIPAA Privacy Officer is the reviewing authority for all such requests. The Deputy Commander for Administration and the Deputy Commander for Clinical Services are the approving authorities.

E-4. Responsibilities

- a. *The HIPAA Privacy Officer.* The HIPAA Privacy Officer will—
 - (1) Receive and process all requests for confidential or alternate means of communi-

cation.

(2) Instruct the requester to complete MEDDAC Form 766 (Temp) (Request to Restrict Medical or Dental Information). Ensure the requester prints “Alternate communication request” in the Purpose of Restrictions block in the Restrictions section. MEDDAC Form 766 (Temp) may be printed from the Electronic Forms page of the Staff Interest section of the MEDDAC’s internet web site.

(a) Ensure the requester clearly indicates, in writing, if the normal disclosure of all or part of his PHI could endanger him.

(b) Ensure the individual clearly understands the pre-conditions and indicates in writing how payment associated with the PHI, if any, will be handled, and specification of an alternative address or other method of contact for processing payment.

(3) Use MEDDAC Form 776-R (Record of Review for Alternate Communication of Protected Health Information) document the processing for each request. Consult the activity responsible for carrying out the proposed change in communication. Ensure the responsible activity outlines its ability to support and manage the alternate communication, including impact on current operations based on available resources (for example, staffing, funding, administrative, logistical, and legal). MEDDAC Form 776-R may be printed (or copied) from the –R Forms section at the back of this regulation or from the Electronic Forms section of the MEDDAC internet web site.

(4) If necessary, consult with the MTF’s legal advisor in SJA and prepare a recommendation for a deputy commander’s approval on MEDDAC Form 776-R.

(5) Use the standard letter format prescribed by AR 25-50 to prepare responses to all requests, whether approved and disapproved (denied).

(6) If the request is approved, forward the approved alternate communication request packet (MEDDAC Form 776-R and the reply letter) to the department chief (that is, the chief of the clinical department, PAD, Managed Care Branch, the Clinical Administrator, or other) responsible for making the alternate communication.

(7) Receive and forward all patient written requests to terminate the alternate communication to the department chief responsible for making the communication.

(8) File and maintain all confidential communication requests and their disposition (approved and disapproved) for a period of at least 6 years from the date the reply letter was sent to patient, or end of alternate communication means, whichever is later. Confidential communication request files must include MEDDAC Form 766 (Temp), MEDDAC Form 776-R, a copy of the reply to the requester, and, if applicable, the department making the communication.

b. *The responsible department chief.* (Within this regulation, the term “department chief” refers to the chief of any organizational element within the MTF that will be responsible for communicating the PHI to the requester). The responsible department chief will—

(1) Upon notification by the HIPAA Privacy Officer, outline the feasibility of making the requested alternate communication on MEDDAC Form 776-R.

(2) Recommend approval of the request if the usual means for communication of PHI will endanger the individual, or if approval will not jeopardize TPO (see paragraph E-3, above), and the required operational adjustments can be readily supported and managed with available resources. Otherwise, recommend disapproval.

(3) Upon agreeing to deliver PHI by alternate communication, deliver the requested

PHI to the individual in a secure and confidential manner whereby the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.

(4) Establish the required controls (for example, training of personnel, conspicuously marked files, and suspense files) to monitor the appropriate delivery of PHI by agreed means until the specified end date established on MEDDAC Form 766 (Temp), or earlier termination date if such was established in writing by the requester.

(5) Appropriately document, file and maintain all requests and records of delivery of alternately communicated PHI for a period of at least 6 years from the end date.

(6) Knowledge of a violation or potential violation of the policy established by this appendix must be reported directly to the HIPAA Privacy Officer.

Appendix F

Allowing Individuals Access to their PHI

F-1. Purpose

The 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, the 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 AR 40-66 and this regulation in responding to an individual's request for access to protected health information.

F-2. References

- a. AR 40-66, Medical Record Administration and Health Care Documentation.
- b. DoD 6025.18-R, DoD Health Information Privacy Regulation.

F-3. Policy

- a. The MTF will take necessary steps to address individuals' requests to access, inspect, and/or obtain copies of their PHI, that is maintained in a designated record set, in a timely and professional manner.
- b. The MTF will adhere to the provisions of AR 40-66 and this regulation in providing individuals access, inspection, and/or copies of their PHI.
- c. In the event that the MTF must extend the time period for responding to a request, the procedure in paragraph F-4, below, will be followed.

F-4. Procedures

- a. When a request for access to PHI is received by an MTF from an individual, the medical record technician (MRT) in Patient Affairs Section, PAD, 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. If a request for access to PHI is received from an individual and that information is not information that is not maintained at the MTF nor accessible by the MTF, the Patient Affairs MRT will act on the individual's request for an accounting not later than 60 days after receipt of the request.
- c. If the time period for the action must be extended, the Patient Affairs MRT will, within the time allowed by paragraph a, above, provide the individual a written statement of the reasons for the delay and the new completion date. (Such extensions will be limited to one per case and will not exceed 30 days.)
- d. Only Medical Records Section personnel who possess appropriate access clearance will access the individual's PHI, using proper access and authorization procedures.

e. Knowledge of a violation or potential violation of the policy established by this appendix will be reported directly to the Chief, PAD and/or the HIPAA Privacy Officer.

Appendix G

Amendment of Medical Records

G-1. References

- a. AR 40-66, Medical Record Administration and Health Care Documentation.
- b. AR 340-21, The Army Privacy Program.
- c. DoD 6025.18-R, DoD Health Information Privacy Regulation.

G-2. Policy

In accordance with current privacy laws and reference documents, individuals have a right to request amendment to their medical records when they believe that there is an error or omission in the respective documentation. While the MHS will accept requests for amendments to health care records, it is not required to agree to the amendment. The MTF may act as the initial recipient and evaluator of a patient request for an amendment of medical records, but final review authority is deferred to the U. S. Army Medical Command (MEDCOM) and approval/disapproval authority is retained by the Privacy Act Officer, Office of The Surgeon General (OTSG), who also retains the authority to review and approve or disapprove all appeals of adverse determinations.

G-3. Procedure for requesting amendment of a medical record

The following procedure describes the process by which a patient may request an amendment to his medical record.

- a. The patient must submit his complaints, if any, and requests for amendment to the Chief, PAD in writing (that is, in a signed letter). The patient should address why he wants information expunged, corrected or added.
- b. The Chief, PAD, will forward the patient's request to the Chief, PAD (MCHO-CL-P), in the office of the Assistant Chief of Staff for Health Policy and Services, MEDCOM, as an enclosure to a memorandum. The chief will include his recommendation and address any provider reluctance to remove information (for example: because it is factual or the events actually happened as recorded). The chief will also include copies of the applicable documents from the patient's medical record as an enclosure to the memorandum.
- c. The MEDCOM PAD will then forward the action to the Privacy Act Officer at OTSG, Records Management Branch (SGPS-AOR), with a copy of the action furnished to OTSG-PAD.
- d. After consulting the appropriate physician consultants and MEDCOM PAD, the OTSG Privacy Act Officer will make an initial decision, which will be given to the Chief, PAD at KACC.
- e. If the patient receives a denial, he has 60 days to write to OTSG to appeal the decision. The appeal will be addressed to HQDA (SGPS-AOR), 5109 Leesburg Pike, 5 Skyline Plaza, Falls Church, and VA 22041-3258.
- f. The OTSG Privacy Act Officer will then prepare a packet for the Department of the Army Privacy Review Board.

Appendix H

Individual Rights to PHI – Accounting of Disclosures

H-1. Purpose

To outline procedures to address the accounting for instances when PHI has been used or disclosed for purposes other than TPO.

H-2. References

- a. AR 40-66, Medical Records Administration and Health Care Administration.
- b. DoD 6025.18-R, DoD Health Information Privacy Regulation.

H-3. Policy

a. IAW current privacy laws and reference documents, individuals have a right to receive an accounting of various instances when PHI concerning them is disclosed, except as noted in paragraph d, below.

b. The Patient Affairs Section in PAD is the only office authorized to release PHI to persons other than the individual to whom the information pertains, except when the release is to carry out TPO.

c. IAW the privacy standards, individuals will be allowed to receive an accounting of all instances where PHI about them is used or disclosed. If requested, individuals will also receive an accounting of disclosures made to or by business associates of the MTF.

d. Individuals will not receive an accounting of instances where PHI about them is used or disclosed for the following purposes:

- (1) To carry out TPO.
- (2) To the individuals of PHI about them.
- (3) For the MTF's patient directory.
- (4) To persons involved in the individual's care or other notification purposes.
- (5) For official military operations, national security or intelligence purposes.
- (6) To correctional institutions or for law enforcement custodial situations.

e. Individuals may request up to a 6-year accounting of disclosures made on or after 14 April 2003. Accountings of disclosures made prior to 14 April 2003, will be provided IAW the guidance contained in AR 40-66.

H-4. Procedure

a. The Patient Affairs Section MRT will—

(1) Utilize the MedRec Millennium/Correspondence Management 9.0 or an equivalent software, or a manual process for documenting and maintaining an accounting of when patients' PHI has been disclosed for purposes other than TPO.

(2) Ensure each accounting of a disclosure includes the following information:

- (a) The date of disclosure.
- (b) The name of the entity or person who received the PHI and, if known, the address of that entity or person.
- (c) A brief description of the PHI disclosed.
- (d) A brief statement of the purpose for the disclosure that reasonably informs the

individual of the basis for the disclosure, or, in lieu of such statement—

1 A copy of the individual's written authorization to use or disclose the protected health information, or

2 A copy of a written request for a disclosure required by the Secretary of the Department of Health and Human Services (HHS) to investigate or otherwise determine the MTF's compliance with applicable laws and regulations.

(3) Within 60 days of the request date, provide a written accounting of instances when the requester's PHI was disclosed.

(4) In the event that an extension is required, provide the requester, not later than 60 days after receipt of the request, a written statement of the reasons for the delay and the date by which the Patient Affairs Section MRT will provide the accounting. The MRT will not extend the time to provide the accounting more than once or longer than 30 days. Therefore, when an extension is required, all accountings will be processed and issued to requester no later than 90 days from date of request.

(5) Not charge the requester for the first accounting in any 12-month period. Any fee imposed for each subsequent request for an accounting by the same individual within the 12-month period will be charged based on cost-based guidance.

(6) Upon imposing a fee, inform the requester in advance of the fee and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(7) Document and retain the following for a period of at least 6 years from the date accounting is issued to a requester.

(a) The information required to be included in an accounting.

(b) The written accounting that is provided to the individual.

(c) The name of Patient Affairs Section MRT responsible for receiving and processing requests for accounting by individuals.

b. The Chief, PAD, will enforce and monitor compliance with this appendix.

Appendix I

Individual Rights to PHI – Filing Complaints

I-1. Purpose

To outline the procedures and mechanism for receiving complaints from individuals regarding the MTF's compliance with the requirement of the privacy standards.

I-2. References

- a. 45 C.F.R. 164.530(d), 164.520(b)(1)(vi), and 9160.306.
- b. DoD 6025.18-R, DoD Health Information Privacy Regulation.

I-3. Policy

a. As specified in the reference publications, the MTF will accept and process complaints concerning internal policies and procedures regarding the use or disclosure of PHI and/or compliance with such policies and procedures.

b. Individuals may file complaints, which must be submitted in writing, when they have reason to believe that any of the following circumstances have occurred with regard to their PHI—

- (1) That the PHI has been improperly used or disclosed.
- (2) That an MTF employee has improperly handled the information.
- (3) That they have wrongfully been denied access to, or an opportunity to amend, the information.
- (4) That the entity's notice does not accurately reflect its information practices.

c. The HIPAA Privacy Officer is the primary point of contact for individuals to file complaints pursuant to this policy. The Chief, PAD, is the alternate point of contact and will assume this responsibility whenever the HIPAA Privacy Officer is scheduled to be absent for seven days or more following receipt of a complaint.

d. As stated in the NOPP, individuals may also complain to HHS if they believe their privacy rights have been violated. Procedures below explain how individuals should file complaints with HHS.

e. All members of the MTF's workforce are prohibited from retaliating against individuals who file complaints, and from requiring individuals to waive their rights to file complaints with HHS as a condition of the provision of treatment, payment, enrollment, or eligibility for medical benefits.

I-4. Procedure

a. *Filing complaints with the MTF.* The HIPAA Privacy Officer or the Chief, PAD (serving as the alternate during the HIPAA Privacy Officer's absence IAW paragraph I-3c, above), will—

(1) Accept all written complaints concerning internal policies and procedures regarding the use or disclosure of PHI. If the complaint is received from the HIPAA e-mail portal, a confirmation e-mail will be returned to acknowledge receipt of the complaint. Hand-delivered or mailed complaints will also be acknowledged in writing.

(2) Discuss the case with the complainant if necessary to clarify the basis of the com-

plaint.

(3) Present the case and the plan for inquiry to the Deputy Commander for Administration (DCA) and legal counsel for approval.

(4) Investigate all pertinent matters of the complaint per the DCA's and/or legal counsel's guidance to determine if there was in fact a privacy violation. If the complaint appears to indicate a violation of the Privacy Rule, initiate a MEDDAC Overprint 410 (Quality Assurance/Risk Management Document for HIPAA Events) and submit it to the Quality Improvement/Risk Manager, then investigate the complaint in cooperation with the Quality Improvement/Risk Manager, legal counsel, and DCA.

(5) Document all findings and present them to the legal counsel and DCA for review and determination of applicable sanctions.

(6) Immediately inform MEDCOM of the complaint, with copies to NARMC Clinical Operations, Building 1, Room A-126, at WRAMC.

(7) If a complaint is validated and/or a privacy violation is confirmed, institute corrective actions to prevent recurrence.

(8) Prepare a written response to the complainant.

(9) Submit a monthly report of complaints received and investigative findings to the MISRT and the Executive Committee.

(10) File and maintain all complaints received, and their dispositions, for a period of at least 6 years from the date of final reply to the patient or closure of case, whichever is later. Complaint files must include the following documentation, as applicable:

(a) The complaint.

(b) The findings of the investigation.

(c) Disposition.

(d) Sanctions applied.

(e) A copy of the reply to the complainant.

b. *Filing Complaints with HHS*. If an individual chooses to file a complaint with HHS, he must—

(1) Contact the Office for Civil Rights (OCR) by one of the following methods:

(a) Internet web site: <http://www.hhs.gov/OCR/hipaa>.

(b) E-mail: OCR@ed.gov

(c) Telephone: 1-800-421-3481

(d) Fax: 202-205-9862

(e) Mailing: US Department of Health and Human Services
Office for Civil Rights - HIPAA
200 Independence Avenue, SW
Washington, DC 20201

(2) File the complaint in writing, either on paper or electronically.

(3) Name the entity (or person) that is the subject of the complaint and describe the actions that have allegedly been violations of the privacy standards.

(4) File the complaint within 180 days of the (the complainant) knew or should have known that the violation occurred.

Appendix J Safeguards to Protecting Protected Health Information

J-1. Purpose

To outline the standards for appropriate administrative, technical and physical safeguards to protect the privacy of PHI at MEDDAC MTFs.

J-2. References

- a. 45 C.F.R. Part 164.
- b. AR 25-55, Army Freedom of Information Act (FOIA) Program.
- c. AR 40-66, Medical Record Administration and Health Care Documentation.
- d. AR 340-21, The Army Privacy Program.
- e. DoD 6025.18-R, DoD Health Information Privacy Regulation.

J-3. The NOPP, policy on disclosure of PHI, and patient authorizations

The MTFs personnel will strive to maintain 100 percent accountability and security of all of its beneficiary's medical records. All medical records will be filed, maintained, accessed and requested IAW AR 40-66. As a general rule, the MTF must know the purpose and audience for every use and disclosure of PHI.

a. The NOPP.

(1) *General.* The NOPP informs patients what KACC will, and will not, do with their PHI IAW the HIPAA law. Specifically, it informs patients that KACC—

- (a) Will do its best to keep their PHI confidential.
- (b) Will use their PHI internally and share it with insurers only as needed for treatment and payment operations.
- (c) Will not send their PHI outside of the core provider and insurer business without a written authorization from the patient.

(2) *Patient rights.* The NOPP informs patients of their rights to—

- (a) Request restrictions on release of their PHI.
- (b) Receive confidential communications concerning their PHI.
- (c) Inspect and copy their medical records.
- (d) Amend their medical records.
- (e) Receive an accounting of any external releases of their PHI.
- (f) Obtain a paper copy of the NOPP on request.
- (g) File a complaint against the MTF, the MEDDAC, or the Government concerning violations of their patient privacy rights.

(3) *Acknowledgement of receipt of the NOPP.* New patients will be given a copy of the NOPP when they are initially encountered, which is usually when they present at an MTF office or clinic, or a registration area, and will be asked to sign an acknowledgment that they have received this notice. (Some MTFs also have the patient sign a consent, which is a written agreement to allow the MTF to use the patient's PHI in day-to-day business; however, this is not required by HIPAA.) The first employee to encounter a patient on behalf of KACC should ensure that the person has received and acknowledged KACC's NOPP. If a patient has not received this document, the employee must arrange for him to get one. If a patient has a question

or concern about how their health information is being handled, the MTF employee should start with the basic agreements about privacy that are detailed in the NOPP as this will answer most questions.

(4) *Direct and indirect treatment.*

(a) The HIPAA law recognizes two types of treatment relationships, direct and indirect.

1 Direct treatment is a treatment relationship between a patient and a health care provider who delivers health care directly to the patient. A pediatrician is an example of a direct relationship.

2 Indirect treatment is a treatment relationship between a patient and a health care provider in which the provider delivers health care to the patient based on the orders of another healthcare provider. The indirect healthcare provider typically provides services to another health care provider, who in turn provides the services to the patient. A radiologist is an example of an indirect relationship.

(b) Although all healthcare providers must have a NOPP available for patient review, only direct treatment providers are required to give a copy of their NOPP to their patients.

b. *PHI.*

(1) *Determining what is PHI.* See the PHI Decision Tree in appendix D, above, to determine if medical information qualifies as PHI. Only health information that identifies an individual is subject to the HIPAA Privacy Rule. Health information that can not reasonably be used to identify an individual is not subject to the Privacy Rule and can be freely disclosed.

(2) *De-identifying health information.* Health information can be de-identified by removing certain identifiers regarding the individual and his relatives, employers, and household members. See appendix E, paragraph E-4c, for a list of these identifiers.

(3) *Verifying the requester and minimizing disclosure.*

(a) Patients are routinely notified that the MTF will use their information in day-to-day business; however, the staff needs to be careful with patients' PHI. The two key principles of being careful with health information are verifying the identity and the authority of the person who is requesting the PHI, and disclosing only the minimum necessary information.

1 Verifying identity. There are many ways to verify that people are who they say they are:

a Ask for a birth date or Social Security number.

b Ask for the mother's maiden name or some other unique information.

c Check a physical signature against a signature on file.

d Make a call-back to a known telephone number.

(b) Verifying authority. Once the identity of the requester is verified, his right to access the PHI must be verified. Routine requests from employees of any of the MEDDAC's MTFs are usually acceptable, as well as those from other MTFs within the Walter Reed Health Care System that normally work with KACC, with regard to the type of PHI that is being requested.

(c) If the requester's identity and the authority to obtain the PHI have been verified, PHI may be disclosed. Give the requester only the information that he really needs to know. Co-workers will usually only ask for what they need. Unusual requests from individuals

you don't know are risky. Limit the information you give out—no more than exactly what they are authorized to receive!

(d) Be very careful with patients' health information. Patients expect that we will protect their information from anyone who does not need to know it, including the MTF's own employees.

(e) The MTF has specific policies and procedures to help its employees decide how to make or request disclosures in their daily work. It is each employee's responsibility to know the policies that apply to him.

(f) Any employee who is in doubt about releasing PHI to a requestor, for whatever reason, should consult his supervisor or the HIPAA Privacy Officer for assistance.

c. *Uses and disclosures.* The minimum necessary disclosure standard is a basic principle of privacy. The MTF's employees should see only the very least amount of a patient's PHI that is necessary to do their job.

d. *New privacy rights.* Under HIPAA, patients have more rights to access and control their PHI than they had in the past. One of these new rights permits the individual to request an accounting of most disclosures of PHI other than routine TPO. To provide these accountings, lists of such disclosures must be maintained. Audit trails in information systems are the best way to track disclosures of PHI. They monitor and track access to PHI and report on all viewing, uses, and disclosures of an individual's PHI.

e. *Damage Control.* The MTF is committed to ensuring that individuals are not harmed by the unauthorized disclosure of their PHI. Any employee who learns, or suspects, that PHI has been released outside of routine business functions, without authorization, will inform his supervisor or the HIPAA Privacy Officer. By law, the MTF is required to mitigate the effects of all unauthorized releases of PHI.

f. *Authorizations.*

(1) After patients have been provided a copy of the NOPP, the MTF is permitted to use their PHI for TPO, provided care is exercised by using the verify requester and the minimum necessary disclosure principles. (See paragraph b(3), above.) Disclosures of PHI other than for routine TPO generally require written authorization. An authorization is a very specific document for a very specific disclosure of PHI. There is no such thing as a "blanket authorization" that allows the MTF to make unspecified types of disclosures and/or for indefinite periods.

(2) Following are examples of situations requiring authorization from a patient:

(a) To release PHI to a life and casualty insurance company in order to obtain disability coverage.

(b) Requested by a physician for a patient to authorize disclosure of his PHI to a pharmaceutical company that is planning a drug trial.

(c) For a pregnant woman to authorize her pregnancy status to be released to a business that markets infant care products.

(3) Following are examples of situations that do not require authorization on the part of the patient for his PHI to be released:

(a) *Required by law.* To be used or disclosed if law or regulation requires the use or disclosure.

(b) *Public health.* To—

1 Prevent or control disease, injury, or disability.

- 2 Report births and deaths.
 - 3 Report child abuse or neglect.
 - 4 Report reactions to medications or problems with products.
 - 5 Notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.
 - 6 Notify the appropriate government authority if it is believed a patient has been the victim of abuse, neglect or domestic violence.
- (c) *Communicable diseases*. May be disclosed, if authorized by law, to a person who might have been exposed to a communicable disease or might otherwise be at risk of contracting or spreading a disease or condition.
- (d) *Health oversight*. May be disclosed to a health oversight agency for activities authorized by law, such as audits, investigations and inspections. These health oversight agencies might include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and civil rights laws.
- (e) *Food and Drug Administration (FDA)*. May be disclosed to a person or company required by the FDA to do the following:
- 1 Report adverse events, product defects, or problems with biologic product deviations.
 - 2 Track products.
 - 3 Enable product recalls.
 - 4 Make repairs or replacements.
 - 5 Conduct post-marketing surveillance as required.
- (f) *Legal proceedings*. May be disclosed during any judicial or administrative proceedings, in response to a court order or administrative tribunal (if such disclosure is expressly authorized), and in certain conditions in response to a subpoena, discovery request, or other lawful process.
- (g) *Law enforcement*. May be disclosed for law enforcement purposes, including the following:
- 1 Responses to legal proceedings.
 - 2 Information requests for identification and location.
 - 3 Circumstances pertaining to victims of a crime.
 - 4 Deaths suspected from criminal conduct.
 - 5 Crimes occurring at an MTF site.
 - 6 Medical emergencies (not on the MTF premises) believed to result from criminal conduct.
- (h) *Coroners, funeral directors, and organ donations*. May be disclosed to coroners or medical examiners for identification to determine the cause of death or for the performance of other duties authorized by law. May also be disclosed to funeral directors as authorized by law, and may be used and disclosed for cadaveric organ, eye, or tissue donations.
- (i) *Research*. May be disclosed to researchers when authorized by law (for example, if their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of PHI.)
- (j) *Criminal activity*. Under applicable Federal and state laws, PHI may be disclosed if it is believed that its use or disclosure is necessary to prevent or lessen a serious and

imminent threat to the health or safety of a person or the public. PHI may also be disclosed if it is necessary for law enforcement authorities to identify or apprehend an individual.

(k) *Military activity and national security.*

1 When the appropriate conditions apply, PHI of individuals who are Armed Forces personnel may be disclosed—

a For activities believed necessary by appropriate military command authorities to ensure the proper execution of the military mission including determination of fitness for duty.

b For determination by the Department of Veteran Affairs for an individual's eligibility for benefits.

c To a foreign military authority if the individual is a member of that foreign military service.

2 With regard to anyone, not only personnel of the Armed Forces, to authorized Federal officials for conducting national security and intelligence activities including protective services to the President and others.

(l) *Workers' compensation.* May be disclosed to comply with workers compensation laws and other similar legally established programs.

(m) *Inmates.* May be used or disclosed for individuals who are inmates of correctional facilities and a military MTF created or received the individual's PHI while provide him care. This disclosure would be necessary for—

1 The correctional institution to provide medical care to the individual.

2 The health and safety of the individual or others.

3 The safety and security of the correctional institution.

(n) *Parental access.* Some state laws concerning minors permit or require disclosure of PHI to parents, guardians, and persons acting in a similar legal status. KACC will act consistent with Maryland law in this regard, which is that teenagers have the right to withhold information from their parents concerning treatment for drugs, alcohol, and sex (for example, birth control pills and pregnancy tests). In some instances, a child as young as 10 years may qualify as a teenager under this Maryland law. If in doubt, contact the HIPAA Privacy Officer for a determination.

(4) There are many reasons for disclosures of PHI outside the normal course of TPO. Some of these disclosures are at the request of the patient while others are at the MTF's request or the request of a third party.

g. *For the patient's use.* Patients often request their PHI to be disclosed to a third party for their own purposes. Examples include, to—

(1) Another insurance company for a different type of coverage.

(2) A government agency conducting suitability investigations.

(3) A prospective employer for a job in which health is an important issue.

(4) A patient's attorney for evaluation of an injury claim.

h. *For KACC's use.* Sometimes the MTF requires a patient's authorization to disclose his PHI for the MTF's benefit. For example, to use the PHI for marketing purposes, published studies, or research.

i. *Before treatment.*

(1) Generally, a patient cannot be required to provide an authorization prior to treatment being provided; however, there are certain exceptions to this rule in which the provision of

treatment may be conditional upon the prior authorization to disclose PHI. For example, prior authorization may be required if—

(a) The treatment is research related.

(b) The health care being provided is solely for the purpose of creating PHI for disclosure to a third party, such as a disability rating examination.

(2) Prior authorization cannot be requested from the patient for the disclosure of psychotherapy notes before treatment is provided.

j. *For research purposes.* Using PHI for research is a complex topic. In general, if PHI is created solely for the purpose of research, authorization must be obtained from the patient for disclosure of that PHI.

k. *For psychotherapy notes.* In most cases, HIPAA requires a patient's authorization before using or disclosing psychotherapy notes.

(1) Psychotherapy notes means anything that a mental health professional records in any medium. It could be documentation or analysis of the content of conversation in a private or family counseling session that is separate from the rest of the patient's medical record.

(2) Authorization for use of psychotherapy notes is not required in the following circumstances:

(a) For use by the originator of psychotherapy notes for treatment.

(b) For use or disclosure by the MTF in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling.

(c) For use or disclosure by the MTF to defend a legal action or other proceeding brought by the patient.

l. *Defective authorizations.* An authorization is considered defective if—

(1) The expiration date has passed or the staff knows the expiration event has passed.

(2) The authorization has not been completely filled out.

(3) The authorization has been revoked by the patient.

(4) The authorization contains any information known or later discovered to be false.

(5) The authorization is a prohibited compound authorization.

m. *Revocation of an authorization.* A patient may revoke an authorization at any time by providing the revocation in writing, except when—

(1) Action has already been taken IAW the provisions of the authorization; however, no further action will be taken following receipt of the written revocation.

(2) The authorization was required by an insurance company as a condition for obtaining insurance coverage.

J-4. Policy for ensuring the privacy and security of PHI

a. The MTF is committed to ensuring the privacy and security of PHI. To support this commitment, the MTF will ensure that the appropriate steps are taken to properly identify and secure patients' PHI, as required under 45 C.F.R. Part 164, and other applicable Federal, State, and/or local laws and regulations.

b. As stated above in paragraph 1-5f, within KACC, the Chief, PAD, is the sole authority for the release of PHI, except for TPO.

c. PHI is individually identifiable health information. This information includes demo-

graphics (for example, age, address, e-mail address), and relates to an individual's past, present or future physical or mental health or condition and related health care services.

d. Routine health information meeting the above definition will be automatically designated as PHI immediately upon its creation, or receipt by the MTF.

e. The MTF's employees will adhere to all applicable laws, regulations, policies and procedures when maintaining, using, and disclosing PHI.

f. The MTF's employees will follow proper procedures to ensure that only the minimum amount PHI, necessary to accomplish the specific purpose of a use or disclosure, is actually used or disclosed, and that only what is minimally needed to accomplish the specific purpose of the request is disclosed.

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

- (1) Disclosure to or requests by a provider for treatment.
- (2) Uses and disclosures made to the individual who is the subject of the information.
- (3) Uses and disclosures pursuant to an authorization by the individual concerned.
- (4) Disclosures made to the HHS.
- (5) Uses and disclosures required by law.
- (6) Uses and disclosures required for compliance with applicable laws and regulations.

h. Health care organizations are permitted to create and use de-identified PHI under certain conditions.

(1) MTF employees may create de-identified information for the following purposes:

- (a) Data quality review.
- (b) Research.

(2) MTF employees may strip the individual identifying elements of PHI.

(3) MTF employees 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 other than the specified re-identification.

(4) De-identified information will not be disclosed if those MTF employees creating or disclosing the information, or any other employees of the MTF, 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.

i. Health care organizations are permitted to create and use a limited data sets under certain conditions. The MTF may use PHI to create limited data sets, and may disclose PHI to business associates to create limited data sets for the following purposes:

- (1) Research.
- (2) Public health.
- (3) Health care operations.

j. KACC will enter into a data use agreement that meets the requirements of 45 C.F.R. §164.514(e) with any proposed recipient of a limited data set, before disclosing any information contained in such limited data set to the recipient. If MTF employees have knowledge that a limited data set recipient has breached or violated a data use agreement, the MTF will take steps to cure the breach or end the violation, and, in the event such actions are unsuccessful, the MTF will discontinue disclosure of PHI to the recipient and report the problem to HHS.

k. If the MTF is the recipient of a limited data set, the MTF will enter into and comply with the terms of a data use agreement consistent with the policies and procedures herein.

l. The MTF may use or disclose PHI for certain purposes without the written authorization of the individual, provided the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure IAW the applicable requirements of HIPAA.

m. In the event of a discrepancy, the following persons, respectively, will be responsible for designating routine health information as PHI:

- (1) The Chief, PAD.
- (2) The Chief, Department of Primary Care.
- (3) The HIPAA Privacy Officer.

n. All proposed uses or disclosures of patient health information will be reviewed by persons having an understanding of the MTF's patient privacy policies and practices, and sufficient expertise to understand and weigh the necessary factors.

o. MTF employees 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.

p. Access to PHI will be reasonably limited by utilizing CHCS1 and applicable patient administration regulations and policies.

q. The following criteria will be used to limit the amount of PHI requested and disclosed by MTF employees:

- (1) Does the individual requesting the disclosure have a complete understanding of the purpose for the use or disclosure of the PHI?

- (2) Are all of the entities and/or individuals identified for whom the requested use or disclosure of the PHI is required?

r. Requests for disclosure of PHI will be reviewed on an individual basis IAW the criteria listed in this appendix.

s. MTF employees may reasonably rely on requests from the following entities to accurately determine the minimum necessary information they will need disclosed to them:

- (1) Public health and law enforcement agencies.
- (2) Other covered entities.

- (3) A professional who is an MTF employee, or is a business associate of the MTF, for the purpose of providing professional services to the MTF, if the professional represents that the information requested is the minimum necessary for the stated purpose.

t. For disclosures for research purposes, MTF employees will review the documentation of required Institutional Review Board or other approval to determining the minimum amount of PHI necessary.

u. MTF employees will make decisions as to whether PHI should be de-identified or if a limited data set should be created for disclosure. If it is decided to create a limited data set in lieu of releasing de-identified PHI, the reason will be documented and maintained.

v. The following individually identifying elements may be removed or otherwise concealed from PHI in order to create de-identified information and/or limited data set:

- (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.
 - (f) All elements of dates (including year) indicative of age 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 and license numbers.
 - (11) Vehicle identifiers and serial numbers, including license plate numbers.
 - (12) Device identifiers and serial numbers.
 - (13) URLs.
 - (14) IP address numbers.
 - (15) Biometric identifiers, such as fingerprints and voiceprints.
 - (16) Full-face photographic images and comparable images.
 - (17) All geographic subdivisions smaller than a state, including—
 - (a) Street address.
 - (b) City.
 - (c) County.
 - (d) Precinct.
 - (e) 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 MTF personnel 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, and
 - (b) The initial three digits of the Zip codes for all such geographic units containing 20,000 or fewer people is changed to 000.
- w. The following process will be used for purposes of removing identifying elements from PHI:
- (1) Depending on the identifying elements, MTF employees must substitute integers for the identifying elements to be used in creating the de-identified information.
 - (2) The legend of integers and the PHI they represent must be kept separate from the de-identified information.
- x. Whenever any of identifiers listed paragraph v, above, are not removed from PHI for disclosure purposes, the PHI will only be disclosed after the MTF employee determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a

subject of the information. The employee will document the methods and results of the analysis that justify such determination.

y. 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.

z. The MTF will comply with all HIPAA regulations and policies in determining what information to include in a limited data set.

aa. Data use agreements, which may be in the form of a formal contract, will not authorize limited data set recipients to use or further disclose PHI in a manner that is inconsistent with the requirements of 45 C.F.R. Part 164, if done by the covered entity.

bb. Data use agreements established between the MTF and limited data set recipients will establish the following:

(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.

cc. Data use agreements between the MTF and limited data set recipients will provide the MTF with adequate assurances that the recipients of limited data sets 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 tertiary 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 MTF in a timely manner.

dd. In situations where an individual is incapacitated or in emergency treatment circumstances the MTF will use or disclose the individual's PHI only IAW—

(1) A prior expressed preference (if any is known), or

(2) The individual's best interest, as determined by the designated health care provider in the exercise of his professional judgment.

ee. Knowledge of a violation or potential violation of this policy must be reported directly to the HIPAA Privacy Officer or the Risk Manager.

Appendix K Allowing Use and Disclosure of PHI Without Patient Authorization

K-1. Purpose

To describe local policies for allowing the use and disclosure of PHI without patient authorization.

K-2. References

- a. AR 40-66, Medical Record Administration and Health Care Documentation.
- b. DoD 6025.18-R, DoD Health Information Privacy Regulation.

K-3. Policy

a. The MTF retains the right to use or disclose PHI without patient authorization in a variety of circumstances. (See appendix J, paragraph J-3f(3), above, for a complete list.)

b. All MTF employees involved with the maintenance and disclosure of health care records and PHI will be familiar with the procedures for the use and release of PHI. These employees will receive appropriate training as described in appendix C. Release of information will be accomplished only by the Patient Affairs MRT, who will rigidly adhere to the following general guidelines for release of information without patient authorization.

(1) *Judicial and administrative releases.* The Patient Affairs MRT may disclose PHI in a judicial or administrative proceeding if the request for such information is made through or pursuant to a court order or administrative tribunal, provided that he releases *only* the PHI that expressly requested and authorized by the order. The Patient Affairs MRT may also release PHI in a judicial or administrative proceeding if the request for such information is made in response to a subpoena, discovery request, or other lawful process. The following additional considerations must be satisfied:

- (a) If a subpoena, it is signed by a judge or Federal magistrate.
- (b) Written evidence must be submitted by the party requesting the PHI, indicating that reasonable attempts have been made to the respective individual, to whom the information pertains, to provide the information.
- (c) Written evidence must be provided, indicating that the individual to whom the information pertains has been given the opportunity to object and that the time period for objection has expired.

(d) All other required administrative remedies or protections have been applied.

(2) *Health oversight releases.* The Patient Affairs MRT may disclose PHI for conducting or supervising health oversight activities. These include audits (civil, administrative and criminal investigations); licensure or disciplinary actions; civil, administrative, and criminal proceedings or actions; and other activities necessary for appropriate oversight of the health care system, of Government benefit programs for which health information is relevant to beneficiary eligibility, and of Government regulatory programs for which health information is necessary for determining compliance with program standards. The following additional considerations must be satisfied:

- (a) Oversight activities may not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other

activity does not arise out of and is not directly related to the receipt of health care; a claim or public health benefits related to health; or qualifications for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) *Research releases.* Individual authorization is not required for release of PHI for research purposes, if the Patient Affairs MRT has obtained documentation that an alteration to, or waiver, in whole or in part, of the individual's authorization for use or disclosure of PHI has been approved by either an Institutional Review Board or a Privacy Board. Specific additional guidelines for the release of PHI for research purposes is provided in appendix E, above.

(4) *Law enforcement release.* The Patient Affairs MRT may disclose PHI for law enforcement purposes to ensure that law enforcement officials can obtain the necessary information needed to investigate a crime or to allow prosecutors to determine the proper charge.

(a) DoD law enforcement officials will comply with AR 40-66 and AR 190-45, and use DA Form 4254 (Request for Private Medical Information) when they request PHI. Generally, DoD law enforcement officials must obtain patient information from the following locations within MTFs: emergency rooms, patient admissions, and wards (whenever incident occur in those places). Staff in these areas should be knowledgeable about the regulations governing information and release to law enforcement.

(b) The Patient Affairs MRT may disclose PHI to comply with a court-ordered warrant, or a subpoena or summons issued by a judge or Federal magistrate, a grand jury, or an administrative request (including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law).

(c) Requested PHI must be pursuant to an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, and the information sought must be relevant and material to a legitimate law enforcement inquiry.

(d) In cases where PHI is requested pursuant to an administrative request, authorized investigative demand, or similar process authorized under law, the request must be specific and limited in scope to the extent reasonably practical for the purpose for which the information is sought, and that de-identified information cannot be reasonably used.

(e) The Patient Affairs MRT may release following PHI to a law enforcement official in response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person:

- 1 Name and address.
- 2 Date and place of birth.
- 3 Social Security number.
- 4 ABO blood type and RH factor.
- 5 Type of injury.
- 6 Date and time of treatment.
- 7 Date and time of death, if applicable.
- 8 Description of distinguishing physical characteristics (for example, height, weight, gender, race, hair and eye color, presence and absence of facial hair, scars and tattoos).

(f) The Patient Affairs MRT *may not release* the following PHI to a law enforcement official in response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person.

- 1 An individual's DNA or DNA analysis.
- 2 Dental records.
- 3 Typing, samples or analysis of body fluids.

(g) The Patient Affairs MRT may disclose PHI concerning an individual who has died to law enforcement officials for the purpose of alerting law enforcement of the death of the individual when the Chief, PAD has reason to believe (suspicion) that the death may have resulted from criminal conduct.

(h) The Patient Affairs MRT may disclose PHI to law enforcement officials when he has good faith basis for evidence of criminal conduct occurrence on the MTF's premises.

(i) The Patient Affairs MRT may disclose PHI in response to a law enforcement official's request concerning an individual who is, or is suspected of, being victim of a crime, if the individual agrees to the disclosure, or if the individual is unable to provide agreement due to incapacity or other emergency circumstance. In such instances, law enforcement officials must provide the Patient Affairs MRT with assurance that the requested PHI will not be used against the victim, and that immediate law enforcement activity, dependent upon the requested disclosure, would be adversely affected by waiting until the individual is able and willing to provide the disclosure.

(j) In situations where he is unable to obtain the individual's agreement due to incapacity or other emergency circumstance, the Patient Affairs MRT must ensure that the disclosure is in the best interests of the individual.

(5) *Public health release.* The Patient Affairs MRT may use or disclose PHI without patient authorization for public health authorities for the full range of public health activities carried out by Federal, State and local public health authorities. The following additional information is provided:

(a) The Patient Affairs MRT may disclosed PHI to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, including but not limited to the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or at the direction of a public health authority to an official of a foreign government agency that is acting in collaboration with a public health authority.

(b) The Patient Affairs MRT may disclose PHI to a public health authority or other appropriate government authority that is authorized by law to receive reports of child abuse or neglect.

(c) The Patient Affairs MRT may disclose PHI to agents of the FDA to collect or report adverse events (or similar activities with respect to food or dietary supplements); product defects or problems (including problems with the use or labeling of a product or biological product deviations); to track products; to enable product recalls, repairs or replacement; look back (that is, locating and notifying individuals who have received products that have been recalled, withdrawn, or the subject of look back); and to conduct post-marketing surveillance.

(d) The Patient Affairs MRT may disclose PHI to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

(e) The Patient Affairs MRT may disclose PHI to an employer concerning an individual who is a member of the workforce of that employer, if the PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance, or if the employer needs such findings in order to comply with its obligations under 29 C.F.R. parts 1904 through 1928, 30 C.F.R. parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance.

(f) As a public health authority in itself, the MTF is permitted to use or disclose PHI in all cases in which it is permitted to disclose such information to outside public health activities.

(6) *Aversion of threats to health and safety.* Consistent with applicable law and standards of ethical conduct, the MTF is permitted to disclose PHI based on a reasonable belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Such disclosures may be made only to persons who are reasonably able to prevent or lessen the threat, including to the target of the threat. The following additional considerations must be satisfied.

(a) The Patient Affairs MRT may use, or disclose PHI to law enforcement authorities, when necessary to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the Chief, PAD reasonably believes may have caused serious physical harm to the victim; or when necessary to identify or apprehend an individual where it appears that the individual has escaped from a correctional institution or from lawful custody.

(b) The Patient Affairs MRT *may not use or disclose* PHI necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the Chief, PAD reasonably believes may have caused serious harm to the victim if such admission in participation is learned by the Chief, PAD or the Patient Affairs MRT, in the course of treatment, to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy.

(c) When the Patient Affairs MRT uses or discloses PHI believed necessary for law enforcement authorities to identify or apprehend an individual pursuant to a statement by another individual admitting participation in a violent crime that is believed to have caused serious physical harm to a victim, such PHI will contain only that specific statement, and may contain only the following PHI:

- 1 Name and address.
- 2 Date and place of birth.
- 3 Social Security number.
- 4 ABO blood type and RH factor.
- 5 Type of injury.
- 6 Date and time of treatment.
- 7 Date and time of death, if applicable.
- 8 Description of distinguishing physical characteristics (for example, height, weight, gender, race, hair and eye color, presence and absence of facial hair, scars and tattoos).

(d) When the Patient Affairs MRT uses or discloses PHI necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or public, which is being

given to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat, or is necessary for law enforcement authorities to identify or apprehend an individual, the MRT must act only upon actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(7) *Cadaveric organ, eye or tissue donation.* The Patient Affairs MRT may use and disclose PHI without patient authorization to organ procurement organizations or other entities engaged in the procurement, banking, or transportation of cadaveric organs, eyes, or tissue for donation and transportation.

(8) *Decedents.* The Patient Affairs MRT may disclose PHI concerning decedents to coroners and medical examiners and to funeral directors to carry out their professional duties, as necessary and consistent with applicable laws. The MRT may disclose PHI about a deceased person, without authorization, to coroners and medical examiners for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law, and to funeral directors to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the MRT may disclose PHI prior to, and in reasonable anticipation of, the individual's death.

(9) *Workers' compensation.* The Patient Affairs MRT may use or disclose PHI as authorized by and to comply with laws relating to workers' compensation or other similar programs established by law, that provide benefits for work-related injuries or illness without regard to fault.

(10) *Victims of abuse, neglect or domestic violence.* The Patient Affairs MRT may exercise professional judgment in conjunction with applicable statutes or regulations when disclosing PHI about an individual to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence. The following additional considerations must be satisfied:

(a) The Patient Affairs MRT may disclose PHI concerning an individual whom the MTF reasonably believes to be the victim of abuse, neglect or domestic violence to the types of agencies listed in paragraph (10), above, provided that one of the following three criteria is met:

1 To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law.

2 If the individual agrees to the disclosure.

3 To the extent the disclosure is expressly authorized by statute or regulation.

(b) If the Patient Affairs MRT discloses PHI concerning an individual who is reasonably believed to be a victim of abuse, neglect, or domestic violence to any type of agency listed above in paragraph (10), above, IAW with laws or regulations, the disclosure must be based upon professional judgment that the disclosure is necessary to prevent serious harm to the individual or other potential victim(s). If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report must state that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(c) In all cases, the Patient Affairs MRT promptly notify the individual concerned that a disclosure report has been made; however, the MRT may refrain from promptly

notifying the individual that a disclosure of his PHI has been made or will be made to any of the above activities if, in the exercise of professional judgment, the MTF believes that informing the individual would place him at risk of serious harm, or if his personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in his best interests, as determined by the MTF's health care providers and the Chief, PAD in the exercise of their professional judgment.

(c) The MTF is required to report child abuse or neglect without restriction to public health authorities, other appropriate government authorities, and required military authorities who are authorized by law to receive reports of child abuse or neglect.

(11) *Specialized government functions.* The Patient Affairs MRT is authorized to use or disclose PHI without individual authorization for a number of specialized government functions, including treatment of foreign military and diplomatic personnel and their dependents who receive health care provided by, or paid for by, the DoD or other Federal agency, or by an entity acting on its behalf pursuant to a country-to-country agreement or Federal statute. The following additional specific considerations are provided:

(a) The Patient Affairs MRT may disclose PHI without individual authorization for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission if the appropriate military authority has published by notice in the Federal Register the appropriate military command authorities and purposes for which the PHI may be used or disclosed. (See DoD 6025.18-R, Section 7.11.)

(b) The Patient Affairs MRT may disclose PHI of foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for U. S. Armed Services personnel.

(c) The Patient Affairs MRT may disclose PHI to authorized Federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401 et seq) and implementing authority (that is, Executive Order 12333).

(d) The Patient Affairs MRT may disclose PHI to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3506, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(e) The Patient Affairs MRT may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual PHI about such inmate or individual, if the correctional institution or law enforcement official represents that such PHI is necessary for the provision of health care to such individuals; or is necessary for the health and safety of such individuals or other inmates; or is necessary for the health and safety of the officers or employees or of others at the correctional institution; or is necessary for the health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution to a, facility or setting to another; or is necessary for law enforcement on the premises of the correctional institution; or is necessary for the administration and maintenance of the safety, security, and good order of the correctional institution.

(f) The Patient Affairs MRT may disclose to the VA the PHI of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by VA of the individual's eligibility for or

entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(12) *As required by law.* Other laws may require uses or disclosures of PHI for purposes not captured by the other provisions of HIPAA or DoD 6025.18-R. The Patient Affairs MRT may make uses and disclosures of PHI as required by such other laws, provided that the requirements governing the use and disclosure of PHI are more restrictive than those described by HIPAA or the DoD guidance. When other laws conflict with those described under HIPAA or DoD 6025.18-R, the more stringent law applies.

(13) *Treatment.* KACC will use and disclose your PHI to provide, coordinate, or manage a patient's health care and any related services. In emergencies, the MTF will use and disclose a patient's PHI so that required treatment can be provided.

(14) *Payment.* As needed, the MTF will use a patient's PHI to obtain payment for his health care services from third party payers, such as insurance companies.

(15) *Health care operations.* As needed, the MTF may use or disclose a patient's PHI for activities such as but not limited to quality assessment activities, investigations, oversight or staff performance reviews, training of medical students, licensing, communications about a product or service, and conducting or arranging for other health care-related activities.

Glossary

Section I Abbreviations

AMEDD

U.S. Army Medical
Department

AR

Army regulation

CBAT

computer-based annual
training

C.F.R.

Code of Federal Regulations

CHAMPUS

Civilian Health and Medical
Program of the Uniformed
Services

DCA

Deputy Commander for
Administration

DoD

Department of Defense

FGGM

Fort George G. Meade

FDA

Food and Drug
Administration

FOIA

Freedom of Information Act

HIPAA

Health Insurance Portability
and Accountability Act

HRD

Human Resources Division

HHS

Department of Health and
Human Services

IAW

in accordance with

IG

inspector general

IP

internet provider

KACC

Kimbrough Ambulatory Care
Center

MEDCOM
U.S. Army Medical
Command

MEDDAC
U.S. Army Medical
Department Activity

MHS
Military Health System

MISRT
Medical Information Security
Readiness Team

MOA
memorandum of agreement

MOU
memorandum of
understanding

MRT
medical record technician

MTF
medical treatment facility

NOPP
Notice of Privacy Practices

OTSG
Office of The Surgeon
General

PAD
Patient Administration
Division

PHI
protected health information

PTMS&E
Plans, Training, Mobilization,

Security and Education
Division

RMB
Resource Management
Branch

SJA
staff judge advocate

TPO
treatment, payment, and
health care operations

UCMJ
Uniform Code of Military
Justice

URL
universal resource locator

U.S.C.
United States Code

WRAMC
Walter Reed Army Medical
Center

Section II Terms

Business associate

Except as provided in paragraph b, below, a business associate, with respect to a covered entity, is a person who:

a. On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the work-force of such covered

entity or arrangement, performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information or other function or activity regulated DoD 6025-18.R, or

b. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

c. A covered entity participating in an organized health care arrangement that performs a function or activity as described in paragraph a, above, for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph b, above, to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service,

become a business associate of other covered entities participating in such organized health care arrangement.

d. A covered entity may be a business associate of another covered entity. This circumstance occurs only when the covered entity is not acting as either a health plan or a provider in its dealings with the other covered entity. An example of this is CHAMPUS/Tricare relationships with some of its managed care support contractors. It does not occur when the covered entity is acting as a health plan or a provider. For example, CHAMPUS/Tricare network providers are not its business associates.

Correctional institution

Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental

institutions through the criminal justice system, witnesses, or others awaiting charges or trial. The term “correctional institution” includes military confinement facilities but does not include internment facilities for enemy prisoners of war, retained personnel, civilian detainees and other detainees provided under the provisions of DoD Directive 2310.1.

Covered functions

Those functions of a covered entity the performance of which makes the entity a health plan or health care provider.

Data aggregation

With respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such PHI by the business associate with the PHI received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set

a. A group of records maintained by or for a covered entity that is one of the following—

- (1) The medical rec-

ords and billing records about individuals maintained by or for a covered health care provider.

(2) Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan.

(3) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

b. For the purposes of this definition, the term “record” means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship

A treatment relationship between an individual and a health care provider that involves face-to-face interaction between the individual and health care provider or that otherwise is not an indirect treatment relationship.

Disclosure

The release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

Employment records

Records that include health information and are—

- a. Maintained by a com-

ponent of the DoD or other entity subject to this regulation.

b. About an individual who is (or seeks or sought to become) a member of the Uniformed Services, employee of the U.S. Government, employee of a DoD contractor, or person with a comparable relationship to the DoD.

c. Not maintained in connection with carrying out any covered function under this regulation.

Health care

Care, services, or supplies related to the health of an individual, and includes but is not limited to the following:

a. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

b. The sale or dispensing of a drug, device, equipment or other item IAW with a prescription.

Health care operations

Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

a. Conducting quality as-

essment and improvement activities, including evaluation and development of clinical guidelines outcome, if obtaining general knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

c. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care

(including stop-loss insurance and excess of loss insurance).

d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

e. Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.

f. Business management and general administrative activities of the entity, including, but not limited to:

(1) Management activities relating to implementation of and compliance with the requirements of this regulation.

(2) Customer service, provided that PHI is not disclosed except as otherwise permitted by this Regulation.

(3) Resolution of internal grievances.

(4) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity.

(5) Consistent with the applicable requirements for creating de-identified

health information or a limited data set, and fundraising for the benefit of the covered entity.

Health information

Any information, in any form or medium, that—

a. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, or school or university, and

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.

Health oversight agency

An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or Government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for

which health information is relevant. The term “health oversight agency” includes any DoD Component authorized under applicable DoD regulation to oversee the MHS, including with respect to matters of quality of care, risk management, program integrity, financial management, standards of conduct, or the effectiveness of the MHS in carrying out its mission.

Health plan

Any DoD program that provides or pays the cost of health care, unless exempted.

a. The following components of the Tricare Program are a health plan under this regulation:

(1) The program that provides health care under the authority of the Department of the Army to members of the uniformed services. (Administrator: Surgeon General of the Army.)

(2) The program that provides health care under the authority of the Department of the Navy to members of the uniformed services. (Administrator: Surgeon General of the Navy.)

(3) The program that provides health care under the authority of the Department of the Air Force to members of the uniformed services. (Administrator: Surgeon General of the Air Force.)

(4) The Supplemental

Care Program for members of the Army, Navy, Marine Corps, and Air Force who receive health care services from providers other than providers of the DoD. (Administrators: Surgeon General of the Army for members of the Army; Surgeon General of the Navy for members of the Navy and Marine Corps; Surgeon General of the Air Force for members of the Air Force.)

(5) The Tricare Prime, Tricare Extra, and Tricare Standard health care options offered under 32 C.F.R. 199.17. (Administrator: Tricare Management Activity.)

(6) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS). (Administrator: Tricare Management Activity.)

b. The following are also included as health plans:

(1) The Tricare Dental Program under 10 U.S.C. 1076a. (Administrator: Tricare Management Activity.)

(2) The Tricare Retiree Dental Program under 10 USC 1076c. (Administrator: Tricare Management Activity.)

(3) The Continued Health Care Benefit Program under 10 U.S.C. 1078a. (Administrator: Tricare Management Activity.)

(4) The Designated Provider Program under 10

U.S.C. 1073. (Administrator: Tricare Management Activity.)

(5) Programs conducted as demonstration projects under 10 U.S.C. 1092, to the extent not otherwise included under a health plan.

c. The term “health plan” excludes the following DoD programs:

(1) Although part of the Tricare Program, the programs that provide health care in medical and dental treatment facilities of the Departments of the Army, Navy, and Air Force to beneficiaries other than members of the armed forces are excluded by HHS regulations from the definition of health plan.

(2) The Women, Infants, and Children (WIC) Program.

(3) Occupational health clinics for civilian employees or contractor personnel.

(4) Any other policy, plan or program to the extent that it provides, or pays for the cost of, workers compensation benefits, liability, accident, automobile, or disability income insurance, or similar insurance coverage.

(5) Any other program whose principal purpose is other than providing or paying the cost of health care.

(6) Any other program (other than one listed in paragraphs a and b, above, whose principal activity is the

direct provision of health care to persons.

(7) Any other program whose principal activity is the making of grants to fund the direct provision of health care to persons.

Indirect treatment relationship

A relationship between an individual and a health care provider in which the health care provider delivers health care to the individual based on the orders of another health care provider, and typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual

The person who is the subject of PHI. (Under certain circumstances, rights of an individual under this regulation may be exercised by a personal representative.

Individually identifiable health information

Information that is a subset of health information, including demographic information collected from an individual, which is created or received by a health care provider, health plan, or employer and 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 identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Marketing

a. To announce a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made—

(1) To inform an individual who is a member of a uniformed service or a covered beneficiary of the MHS of benefits, services, coverage’s, limitations, costs, procedures, rights, obligations, options, and other information concerning the MHS as established by law and applicable regulations.

(2) Otherwise to describe a health related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communication about—

(a) The entities participating in a health care provider network or health plan

network.

(b) Replacement of, or enhancements to, a health plan.

(c) Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(3) For treatment of the individual.

(4) For case management or care coordination of the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

b. An arrangement between a covered entity and any other entity whereby the covered entity disclosed PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Military Health System (MHS)

All DoD health plans and all DoD health care providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by, the Tricare Management Activity, the Army, the Navy, or

the Air Force.

Required by law

A mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.

a. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a Government program providing public benefits.

b. Required by law includes any mandate contained in a DoD Regulation that requires a covered entity (or other person functioning under the authority of a covered entity) to make a use or disclosure and is enforceable in a court of law. The attribute of being enforceable in a court of law means that in a court or court-martial proceeding, a person required by

the mandate to comply would be held to have a legal duty to comply or, in the case of noncompliance, to have had a legal duty to have complied. Required by law also includes any DoD regulation requiring the production of information necessary to establish eligibility for reimbursement or coverage under CHAMPUS/Tricare.

Research

A systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to general knowledge.

State

One of the following:

a. For a health plan established or regulated by Federal law, state is defined in the applicable section of the United States Code for such health plan.

b. For all other purposes, state is defined as any of the several states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Transaction

The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

a. Health care claims or

equivalent encounter information.

b. Health care payment and remittance advice.

c. Coordination of benefits.

d. Health care claim status.

e. Enrollment and disenrollment in a health plan.

f. Eligibility for a health plan.

g. Health plan premium payments.

h. Referral certification and authorization.

i. First report of injury.

j. Health claims attachments.

k. Other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation.

Treatment

The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use

With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce

Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

