



HEALTH AFFAIRS

THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D. C. 20301-1200

AS

RECEIVED

02:17:13 PM 4/25

SPEAKER'S CLERK  
U.S. HOUSE OF REPS.

APR 24 2003

T 02424

The Honorable J. Dennis Hastert  
Speaker of the House of Representatives  
Washington, DC 20510-6050

MAY 12 2003

Dear Mr. Speaker:

I am pleased to provide you this final report on the development and implementation of regulations to improve privacy protections of medical records held by the Department of Defense (DoD), as required by Section 756 of the National Defense Authorization Act for Fiscal Year 2001.

The Act required the submission to Congress of a comprehensive plan to improve privacy protections for medical records maintained by DoD. DoD's plan is also consistent with the regulations promulgated under section 264(c) issued by the Secretary of the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The law further directed that, notwithstanding any other law, DoD issue interim regulations pending full implementation of the comprehensive plan, to improve privacy protections. By statutory specification, the interim regulations are to provide maximum protections for privacy consistent with actions necessary for purposes of national security, law enforcement, patient treatment, public health reporting, accreditation and licensure review activities, external peer review and other quality assurance program activities, fraud and abuse prevention, and other purposes. The recognition of the need to use medical information for these purposes is a critically important feature of this statute.

DoD's interim regulations to improve privacy protections for DoD medical records were signed on October 30, 2000. Work on the comprehensive plan required by the statute was delayed by the HHS review to determine the finality of the HIPAA regulations issued December 28, 2000. An interim report submitted on March 11, 2002 explained that the report was delayed because the HIPAA Privacy Rule had not been finalized by HHS. On April 14, 2001, HHS announced that the Privacy Rule would take effect with a full compliance date of April 14, 2003.

DoD's comprehensive plan consists of the following:

During the spring and summer of 2001, DoD began the work to analyze the components of the Privacy rule and develop the necessary implementing regulation. At the same time, resources were identified and assigned within the Army, Navy, Air Force and Coast Guard to begin the identification of Service specific requirements. Throughout the course of DoD's processes to establish these privacy protections, we have included the uniformed services in each decision evolution. Uniformed service representatives

were included in the selection of web based tools designed to train the work force and implement the policy requirements at treatment facilities. Service involvement has been crucial to the effectiveness of the program implementation.

DoD has established, under the authority of the Assistant Secretary of Defense (Health Affairs), a permanent, full time Privacy Officer position to ensure long term continuity of privacy protections of DoD and its components. This incumbent will serve as DoD's liaison for implementation of subsequent changes between HHS and DoD's treatment facilities. DoD has begun development of additional Privacy Officer training to meet the needs presented by our ever mobile workforce.

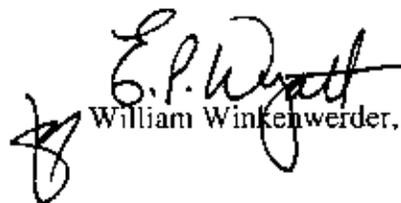
An aggressive briefing schedule has been in place since spring 2002. We continue to brief audiences ranging from senior DoD Service leadership to treatment facility staff.

DoD has assembled long term budget estimates from all uniformed services and included those figures in the DoD Program Objective Memorandum for fiscal years 04-09. The financial support of this program in future years will be essential in the maintenance of these important privacy protections.

DoD has made a significant commitment to protect the medical records and health information it maintains. The finalized DoD Health Information Privacy Regulation is enclosed. This regulation implemented the Department of Health and Human Services Privacy Rule and was effective on April 14, 2003. The application of the policies, procedures, and requirements, along with the completion of our workforce training, will form the first stage of the program to enhance our protection of health information. Long term plans are in development and resources are available to sustain this program into the future. We are confident we will fully meet the requirements of the HIPAA Privacy Rule and protect health information entrusted to the DoD and its components.

Thank you for your interest in the Military Health System.

Sincerely,

  
William Winkenwerder, Jr., MD

Enclosure:  
As stated



DoD 6025.18-R

# DoD HEALTH INFORMATION PRIVACY REGULATION

JANUARY 2003

ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS



HEALTH AFFAIRS

THE ASSISTANT SECRETARY OF DEFENSE  
WASHINGTON, D. C. 20301-1200

JAN 24 2003

FOREWORD

This Regulation is issued under the authority of DoD Directive 6025.18, "Privacy of Individually Identifiable Health Information in DoD Health Care Programs," December 19, 2002 (reference (a)). It prescribes the uses and disclosures of protected health information.

This Regulation is based on the requirements of the Health Insurance Portability and Accountability Act, Public Law 104-191 (reference (b)). Although it covers much of the same ground as the Privacy Act of 1974 (reference (c)), this Regulation in no way impacts the need for the Department of Defense to comply with reference (c) which has been implemented within DoD by DoD 5400.11-R (reference (d)).

This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

This Regulation is effective April 14, 2003, and is mandatory for use by all the DoD Components.

Send recommended changes to this Regulation to the following address:

Director, Information Management, Technology and Reengineering  
TRICARE Management Activity  
Skyline Five, Suite 810, 5111 Leesburg Pike  
Falls Church, Virginia 22041-3206

The DoD Components may obtain copies of this Regulation through their own publications channels. Approved for public release; distribution unlimited. Authorized registered users may obtain copies of the publication from the Defense Technical Information Center, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218. Other Federal Agencies and the public may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161. Copies are also available via the World Wide Web at: <http://www.dtic.mil/wha/directives>.

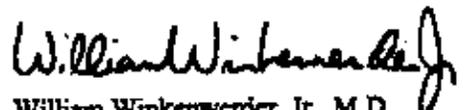
  
William Winkenwerder, Jr., M.D.  
Assistant Secretary of Defense  
(Health Affairs)

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD	2
TABLE OF CONTENTS	3
REFERENCES	7
DEFINITIONS	9
CHAPTER 1 - AUTHORITIES IN GENERAL	23
C1.1. GENERAL PROVISIONS	23
C1.2. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION	24
C1.3. SPECIAL RULES AND OTHER REQUIREMENTS RELATING TO USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION	25
C1.4. OBLIGATIONS OF THE MHS TO FULFILL RIGHTS OF INDIVIDUALS CONCERNING PROTECTED HEALTH INFORMATION	26
C1.5. ADDITIONAL ADMINISTRATIVE REQUIREMENTS FOR THE MHS TO IMPLEMENT HEALTH INFORMATION PRIVACY PROTECTIONS	27
C1.6. COMPLIANCE DATE	28
CHAPTER 2 - APPLICABILITY, SCOPE, ENFORCEMENT, AND RELATIONSHIP TO OTHER LAWS	29
C2.1. APPLICABILITY	29
C2.2. NON-APPLICABILITY	29
C2.3. INSPECTOR GENERAL	30
C2.4. PREEMPTION OF STATE LAW	30
C2.5. COMPLIANCE AND ENFORCEMENT BY THE SECRETARY OF HHS	31
C2.6. RELATIONSHIP TO PRIVACY ACT	33
C2.7. NO PRIVATE CAUSE OF ACTION	33
C2.8. RELATIONSHIP TO FREEDOM OF INFORMATION ACT	34
CHAPTER 3 - ORGANIZATIONAL RESPONSIBILITIES WITHIN THE MILITARY HEALTH SYSTEM UNDER THIS REGULATION	35
C3.1. PURPOSE	35
C3.2. COVERED ENTITIES IN THE MHS	35
C3.3. THE MHS AND ORGANIZED HEALTHCARE ARRANGEMENTS	36
C3.4. BUSINESS ASSOCIATE ARRANGEMENTS AMONG AND FOR THE DoD	38
COMPONENTS	
C3.5. REQUIREMENTS FOR A COVERED ENTITY WITH MULTIPLE COVERED FUNCTIONS	40

TABLE OF CONTENTS-Continued

	<u>Page</u>
CHAPTER 4 - USES OR DISCLOSURES TO CARRY OUT TREATMENT, PAYMENT AND HEALTHCARE OPERATIONS	42
C4.1. STANDARD: & PERMITTED USES AND DISCLOSURES	42
C4.2. IMPLEMENTATION SPECIFICATIONS: TREATMENT, PAYMENT, AND HEALTHCARE OPERATIONS	42
CHAPTER 5 - USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION IS REQUIRED	44
C5.1. STANDARD: AUTHORIZATION FOR USES AND DISCLOSURES	44
C5.2. IMPLEMENTATION SPECIFICATIONS: GENERAL REQUIREMENTS	45
C5.3. IMPLEMENTATION SPECIFICATIONS: CORE ELEMENTS AND REQUIREMENTS	48
C5.4. AUTHORIZATION REQUIRED UNDER SPECIAL RULES FOR ALCOHOL AND DRUG ABUSE PROGRAM PATIENT RECORDS	49
CHAPTER 6 - USES AND DISCLOSURES REQUIRING AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR TO OBJECT	50
C6.1. STANDARD: USE AND DISCLOSURE FOR FACILITY DIRECTORIES	50
C6.2. STANDARD: USES AND DISCLOSURES FOR INVOLVEMENT IN THE INDIVIDUAL'S CARE AND NOTIFICATION PURPOSES	51
CHAPTER 7 - USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED	54
C7.1. STANDARD: USES AND DISCLOSURES REQUIRED BY LAW	54
C7.2. STANDARD: USES AND DISCLOSURE FOR PUBLIC HEALTH ACTIVITIES	54
C7.3. STANDARD: DISCLOSURES ABOUT VICTIMS OF ABUSE, NEGLECT, OR DOMESTIC VIOLENCE	56
C7.4. STANDARD: USES AND DISCLOSURES FOR HEALTH OVERSIGHT ACTIVITIES	57
C7.5. STANDARD: DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS	59
C7.6. STANDARD: DISCLOSURES FOR LAW ENFORCEMENT PURPOSES	61
C7.7. STANDARD: USES AND DISCLOSURES ABOUT DECEDENTS	65
C7.8. STANDARD: USES AND DISCLOSURES FOR CADAVERIC ORGAN, EYE OR TISSUE DONATION PURPOSES	65
C7.9. STANDARD: USES AND DISCLOSURES FOR RESEARCH INVOLVING MINIMAL RISK	65
C7.10. STANDARD: USES AND DISCLOSURES TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY	68
C7.11. STANDARD: USES AND DISCLOSURES FOR SPECIALIZED GOVERNMENT FUNCTIONS	69
C7.12. STANDARD: DISCLOSURES FOR WORKER'S COMPENSATION	72

TABLE OF CONTENTS-Continued

	<u>Page</u>
CHAPTER 8 - SPECIAL RULES AND OTHER REQUIREMENTS RELATING TO USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION	73
C8.1. DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION	73
C8.2. MINIMUM NECESSARY RULE	75
C8.3. LIMITED DATA SET	78
C8.4. INCIDENTAL USES AND DISCLOSURES RULE	80
C8.5. STANDARD: DISCLOSURE TO BUSINESS ASSOCIATES	82
C8.6. STANDARD: DISCLOSURES BY WHISTLEBLOWERS AND WORKFORCE MEMBER CRIME VICTIMS	82
C8.7. PERSONAL REPRESENTATIVES	83
C8.8. STANDARD: DECEASED INDIVIDUALS	85
C8.9. SPECIAL RULES FOR ALCOHOL AND DRUG ABUSE PROGRAM PATIENT RECORDS	85
CHAPTER 9 - NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION	87
C9.1. STANDARD: NOTICE OF PRIVACY PRACTICE	87
C9.2. IMPLEMENTATION SPECIFICATIONS: CONTENT OF NOTICE	87
C9.3. IMPLEMENTATION SPECIFICATIONS: PROVISIONS OF NOTICE	87
C9.4. IMPLEMENTATION SPECIFICATIONS: JOINT NOTICE BY SEPARATE COVERED ENTITIES	89
C9.5. IMPLEMENTATION SPECIFICATIONS: DOCUMENTATION	90
CHAPTER 10 - RIGHTS TO REQUEST PRIVACY PROTECTION FOR PROTECTED HEALTH INFORMATION	91
C10.1. RIGHT TO REQUEST RESTRICTION	91
C10.2. RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS	93
CHAPTER 11 - ACCESS OF INDIVIDUALS TO PROTECTED HEALTH INFORMATION	94
C11.1. STANDARD: ACCESS TO PROTECTED HEALTH INFORMATION	94
C11.2. IMPLEMENTATION SPECIFICATIONS: REQUESTS FOR ACCESS AND TIMELY ACTION	96
C11.3. IMPLEMENTATION SPECIFICATIONS: PROVISION OF ACCESS	97
C11.4. IMPLEMENTATION SPECIFICATIONS: DENIAL OF ACCESS	98
C11.5. IMPLEMENTATION SPECIFICATIONS: DOCUMENTATION	99

TABLE OF CONTENTS-Continued

	<u>Page</u>
CHAPTER 12 - AMENDMENT OF PROTECTED HEALTH INFORMATION	101
C12.1. STANDARD: RIGHT TO AMEND	101
C12.2. IMPLEMENTATION SPECIFICATIONS: REQUESTS FOR AMENDMENT AND TIMELY ACTION	101
C12.3. IMPLEMENTATION SPECIFICATIONS: ACCEPTING THE AMENDMENT	102
C12.4. IMPLEMENTATION SPECIFICATIONS: DENYING THE AMENDMENT	103
C12.5. IMPLEMENTATION SPECIFICATIONS: ACTIONS ON NOTICES OF AMFNDMENT	104
C12.6. IMPLEMENTATION SPECIFICATIONS: DOCUMENTATION	105
C12.7. RELATIONSHIP TO PRIVACY ACT	105
CHAPTER 13 - ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION	106
C13.1. STANDARD: RIGHT TO AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION	106
C13.2. IMPLEMENTATION SPECIFICATIONS: CONTENT OF ACCOUNTING	107
C13.3. IMPLEMENTATION SPECIFICATIONS: PROVISION OF ACCOUNTING	109
C13.4. IMPLEMENTATION SPECIFICATIONS: DOCUMENTATION	109
C13.5. RELATIONSHIP TO PRIVACY ACT	110
CHAPTER 14 - ADMINISTRATIVE REQUIREMENTS, TRANSITION PROVISIONS, AND COMPLIANCE DATES	111
C14.1. PERSONNEL DESIGNATIONS	111
C14.2. TRAINING	111
C14.3. SAFEGUARDS	112
C14.4. COMPLAINTS	112
C14.5. SANCTIONS	113
C14.6. STANDARD: MITIGATION	113
C14.7. STANDARD: REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS	113
C14.8. STANDARD: WAIVER OF RIGHTS	114
C14.9. POLICIES AND PROCEDURES	114
C14.10. DOCUMENTATION	116
C14.11. STANDARD: EFFECT OF PRIOR AUTHORIZATIONS	116
C14.12. STANDARD: EFFECT OF PRIOR CONTRACTS OR OTHER ARRANGEMENTS WITH BUSINESS ASSOCIATES	117
C14.13. COMPLIANCE DATE FOR IMPLEMENTATION OF PRIVACY STANDARDS	118

## REFERENCES

- (a) DoD Directive 6025.18, "Privacy of Individuals Identifiable Health Information in DoD Health Care Programs," December 19, 2002
- (b) Public Law 104-191
- (c) Section 552a of title 5, United States Code
- (d) DoD 5400.11-R, "Department of Defense Privacy Program," August 1983
- (e) DoD Directive 2310.1, "DoD Program for Enemy Prisoners of War (EPOW) and Other Detainees (Short Title: DoD Enemy POW Detainee Program)," August 18, 1994
- (f) DoD 5025.1-M, "DoD Directives System Procedures," current edition
- (g) Title 45, Code of Federal Regulations, "Public Welfare," Parts 160 - 164, current edition
- (h) Title 32, Code of Federal Regulations, "National Defense," current edition
- (i) Chapter 163 of title 10, United States Code
- (j) DoD Directive 6490.2, "Joint Medical Surveillance," August 30, 1997
- (k) DoD Directive 5136.12, "TRICARE Management Activity (TMA)," May 31, 2001
- (l) Sections 1320a-7c, 1320d - 1320d-8 of title 42, United States Code
- (m) DoD Directive 1010.1, "Military Personnel Drug Abuse Testing Program," December 9, 1994
- (n) DoD Directive 1010.9, "DoD Civilian Employee Drug Abuse Testing Program," August 23, 1988
- (o) DoD Directive 5154.24, "Armed Forces Institute of Pathology (AFIP)," October 3, 2001
- (p) Appendix of title 5, United States Code
- (q) Section 552 of title 5, United States Code
- (r) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 1998
- (s) Sections 2671 - 2680 of title 28, United States Code
- (t) Title 29, Code of Federal Regulations, "Labor," current edition
- (u) Title 30, Code of Federal Regulations, "Mineral Resources," current edition
- (v) Chapter 47 of title 10, United States Code
- (w) DoD Directive 1308.1, "DoD Physical Fitness and Body Fat Program," July 20, 1995
- (x) DoD Instruction 1332.38, "Physical Disability Evaluation," November 14, 1996
- (y) DoD Directive 5210.42, "Nuclear Weapons Personnel Reliability Program (PRP)," January 8, 2001
- (z) Section 401 of title 50, United States Code
- (aa) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (ab) Sections 871, 879, and 3056 of title 18, United States Code

- (ac) Section 2709(a) (3) of title 22, United States Code
- (ad) Section 263a and 290dd -2 of title 42, United States Code
- (ae) Title 42, Code of Federal Regulations, "Public Health," current edition
- (af) Chapter 75 of title 5, United States Code

## DL1.1. DEFINITIONS

### DL1.1.1. Business Associate

DL1.1.1.1. Except as provided in subparagraph DL1.1.1.2., business associate, with respect to a covered entity, is a person who:

DL1.1.1.1.1. On behalf of such covered entity or of an organized healthcare arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce 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 by this Regulation; or

DL1.1.1.1.2. 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 healthcare 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.

DL1.1.1.2. A covered entity participating in an organized healthcare arrangement that performs a function or activity as described by subparagraph DL1.1.1.1. for or on behalf of such organized healthcare arrangement, or that provides a service as described in subparagraph DL1.1.1.1.2. to or for such organized healthcare 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 healthcare arrangement.

DL1.1.1.3. 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's 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, the CHAMPUS/TRICARE network providers are not its business associates.

DL1.1.2. 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 (reference (e)).

**DL1.1.3. Covered Entity.** A health plan or a healthcare provider who transmits any health information in electronic form in connection with a transaction (see paragraph DL1.1.35.) covered by this Regulation, e.g. ACS X12N 837 healthcare claims, ASC X12N 270/271 eligibility inquiries and responses, and the electronic forms of other transactions identified at DL1.1.35. In the case of a health plan administered by the Department of Defense, the covered entity is the DoD Component (or subcomponent) that functions as the administrator of the health plan. (See paragraph DL1.1.17. for additional information on health plan administrators.) To the extent this Regulation prescribes duties to be performed by covered entities, the term refers only to DoD covered entities. Under subparagraph C3.2.2., all covered entities of the Military Health System (MHS) (including both health plans and healthcare providers) are designated as a single covered entity. Not all healthcare providers affiliated with the Armed Forces are covered entities; among those who are not are providers associated with Military Entrance Processing Stations (MEPS) and Reserve components practicing outside the authority of military treatment facilities (MTFs) who do not engage in electronic transactions covered by the Regulation.

**DL1.1.4. Covered Functions.** Those functions of a covered entity the performance of which makes the entity a health plan or healthcare provider.

**DL1.1.5. 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 protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the healthcare operations of the respective covered entities.

**DL1.1.6. Designated Record Set**

**DL1.1.6.1.** A group of records maintained by or for a covered entity that is:

DL1.1.6.1.1. The medical records and billing records about individuals maintained by or for a covered healthcare provider.

DL1.1.6.1.2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

DL1.1.6.1.3. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

DL1.1.6.2. For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

DL1.1.7. Direct Treatment Relationship. A treatment relationship between an individual and a healthcare provider that involves face-to-face interaction between the individual and healthcare provider or that otherwise is not an indirect treatment relationship (as defined in paragraph DL1.1.18.).

DL1.1.8. Disclosure. The release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

DL1.1.9. DoD Regulation. As defined in this Regulation, any DoD Directive, DoD Instruction, or DoD Publication issued according to DoD 5025.1-M (reference (f)) or any Military Department of Military Service regulation or similar issuance. DoD Regulation also includes the Manual for Courts-Martial or other issuance of the President applicable to the Armed Forces.

DL1.1.10. Employment Records. Records that include health information and:

DL1.1.10.1. Are maintained by a component of the Department of Defense or other entity subject to this Regulation;

DL1.1.10.2. Are about an individual who is (or seeks or sought to become) a member of the Uniformed Services, employee of the United States Government, employee of a Department of Defense contractor, or person with a comparable relationship to the Department of Defense; and

DL1.1.10.3. Are not maintained in connection with carrying out any covered function under this Regulation.

DL1.1.11. Department of Health and Human Services (HHS) Regulation. 45 CFR Parts 160 through 164 (reference (g)).

DL1.1.12. Healthcare. Care, services, or supplies related to the health of an individual. Healthcare includes, but is not limited to, the following:

DL1.1.12.1. 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

DL1.1.12.2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

DL1.1.13. Healthcare Operations. Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

DL1.1.13.1. Conducting quality assessment 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 healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment.

DL1.1.13.2. Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities.

DL1.1.13.3. 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 healthcare (including stop-loss insurance and excess of loss insurance).

DL1.1.13.4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

DL1.1.13.5. 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.

DL1.1.13.6. Business management and general administrative activities of the entity, including, but not limited to:

DL1.1.13.6.1. Management activities relating to implementation of and compliance with the requirements of this Regulation.

DL1.1.13.6.2. Customer service, if protected health information is not disclosed except as otherwise permitted by this Regulation.

DL1.1.13.6.3. Resolution of internal grievances.

DL1.1.13.6.4. 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 shall become a covered entity and due diligence related to such activity.

DL1.1.13.6.5. Consistent with the applicable requirements of Chapter 8, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

DL1.1.14. Healthcare Provider. Any medical treatment facility or, dental treatment facility This includes garrison clinics and such facilities in a military operational unit, ship, or aircraft, and any other person or organization outside of such facilities' workforce who furnishes, bills, or is paid for healthcare in the normal course of business. This term includes occupational health clinics for civilian employees or contractor personnel.

DL1.1.15. Health Information. Any information, in any form or medium, that:

DL1.1.15.1. Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, or school or university; and

DL1.1.15.2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

DL1.1.16. 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 healthcare 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.

DL1.1.17. Health Plan. Any DoD program that provides or pays the cost of healthcare, unless exempted under subparagraph DL1.1.17.3.

DL1.1.17.1. The following components of the TRICARE Program are a health plan under this Regulation:

DL1.1.17.1.1. The program that provides healthcare under the authority of the Department of the Army to members of the Uniformed Services. (Administrator: Surgeon General of the Army.)

DL1.1.17.1.2. The program that provides healthcare under the authority of the Department of the Navy to members of the Uniformed Services. (Administrator: Surgeon General of the Navy.)

DL1.1.17.1.3. The program that provides healthcare under the authority of the Department of the Air Force to members of the Uniformed Services. (Administrator: Surgeon General of the Air Force.)

DL1.1.17.1.4 The Supplemental Care Program for members of the Army, the Navy, the Marine Corps, and the Air Force who receive healthcare services from providers other than providers of the Department of Defense. (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.)

DL1.1.17.1.5. The TRICARE Prime, TRICARE Extra, and TRICARE Standard healthcare options offered under 32 CFR 199.17 (reference (h)). (Administrator: TRICARE Management Activity.)

DL1.1.17.1.6. The Civilian Health and Medical Program of the Uniformed Services. (Administrator: TRICARE Management Activity.)

DL1.1.17.2. The following are also included as health plans:

DL1.1.17.2.1. The TRICARE Dental Program under 10 U.S.C. 1076a (reference (i)). (Administrator: TRICARE Management Activity.)

DL1.1.17.2.2. The TRICARE Retiree Dental Program under 10 USC 1076c (reference (i)). (Administrator: TRICARE Management Activity.)

DL1.1.17.2.3. The Continued Health Care Benefit Program under 10 U.S.C. 1078a (reference (i)). (Administrator: TRICARE Management Activity.)

DL1.1.17.2.4. The Designated Provider Program under 10 U.S.C. 1073 note (reference (i)). (Administrator: TRICARE Management Activity.)

DL1.1.17.2.5. Programs conducted as demonstration projects under 10 U.S.C. 1092 (reference (i)) to the extent not otherwise included under a health plan.

DL1.1.17.3. Health plan excludes the following DoD programs:

DL1.1.17.3.1. Although part of the TRICARE Program, the programs that provide healthcare 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 the HHS regulations from the definition of health plan.

DL1.1.17.3.2. The Women, Infants, and Children (WIC) program.

DL1.1.17.3.3. Occupational health clinics for civilian employees or contractor personnel.

DL1.1.17.3.4. 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.

DL1.1.17.3.5. Any other program whose principal purpose is other than providing, or paying the cost of, healthcare.

DL1.1.17.3.6. Any other program (other than one listed in subparagraph DL1.1.17.1. or DL1.1.17.2.) whose principal activity is the direct provision of healthcare to persons.

DL1.1.17.3.7. Any other program whose principal activity is the making of grants to fund the direct provision of healthcare to persons.

DL1.1.18. Indirect Treatment Relationship. A relationship between an individual and a healthcare provider in which:

DL1.1.18.1. The healthcare provider delivers healthcare to the individual based on the orders of another healthcare provider; and

DL1.1.18.2. The healthcare provider typically provides services or products, or reports the diagnosis or results associated with the healthcare, directly to another healthcare provider, who provides the services or products or reports to the individual

DL1.1.19. Individual. The person who is the subject of protected health information. (Under certain circumstances, rights of an individual under this Regulation may be exercised by a personal representative. See, for example, section C8.7.)

DL1.1.20. Individually Identifiable Health Information. Information that is a subset of health information, including demographic information collected from an individual, and:

DL1.1.20.1. Is created or received by a healthcare provider, health plan, or employer; and

DL1.1.20.2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and

DL1.1.20.2.1. That identifies the individual; or

DL1.1.20.2.2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

DL1.1.21. Inmate. A person incarcerated in or otherwise confined to a correctional institution.

DL1.1.22. Law Enforcement Official. An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

DL1.1.22.1. Investigate or conduct an official inquiry into a potential violation of law; or

DL1.1.22.2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

DL1.1.23. Marketing

DL1.1.23.1. 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:

DL1.1.23.1.1. To inform an individual who is a member of a Uniformed Service or a covered beneficiary of the MHS of benefits, services, coverages, limitations, costs, procedures, rights, obligations, options, and other information concerning the MHS as established by law and applicable regulations.

DL1.1.23.1.2. 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: the entities participating in a healthcare provider network or health plan network; replacement of, or enhancements to, a health plan; and 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.

DL1.1.23.1.3. For treatment of the individual; or

DL1.1.23.1.4. For case management or care coordination of the individual, or to direct or recommend alternative treatments, therapies, healthcare providers, or settings of care to the individual.

DL1.1.23.2. An arrangement between a covered entity and any other entity whereby the covered entity disclosed protected health information 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.

DL1.1.24. Military Health System (MHS). All DoD health plans and all DoD healthcare 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.

DL1.1.25. Military Treatment Facility (MTF). A military facility established for the purpose of furnishing medical and/or dental care to eligible individuals.

DL1.1.26. Organized Healthcare Arrangement. The MHS is an organized healthcare arrangement. See Chapter 3 of this Regulation.

DL1.1.27. Payment

DL1.1.27.1. The activities undertaken by:

DL1.1.27.1.1. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

DL1.1.27.1.2. A healthcare provider or health plan to obtain or provide reimbursement for the provision of healthcare; and

DL1.1.27.2. The activities in subparagraph DL1.1.27.1. of this definition relate to the individual to whom healthcare is provided and include, but are not limited to:

DL1.1.27.2.1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims.

DL1.1.27.2.2. Risk adjusting amounts due based on enrollee health status and demographic characteristics.

DL1.1.27.2.3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing.

DL1.1.27.2.4. Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.

DL1.1.27.2.5. Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services.

DL1.1.27.2.6. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

DL1.1.27.2.6.1. Name and address.

DL1.1.27.2.6.2. Date of birth.

DL1.1.27.2.6.3. Social security number.

DL1.1.27.2.6.4. Payment history.

DL1.1.27.2.6.5. Account number; and

DL1.1.27.2.6.6. Name and address of the healthcare provider and/or health plan.

DL1.1.28. Protected Health Information. Individually identifiable health information:

DL1.1.28.1. Except as provided in subparagraph DL1.1.28.2. of this definition, that is transmitted or maintained by electronic or any other form or medium.

DL1.1.28.2. Protected health information excludes individually identifiable health information in employment records held by a covered entity in its role as employer.

DL1.1.29. Psychotherapy Notes. Notes recorded (in any medium) by a healthcare provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

DL1.1.30. Public Health Authority. 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 responsible for public health matters as part of its official mandate. The term "public health authority" includes any DoD Component authorized under applicable DoD Regulation to carry out public health activities, including medical surveillance activities under DoD Directive 6490.2 (reference (j)).

DL1.1.31. Required By Law. A mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law.

DL1.1.31.1. 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 healthcare 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.

DL1.1.31.2. 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 non-compliance, 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.

DL1.1.32. Research. A systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

DL1.1.33. Secretary of Health and Human Services (HHS). The Secretary of HHS or any other officer or employee of HHS that has been delegated relevant authority.

DL1.1.34. State. One of the following:

DL1.1.34.1. 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.

DL1.1.34.2. 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.

DL1.1.35. Transaction. The transmission of information between two parties to carry out financial or administrative activities related to healthcare. It includes the following types of information transmissions:

DL1.1.35.1. Healthcare claims or equivalent encounter information.

DL1.1.35.2. Healthcare payment and remittance advice.

DL1.1.35.3. Coordination of benefits.

DL1.1.35.4. Healthcare claim status.

DL1.1.35.5. Enrollment and disenrollment in a health plan.

DL1.1.35.6. Eligibility for a health plan.

DL1.1.35.7. Health plan premium payments.

DL1.1.35.8. Referral certification and authorization.

DL1.1.35.9. First report of injury.

DL1.1.35.10. Health claims attachments.

DL1.1.35.11. Other transactions that the Secretary of HHS may prescribe by Regulation.

DL1.1.36. Treatment. The provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for healthcare from one healthcare provider to another.

DL1.1.37. TRICARE Management Activity. The DoD Field Activity established by DoD Directive 5136.12 (reference (k)). TRICARE Management Activity includes the activities of TRICARE Regional Offices and TRICARE Lead Agents in accordance with that Directive.

DL1.1.38. 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.

DL1.1.39. 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.

C1. CHAPTER 1  
AUTHORITIES IN GENERAL

C1.1. GENERAL PROVISIONS

C1.1.1. Statutory Basis and Purpose. The requirements of this Regulation implement sections 1171 through 1179 of the Social Security Act (reference (l)), with which covered entities of the Department of Defense are required to comply, and the implementing HHS Privacy Regulation (reference (g)).

C1.1.2. Applicability. This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components"). See also sections C2.1. and C2.2. of this Regulation which reference the entities to which the standards, requirements and implementation specifications are and are not applicable.

C1.1.3. Penalties for Non-Compliance. As specified in section C2.5., the Secretary of HHS has authority over matters of compliance with the HHS Privacy Regulation (reference (g)) and the initiation of penalties for non-compliance. Violations of the HHS Privacy Regulation by any person are punishable by civil money penalties of up to \$100 for each violation. In addition, a wrongful use or disclosure of protected health information is subject to criminal penalties of up to a \$50,000 fine and 1-year imprisonment. Offenses committed under false pretenses or for commercial purposes carry more severe penalties.

C1.1.4. Pre-emption of State Law. Subject to the exceptions specified in section C2.4., this Regulation generally applies to the activities of the MHS, without regard to any contrary provisions of State law.

C1.1.5. Relationship with the Privacy Act. In general, protected health information covered by this Regulation is also covered by the Privacy Act and the Department of Defense's implementing regulation (references (c) and (d)) when the information pertains to a living U.S. citizen or alien admitted for permanent residence. As provided in section C2.6., covered entities under this Regulation shall also comply with the Privacy Act Regulation.

C1.1.6. Other Matters of General Authority. Other matters of general authority under this Regulation are addressed in Chapter 2.

## C1.2. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

C1.2.1. General Prohibition. In general, personally identifiable health information of individuals, both living and deceased, shall not be used or disclosed except for specifically permitted purposes. Uses and disclosures of protected health information are discussed in Chapters 4 through 8.

C1.2.2. Uses and Disclosures of Protected Health Information for Treatment, Payment, and Healthcare Operations. Subject to the specific provisions of Chapter 4, covered entities may use and disclose protected health information for treatment, payment, or healthcare operations. These are essential, every day activities of health plans and healthcare providers. These activities are generally permitted, consistent with Chapter 4, to be conducted without the need for authorization from the subject of the protected health information being used or disclosed.

C1.2.3. General Prohibition on Other Uses and Disclosures of Protected Health Information Without Written Authorization. Except for purposes of treatment, payment, and healthcare operations (discussed in paragraph C1.2.2.) and other exceptions (discussed in paragraphs C1.2.4. and C1.2.5.), other uses and disclosures of protected health information are generally prohibited without the written authorization of the patient. Specific provisions pertaining to this general rule are addressed in Chapter 5, including specifications for valid authorizations.

C1.2.4. Special Rules for Psychotherapy Notes. Paragraph C5.1.2. establishes special rules that protect the privacy of psychotherapy notes even more than other health information. Psychotherapy notes are subject to fewer exceptions to the general rule requiring written authorization from the individual for uses and disclosures.

C1.2.5. Other Uses and Disclosures That May Be Made, Unless Objected To. There are several other uses and disclosures that may generally be made, but the patient must be given an opportunity to object. These uses and disclosures involve patient directories providing limited information about patients receiving treatment, information provided to others involved in the healthcare of the patient, and information used in for disaster relief purposes. The specific provisions applicable to these uses and disclosures are in Chapter 6.

C1.2.6. Other Permitted and Required Uses and Disclosures That May Be Made Without Authorization or Opportunity to Object. The MHS may, subject to specific terms and conditions addressed in Chapter 7, use or disclose protected health information in the following situations without the individual's authorization or opportunity to object.

C1.2.6.1. When required by law or Government regulation. (See section C7.1.)

C1.2.6.2. For public health purposes. (See section C7.2.)

C1.2.6.3. About victims of abuse or neglect. (See section C7.3.)

C1.2.6.4. For health oversight activities authorized by law. (See section C7.4.)

C1.2.6.5. For judicial or administrative proceedings. (See section C7.5.)

C1.2.6.6. For law enforcement purposes. (See section C7.6.)

C1.2.6.7. Concerning decedents in limited circumstances. (See section C7.7.)

C1.2.6.8. For cadaveric organ, eye, or tissue donation purposes. (See section C7.8.)

C1.2.6.9. For research involving minimal risk. See section C7.9.

C1.2.6.10. To avert a serious threat to health or safety. (See section C7.10.)

C1.2.6.11. For specialized Government functions, including certain activities relating to Armed Forces personnel. (See section C7.11.)

C1.2.6.12. For workers' compensation programs. (See section C7.12.)

### C1.3. SPECIAL RULES AND OTHER REQUIREMENTS RELATING TO USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

There are a number of special rules and other requirements relating to uses and disclosures of personally identifiable health information. As provided in Chapter 8, these include:

C1.3.1. Standards for de-identification of personally identifiable health information. (See section C8.1.)

C1.3.2. Requirements for using and disclosing the minimum amount necessary to accomplish a valid use or disclosure purpose. (See section C8.2.)

C1.3.3. Clarification regarding incidental uses and disclosures. (See section C8.4.)

C1.3.4. Disclosures to business associates. (See section C8.5.)

C1.3.5. Disclosures by whistleblowers and workforce member crime victims. (See section C8.6.)

C1.3.6. Rules for dealing with personal representatives on behalf of individuals. (See section C8.7.)

#### C1.4. OBLIGATIONS OF THE MHS TO FULFILL RIGHTS OF INDIVIDUALS CONCERNING PROTECTED HEALTH INFORMATION

C1.4.1. In general, as provided in Chapter 9, an individual has a right to notice of uses and disclosures of protected health information that may be made by the MHS, and of the individual's rights and the MHS' legal duties with respect to protected health information.

C1.4.2. Individuals generally have the right to request additional privacy protections, as provided in Chapter 10. This includes a right to request restrictions on certain uses and disclosures, to which the MHS is not required to agree (see section C10.1.), and a right to receive confidential communications by alternative means or at alternative locations when reasonable (see section C10.2.).

C1.4.3. Individuals generally have a right of access to inspect and obtain a copy of protected health information about them, subject to some limitations, as provided in Chapter 11.

C1.4.4. Individuals generally have a right to amend protected health information about them if it is inaccurate or incomplete, under procedures outlined in Chapter 12.

C1.4.5. The MHS shall provide patients the ability to receive an accounting of certain disclosures that have been made of their protected health information, as provided in Chapter 13.

C1.5. ADDITIONAL ADMINISTRATIVE REQUIREMENTS FOR THE MHS TO IMPLEMENT HEALTH INFORMATION PRIVACY PROTECTIONS

To the extent provided in Chapter 14, the MHS is required to implement a series of administrative requirements to protect health information privacy. These include:

- C1.5.1. Designation of a privacy official. (See section C14.1.)
- C1.5.2. Training of the workforce involved in functions covered by this Regulation. (See section C14.2.)
- C1.5.3. Establishment of administrative, technical, and physical safeguards to protect the privacy of protected health information. (See section C14.3.)
- C1.5.4. Creation of a complaint process. (See section C14.4.)
- C1.5.5. Maintenance of a system of sanctions against members of the workforce who fail to comply with requirements of this Regulation. (See section C14.5.)
- C1.5.6. Duty of mitigation of harmful effects of improper uses and disclosures of protected health information. (See section C14.6.)
- C1.5.7. Restraint from intimidating or retaliatory acts relating to the exercise of rights under this Regulation. (See section C14.7.)
- C1.5.8. Restraint from requiring individuals to waive rights under this Regulation. (See section C14.8.)
- C1.5.9. Implementation of policies and procedures to implement privacy protections. (See section C14.9.)
- C1.5.10. Documentation of compliance with this Regulation. (See section C14.10.)
- C1.5.11. Transition provisions regarding patient authorizations and business associate relationships prior to the compliance date of this Regulation. (See sections C14.11. and C14.12.)

**C1.6. COMPLIANCE DATE**

As provided in section C14.13., the compliance date of this Regulation is April 14, 2003.

## C2. CHAPTER 2

### APPLICABILITY, SCOPE, ENFORCEMENT, AND RELATIONSHIP TO OTHER LAWS

#### C2.1. APPLICABILITY

Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this Regulation apply to the following entities:

C2.1.1. A health plan.

C2.1.2. A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by this Regulation.

#### C2.2. NON-APPLICABILITY

This Regulation does not apply to:

C2.2.1. A drug testing program of the Department of Defense carried out under the authority of DoD Directive 1010.1 (reference (m)) or DoD Directive 1010.9 (reference (n)).

C2.2.2. The provision of healthcare to foreign national beneficiaries of the MHS when such care is provided in a country other than the United States.

C2.2.3. The Armed Forces Repository of Specimen Samples for the Identification of Remains, established and operated under the authority of DoD Directive 5154.24 (reference (o)).

C2.2.4. The provision of healthcare to enemy prisoners of war, retained personnel, civilian internees and other detainees under the provisions of DoD Directive 2310.1 (reference (e)).

C2.2.5. Education records maintained by domestic or overseas schools operated by the Department of Defense.

C2.2.6. Records maintained by day care centers operated by the Department of Defense.

C2.2.7. Reserve component medical activities that are not practicing in an MTF.

#### C2.2.8. Military Entrance Processing Stations.

C2.2.9. Reserve component practicing outside the authority of MTFs who do not engage in electronic transactions covered by this Regulation.

### C2.3. INSPECTOR GENERAL

As required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5) (reference (l)), nothing in this Regulation shall be construed to diminish the authority of any statutory Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.) (reference (p)).

### C2.4. PREEMPTION OF STATE LAW

C2.4.1. General Rule Under HHS Regulation. In general, the HHS Regulation (reference (g)) establishes rules, exceptions, and procedures governing the determination of the preemption of state law by reference (g). As a general rule, a standard, requirement, or implementation specification adopted under reference (g) that is contrary to a provision of State law preempts the provision of State law. Exceptions to this general rule include the circumstance in which the provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under the HHS Regulation. Exceptions also include circumstances in which the provision of State law, including State procedures established under such law, as applicable, provide for the reporting of disease or injury, child or domestic abuse or neglect, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

C2.4.2. General Rule Under This Regulation. As a general rule, State laws pertaining to healthcare are not applicable to healthcare programs and activities of the Department of Defense. However, there are some matters concerning which DoD rules and procedures call for the DoD Components to follow State law.

C2.4.2.1. For example, in cases involving disclosure of protected health information about a minor to a parent, guardian, or person acting in loco parentis of such minor, the State law of the State where the treatment is provided shall be applied.

C2.4.2.2. In any other case in which there is a conflict between this Regulation and State law, this Regulation shall apply, unless DoD rules, procedures, or other applicable policy call for the DoD Components to follow State law with respect to the matter at issue.

## C2.5. COMPLIANCE AND ENFORCEMENT BY THE SECRETARY OF HHS

C2.5.1. Rules and procedures established by the Secretary of HHS pursuant to the HHS regulations are applicable to covered entities of the Department of Defense.

### C2.5.2. Complaints to the Department of HHS.

C2.5.2.1. A person who believes the MHS is not complying with the applicable requirements of the HHS Regulation (reference (g)) may file a complaint with the Department of HHS. Such complaints shall meet the following requirements:

C2.5.2.1.1. A complaint shall be filed in writing, either on paper or electronically.

C2.5.2.1.2. A complaint shall name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of the HHS regulations.

C2.5.2.1.3. A complaint shall be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless the Secretary of HHS waives this time limit for good cause shown.

C2.5.2.1.4. The Secretary of HHS may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

C2.5.2.2. The Secretary of HHS may investigate complaints referred to in subparagraph C2.5.2.1. Such investigation may include a review of the pertinent policies, procedures, or practices of the MHS and of the circumstances regarding any alleged acts or omissions concerning compliance.

C2.5.3. Compliance Reviews. The Secretary of HHS may conduct compliance reviews to determine if covered entities are complying with the applicable requirements of the HHS regulations.

C2.5.4. Responsibilities of Covered Entities in Relation to HHS Compliance and Enforcement

C2.5.4.1. Records and Compliance Reports. A covered entity shall keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary of HHS determines necessary to ascertain whether the covered entity has complied or is complying with the applicable requirements of the HHS regulations.

C2.5.4.2. Cooperate With Complaint Investigations and Compliance Reviews. A covered entity shall cooperate with the Secretary of HHS, if the Secretary of HHS undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the HHS regulations.

C2.5.4.3. Permit Access to Information

C2.5.4.3.1. A covered entity shall permit access by the Secretary of HHS during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of the HHS regulations. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary of HHS at any time and without notice.

C2.5.4.3.2. If any information required of a covered entity under this subparagraph is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity shall so certify and set forth what efforts it has made to obtain the information.

C2.5.4.3.3. Protected health information obtained by the Secretary of HHS in connection with an investigation or compliance review shall not be disclosed by the Secretary of HHS, except if necessary for ascertaining or enforcing compliance with the applicable requirements of the HHS regulations, or if otherwise required by law.

C2.5.4.3.4. In the event any information sought by the Secretary of HHS under subparagraph C2.5.4.3. is classified in the interest of national security or defense, the covered entity shall make appropriate arrangements for access by the Secretary of HHS consistent with applicable requirements for handling classified information.

C2.5.5. Penalties for Non-compliance. Sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) (reference (l)) provide penalties for non-compliance with the HHS regulations.

C2.5.5.1. There are civil penalties of not more than \$100 for each violation for a failure by any person to comply with requirements of the law and implementing HHS regulations.

C2.5.5.2. There are criminal penalties, including fines of up to \$50,000 and imprisonment for up to 1 year, for the wrongful disclosure by any person of individually identifiable health information.

## C2.6. RELATIONSHIP TO PRIVACY ACT

In addition to responsibilities to comply with this Regulation, covered entities are also responsible for compliance with the DoD Privacy Act Program Regulation (reference (d)).

C2.6.1. Although nothing in this Regulation violates reference (d), compliance with this Regulation does not necessarily satisfy all requirements of reference (d). For example, an authorized disclosure under Chapter 7 of this Regulation may require additional actions under reference (d), such as the establishment of a "routine use" in the system notice for the pertinent medical record system, which specifically identifies to whom the disclosure is made and for what purpose.

C2.6.2. Compliance with (reference (d)) in connection with protected health information does not necessarily satisfy requirements of this Regulation. For example, an authorized routine use of medical records under reference (d) is not necessarily a disclosure that can be made under this Regulation.

C2.6.3. Nothing in this Regulation creates any right or obligation under reference (d).

## C2.7. NO PRIVATE CAUSE OF ACTION

C2.7.1. There is no private cause of action under the statute referred to in section C2.1., the HHS regulations, or this Regulation. Potential remedies for alleged violations of that statute and the HHS regulations are those referred to in section C2.5. Potential remedies for alleged violations of this Regulation are addressed in sections

C14.4. and C14.5. Nothing in this Regulation gives an individual a right to initiate a legal action in court for any alleged violations.

C2.7.2. Although, as stated in section C2.7., there is overlap between this Regulation and reference (d), alleged or actual violations of this Regulation do not constitute a violation of reference (d) or give rise to a cause of action under reference (c).

## C2.8. RELATIONSHIP TO FREEDOM OF INFORMATION ACT

In general, the Freedom of Information Act (reference (q)) requires Government Agencies to provide access to records in the possession of the agencies to members of the public who request it. This Act, however, is subject to exception, among which is when access would cause an unwarranted invasion of personal privacy. Access to protected health information, other than that specifically provided for in this Regulation, would generally cause an unwarranted invasion of personal privacy of the individual to whom the protected health information pertains. Thus, the reference (q) would generally not affect matters governed by this Regulation. Requests under reference (q) are handled under DoD 5400.7-R (reference (r)).

### C3. CHAPTER 3

#### ORGANIZATIONAL RESPONSIBILITIES WITHIN THE MILITARY HEALTH SYSTEM UNDER THIS REGULATION

##### C3.1. PURPOSE

This Chapter establishes organizational responsibilities for covered entities that are part of the MHS and for business associates that are Components of the Department of Defense to comply with this Regulation.

##### C3.2. COVERED ENTITIES IN THE MHS

C3.2.1. The MHS includes all DoD health plans and all DoD healthcare 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.

C3.2.2. All such covered entities are under the common control of the Assistant Secretary of Defense for Health Affairs (ASD(HA)). These affiliated covered entities are hereby designated as a single covered entity. Unless otherwise specifically stated in this Regulation, responsibilities of MHS covered entities under this Regulation shall be construed as responsibilities of the MHS, under the management control of the ASD(HA), and, for purposes of activities subject to this Regulation, under the management control of the Director, TRICARE Management Activity.

C3.2.3. All covered entities that are components of the MHS shall carry out responsibilities in this Regulation consistent with the direction of the Director, TRICARE Management Activity.

C3.2.3.1. Each military treatment facility and dental treatment facility (sometimes collectively referred to as MTFs) is the designated covered entity for all institutional healthcare provided by the facility and for all other healthcare provided by providers assigned to, employed by, or otherwise providing services in or on behalf of the facility. In the case of contracted healthcare providers providing personal services or non-personal services in an MTF or dental treatment facility, the designated covered entity shall be the designated military treatment facility or dental treatment facility, unless otherwise specifically provided in the applicable contract. Unless so otherwise specifically provided in the applicable contract, each contract provider shall be required to comply with all requirements of or arising from this Regulation to the same extent as healthcare providers who are employees of the facility.

C3.2.3.2. All healthcare providers that are covered entities under this Regulation and are not providing services in or on behalf of a medical or dental treatment facility (for example, shipboard or field deployed medical personnel) are included in a covered entity, as follows:

C3.2.3.2.1. Providers under the control of the Department of the Army are included in a covered entity under the Surgeon General of the Army.

C3.2.3.2.2. Providers under the control of the Department of the Navy are included in a covered entity under the Surgeon General of the Navy.

C3.2.3.2.3. Providers under the control of the Department of the Air Force are included in a covered entity under the Surgeon General of the Air Force.

### C3.3. THE MHS AND ORGANIZED HEALTHCARE ARRANGEMENTS

C3.3.1. For certain purposes under this Regulation, such as the establishment of a covered entity's rules and procedures for uses and disclosures of protected health information for treatment, payment, or healthcare operations, such rules and procedures established by an organized healthcare arrangement of which the covered entity is a part are recognized as the rules and procedures of the covered entity. For this purpose, this section identifies the MHS, the MHS and certain elements of the Coast Guard, and elements of the MHS as organized healthcare arrangements.

C3.3.2. The following are organized healthcare arrangements of the MHS:

C3.3.2.1. The MHS is an organized healthcare arrangement consisting of all of the covered entities identified in section C3.2. Policies and procedures for the MHS

are established principally by the ASD(HA), but may also be established by the Under Secretary of Defense for Personnel and Readiness, or the Secretary of Defense. Such policies and procedures may also be established by the Director of the TRICARE Management Activity to the extent of the Director's authorities under DoD Directive 5136.12 (reference (k)), or as otherwise delegated by the ASD(HA).

C3.3.2.2. Healthcare personnel and related assets of the Department of the Army are under the Surgeon General of the Army and are part of an organized healthcare arrangement that includes the U.S. Army Medical Command and the covered entities identified in subparagraph C3.2.3.2.1. Policies and procedures for this organized healthcare arrangement are established principally by the Surgeon General of the Army, but may also be established by or on behalf of the Chief of Staff of the Army, the Assistant Secretary of the Army for Manpower and Reserve Affairs, or the Secretary of the Army.

C3.3.2.3. Healthcare personnel and related assets of the Department of the Navy are under the Surgeon General of the Navy and are part of an organized healthcare arrangement that includes the Bureau of Medicine and Surgery and the covered entities identified in subparagraph C3.2.3.2.2. Policies and procedures for this organized healthcare arrangement are established principally by the Surgeon General of the Navy, but may also be established by or on behalf of the Chief of Naval Operations, the Assistant Secretary of the Navy for Manpower and Reserve Affairs, or the Secretary of the Navy.

C3.3.2.4. Healthcare personnel and related assets of the Department of the Air Force are under the Surgeon General of the Air Force and are part of an organized healthcare arrangement that includes the Air Force Medical Operations Agency and the covered entities identified in subparagraph C3.2.3.2.3. Policies and procedures for this organized healthcare arrangement are established principally by the Surgeon General of the Air Force, but may also be established by or on behalf of the Chief of Staff of the Air Force, the Assistant Secretary of the Air Force for Manpower and Reserve Affairs, or the Secretary of the Air Force.

C3.3.3. The MHS is also part of an organized healthcare arrangement with the Coast Guard. The following elements of the Coast Guard are part of that organized healthcare arrangement:

C3.3.3.1. Providers under the control of the Coast Guard and under the Director, Health and Safety Directorate of the Coast Guard.

C3.3.3.2. The Coast Guard Health Care Program.

### C3.4. BUSINESS ASSOCIATE ARRANGEMENTS AMONG AND FOR THE DoD COMPONENTS

C3.4.1. The DoD Components (including some that are themselves covered entities) sometimes perform functions for covered entities that are covered functions under this Regulation. In other cases business associate functions for DoD covered entities may be carried out by other Government Agencies or by non-governmental entities under contract. This section establishes requirements applicable to all business associates that are:

C3.4.1.1. The DoD Components, for which the requirements are established by this Regulation, thus not requiring a written Business Associate agreement.

C3.4.1.2. Other Government Agencies, for which the requirements shall be incorporated (or incorporated by reference) into the memorandum of agreement (or other applicable documentation of the arrangement) between the DoD Component and the other Government Agency.

C3.4.1.3. Other entities, for which the requirements shall be incorporated (or incorporated by reference) into the contract or agreement with the other entity.

C3.4.2. The following requirements are applicable to uses and disclosures of protected health information by business associates. Additional requirements may be added to contracts and agreements at the discretion of the DoD Component.

C3.4.2.1. A business associate may not use or further disclose such information in a manner that would violate the requirements of this Regulation, except that:

C3.4.2.1.1. A business associate may use and disclose such information for the proper management and administration of the business associate; and

C3.4.2.1.2. A business associate may provide data aggregation services relating to the healthcare operations of the covered entity.

C3.4.2.2. A business associate shall:

C3.4.2.2.1. Not use or further disclose the information other than as permitted or required by DoD Regulation or as required by law.

C3.4.2.2.2. Use appropriate safeguards to prevent use or disclosure of the information other than as allowed by this Regulation.

C3.4.2.2.3. Report to the covered entity any use or disclosure of the information not allowed by this Regulation of which it becomes aware.

C3.4.2.2.4. Ensure that any person or contractor to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity is subject to or agrees to the same restrictions and conditions that apply to the business associate with respect to such information.

C3.4.2.2.5. Make available protected health information in accordance with Chapter 11.

C3.4.2.2.6. Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with Chapter 12.

C3.4.2.2.7. Make available the information required to provide an accounting of disclosures in accordance with Chapter 13.

C3.4.2.2.8. Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary of HHS for purposes of determining the covered entity's compliance with the HSS regulations; and

C3.4.2.2.9. At termination of the performance by the business associate functions, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, maintain compliance with this Regulation and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. Any action taken should be appropriately documented.

### C3.4.3. Other Arrangements

C3.4.3.1. If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition

of business associate in this Regulation to a covered entity, such covered entity may disclose protected health information to the business associate necessary to comply with the legal mandate. This may be done without meeting the requirements of section C3.4., if that the covered entity attempts in good faith to obtain satisfactory assurances that the business associate shall honor the provisions of subparagraph C3.4.2.2. If such attempt fails, the attempt and the reasons that such assurances cannot be obtained shall be documented.

C3.4.3.2. The business associate may use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

C3.4.3.2.1. For the proper management and administration of the business associate; or

C3.4.3.2.2. To carry out the legal responsibilities of the business associate.

C3.4.3.3. The business associate may disclose the information received by the business associate in its capacity as a business associate for the purposes described in subparagraph C3.4.3.2., if:

C3.4.3.3.1. The disclosure is required by law; or

C3.4.3.3.2. The business associate obtains reasonable assurances from the person to whom the information is disclosed that it shall be held confidentially and used or further disclosed only as required by law or for the purpose it was disclosed to the person; and the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

### C3.5. REQUIREMENTS FOR A COVERED ENTITY WITH MULTIPLE COVERED FUNCTIONS

C3.5.1. A covered entity that performs multiple covered functions that would make the entity a combination of a health plan and a covered healthcare provider shall comply with the standards, requirements, and implementation specifications of this Regulation, as applicable to the health plan or healthcare provider covered functions performed.

C3.5.2. A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or healthcare provider services, but not both, only for purposes related to the appropriate function being performed.

#### C4. CHAPTER 4

### USES OR DISCLOSURES TO CARRY OUT TREATMENT, PAYMENT AND HEALTHCARE OPERATIONS

#### C4.1. STANDARD: PERMITTED USES AND DISCLOSURES

Except uses or disclosures that require an authorization under sections C5.1.2. and C5.1.3., a covered entity may use or disclose protected health information for treatment, payment, or healthcare operations as set forth in section C4.2., if that such use or disclosure is consistent with other applicable requirements of this Regulation.

#### C4.2. IMPLEMENTATION SPECIFICATIONS: TREATMENT, PAYMENT, AND HEALTHCARE OPERATIONS

C4.2.1. A covered entity may use or disclose protected health information for its own treatment, payment, or healthcare operations.

C4.2.2. A covered entity may disclose protected health information for treatment activities of a healthcare provider.

C4.2.3. A covered entity may disclose protected health information to another covered entity or a healthcare provider for the payment activities of the entity that receives the information.

C4.2.4. A covered entity may disclose protected health information to another covered entity for healthcare operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

C4.2.4.1. For a purpose listed in subparagraphs DL1.1.13.1. and DL1.1.13.2.;

or

C4.2.4.2. For the purpose of healthcare fraud and abuse detection or compliance.

C4.2.5. A covered entity that participates in an organized healthcare arrangement (including under section C3.3.) may disclose protected health information about an individual to another covered entity that participates in the organized healthcare arrangement for any healthcare operations activities of the organized healthcare arrangement.

## C5. CHAPTER 5

### USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION IS REQUIRED

#### C5.1. STANDARD: AUTHORIZATION FOR USES AND DISCLOSURES

Each MTF shall establish standard operating procedures for uses and disclosures of authorization as covered in this Chapter.

C5.1.1. Authorization Required: General Rule. Except as otherwise permitted or required by this Regulation, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for use or disclosure of protected health information, such use or disclosure shall be consistent with such authorization.

C5.1.2. Authorization Required: Psychotherapy Notes. Notwithstanding any other provision of this Regulation, other than transition provisions provided for in Chapter 14, a covered entity shall obtain an authorization for any use or disclosure of psychotherapy notes, except:

C5.1.2.1. To carry out the following treatment, payment, or healthcare operations:

C5.1.2.1.1. Use by the originator of the psychotherapy notes for treatment.

C5.1.2.1.2. Use or disclosure by the covered entity for its own training programs that students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

C5.1.2.1.3. Use or disclosure by the covered entity to defend itself (or to defend the United States in a claim or action brought under the Federal Tort Claims Act (reference (s)) or Military Claims Act, 10 U.S.C. chapter 163 (reference (i)) arising from any alleged act or omission of the covered entity) in a legal action or other proceeding brought by the individual.

C5.1.2.2. A use or disclosure that is:

C5.1.2.2.1. Required by the Secretary of HHS in relation to compliance activities of the Secretary of HHS referred to in section C2.5.; or

C5.1.2.2.2. Permitted by section C7.1., pertaining to uses and disclosures required by law; or

C5.1.2.2.3. Permitted by section C7.4., pertaining to uses and disclosures for health oversight activities, with respect to the oversight of the originator of the psychotherapy notes; or

C5.1.2.2.4. Permitted by section C7.7., pertaining to uses and disclosures about decedents to coroners and medical examiners; or

C5.1.2.2.5. Permitted by subparagraph C7.10.1.1., pertaining to uses and disclosures to avert a serious and imminent threat to health or safety of a person or the public, which may include a serious and imminent threat to military personnel or members of the public or a serious or imminent threat to a specific military mission or national security under circumstances which in turn create a serious and imminent threat to a person or the public.

#### C5.1.3. Authorization Required: Marketing

C5.1.3.1. Notwithstanding any provision of this Chapter, other than the transition provisions in Chapter 14, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

C5.1.3.1.1. A face-to-face communication made by a covered entity to an individual; or

C5.1.3.1.2. A promotional gift of nominal value provided by the covered entity.

C5.1.3.2. If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

### C5.2. IMPLEMENTATION SPECIFICATIONS: GENERAL REQUIREMENTS

#### C5.2.1. Valid Authorizations

C5.2.1.1. A valid authorization is a document that contains the elements listed in subparagraph C5.1.3.2., paragraphs C5.3.1. and C5.3.2., as applicable.

C5.2.1.2. A valid authorization may contain elements or information in addition to the elements required by this section, if such additional elements or information are not inconsistent with the elements required by this section.

C5.2.2. Defective Authorizations. An authorization is not valid, if the document submitted has any of the following defects:

C5.2.2.1. The expiration date has passed or the expiration event is known by the covered entity to have occurred.

C5.2.2.2. The authorization has not been filled out completely, with respect to an element described by section C5.3., if applicable.

C5.2.2.3. The authorization is known by the covered entity to have been revoked.

C5.2.2.4. The authorization violates paragraphs C5.2.3. or C5.2.4., if applicable.

C5.2.2.5. Any material information in the authorization is known by the covered entity to be false.

C5.2.3. Compound Authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

C5.2.3.1. An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research.

C5.2.3.2. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

C5.2.3.3. An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph C5.2.4. on the provision of one of the authorizations.

C5.2.4. Prohibition on Conditioning of Authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

C5.2.4.1. A covered healthcare provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information under this Chapter.

C5.2.4.2. A covered entity may condition the provision of healthcare that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party. Examples of this include physical exams performed in order for a family member to participate in a school's extracurricular activities.

C5.2.5. Revocation of Authorizations. An individual may revoke an authorization provided under this section at any time, if the revocation is in writing, except if:

C5.2.5.1. The covered entity has taken action in reliance thereon; or

C5.2.5.2. The authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

C5.2.6. Documentation. A covered entity shall document and retain any signed authorization and/or revocation under this section as required by section C14.10.

C5.2.7. Review of Authorizations. A covered entity shall review on a periodic basis any authorization provided under this section. If the review discloses any question over the authorization's continuing validity, the covered entity shall contact the individual who provided the authorization to clarify/verify contents of the authorization.

C5.2.8. Processing of Authorizations. Authorizations involving use or disclosure of protected health information in the possession of an MTF, should be directed to the Privacy Officer of the MTF involved. Authorizations involving the use or disclosure of protected health information in the possession of the health plan should be directed to the TRICARE Management Activity Privacy Officer.

### C5.3. IMPLEMENTATION SPECIFICATIONS: CORE ELEMENTS AND REQUIREMENTS

C5.3.1. Core Elements. A valid authorization under this section shall contain at least the following elements:

C5.3.1.1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

C5.3.1.2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

C5.3.1.3. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

C5.3.1.4. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

C5.3.1.5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

C5.3.1.6. Signature of the individual and date. If a personal representative of the individual signs the authorization, a description of such representative's authority to act for the individual shall also be provided.

C5.3.2. Required Statements. In addition to the core elements, the authorization shall contain statements adequate to place the individual on notice of all of the following:

C5.3.2.1. The individual's right to revoke the authorization in writing, and either:

C5.3.2.1.1. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

C5.3.2.1.2. The information in subparagraph C5.3.2.1.1. is included in the notice required by Chapter 9, a reference to the covered entity's notice.

C5.3.2.2. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

C5.3.2.2.1. The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph C5.2.4. applies; or

C5.3.2.2.2. The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph C5.2.4., the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

C5.3.2.3. The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this rule.

C5.3.3. Plain Language Requirement. The authorization shall be written in plain language.

C5.3.4. Copy to the Individual. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

#### C5.4. AUTHORIZATION REQUIRED UNDER SPECIAL RULES FOR ALCOHOL AND DRUG ABUSE PROGRAM PATIENT RECORDS

An authorization is generally required for uses and disclosures of alcohol and drug abuse program patient records under special rules discussed in section C8.9.

## C6. CHAPTER 6

### USES AND DISCLOSURES REQUIRING AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR TO OBJECT

A covered entity may use or disclose protected health information when the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this Chapter. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section. If an individual objects, that objection shall be documented by the covered entity and shall remain valid for the duration of that episode of care.

#### C6.1. STANDARD: USE AND DISCLOSURE FOR FACILITY DIRECTORIES

C6.1.1. Permitted Uses and Disclosure. Except when an objection is expressed in accordance with paragraphs C6.1.2. or C6.1.3., a covered healthcare provider may:

C6.1.1.1. Use the following protected health information to maintain a directory of individuals in its facility:

C6.1.1.1.1. The individual's name.

C6.1.1.1.2. The individual's location in the covered healthcare provider's facility.

C6.1.1.1.3. The individual's condition described in general terms that does not communicate specific medical information about the individual (using descriptions such as "stable," "good," "fair," "serious," "critical," "conscious," "semiconscious," and "unconscious"); and

C6.1.1.1.4. The individual's religious affiliation for use only by members of the clergy.

C6.1.1.2. Disclose for directory purposes such information:

C6.1.1.2.1. To members of the clergy; or

C6.1.1.2.2. Except for religious affiliation, to other persons who ask for the individual by name.

C6.1.2. Opportunity to Object. A covered healthcare provider shall inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph C6.1.1. If an individual objects, that objection should be documented by the covered entity and shall remain valid for the duration of that episode of care.

### C6.1.3. Emergency Circumstances

C6.1.3.1. If the opportunity to object to uses or disclosures required by paragraph C6.1.2. cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered healthcare provider may use or disclose some or all of the protected health information permitted by paragraph C6.1.1. for the facility's directory, if such disclosure is:

C6.1.3.1.1. Consistent with a prior expressed preference of the individual, if any, that is known to the covered healthcare provider; and

C6.1.3.1.2. In the individual's best interest as determined by the covered healthcare provider, in the exercise of professional judgment.

C6.1.3.2. The covered healthcare provider shall inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph C6.1.2. when it becomes practicable to do so.

## C6.2. STANDARD: USES AND DISCLOSURES FOR INVOLVEMENT IN THE INDIVIDUAL'S CARE AND NOTIFICATION PURPOSES

### C6.2.1. Permitted Uses and Disclosures

C6.2.1.1. A covered entity may, in accordance with paragraphs C6.2.2. or C6.2.3., disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's healthcare.

C6.2.1.2. A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes shall be in accordance with paragraphs C6.2.2., C6.2.3., or C6.2.4., as applicable.

C6.2.2. Uses and Disclosures With the Individual Present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph C6.2.1. and has the capacity to make healthcare decisions, the covered entity may use or disclose the protected health information if it:

C6.2.2.1. Obtains the individual's agreement.

C6.2.2.2. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

C6.2.2.3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

C6.2.3. Limited Uses and Disclosures When the Individual Is Not Present. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's healthcare. A covered entity may use professional judgment and its experience with common practice and guidance from respective Service regulations to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

C6.2.4. Use and Disclosures for Disaster Relief Purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by subparagraph C6.2.1.2. The requirements in paragraphs C6.2.2. and C6.2.3. apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

## C7. CHAPTER 7

### USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED

A covered entity may use or disclose protected health information without the written authorization of the individual as described in Chapter 5 or the opportunity for the individual to agree or object as described in Chapter 6 in the situations covered by this Chapter, subject to the applicable requirements of this Chapter. When the covered entity is required by this Chapter to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this Chapter, the covered entity's information and the individual's agreement may be given orally (in which case the covered entity shall establish appropriate documentation of such oral communication). (NOTE: as required by section C2.6., a disclosure permitted by this Chapter must also be considered under the standards of the Privacy Act Program Regulation, DoD 5400.11-R (reference (d)), to determine whether it is also covered by that Regulation and whether disclosure is permitted under that Regulation.)

#### C7.1. STANDARD: USES AND DISCLOSURES REQUIRED BY LAW

C7.1.1. A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

C7.1.2. A covered entity shall meet the requirements described in sections C7.3., C7.5., or C7.6. for uses or disclosures required by law.

#### C7.2. STANDARD: USES AND DISCLOSURE FOR PUBLIC HEALTH ACTIVITIES

C7.2.1. Permitted Disclosures. A covered entity may disclose protected health information for public health activities to:

C7.2.1.1. 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.

C7.2.1.2. A public health authority or other Government authority authorized by law to receive reports of child abuse or neglect.

C7.2.1.3. A person subject to the jurisdiction of the Food and Drug Administration (FDA) addressing an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

C7.2.1.3.1. Collecting or reporting adverse events (or similar reports, food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations.

C7.2.1.3.2. Tracking FDA-regulated products.

C7.2.1.3.3. Enabling product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

C7.2.1.3.4. Conducting post-marketing surveillance.

C7.2.1.4. 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 or required by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

C7.2.1.5. An employer, about an individual who is a member of the workforce of the employer, if:

C7.2.1.5.1. The covered entity is a healthcare provider who is a member of the workforce of such employer or who provides healthcare to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work related illness or injury.

C7.2.1.5.2. The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

C7.2.1.5.3. The employer needs such findings in order to comply with its obligations, under Regulations of the Occupational Safety and Health Administration at

29 CFR parts 1904 through 1928 (reference (t)), the Mine Safety and Health Administration at 30 CFR parts 50 through 90 (reference (u)), or under State law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

C7.2.1.5.4. The covered healthcare provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time the healthcare is provided, or if the healthcare is provided on the work site of the employer, by posting the notice in a prominent place at the location where the healthcare is provided.

C7.2.2. Permitted Uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases for which it is permitted to disclose such information for public health activities under paragraph C7.2.1.

C7.2.3. DoD Administered Public Health Activities. Activities of the Department of Defense authorized by applicable DoD Regulation to carry out functions identified in paragraph C7.2.1. are included as public health activities for purposes of that paragraph.

### C7.3. STANDARD: DISCLOSURES ABOUT VICTIMS OF ABUSE, NEGLECT, OR DOMESTIC VIOLENCE

C7.3.1. Permitted Disclosures. Except for reports of child abuse or neglect permitted by subparagraph C7.2.1.2., a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence 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:

C7.3.1.1. When the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law.

C7.3.1.2. If the individual agrees to the disclosure; or

C7.3.1.3. When the disclosure is expressly authorized by statute or regulation  
and:

C7.3.1.3.1. The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

C7.3.1.3.2. If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information 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.

C7.3.2. Informing the Individual. A covered entity that makes a disclosure permitted by paragraph C7.3.1. shall promptly inform the individual that such a report has been or shall be made, except if:

C7.3.2.1. The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

C7.3.2.2. The covered entity informs a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

C7.3.3. DoD Domestic Abuse Prevention Activities. Activities of the Department of Defense authorized by applicable DoD Regulation to receive reports of abuse, neglect, or domestic violence consistent with the purpose of paragraph C7.3.1. are included as authorized Government authorities for purposes of that paragraph.

#### C7.4. STANDARD: USES AND DISCLOSURES FOR HEALTH OVERSIGHT ACTIVITIES

C7.4.1. Permitted Disclosures. A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

C7.4.1.1. The healthcare system.

C7.4.1.2. Government benefit programs for which health information is relevant to beneficiary eligibility.

C7.4.1.3. Entities subject to Government regulatory programs for which health information is necessary for determining compliance with program standards; or

C7.4.1.4. Entities subject to civil rights laws for which health information is necessary for determining compliance.

C7.4.2. Exception to Health Oversight Activities. For the purpose of the disclosures permitted by paragraph C7.4.1., a health oversight activity does 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:

C7.4.2.1. The receipt of healthcare.

C7.4.2.2. A claim for public benefits related to health; or

C7.4.2.3. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

C7.4.3. Joint Activities or Investigations. Notwithstanding paragraph C7.4.2., if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of section C7.4.

C7.4.4. Permitted Uses. If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by section C7.4.

C7.4.5. DoD Health Oversight Activities. Any activity of the Department of Defense authorized by applicable DoD Regulation to carry out health oversight functions is included as a health oversight agency for purposes of section C7.4.

## C7.5. STANDARD: DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

**C7.5.1. Permitted Disclosures.** A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

C7.5.1.1. In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

C7.5.1.2. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

C7.5.1.2.1. The covered entity receives satisfactory assurance, as described in subparagraph C7.5.1.3., from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

C7.5.1.2.2. The covered entity receives satisfactory assurance, as described in subparagraph C7.5.1.4., from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of subparagraph C7.5.1.5. of this section.

C7.5.1.3. For the purposes of subparagraph C7.5.1.2.1., a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

C7.5.1.3.1. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

C7.5.1.3.2. The notice included sufficient information about the litigation or proceeding for which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

C7.5.1.3.3. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

C7.5.1.3.3.1. No objections were filed; or

C7.5.1.3.3.2. All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

C7.5.1.4. For the purposes of subparagraph C7.5.1.2.2., a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

C7.5.1.4.1. The parties to the dispute concerning the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

C7.5.1.4.2. The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

C7.5.1.5. For purposes of paragraph C7.5.1., a qualified protective order concerning the protected health information requested under paragraph C7.5.2., is an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

C7.5.1.5.1. Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

C7.5.1.5.2. Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

C7.5.1.6. Notwithstanding subparagraph C7.5.1.2., a covered entity may disclose protected health information in response to lawful process described in subparagraph C7.5.1.2. without receiving satisfactory assurance under subparagraphs C7.5.1.2.1. or C7.5.1.2.2., if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of subparagraph C7.5.1.3. or to seek a qualified protective order sufficient to meet the requirements of subparagraph C7.5.1.4.

C7.5.2. Other Uses and Disclosures Under This Chapter. The provisions of this section do not supersede other provisions of this Chapter that otherwise permit or restrict uses or disclosures of protected health information.

C7.5.3. Relationship to Privacy Act Disclosures Pursuant to the Order of a Court of Competent Jurisdiction. Under 5 U.S.C. 552a(b)(11) (reference (c)), a Federal Agency may disclose Privacy Act-protected information pursuant to the order of a court (i.e., an order that has been reviewed and approved by a judge) of competent jurisdiction. In certain cases, the authority to disclose protected health information in response to an order of a court or administrative tribunal may be broader than the related authority under the Privacy Act (reference (c)). In such cases, other Privacy Act rules and procedures, such as the establishment of a routine use permitting disclosure, and where compulsory legal process is concerned, notification of the individual when the process becomes a matter of public record, may also apply. As stated in section C2.6., a disclosure of protected health information must be in accord with both this Regulation and the Privacy Act and its implementing Regulation (references (c) and (d)).

C7.5.4. Administrative or Judicial Proceedings in Relation to Courts-Martial Procedures. Any order from a military judge in connection with any process under the Uniform Code of Military Justice (reference (v)) is an order covered by subparagraph C7.5.1.1.

## C7.6. STANDARD: DISCLOSURES FOR LAW ENFORCEMENT PURPOSES

A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs C7.6.1. through C7.6.6. are met, as applicable.

C7.6.1. Permitted Disclosures: Pursuant to Process and as Otherwise Required By Law. A covered entity may disclose protected health information:

C7.6.1.1. As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to subparagraph C7.2.1.2. (reports of child abuse and neglect) or C7.3.1.1. (reports required by law of abuse, neglect or domestic violence); or

C7.6.1.2. In compliance with and as limited by the relevant requirements of:

C7.6.1.2.1. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

C7.6.1.2.2. A grand jury subpoena; or

C7.6.1.2.3. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, if:

C7.6.1.2.3.1. The information sought is relevant and material to a legitimate law enforcement inquiry;

C7.6.1.2.3.2. The request is in writing, specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

C7.6.1.2.3.3. De-identified information could not reasonably be used.

C7.6.2. Permitted Disclosures: Limited Information for Identification and Location Purposes. Except for disclosures required by law as permitted by paragraph C7.6.1., a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, if:

C7.6.2.1. The covered entity may disclose only the following information:

C7.6.2.1.1. Name and address.

C7.6.2.1.2. Date and place of birth.

C7.6.2.1.3. Social security number.

C7.6.2.1.4. ABO blood type and rh factor.

C7.6.2.1.5. Type of injury.

C7.6.2.1.6. Date and time of treatment.

C7.6.2.1.7. Date and time of death, if applicable; and

C7.6.2.1.8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

C7.6.2.2. Except as permitted by subparagraph C7.6.2.1., the covered entity may not disclose for the purposes of identification or location under paragraph C7.6.2. any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

C7.6.3. Permitted Disclosure: Victims of a Crime. Except for disclosures required by law as permitted by paragraph C7.6.1., a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to section C7.2. (disclosures for public health activities) or C7.3. (disclosures about victims of abuse, neglect, or domestic violence), if:

C7.6.3.1. The individual agrees to the disclosure; or

C7.6.3.2. The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, if:

C7.6.3.2.1. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim.

C7.6.3.2.2. The law enforcement official represents that immediate law 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; and

C7.6.3.2.3. The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

C7.6.4. Permitted Disclosure: Decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

C7.6.5. Permitted Disclosure: Crime on Premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

C7.6.6. Permitted Disclosure: Reporting Crime in Emergencies.

C7.6.6.1. A covered healthcare provider providing emergency healthcare in response to a medical emergency, other than such emergency on the premises of the covered healthcare provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

C7.6.6.1.1. The commission and nature of a crime.

C7.6.6.1.2. The location of such crime or of the victim(s) of such crime;  
and

C7.6.6.1.3. The identity, description, and location of the perpetrator of such crime.

C7.6.6.2. If a covered healthcare provider believes that the medical emergency described in subparagraph C7.6.6.1. is the result of abuse, neglect, or domestic violence of the individual in need of emergency healthcare, subparagraph C7.6.6.1. does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to section C7.3.

## C7.7. STANDARD: USES AND DISCLOSURES ABOUT DECEDENTS

C7.7.1. Coroners and Medical Examiners. A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

C7.7.2. Armed Force Medical Examiner. Any official of the Department of Defense authorized to perform functions under the authority of the Armed Forces Medical Examiner system under DoD Directive 5154.24 (reference (o)), is a medical examiner under paragraph C7.7.1.

C7.7.3. Funeral Directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties concerning the decedent.

C7.8. STANDARD: USES AND DISCLOSURES FOR CADAVERIC ORGAN, EYE OR TISSUE DONATION PURPOSES

A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

C7.9. STANDARD: USES AND DISCLOSURES FOR RESEARCH INVOLVING MINIMAL RISK

C7.9.1. Permitted Uses and Disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, if the requirements of subparagraph C7.9.1.1., C7.9.1.2., or C7.9.1.3. are met.

C7.9.1.1. Board Approval of a Waiver of Authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by Chapter 6 for use or disclosure of protected health information has, in the case of research conducted or supported by a DoD Component, been approved by an Institutional Review Board (IRB) established in accordance with 32 CFR 219.107 (reference (h)).

C7.9.1.1.1. In the case of research not conducted or supported by a DoD Component but conducted or supported by another Federal Agency, the required approval would be by an IRB, established in accordance with the Agency's regulation comparable to reference (h).

C7.9.1.1.2. In the case of research not conducted or supported by a Federal Agency, the required approval would be by a privacy board that:

C7.9.1.1.2.1. Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests.

C7.9.1.1.2.2. Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

C7.9.1.1.2.3. Does not have any member participating in a review of any project for which the member has a conflict of interest.

C7.9.1.2. Reviews Preparatory to Research. The covered entity obtains from the researcher representations that:

C7.9.1.2.1. Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

C7.9.1.2.2. No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

C7.9.1.2.3. The protected health information for which use or access is sought is necessary for the research purposes.

C7.9.1.3. Research on Decedent's Information. The covered entity obtains from the researcher:

C7.9.1.3.1. Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

C7.9.1.3.2. Documentation, at the request of the covered entity, of the death of such individuals; and

C7.9.1.3.3. Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

C7.9.2. Documentation of Waiver Approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under subparagraph C7.9.1.1., the documentation must include all of the following:

C7.9.2.1. Identification and Date of Action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

C7.9.2.2. Waiver Criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

C7.9.2.2.1. The use or disclosure of protected health information involves no more than minimal risk to the privacy of the individuals, based on, at least, the presence of the following elements:

C7.9.2.2.1.1. An adequate plan to protect the identifiers from improper use and disclosure;

C7.9.2.2.1.2. An adequate plan to destroy the identifiers at the earliest opportunity consistent with the content of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law.

C7.9.2.2.1.3. Adequate written assurances that the protected health information shall not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this Regulation.

C7.9.2.2.2. The research could not practicably be conducted without the waiver or alteration; and

C7.9.2.2.3. The research could not practicably be conducted without access to and use of the protected health information.

C7.9.2.3. Protected Health Information Needed. A brief description of the protected health information for which use or access has been determined necessary by the IRB or privacy board, pursuant to subparagraph C7.9.2.2.4.

C7.9.2.4. Review and Approval Procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

C7.9.2.4.1. An IRB must follow the requirements of the Common Rule, including the normal review procedures or the expedited review procedures (32 CFR 219.108(b), 219.110 (reference (h)) or comparable regulation of another Executive Agency).

C7.9.2.4.2. A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in subparagraph C7.9.1.1.2.2., and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with subparagraph C7.9.2.4.3.

C7.9.2.4.3. A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

C7.9.2.5. Required Signature. The documentation of the alteration or waiver of authorization shall be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

#### C7.10. STANDARD: USES AND DISCLOSURES TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

C7.10.1. Permitted Disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

C7.10.1.1. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

C7.10.1.2. Is 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 covered entity reasonably believes may have caused serious physical harm to the victim. However, such a use or disclosure may not be made if such statement is made in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or in the course of counseling or therapy, or through a request by the individual to initiate or to be referred for such treatment, counseling, or therapy. In addition, any such disclosure shall reveal only the statement by the individual and the protected health information described in subparagraph C7.6.2.1.

C7.10.1.3. Is necessary for law enforcement authorities to identify or apprehend an individual where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

C7.10.2. Presumption of Good Faith Belief. A covered entity that uses or discloses protected health information pursuant to paragraph C7.10.1. is presumed to

have acted in good faith with regard to a belief described in paragraph C7.10.1. if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

C7.10.3. Notification Requirement. If the covered entity acting under the authority of subparagraph C7.10.1.1. makes a disclosure to a person or entity outside the Department of Defense, the covered entity shall seek to notify the person who is the subject of the protected health information disclosed. Notification sent to the last known address of the individual as reflected in the records of the covered entity is sufficient for this purpose.

## C7.11. STANDARD: USES AND DISCLOSURES FOR SPECIALIZED GOVERNMENT FUNCTIONS

### C7.11.1. Armed Forces Personnel

C7.11.1.1. General Rule. A covered entity (including a covered entity not part of or affiliated with the Department of Defense) may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission.

C7.11.1.2. Appropriate Military Command Authorities. For purposes of subparagraph C7.11.1.1., appropriate Military Command authorities are the following:

C7.11.1.2.1. All Commanders who exercise authority over an individual who is a member of the Armed Forces, or other person designated by such a commander to receive protected health information in order to carry out an activity under the authority of the Commander.

C7.11.1.2.2. The Secretary of Defense, the Secretary of the Military Department responsible for the Armed Force for which the individual is a member, or the Secretary of Transportation when a member of the Coast Guard when it is not operating as a service in the Department of the Navy.

C7.11.1.2.3. Any official delegated authority by a Secretary listed in subparagraph C7.11.1.2.2. to take an action designed to ensure the proper execution of the military mission.

C7.11.1.3. Purposes for Which the Protected Health Information May Be Used or Disclosed. For purposes of subparagraph C7.11.1.1., the purposes for which

any and all of the protected health information of an individual who is a member of the Armed Forces may be used or disclosed are the following:

C7.11.1.3.1. To determine the member's fitness for duty, including but not limited to the member's compliance with standards and all other activities carried out under the authority of DoD Directive 1308.1 (reference (w)), DoD Directive 1332.38 (reference (x)), DoD Directive 5210.42 (reference (y)), and similar requirements.

C7.11.1.3.2. To determine the member's fitness to perform any particular mission, assignment, order, or duty, including compliance with any actions required as a precondition to performance of such mission, assignment, order, or duty.

C7.11.1.3.3. To carry out activities under the authority of DoD Directive 6490.2 (reference (j)).

C7.11.1.3.4. To report on casualties in any military operation or activity in accordance with applicable military regulations or procedures.

C7.11.1.3.5. To carry out any other activity necessary to the proper execution of the mission of the Armed Forces.

C7.11.1.4. Federal Register Notice. The operation of subparagraph C7.11.1.1. requires the publication of a notice in the Federal Register containing the provisions of subparagraphs C7.11.1.2. and C7.11.1.3.

C7.11.2. Separation or Discharge From Military Service. A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information 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 DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

C7.11.3. Foreign Military Personnel. A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under paragraph C7.11.1.

C7.11.4. National Security and Intelligence Activities. A covered entity may disclose protected health information to authorized Department of Defense and other 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.) (reference (z)) and implementing authority (e.g., Executive Order 12333) (reference (aa)).

C7.11.5. Protective Services for the President and Others. A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 (reference (ab)), or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3) (reference (ac)), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (reference (ab)).

C7.11.6. Correctional Institutions and Other Law Enforcement Custodial Situations

C7.11.6.1. Permitted Disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

C7.11.6.1.1. The provision of healthcare to such individuals.

C7.11.6.1.2. The health and safety of such individual or other inmates.

C7.11.6.1.3. The health and safety of the officers or employees of or others at the correctional institution.

C7.11.6.1.4. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another.

C7.11.6.1.5. Law enforcement on the premises of the correctional institution; and

C7.11.6.1.6. The administration and maintenance of the safety, security, and good order of the correctional institution.

C7.11.6.2. Permitted Uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose that protected health information may be disclosed.

C7.11.6.3. No Application After Release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

C7.11.7. Covered Entities That Are Government Programs Providing Public Benefits.

C7.11.7.1. A health plan that is a Government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a Government program providing public benefits if the sharing of eligibility or enrollment information among such Government Agencies or the maintenance of such information in a single or combined data system accessible to all such Government Agencies is required or expressly authorized by statute or regulation.

C7.11.7.2. A covered entity that is a Government Agency administering a Government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a Government Agency administering a Government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

C7.12. STANDARD: DISCLOSURES FOR WORKERS COMPENSATION

A covered entity may disclose protected health information as authorized by and to the extent necessary 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.

## C8. CHAPTER 8

### SPECIAL RULES AND OTHER REQUIREMENTS RELATING TO USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

#### C8.1. DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

C8.1.1. Standard: Uses and Disclosures of De-Identified Protected Health Information. A covered entity may use protected health information to create information that is not individually identifiable health information, or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

C8.1.2. Standard: De-Identification of Protected Health Information. Health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

C8.1.3. Implementation Specifications: Requirements for De-Identification of Protected Health Information. A covered entity may determine that health information is not individually identifiable health information only if:

C8.1.3.1. A person with adequate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, applying such principles and methods, 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, and documents the methods and results of the analysis that justify such determination; or

C8.1.3.2. The identifiers listed in subparagraph C8.1.3.3. of the individual or of relatives, employers, or household members of the individual, are removed and the covered entity does not 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.

C8.1.3.3. The identifiers referred to in subparagraph C8.1.3.2. are the following:

C8.1.3.3.1. Names.

C8.1.3.3.2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

C8.1.3.3.2.1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

C8.1.3.3.2.2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

C8.1.3.3.3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

C8.1.3.3.4. Telephone numbers.

C8.1.3.3.5. Fax numbers.

C8.1.3.3.6. Electronic mail addresses.

C8.1.3.3.7. Social security numbers.

C8.1.3.3.8. Medical record numbers.

C8.1.3.3.9. Health plan beneficiary numbers.

C8.1.3.3.10. Account numbers.

C8.1.3.3.11. Certificate or license numbers.

C8.1.3.3.12. Vehicle identifiers and serial numbers, including license plate numbers.

C8.1.3.3.13. Device identifiers and serial numbers.

C8.1.3.3.14. Web Universal Resource Locators (URLs).

C8.1.3.3.15. Internet Protocol (IP) address numbers.

C8.1.3.3.16. Biometric identifiers, including finger and voice prints.

C8.1.3.3.17. Full-face photographic images and any comparable images.

and

C8.1.3.3.18. Any other unique identifying number, characteristic, or code, except as permitted by paragraph C8.1.4.

C8.1.4. Implementation Specifications: Re-Identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, if:

C8.1.4.1. Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

C8.1.4.2. Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

## C8.2. MJNIMUM NECESSARY RULE

C8.2.1. Standard: Minimum Necessary. When using or disclosing protected health information in any form or when requesting protected health information from another covered entity, a covered entity shall make reasonable efforts to limit the use, disclosure, or request of protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The "reasonable efforts" standard applies to the implementation specifications in sections C8.3., C8.4., C8.5., C8.6., and C8.7.

C8.2.2. Minimum Necessary Does Not Apply. The minimum necessary rule does not apply to:

C8.2.2.1. Disclosures to or requests by a healthcare provider for treatment.

C8.2.2.2. Uses and disclosures for purposes of a medical training program.

C8.2.2.3. Uses or disclosures made to the individual.

C8.2.2.4. Uses and disclosures made pursuant to an authorization under Chapter 5.

C8.2.2.5. Disclosures made to the Secretary of HHS referred to in section C2.5.

C8.2.2.6. Uses or disclosures that are required by law, as described by section C7.1.

C8.2.2.7. Uses or disclosures that are required for compliance with this Regulation.

C8.2.3. Implementation Specifications: Minimum Necessary Uses of Protected Health Information.

C8.2.3.1. A covered entity shall identify:

C8.2.3.1.1. Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

C8.2.3.1.2. For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

C8.2.3.2. A covered entity shall make reasonable efforts to limit the access of such persons or classes identified in subparagraph C8.2.3.1.1. to protected health information consistent with subparagraph C8.2.3.1.2.

C8.2.4. Implementation Specification: Minimum Necessary Disclosures of Protected Health Information

C8.2.4.1. For any type of disclosure that it makes on a routine and recurring basis, a covered entity shall implement policies and procedures (may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

C8.2.4.2. For all other disclosures, a covered entity shall:

C8.2.4.2.1. Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

C8.2.4.2.2. Review requests for disclosure on an individual basis in accordance with such criteria.

C8.2.4.3. A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

C8.2.4.3.1. Making disclosures to public officials that are permitted under Chapter 7, if the public official represents that the information requested is the minimum necessary for the stated purpose(s).

C8.2.4.3.2. The information is requested by another covered entity.

C8.2.4.3.3. The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

C8.2.4.3.4. Documentation or representations that comply with the applicable requirements of section C7.9. have been provided by a person requesting the information for research purposes.

C8.2.5. Implementation Specifications: Minimum Necessary Requests for Protected Health Information

C8.2.5.1. A covered entity shall limit any request for protected health information to that reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

C8.2.5.2. For a request that is made on a routine and recurring basis, a covered entity shall implement policies and procedures (may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

C8.2.5.3. For all other requests, a covered entity shall:

C8.2.5.3.1. Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

C8.2.5.3.2. Review requests for disclosure on an individual basis in accordance with such criteria.

C8.2.6. Implementation Specification: Other Content Requirement. For all uses, disclosures, or requests to which the requirements in section C8.2. apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

### C8.3. LIMITED DATA SET

C8.3.1. Standard: Limited Data Set. A covered entity may use or disclose a limited data set that meets the requirements of paragraphs C8.3.2. and C8.3.3., if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph C8.3.4.

C8.3.2. Implementation Specification: Limited Data Set. A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

C8.3.2.1. Names.

C8.3.2.2. Postal address information, other than town or city, State and zip code.

C8.3.2.3. Telephone numbers.

C8.3.2.4. Fax number.

C8.3.2.5. Electronic mail addresses.

C8.3.2.6. Social security numbers.

C8.3.2.7. Medical record numbers.

C8.3.2.8. Health plan beneficiary numbers.

C8.3.2.9. Account numbers.

C8.3.2.10. Certificate/license numbers.

C8.3.2.11. Vehicle identifiers and serial numbers, including license plate numbers.

C8.3.2.12. Device identifiers and serial numbers.

C8.3.2.13. Web Universal Resource Locators (URLs).

C8.3.2.14. Internet Protocol (IP) address numbers.

C8.3.2.15. Biometric identifiers, including finger and voice prints; and

C8.3.2.16. Full-face photographic images and any comparable images.

C8.3.3. Implementation Specifications: Permitted Purposes for Uses and Disclosures

C8.3.3.1. A covered entity may use or disclose a limited data set under paragraph C8.3.1. for the purposes of research, public health, or healthcare operations.

C8.3.3.2. A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph C8.3.2., or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

C8.3.4. Implementation Specifications: Data Use Agreement

C8.3.4.1. Agreement Required. A covered entity may use or disclose a limited data set under paragraph C8.3.1. if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient shall only use or disclose the protected health information for limited purposes.

C8.3.4.2. Contents. A data use agreement between the covered entity and the limited data set recipient must:

C8.3.4.2.1. Establish the permitted uses and disclosures of such information by the limited data set recipient consistent with paragraph C8.3.3. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate this requirement, if done by the covered entity.

C8.3.4.2.2. Establish who is permitted to use or receive the limited data set; and

C8.3.4.2.3. Provide that the limited data set recipient shall:

C8.3.4.2.3.1. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law.

C8.3.4.2.3.2. Use appropriate safeguards to prevent use or disclosure of the information other than as provided by the data use agreement.

C8.3.4.2.3.3. Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware.

C8.3.4.2.3.4. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

C8.3.4.2.3.5. Not identify the information or contact the individuals.

#### C8.3.4.3. Compliance

C8.3.4.3.1. A covered entity is not in compliance with the standards of paragraph C8.3.1. if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

C8.3.4.3.1.1. Discontinued disclosure of protected health information to the recipient; and

C8.3.4.3.1.2. Reported the problem to the Secretary.

C8.3.4.3.2. A covered entity that is a limited data set recipient and violates a data use agreement will be in non-compliance with the standards, implementation specifications and requirements of paragraph C8.3.1.

### C8.4. INCIDENTAL USES AND DISCLOSURES RULE

C8.4.1. Subject to the conditions stated in paragraph C8.4.2., a covered entity is permitted to use or disclose protected health information as incident to a use or disclosure otherwise permitted or required by this Regulation.

C8.4.2. The incidental uses and disclosures rule applies only when the covered entity has complied with the following:

C8.4.2.1. The minimum necessary rule under section C8.2. by making reasonable efforts to limit the use or disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use or disclosure, consistent with that section; and

C8.4.2.2. The requirement of section C14.3. by having in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information, consistent with that section.

C8.4.3. Examples of Application of Incidental Uses and Disclosures Rule. Subject to compliance by a covered entity of the conditions established in paragraph C8.4.2., the following are several examples of incidental uses and disclosures that are permitted under paragraph C8.4.1.:

C8.4.3.1. Confidential conversations among healthcare providers or with patients when there is a possibility they may be overheard.

C8.4.3.2. Using sign-in sheets in waiting rooms or calling patients in waiting rooms by name.

C8.4.3.3. Posting the patient's name on the wall outside the patient's room;

C8.4.3.4. Maintaining patient charts at the patient's bedside.

C8.4.3.5. Using X-ray lightboards; and

C8.4.3.6. Discussing a patient's condition during training rounds in connection with a healthcare professional training program.

C8.4.4. Nonapplicability of the Incidental Uses and Disclosures Rule. The incidental uses and disclosure rule of paragraph C8.4.1. does not excuse non-compliance with this Regulation due to mistakes, neglect, a failure to have in place appropriate safeguards, or a failure to make reasonable efforts to limit the use or disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use or disclosure.

## C8.5. STANDARD: DISCLOSURE TO BUSINESS ASSOCIATES

C8.5.1. A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate shall appropriately safeguard the information.

C8.5.2. This standard does not apply with respect to disclosures by a covered entity to a healthcare provider concerning the treatment of the individual.

C8.5.3. A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity shall be in non-compliance with the standards, implementation specifications, and requirements of this section and section C3.4.

C8.5.4. Implementation Specification: Documentation. A covered entity shall document the satisfactory assurances required by paragraph C3.4.1. through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of section C3.4. As stated in section C3.4., in the case of a business associate that is a DoD Component and is covered by this Regulation, section C3.4. provides the documentation required by this section.

## C8.6. STANDARD: DISCLOSURES BY WHISTLEBLOWERS AND WORKFORCE MEMBER CRIME VICTIMS

C8.6.1. Disclosures By Whistleblowers. A covered entity is not considered to have violated the requirements of this Regulation if a member of its workforce or a business associate discloses protected health information, if:

C8.6.1.1. The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

C8.6.1.2. The disclosure is to:

C8.6.1.2.1. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

C8.6.1.2.2. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in subparagraph C8.6.1.1.

C8.6.2. Disclosures By Workforce Members Who Are Victims of a Crime. A covered entity is not considered to have violated the requirements of this Regulation if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, if:

C8.6.2.1. The protected health information disclosed is about the suspected perpetrator of the criminal act; and

C8.6.2.2. The protected health information disclosed is limited to the identification information listed in subparagraph C7.6.2.1.

## C8.7. PERSONAL REPRESENTATIVES

C8.7.1. Standard: Personal Representatives. As specified in this section C8.7., a covered entity shall, except as provided in paragraphs C8.7.3. and C8.7.5., treat a personal representative as the individual for purposes of this Regulation.

C8.7.2. Implementation Specification: Adults and Emancipated Minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to healthcare, a covered entity shall treat such person as a personal representative under this Regulation, regarding protected health information relevant to such personal representation.

### C8.7.3. Implementation Specification: Unemancipated Minors

C8.7.3.1. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to healthcare, a covered entity shall treat such person as a personal representative under this Regulation, regarding protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, regarding protected health information pertaining to a healthcare service, if:

C8.7.3.1.1. The minor provides informed consent to such healthcare service; no other informed consent to such healthcare service is required by law, regardless of whether the informed consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

C8.7.3.1.2. The minor may lawfully obtain such healthcare service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such healthcare service; or

C8.7.3.1.3. A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered healthcare provider and the minor with respect to such healthcare service.

C8.7.3.2. Notwithstanding the provisions of subparagraph C8.7.3.1.:

C8.7.3.2.1. To the extent permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with Chapter 11 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis.;

C8.7.3.2.2. To the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with Chapter 11 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis.

C8.7.3.2.3. Where the parent, guardian, or other person acting in loco parentis is not the personal representative under subparagraphs C8.7.3.1.1., C8.7.3.1.2., or C8.7.3.1.3., and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under Chapter 11 to a parent, guardian, or other person acting in loco parentis if such action is consistent with State or other applicable law, if such decision must be made by a licensed healthcare professional in the exercise of professional judgment.

C8.7.3.3. Notwithstanding the provisions of subparagraph C8.7.3.1., a covered entity shall, consistent with State or other applicable law, provide a right of access, as set forth in Chapter 11 to either a parent, guardian, or other person acting in loco parentis, as the personal representative of the unemancipated minor, the unemancipated minor, or both.

**C8.7.4. Implementation Specification: Deceased Individuals.** If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity shall treat such person as a personal representative under this Regulation, regarding protected health information relevant to such personal representation.

**C8.7.5. Implementation Specification: Abuse, Neglect, Endangerment Situations.** Notwithstanding a State law or any requirement of this section to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

C8.7.5.1. The covered entity has a reasonable belief that:

C8.7.5.1.1. The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

C8.7.5.1.2. Treating such person as the personal representative could endanger the individual; and

C8.7.5.1.3. The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

## **C8.8. STANDARD: DECEASED INDIVIDUALS**

A covered entity shall comply with the requirements of this Chapter regarding the protected health information of a deceased individual.

## **C8.9. SPECIAL RULES FOR ALCOHOL AND DRUG ABUSE PROGRAM PATIENT RECORDS**

Covered entities shall comply with the special rules protecting the confidentiality of alcohol and drug abuse patient records in federally assisted alcohol and drug abuse programs. Those rules are under the authority of The Alcohol, Drug Abuse, and Mental Health Administration Reorganization Act (ADAMHA), 42 U.S.C. 290dd-2 (reference (ad)) and appear at 42 CFR Part 2 (reference (ae)). To the extent those rules apply to protected health information of the covered entity, the covered entity shall comply with both those rules and this Regulation. To the extent any use or disclosure is authorized by this Regulation but prohibited by reference (ae), the prohibition shall control. Any use or disclosure is authorized by reference (ae) but prohibited by this Regulation, the

prohibition shall control. Covered alcohol and drug abuse patient records may only be used or disclosed if the requirements of both this Regulation and 42 CFR Part 2 (reference (a)) are satisfied.

## C9. CHAPTER 9

### NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION

#### C9.1. STANDARD: NOTICE OF PRIVACY PRACTICE

C9.1.1. Right to Notice. Except as provided by paragraph C9.1.2., an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

C9.1.2. Exception for Inmates. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

C9.1.3. Uses and Disclosures Consistent With Notice. A covered entity that is required to have a notice under paragraph C9.1.1. may not use or disclose protected health information in a manner inconsistent with the notice.

#### C9.2. IMPLEMENTATION SPECIFICATIONS: CONTENT OF NOTICE

C9.2.1. Required Elements. The Department of Defense shall provide one notice for its health plans and providers. The MHS Notice of Privacy Practices is issued through the TRICARE Management Activity (TMA).

C9.2.2. Revisions to the Notice. The covered entity, i.e., TMA, shall promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice that reflects the material change.

#### C9.3. IMPLEMENTATION SPECIFICATIONS: PROVISIONS OF NOTICE

A covered entity shall make the notice required by this section available on request to any person and to individuals as specified in paragraphs C9.3.1. through C9.3.3.4., as applicable.

##### C9.3.1. Specific Requirements for Health Plans

C9.3.1.1. A health plan shall provide notice:

C9.3.1.1.1. No later than the compliance date for the health plan, to individuals then covered by the plan.

C9.3.1.1.2. Thereafter, to individuals who newly become covered by the plan at the time or prior to the time they become covered; and

C9.3.1.1.3. Within 60 days of a material revision to the notice, to individuals then covered by the plan.

C9.3.1.2. No less frequently than once every 3 years, the health plan shall notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

C9.3.1.3. The health plan satisfies the requirements of paragraph C9.3.1. if notice is provided to the sponsor under coverage

C9.3.2. Specific Requirements for Certain Covered Healthcare Providers. A covered healthcare provider that has a direct treatment relationship with an individual shall:

C9.3.2.1. Provide the notice:

C9.3.2.1.1. No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered healthcare provider; or

C9.3.2.1.2. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

C9.3.2.2. Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with subparagraph C9.3.2.1., and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

C9.3.2.3. If the covered healthcare provider maintains a physical service delivery site:

C9.3.2.3.1. Have the notice available at the service delivery site for individuals to request to take with them; and

C9.3.2.3.2. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered healthcare provider to be able to read the notice; and

C9.3.2.4. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of subparagraph C9.3.2.3., if applicable.

### C9.3.3. Specific Requirements for Electronic Notice

C9.3.3.1. A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits shall prominently post its notice on the web site and make the notice available electronically through the web site.

C9.3.3.2. A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice shall be provided to the individual. Provision of electronic notice by the covered entity shall satisfy the provision requirements of section C9.3. when timely made in accordance with paragraph C9.3.1. or C9.3.2.

C9.3.3.3. For purposes of subparagraph C9.3.2.1., if the first service delivery to an individual is delivered electronically, the covered healthcare provider shall provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in subparagraph C9.3.2.2. apply to electronic notice.

C9.3.3.4. The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

## C9.4. IMPLEMENTATION SPECIFICATIONS: JOINT NOTICE BY SEPARATE COVERED ENTITIES

All covered entities that are components of the MHS (and thus participate in that organized healthcare arrangement) shall comply with this section by a joint notice.

C9.4.1. The covered entities of the MHS shall abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized healthcare arrangement.

C9.4.2. The covered entities included in the joint notice shall provide the notice to individuals in accordance with the applicable implementation specifications of section C9.3. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice satisfies the provision requirement of section C9.3. regarding all others covered by the joint notice.

#### C9.5. IMPLEMENTATION SPECIFICATIONS: DOCUMENTATION

A covered entity shall document compliance with the notice requirements, as required by paragraph C9.3.2., by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph C9.3.2.

C10. CHAPTER 10

RIGHTS TO REQUEST PRIVACY PROTECTION FOR PROTECTED HEALTH INFORMATION

C10.1. RIGHT TO REQUEST RESTRICTION

C10.1.1. Standard: Right of an Individual to Request Restriction of Uses and

C10.1.1.1. A covered entity shall permit an individual to request that the covered entity restrict:

C10.1.1.1.1. Uses or disclosures of protected health information about the individual to carry out treatment, payment, or healthcare operations; and

C10.1.1.1.2. Disclosures permitted under section C6.2. (concerning uses and disclosures for involvement in the individual's care).

C10.1.1.2. A covered entity is not required to agree to a restriction.

C10.1.1.3. A covered entity that agrees to a restriction under subparagraph C10.1.1.1. may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a healthcare provider, to provide such treatment to the individual.

C10.1.1.4. If restricted protected health information is disclosed to a healthcare provider for emergency treatment under subparagraph C10.1.1.3., the covered entity shall request that such healthcare provider not further use or disclose the information.

C10.1.1.5. A restriction agreed to by a covered entity under section C10.1. is not effective under this Chapter to prevent uses or disclosures permitted or required under section C6.1. (concerning facility directories) or Chapters 8 (concerning uses and disclosures for which authorization or opportunity to agree or object is not required), Chapter 12 (concerning access of individuals to protected health information), or Chapter 14 (concerning accounting of disclosures).

C10.1.1.6. Requests for restrictions under this paragraph C10.1.1. shall be made either orally or in writing to the person or office that would be obliged to comply with the restriction. No restriction shall be effective above the management authority level that agreed to the restriction. No restriction shall be effective unless the person agreeing to the restriction is actually authorized to agree to it and establishes a written record of the restriction. For example, if compliance would only be required by an MTF, the request should be made to the Privacy Officer of the MTF and not be transferred to another MTF. If compliance would be required of the entire MHS, the request would be made to the Privacy Officer, TMA. The deciding official for the most senior management authority that would be required to comply with the restriction shall determine whether the request shall be agreed to, notify the person making the request of the decision in writing, and take any appropriate implementation action.

C10.1.1.7. The decision whether to agree to a restriction requested by an individual is subject to the discretion of the covered entity. The restriction should be denied if the covered entity cannot reasonably accommodate the request, if it conflicts with this Regulation, or for other appropriate reasons.

C10.1.1.8. A response to a request for restriction should be provided to the individual requesting it as soon as practicable, and should include the rationale for denying it, if the request is denied in whole or part.

C10.1.2. Implementation Specifications: Terminating a Restriction. A covered entity may terminate its agreement to a restriction, if:

C10.1.2.1. The individual agrees to or requests the termination in writing.

C10.1.2.2. The individual orally agrees to the termination and the oral agreement is documented; or

C10.1.2.3. The covered entity informs the individual in writing that it is terminating its agreement to a restriction and documents that the individual has been so informed, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

C10.1.3. Implementation Specification: Documentation. A covered entity that agrees to a restriction shall document the restriction in accordance with section C14.10.

## C10.2. RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

### C10.2.1. Standard: Confidential Communications Requirements

C10.2.1.1. A covered healthcare provider shall permit individuals to request and shall accommodate reasonable requests by individuals to receive communications of protected health information from the covered healthcare provider by alternative means or at alternative locations.

C10.2.1.2. A health plan shall permit individuals to request and shall accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

### C10.2.2. Implementation Specifications: Conditions on Providing Confidential Communications

C10.2.2.1. A covered entity may require the individual to make a written request for a confidential communication described in paragraph C10.2.1.

C10.2.2.2. A covered entity may condition the provision of a reasonable accommodation on:

C10.2.2.2.1. When appropriate, information as to how payment, if any, shall be handled; and

C10.2.2.2.2. Specification of an alternative address or other method of

C10.2.2.3. A covered healthcare provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

C10.2.2.4. A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

## C11. CHAPTER 11

### ACCESS OF INDIVIDUALS TO PROTECTED HEALTH INFORMATION

#### C11.1. STANDARD: ACCESS TO PROTECTED HEALTH INFORMATION

C11.1.1. Right of Access. Except as otherwise provided in paragraphs C11.1.2. or C11.1.3., an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set. In addition, when an individual requests access to his or her record and the record is contained in a Privacy Act system of records, access may be denied only when denial is authorized both under this Regulation (paragraphs C11.1.2. or C11.1.3.) and the Privacy Act Regulations (as described in paragraph C11.1.4.).

C11.1.2. Unreviewable Grounds for Denial. Subject to paragraph C11.1.4., a covered entity may deny an individual access without providing the individual an opportunity for review, under the following circumstances.

C11.1.2.1. Psychotherapy notes.

C11.1.2.2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

C11.1.2.3. Protected health information maintained by a covered entity that is subject to the Clinical Laboratory Improvements Amendments of 1988 (42 U.S.C. 263a) (reference (ad)) to the extent the provision of access to the individual would be prohibited by law, or exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2) (reference (ae)).

C11.1.2.4. Quality assurance information that may not be disclosed under 10 U.S.C. 1102 (reference (i)).

C11.1.2.5. A covered entity that is a correctional institution or a covered healthcare provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

C11.1.2.6. An individual's access to protected health information created or obtained by a covered healthcare provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, if the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered healthcare provider has informed the individual that the right of access shall be reinstated upon completion of the research.

C11.1.2.7. An individual's access to protected health information that is contained in records that are subject to the Privacy Act (reference (c)) may be denied, if the denial of access under reference (c) would meet the requirements of that law. Examples of records for which access may be denied under certain terms of reference (c) include records classified in the interest of national defense or foreign policy and certain investigatory material.

C11.1.2.8. An individual's access may be denied if the protected health information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

C11.1.3. Reviewable Grounds for Denial. A covered entity may deny an individual access, if the individual is given a right to have such denials reviewed, as required by paragraph C11.1.5., under the following circumstances:

C11.1.3.1. A licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

C11.1.3.2. The protected health information makes reference to another person (unless such other person is a healthcare provider) and a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

C11.1.3.3. The request for access is made by the individual's personal representative and a licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

C11.1.4. Relationship to the Privacy Act. The Privacy Act (reference (c)) generally gives individuals unqualified access to information in systems of records maintained by Federal Agencies. In some cases, protected health information that is the subject to a request for access covered by this Chapter is also subject to the access

rules of the Privacy Act. In such cases, access must be granted unless the protected health information may be withheld pursuant to both the provisions of this Regulation (paragraphs C11.1.2. or C11.1.3.) and the Privacy Act Regulation (reference (d)). In the event of a disagreement between a DoD-affiliated covered entity and a Commander concerning the disclosure of protected health information, the covered entity shall seek the advice of the cognizant Judge Advocate General or command counsel.

C11.1.5. Review of a Denial of Access. If access is denied on a ground permitted under paragraph C11.1.3., the individual has the right to have the denial reviewed by a licensed healthcare professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity shall provide or deny access in accordance with the determination of the reviewing official under paragraph C11.4.4.

## C11.2. IMPLEMENTATION SPECIFICATIONS: REQUESTS FOR ACCESS AND TIMELY ACTION

C11.2.1. Individual's Request for Access. The covered entity shall permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, if it informs individuals of such a requirement.

### C11.2.2. Timely Action by the Covered Entity

C11.2.2.1. Except as provided in subparagraph C11.2.2.2., the covered entity shall act on a request for access no later than 30 days after receipt of the request as follows.

C11.2.2.1.1. If the covered entity grants the request, in whole or in part, it shall inform the individual of the acceptance of the request and provide the access requested, in accordance with section C11.3.

C11.2.2.1.2. If the covered entity denies the request, in whole or in part, it shall provide the individual with a written denial, in accordance with section C11.4.

C11.2.2.2. If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity shall take an action required by subparagraph C11.2.2.1. by no later than 60 days from the receipt of such a request.

C11.2.2.3. If the covered entity is unable to take an action required by subparagraph C11.2.2.1.1. or C11.2.2.1.2. within the time required by subparagraph C11.2.2.1. or C11.2.2.2., as applicable, the covered entity may extend the time for such actions by no more than 30 days, if:

C11.2.2.3.1. The covered entity, within the time limit set by subparagraph

C11.2.2.1. or C11.2.2.2., as applicable, provides the individual with a written statement of the reasons for the delay and the date that the covered entity shall complete its action on the request; and

C11.2.2.3.2. The covered entity may have only one such extension of time for action on a request for access.

### C11.3. IMPLEMENTATION SPECIFICATIONS: PROVISION OF ACCESS

If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity shall comply with the following requirements:

C11.3.1. Providing the Access Requested. The covered entity shall provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

#### C11.3.2. Form of Access Requested

C11.3.2.1. The covered entity shall provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

C11.3.2.2. The covered entity may provide the individual with a summary of the protected health information requested, instead of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

C11.3.2.2.1. The individual agrees in advance to such a summary or explanation; and

C11.3.2.2.2. The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

C11.3.2.2.3. Time and Manner of Access. The covered entity shall provide the access as requested by the individual in a timely manner as required by paragraph C11.2.2., including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

C11.3.2.2.4. Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee in accordance with the Service regulation, if the fee includes only the cost of:

C11.3.2.2.4.1. Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual.

C11.3.2.2.4.2. Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by subparagraph C11.3.2.2.

#### C11.4. IMPLEMENTATION SPECIFICATIONS: DENIAL OF ACCESS

If the covered entity denies access, in whole or in part, to protected health information, the covered entity shall comply with the following requirements. In addition, if the protected health information is also covered by the Privacy Act, the covered entity shall also comply with the requirements of reference (d) (or the other Privacy Act implementing regulations of that DoD Component).

C11.4.1. Making Other Information Accessible. The covered entity shall, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information that the covered entity has a ground to deny

C11.4.2. Denial. The covered entity shall provide a timely, written denial to the individual, in accordance with paragraph C11.2.2. The denial shall be in plain language and contain:

C11.4.2.1. The basis for the denial.

C11.4.2.2. If applicable, a statement of the individual's review rights under paragraph C11.1.4., including a description of how the individual may exercise such review rights; and

C11.4.2.3. A description of how the individual may complain to the covered entity pursuant to the complaint procedures in section C14.4. or to the Secretary of HHS pursuant to the procedures in 45 CFR 160.306 (reference (g)). The description shall include the name, or title, and telephone number of the contact person or office designated in subparagraph C14.1.1.2.

C11.4.3. Other Responsibility. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity shall inform the individual where to direct the request for access.

C11.4.4. Review of Denial Requested. If the individual has requested a review of a denial under paragraph C11.1.5., the covered entity shall designate a licensed healthcare professional, who was not directly involved in the denial to review the decision to deny access. The covered entity shall promptly refer a request for review to such designated reviewing official. The designated reviewing official shall determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph C11.1.3. The covered entity shall promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this Chapter to carry out the designated reviewing official's determination.

#### C11.5. IMPLEMENTATION SPECIFICATION: DOCUMENTATION

A covered entity shall document the following and retain the documentation as required by section C14.10.:

C11.5.1. The designated record sets that are subject to access by individuals; and

C11.5.2. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

## C12. CHAPTER 12

### AMENDMENT OF PROTECTED HEALTH INFORMATION

#### C12.1. STANDARD: RIGHT TO AMEND

C12.1.1. Right to Amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

C12.1.2. Denial of Amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

C12.1.2.1. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment.

C12.1.2.2. Is not part of the designated record set.

C12.1.2.3. Would not be available for inspection under Chapter 11; or

C12.1.2.4. Is accurate and complete.

#### C12.2. IMPLEMENTATION SPECIFICATIONS: REQUESTS FOR AMENDMENT AND TIMELY ACTION

C12.2.1. Individual's Request for Amendment. The covered entity shall permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, if it informs individuals in advance of such requirements.

#### C12.2.2. Timely Action by the Covered Entity

C12.2.2.1. The covered entity shall act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows:

C12.2.2.1.1. If the covered entity grants the requested amendment, in whole or in part, it shall take the actions required by paragraphs C12.3.1. and C12.3.2.

C12.2.2.1.2. If the covered entity denies the requested amendment, in whole or in part, it shall provide the individual with a written denial, in accordance with paragraph C12.4.1.

C12.2.2.2. If the covered entity is unable to act on the amendment within the time required by paragraph C12.2.1., the covered entity may extend the time for such action by no more than 30 days, if:

C12.2.2.2.1. The covered entity, within the time limit set by subparagraph C12.2.2.1., provides the individual with a written statement of the reasons for the delay and the date that the covered entity shall complete its action on the request; and

C12.2.2.2.2. The covered entity may have only one such extension of time for action on a request for an amendment.

### C12.3. IMPLEMENTATION SPECIFICATIONS: ACCEPTING THE AMENDMENT

If the covered entity accepts the requested amendment, in whole or in part, the covered entity shall comply with the following requirements:

C12.3.1. Making the Amendment. The covered entity shall make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

C12.3.2. Informing the Individual. In accordance with section C12.2., the covered entity shall with a timely, written acceptance and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons to be informed under paragraph C12.3.3.

C12.3.3. Informing Others. The covered entity shall make reasonable efforts to inform and provide the amendment within a reasonable time to:

C12.3.3.1. Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

C12.3.3.2. Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

#### C12.4. IMPLEMENTATION SPECIFICATIONS: DENYING THE AMENDMENT

If the covered entity denies the requested amendment, in whole or in part, the covered entity shall comply with the following requirements:

C12.4.1. Denial. The covered entity shall provide the individual with a timely, written denial, in accordance with paragraph C12.2.2. The denial shall use plain language and contain:

C12.4.1.1. The basis for the denial, in accordance with paragraph C12.1.2.

C12.4.1.2. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.

C12.4.1.3. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

C12.4.1.4. A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in section C14.4. or to the Secretary of HHS pursuant to the procedures established in 45 CFR 160.306 (reference (g)). The description shall include the name, or title, and telephone number of the contact person or office designated in subparagraph C14.1.1.2.

C12.4.2. Statement of Disagreement. The covered entity shall permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

C12.4.3. Rebuttal Statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity shall provide a copy to the individual who submitted the statement of disagreement.

C12.4.4. Recordkeeping. The covered entity shall, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

#### C12.4.5. Future Disclosures

C12.4.5.1. If a statement of disagreement has been submitted by the individual, the covered entity shall include the material appended in accordance with paragraph C12.4.4., or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information relating to the disagreement.

C12.4.5.2. If the individual has not submitted a written statement of disagreement, the covered entity shall include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with subparagraph C12.4.1.3.

C12.4.5.3. When a subsequent disclosure described in subparagraph C12.4.5.1. or C12.4.5.2. is made using a standard transaction under 45 CFR 162 (reference (g)) that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by subparagraph C12.4.5.1. or C12.4.5.2., as applicable, to the recipient of the standard transaction.

### C12.5. IMPLEMENTATION SPECIFICATION: ACTIONS ON NOTICES OF AMENDMENT

A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph C12.3.3., shall amend the protected health information in designated record sets as provided by paragraph C12.3.1.

#### C12.6. IMPLEMENTATION SPECIFICATION: DOCUMENTATION

A covered entity shall document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by section C14.10.

#### C12.7. RELATIONSHIP TO PRIVACY ACT

The Privacy Act (reference (c)) also has provisions (5 U.S.C. 552a(d)(2)) regarding amendment of reference (c) protected information. In any case that protected health information is subject to both this Chapter and reference (c) requirements, the reference (c) requirements shall continue to apply to matters of amendment according to such requirements.

C13. CHAPTER 13

ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

C13.1. STANDARD: RIGHT TO AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

C13.1.1. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the 6 years prior to the date that the accounting is requested, except for disclosures:

C13.1.1.1. To carry out treatment, payment and healthcare operations as provided in Chapter 4.

C13.1.1.2. To individuals of protected health information about them.

C13.1.1.3. Pursuant to an authorization under Chapter 5.

C13.1.1.4. For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in Chapter 6.

C13.1.1.5. For national security or intelligence purposes as provided in paragraph C7.11.4.

C13.1.1.6. To correctional institutions or law enforcement officials as provided in paragraph C7.11.6.

C13.1.1.7. As part of a limited data set in accordance with section C8.3.

C13.1.1.8. Incident to a use or disclosure otherwise permitted or required by this Regulation, as provided in section C8.4.

C13.1.1.9. That occurred prior to the compliance date for the covered entity.

C13.1.2. The covered entity shall take the following actions under the circumstances stated:

C13.1.2.1. The covered entity shall temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in sections C7.4. or C7.6., respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a

written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time that such a suspension is required.

C13.1.2.2. If the agency or official statement in subparagraph C13.1.2.1., above is made orally, the covered entity shall:

C13.1.2.2.1. Document the statement, including the identity of the agency or official making the statement;

C13.1.2.2.2. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

C13.1.2.2.3. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to subparagraph C13.1.2.1. is submitted during that time.

C13.1.3. An individual may request an accounting of disclosures for a period of time less than 6 years from the date of the request.

#### C13.2. IMPLEMENTATION SPECIFICATIONS: CONTENT OF ACCOUNTING

The covered entity shall provide the individual with a written accounting that meets the following requirements:

C13.2.1. Except as otherwise provided by section C13.1., the accounting shall include disclosures of protected health information that occurred during the 6 years (or such shorter time period at the request of the individual as provided in paragraph C13.1.3. of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

C13.2.2. Except as otherwise provided by paragraphs C13.2.3. or C13.2.4., the accounting shall include for each disclosure:

C13.2.2.1. The date of the disclosure.

C13.2.2.2. The name of the entity or person who received the protected health information and, if known, the address of such entity or person.

C13.2.2.3. A brief description of the protected health information disclosed.

C13.2.2.4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement, a

copy of a written request for disclosure under section C2.5. (disclosures to the Secretary of HHS) or Chapter 8, if any.

C13.2.3. If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under subparagraph C2.5.4.3. or Chapter 7, or pursuant to a single authorization under Chapter 5, the accounting may, with respect to such multiple disclosures, provide the following:

C13.2.3.1. The information required by paragraph C13.2.2., above for the first disclosure during the accounting period.

C13.2.3.2. The frequency, periodicity, or number of the disclosures made during the accounting period; and

C13.2.3.3. The date of the last such disclosure during the accounting period.

C13.2.4. If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with Chapter 7 for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

C13.2.4.1. The name of the protocol or other research activity;

C13.2.4.2. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selection particular records;

C13.2.4.3. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

C13.2.4.4. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

C13.2.4.5. A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

C13.2.5. If the covered entity provides an accounting for research disclosures in accordance with C13.2.4. and if it is reasonably likely that the protected health

information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

### C13.3. IMPLEMENTATION SPECIFICATIONS: PROVISION OF ACCOUNTING

C13.3.1. The covered entity shall act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows:

C13.3.1.1. The covered entity shall provide the individual with the accounting requested; or

C13.3.1.2. If the covered entity is unable to provide the accounting within the time required by paragraph C13.3.1., the covered entity may extend the time to provide the accounting by no more than 30 days, if:

C13.3.1.2.1. The covered entity, within the time limit set by paragraph C13.3.1., provides the individual with a written statement of the reasons for the delay and the date by which the covered entity shall provide the accounting; and

C13.3.1.2.2. The covered entity may have only one such extension of time for action on a request for an accounting.

C13.3.2. The covered entity shall provide the first accounting to an individual in any 12-month period without charge. The covered entity may impose a reasonable, cost-based fee in accordance with Service regulations for each subsequent request for an accounting by the same individual within the 12 month period, if the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

### C13.4. IMPLEMENTATION SPECIFICATION: DOCUMENTATION

A covered entity shall document the following and retain the documentation as required by Chapter 14:

C13.4.1. The information required being included in an accounting under section C13.2. for disclosures of protected health information that are subject to an accounting under section C13.1.

C13.4.2. The written accounting that is provided to the individual under this Chapter; and

C13.4.3. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

#### C13.5. RELATIONSHIP TO PRIVACY ACT

The Privacy Act (reference (c)) also has provisions (§ U.S.C. 552a(e)) requiring an accounting of certain disclosures of reference (c) protected information. In any case that protected health information disclosures are subject to both this Chapter and reference (c) requirements, reference (c) requirements shall continue to apply to the disclosures according to such requirements.

C14. CHAPTER 14  
ADMINISTRATIVE REQUIREMENTS, TRANSITION PROVISIONS, AND  
COMPLIANCE DATES

C14.1. PERSONNEL DESIGNATIONS

C14.1.1. Standard: Personnel Designations

C14.1.1.1. A covered entity shall designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

C14.1.1.2. A covered entity shall designate a contact person or office that is responsible for receiving complaints under this section and able to provide further information about matters covered by the notice required by Chapter 9.

C14.1.2. Implementation Specification: Personnel Designations. A covered entity shall document the personnel designations in paragraph C14.1.1. as required by section C14.10.

C14.2. TRAINING

C14.2.1. Standard: Training. A covered entity shall train all members of its workforce on the policies and procedures regarding protected health information required by this Chapter, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

C14.2.2. Implementation Specifications: Training

C14.2.2.1. A covered entity shall provide training that meets the requirements of paragraph C14.2.1., as follows:

C14.2.2.1.1. To each member of the covered entity's workforce by no later than the compliance date for the covered entity.

C14.2.2.1.2. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

C14.2.2.1.3. To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this Chapter, within a reasonable period of time after the material change becomes effective in accordance with section C14.9.

C14.2.2.2. Contracted healthcare providers and other contracted personnel providing services in a military treatment facility or dental treatment facility as described in subparagraph C3.2.2.2.1. shall be included in the training described in paragraph C14.2.2.

C14.2.2.3. A covered entity shall document that the training as described in subparagraph C14.2.2.1. has been provided, as required by section C14.10.

### C14.3. SAFEGUARDS

C14.3.1. Standard: Safeguards. A covered entity shall have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

#### C14.3.2. Implementation Specification: Safeguards

C14.3.2.1. A covered entity shall reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this Regulation.

C14.3.2.2. A covered entity shall reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

### C14.4. COMPLAINTS

C14.4.1. Standard: Complaints to the Covered Entity. A covered entity shall provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this Chapter or its compliance with such policies and procedures or the requirements of this Chapter.

C14.4.2. Implementation Specification: Documentation of Complaints. As required by section C14.10., a covered entity shall document all complaints received, and their disposition, if any.

## C14.5. SANCTIONS

C14.5.1. Standard: Sanctions. A covered entity shall have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this Regulation. For members of the military this may include action under the Uniform Code of Military Justice (reference (v)), administrative, or other appropriate sanctions. For civilian employees sanctions should be applied consistent with the provisions of Chapter 75 of title 5, United States Code (reference (af)). For contractor personnel subject to this section sanctions may include actions permissible under applicable procurement regulations. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of section C8.6. (disclosures by whistleblowers and workforce member crime victims) or paragraph C14.7.2.

C14.5.2. Implementation Specification: Documentation. As required by section C14.10., a covered entity shall document the sanctions that are applied, if any.

## C14.6. STANDARD: MITIGATION

A covered entity shall mitigate, when practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this Chapter by the covered entity or its business associate.

## C14.7. STANDARD: REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS

A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

C14.7.1. Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this Chapter, including the filing of a complaint under this section.

C14.7.2. Individuals and Others. Any individual or other person for:

C14.7.2.1. Filing of a complaint with the Secretary of HHS under subpart C of 45 CFR part 160 (reference (g)).

C14.7.2.2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act (reference (I)); or

C14.7.2.3. Opposing any act or practice made unlawful by this Regulation, if the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this Chapter.

#### C14.8. STANDARD: WAIVER OF RIGHTS

A covered entity may not require individuals to waive their rights under this Regulation as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

#### C14.9. POLICIES AND PROCEDURES

C14.9.1. Standard: Policies and Procedures. A covered entity shall implement policies and procedures on protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this Chapter. The policies and procedures shall be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this Chapter.

#### C14.9.2. Standard: Changes to Policies or Procedures

C14.9.2.1. A covered entity shall change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this Chapter.

C14.9.2.2. When a covered entity changes a privacy practice that is stated in the notice described in Chapter 9, and makes corresponding changes to its policies and

procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision; or

C14.9.2.3. A covered entity may make any other changes to policies and procedures at any time, if the changes are documented and implemented in accordance with paragraph C14.9.5.

C14.9.3. Implementation Specification: Changes in Law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity shall promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by Chapter 9, the covered entity shall promptly make the appropriate revisions to the notice in accordance with paragraph C9.2.2. Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

C14.9.4. Implementation Specifications: Changes to Privacy Practices Stated in the Notice

C14.9.4.1. To implement a change as provided by subparagraph C14.9.2.2., a covered entity shall:

C14.9.4.1.1. Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this Chapter;

C14.9.4.1.2. Document the policy or procedure, as revised, as required by section C14.10; and

C14.9.4.1.3. Revise the notice as required by paragraph C9.2.2. to state the changed practice and make the revised notice available as required by section C9.3. The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

C14.9.5. Implementation Specification: Changes to Other Policies or Procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by Chapter 9, if:

C14.9.5.1. The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this Chapter; and

C14.9.5.2. Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by section C14.10.

## C14.10. DOCUMENTATION

C14.10.1. Standard: Documentation. A covered entity shall:

C14.10.1.1. Maintain the policies and procedures provided for in section C14.9. in written or electronic form.

C14.10.1.2. If written communication is required by this Regulation, maintain communication, or an electronic copy, as documentation; and

C14.10.1.3. If documented action, activity, or designation is required by this Regulation, maintain a written or electronic record of such action, activity, or designation.

C14.10.2. Implementation Specification: Retention Period. A covered entity shall retain the documentation required by paragraph C14.10.1. for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

## C14.11. STANDARD: EFFECT OF PRIOR AUTHORIZATIONS

Notwithstanding Chapter 5 (authorizations) and section C7.9. (research involving minimum risk), a covered entity may use or disclose protected health information, consistent with this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.

C14.11.1. Implementation Specification: Effect of Prior Authorization for Purposes Other Than Research. Notwithstanding any provisions in Chapter 5, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this Regulation pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this Regulation, if the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with section C10.1.

C14.11.2. Implementation Specification: Effect of Prior Permission for Research. Notwithstanding any provisions in Chapter 5 and section C7.9., a covered entity may to the extent allowed by one of the following permissions, use or disclose, for a research

study, protected health information that it created or received either before or after the applicable compliance date of this Regulation, if there is no agreed-to restriction in accordance with section C10.1. and the covered entity has obtained, prior to the applicable compliance date, either:

C14.11.2.1. An authorization or other express legal permission from an individual to use or disclose protected health information for the research.

C14.11.2.2. The informed consent of the individual to participate in the research; or

C14.11.2.3. A waiver, by an IRB, of informed consent for the research, in accordance with 32 CFR 219.116(d) (reference (h)) (or comparable regulation of another Federal Agency), if a covered entity shall obtain authorization in accordance with Chapter 5 if, after the compliance date, informed consent is sought from an individual participating in the research.

#### C14.12. STANDARD: EFFECT OF PRIOR CONTRACTS OR OTHER ARRANGEMENTS WITH BUSINESS ASSOCIATES

Notwithstanding any other provisions of this Regulation, a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with section C3.4. consistent with the requirements, and only for such time, set forth in paragraph C14.12.1.

##### C14.12.1. Implementation Specification: Deemed Compliance

C14.12.1.1. Qualification. Notwithstanding other sections of this Regulation, a covered entity is deemed to be in compliance with the documentation, contract and similar requirements of section C3.4., regarding a particular business associate relationship, for the time period set forth in subparagraph C14.12.1.2., if:

C14.12.1.1.1. Prior to the effective date of this provision, such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; and

C14.12. -. The contract or other arrangement is not renewed or modified from the effective date of this provision and until the compliance date of this Regulation.

C14.12.1.2. Limited Deemed Compliance Period. A prior contract or other arrangement that meets the qualification requirements in subparagraph C14.12.1.1., shall be deemed compliant until the earlier of the date such contract or other arrangement is renewed or modified on or after the compliance date of this Regulation, or April 14, 2004.

C14.12.1.3. Covered Entity Responsibilities. Nothing in this paragraph shall alter the requirements of a covered entity to comply with Chapters 2, 11 (concerning access of individuals to protected health information), Chapter 12 (concerning amendment of protected health information), Chapter 13 (concerning accounting of disclosures of protected health information) regarding protected health information held by a business associate, and 14 (concerning mitigation of harmful effects of disclosures made in violation of policies).

#### C14.13. COMPLIANCE DATE FOR IMPLEMENTATION OF PRIVACY STANDARDS

Covered entities shall comply with the privacy standards in this Regulation by April 14, 2003.