



TMA PRIVACY & CIVIL LIBERTIES OFFICE

Health Information Privacy & Security Training Manual 2013



WELCOME LETTER

From the Director

We are in the midst of an exciting time of transition. Organizationally, TRICARE Management Activity is being cycled into a newer and larger organization as of October 1st, 2013, the Defense Health Agency (DHA). The Privacy and Civil Liberties Office will remain a bulwark of protection for our beneficiaries' personally identifiable information and protected health information at home and across the globe. Part of this transition will include new liaisons with the Services and other DoD organizations. Our mission will remain the same – protect information and comply with applicable laws and regulations.

The Health Insurance Portability and Accountability Act (HIPAA) is undergoing significant transformations, short and long term. In January of this year, the Department of Health and Human Services (HHS) published the Final Omnibus Rule, which modifies breach analysis, expands the role of business associates, and gives our beneficiaries some new rights, among other changes. There has been a steady change in HIPAA implementation for several years, and the trend is continuing. I refer to enhanced HIPAA enforcement, periodic audits conducted by HHS, and a large-scale shift toward the increased use of electronic medical records, both internally and externally for continuum of care purposes. These external parties include not only Veterans Affairs and Social Security Administration, but also private parties and other agencies.

Other transitions include the way in which our information security goals are accomplished, including an ongoing effort to produce a unified information security framework in alignment with the National Institute of Science and Technology (NIST) standards, and the development of a privacy overlay that attaches HIPAA Security requirements to the NIST standards through supplemental guidance.

These various factors give us a rich environment, full of challenge, yet full of opportunity. As we navigate these uncharted waters, we will reach our goal of privacy protection by holding fast to our core principles, including diligent exercise of care, and good follow-through using our best practices. When in doubt, please consult. The TMA Privacy and Civil Liberties Office is here for the greater organization and, though the name will change, it will retain an active role as part of the forthcoming DHA. It will take each and every one of us to succeed, but this is a good thing, because each and every one of us has what it takes to steer through these tides of change.



Linda S. Thomas, Director
TMA Privacy and Civil Liberties Office

HEALTH INFORMATION PRIVACY & SECURITY TRAINING

TABLE OF CONTENTS

Your Manual for Survival

Overview	1
HIPAA Privacy	2
HIPAA Security	8
Final HIPAA Omnibus Rule	12
Breaches and Complaints.	16
Human Research Protection Program	20
Data Sharing	22
Integrated Electronic Health Record	26
Virtual Lifetime Electronic Record	28
Military Command Exception.	30
HIPAA Audits	36
HIPAA Transactions, Code Sets, & Identifiers.	38

TMA PRIVACY & CIVIL LIBERTIES OFFICE

Overview

The TRICARE Management Activity (TMA) Privacy and Civil Liberties Office (Privacy Office) oversees the protection of personally identifiable information (PII) and protected health information (PHI) within the Military Health System (MHS), one of the largest integrated health care delivery systems in the United States, serving over 9.5 million eligible beneficiaries.

The TMA Privacy Office supports MHS compliance with federal privacy and security laws, and DoD regulations and guidelines. Each functional area within the TMA Privacy Office facilitates this mission by:

- Ensuring that DoD Health Affairs (HA) and TMA policies and business practices comply with federal laws, DoD regulations, and guidelines governing the privacy and security of PII/PHI, and in the development and revision of TMA privacy-related plans, policies, and procedures
- Managing and evaluating potential risks and threats to the privacy and security of MHS health data by performing critical reviews through:
 - Evaluation of privacy and security safeguards, including conducting annual Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Risk Assessments
 - Performance of Internal Privacy Office Compliance Assessments
 - Establishment of organization performance metrics to identify and measure potential compliance risks
- Engaging TMA stakeholders by developing and delivering education and awareness materials and ongoing workforce privacy and HIPAA security training

The TMA Privacy Office also provides dedicated assistance to the TMA Deputy Director and the Office of the Assistant Secretary of Defense in responding to inquiries from Congress, the Office of Management and Budget, the Department of Health and Human Services, and the Department of Veterans Affairs, as well as other federal agencies and DoD components, on matters related to privacy and HIPAA security.

This guide is a product of our training and awareness program and contains a summary of key programs and initiatives that will help the reader “survive” in the complex and demanding privacy and HIPAA security world.

HIPAA PRIVACY

Surviving the HIPAA Privacy Rule

The privacy of personal information, particularly health information, is a key issue across the globe. Individuals continue to express concern about losing control of their protected health information (PHI) as more of their information is computerized. Knowledge and implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule is a key covered entity (CE) survival skill in protecting PHI as well as permitting the flow of information for purposes of medical care and a variety of other essential activities.

KEY TERMS

HIPAA – Law that provides a comprehensive and uniform federal standard for the protection of health information. It applies to health care plans, health care clearinghouses and certain health care providers (“covered entities”). The law is implemented by the Department of Health and Human Services (HHS) through the adoption of standards, including standards for protecting the privacy and security of individually identifiable health information.

CE – A health plan, a healthcare clearinghouse, or a healthcare provider that conducts one or more covered transactions in electronic form.

PHI – Individually identifiable health information created or received by a CE that relates to the past, present or future physical or mental health of an individual and is transmitted or maintained in electronic, paper, or any other form. It excludes health information in employment records held by a CE in its role as employer. PHI does not include health information of persons deceased more than 50 years.

BUSINESS ASSOCIATE (BA) – A person or entity that creates, receives, maintains, or transmits PHI on behalf of the CE and is not considered a member of the CE workforce.

BUSINESS ASSOCIATE AGREEMENT (BAA) – A legal agreement between a CE and its BA that outlines responsibilities and obligations for compliance with HIPAA and the handling of PHI.

NOTICE OF PRIVACY PRACTICES (NOPP) – Document generated by a CE that describes how an individual's PHI may be used/disclosed, outlines individual privacy rights, describes CE obligations under HIPAA, and outlines the process for filing a complaint.

ORGANIZED HEALTH CARE ARRANGEMENT (OHCA) – All CEs under management authority of another entity. OHCA members may exchange PHI with each other for treatment, payment, and healthcare operations (TPO) reasons, have a joint NoPP, and share a common BA.

- The Military Health System (MHS) is organized as an OHCA and includes certain elements of the U.S. Coast Guard
- MHS includes all DoD health plans and all DoD healthcare providers

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC CLINICAL HEALTH (HITECH) ACT – The HITECH Act is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology in general (e.g. creation of a national health care infrastructure) and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers. The legislation anticipates a massive expansion in the exchange of electronic protected health information (ePHI), and therefore also widens the scope of privacy and security protections available under HIPAA. It also increases the potential legal liability for HIPAA non-compliance and provides for more enforcement.

USE – The sharing, employment, application, utilization, examination or analysis of PHI within an entity that maintains such information.

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

MINIMUM NECESSARY – Limiting the use, disclosure, and request for PHI to only the minimum amount needed to carry out the use or purpose of the disclosure. Exceptions to this standard are as follows:

- Disclosures to or by a healthcare provider for treatment purposes
- Disclosures to individuals or pursuant to individual's authorization
- Disclosures to HHS for HIPAA compliance purposes
- Uses or disclosures required by law

HIPAA INDIVIDUAL PRIVACY RIGHTS

HIPAA requires individuals be given certain rights, and the CE is responsible for responding to an individual's request to invoke any of these rights. The seven rights and the CE response to each are listed on the right:



<h2>I. RIGHT TO A NOPP</h2> <p>Notifies individuals how their PHI will be used and/or disclosed by the CE</p> <p>Describes individual privacy rights</p> <p>Outlines CE responsibilities and legal obligations</p> <p>Informs individual how to file a complaint</p>	<h2>CE RESPONSE</h2> <p>Use plain language in notice</p> <p>Obtain receipt of acknowledgement unless an emergency situation</p> <p>Ensure information on availability and distribution of notice</p> <p>Outline format of notice (i.e. Braille, large print, audio, etc.)</p> <p>Update notice when material changes</p> <p>Notify every three years of availability of notice and how to obtain the notice</p>
<h2>2. RIGHT OF ACCESS</h2> <p>Right to inspect and obtain a copy of PHI from a CE designated record set</p> <p>Right to receive PHI in electronic record in form/format requested if information maintained in an electronic record, including right to have PHI sent to designee, if desired - per HITECH</p> <p>Right to have PHI sent by unencrypted e-mail upon individual request</p> <p>Exceptions: Psychotherapy notes and information for a legal proceeding</p>	<h2>CE RESPONSE</h2> <p>Act on request no less than 30 days after receipt of request but no more than 60 days if there is a delay</p> <p>Provide written statement of reasons for delay and date CE will finalize the request</p> <p>Provide in form/format requested if readily producible; if not, in hard copy form or other agreed upon form</p> <p>Provide electronic access in form/format requested, if PHI maintained electronically; if not, in readable electronic form or other agreed upon form</p>
<h2>3. RIGHT TO ACCOUNTING OF DISCLOSURES</h2> <p>Right to know who has received PHI for reasons other than:</p> <ul style="list-style-type: none"> • Treatment, payment, or health care operations (TPO) • Disclosures specifically authorized by the patient • Incidental disclosures • As part of limited data set • Disclosures to law enforcement • Facility directory or persons involved in individual's care • Disclosures for specialized government functions 	<h2>CE RESPONSE</h2> <p>CE must act on individual's request for accounting no later than 60 days after the request. CE can have one 30 day extension if individual notified</p> <p>Must include disclosures for a period up to six years before the date of the request</p> <p>Documentation requirements</p> <p>MHS uses the Protected Health Information Management Tool (PHIMT) as a method for disclosure accounting</p>

4. RIGHT TO REQUEST AN AMENDMENT

Individual may request CE to amend PHI in a designated record set

Individual may provide statement if disagree with CE decision

Individual has right to a copy of CE rebuttal statement

CE RESPONSE

Right to require written requests; must respond within 60 days. CE can have one 30 day extension if individual notified. Able to deny if PHI not created by CE unless individual provides reasonable basis to believe that the originator of PHI is no longer available to act on the request

Able to deny if PHI would not be available for inspection under the individual's right to inspect and copy

Able to deny if PHI is accurate and complete

If accepted, include amendment to the record

Inform all who might possess amended PHI including BAs

5. RIGHT TO REQUEST RESTRICTIONS

Individual has right to request PHI restriction on use/disclosure to carry out TPO and disclosures to third parties

Individual must be informed of decision and any delay in writing; and provided completion date

Individual has right to request termination, in writing or orally (if documented)

HITECH provides individual right to request restriction on disclosures to health plans for services paid out of pocket

CE RESPONSE

CE is not required to agree, unless the disclosure is to a health plan for payment or healthcare operations and patient paid out of pocket in full (per HITECH)

CE must document and follow terms of restriction, if agree

CE can break agreed-upon restriction in emergency situations

CE can terminate if informs individual in writing and documents

Right not transferrable to another Military Treatment Facility (MTF); MTF request not effective throughout entire MHS

6. RIGHT TO CONFIDENTIAL COMMUNICATIONS	CE RESPONSE
<p>Individual has right to have PHI communicated via specified confidential means</p> <p>May restrict communication to one method or to alternate location</p>	<p>May require written request</p> <p>Healthcare providers must accommodate reasonable requests and cannot require explanation for request</p> <p>Health plans must accommodate reasonable requests if individual states disclosure could endanger him/her</p>
7. RIGHT TO FILE A COMPLAINT	CE RESPONSE
<p>With MTF</p> <p>With TRICARE Management Activity</p> <p>With Secretary, HHS</p> <p>Must be filed with HHS within 180 days of knowledge of incident</p>	<p>Establish a complaint process</p> <p>Must include information in NoPP about how to file complaint with Secretary, HHS, and the CE</p>

HITECH ACT

The key HIPAA-centric components of the HITECH Act modify HIPAA Privacy, Security and Enforcement Rules; modify the Breach Notification Rule; strengthen privacy protections for genetic information, and make BAs of CEs directly liable for HIPAA compliance. For more information see the Final HIPAA Omnibus Rule chapter.

POINT OF CONTACT

PrivacyMail@tma.osd.mil
for HIPAA Privacy-related questions

RESOURCES

Enclosed CD
Please see the enclosed CD for a detailed presentation on HIPAA Privacy

HIPAA Privacy Web Page
<http://www.tricare.mil/tma/privacy/hipaa-privacyrule.aspx>

DoD Health Information Privacy Regulation
DoD 6025.18-R, dated January 2003

HIPAA Privacy Rule
45 CFR Parts 160 and 164

HIPAA SECURITY

Putting HIPAA Security Safeguards to Work

The basic purpose of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule is to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) when it is stored, maintained, or transmitted. Complying with HIPAA Security Rule business practices and information technology safeguards help medical facilities survive threats and hazards to ePHI on a daily basis.

ePHI – Protected health information (PHI) in electronic form that is transmitted or maintained by electronic media. Medical information transmitted by traditional fax or by voice over the telephone or by paper copy is PHI. These materials are not considered ePHI.

WHO'S COVERED?

HIPAA Covered Entities (CE)	Examples in the DoD
Healthcare providers (including mental health) that transmit health information electronically in connection with certain transactions (such as claims)	Military treatment facilities (MTF) (medical/dental)
Individual and group health plans	TRICARE Health Plan
Healthcare clearinghouses	Companies that perform electronic billing on behalf of MTFs
Business associates (BA)	Healthcare services support contractors and other contractors that provide services that require access to PHI

THE HIPAA SECURITY RULE SAFEGUARDS

ADMINISTRATIVE SAFEGUARDS are designed to protect ePHI and to manage the conduct of the DoD CE's workforce using ePHI in the performance of their jobs. There are nine administrative safeguards identified in DoD 8580.02-R.

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- BA Contracts and Other Arrangements
- Evaluation

The Security Management Process is a crucial standard (DoD 8580.02-R, C.2.2) in the HIPAA Security Rule and contains the implementation specifications of Risk Analysis and Risk Management. These two specifications “form the foundation upon which an entity’s necessary security activities are built.”

For the Information Access Management standard (DoD 8580.02-R, C.2.5), the policies and procedures adopted for addressing the Information Access Management standard must be guided by DoD 6025.18-R and the Minimum Necessary Standard.

DoD 8580.02-R requires, at a minimum, annual technical and non-technical security evaluations (C2.9). These evaluations are based initially on the standards implemented under DoD 8580.02-R and subsequently changed in response to environmental or operational changes affecting the security of ePHI.

Annual security evaluations should include a review of the organizational safeguards, policies, and procedures in place, as well as a review of the security of the information systems and data.

PHYSICAL SAFEGUARDS, as defined by DoD 8580.02-R, are “physical measures, policies, and procedures to protect a CE’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

The Access Control and Validation Procedures specification (DoD 8580.02-R, C.3.2.5) requires policies and procedures for determining a person’s identity, as well as controlling a person’s access based on his/her job role. This may include implementing measures such as sign-in and/or escort for visitors to the areas of the facility that house information systems, hardware or software containing ePHI.

The Maintenance Records specification (DoD 8580.02-R, C.3.2.6) requires the DoD CE to keep records for all repairs performed at a facility, including who performed them, what was done, and when it was done. This includes implementing policies and procedures to document repairs and modifications to the physical components of a facility that are related to security, such as hardware, walls, doors, or locks.

According to the Accountability specification (DoD 8580.02-R, C.3.5.5) of the Device and Media Controls (C3.5) standard, the DoD CE must implement procedures to maintain logs, including maintenance records to keep track of: who has the devices or media, when they had possession, and where they kept the devices or media from the time of original receipt to time of final disposal or transfer to another person or entity.

TECHNICAL SAFEGUARDS, as defined by DoD 8580.02-R, are the technology and the policies and procedures for the use, the protection, and access to ePHI.

- Access Controls
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Access Controls carry out the implementation of the Information Access Management standard which set the rules about which workforce members can and should have access to which kinds of data, how much data they should access (in accordance with the minimum necessary rule), and what privileges they should have (read, write, etc.) in order to perform job functions.

Because electronically stored information can be lost, stolen, damaged, or destroyed if stored improperly or when equipment is moved, implementation specification for Data Backup and Storage (DoD 8580.02-R, C.3.5.6) requires that the DoD CE “create retrievable, exact copies of ePHI, when needed, before movement of equipment.”

DoD 8580.02-R does not require DoD CEs to protect unsolicited inbound transmissions, such as in e-mail from patients. However, as required by Assistant Secretary of Defense for Health Affairs (ASD(HA)) Memorandum, “Military Health System (MHS) Information Assurance (IA) Policy Guidance and MHS IA Implementation Guides,” 23 Feb 2010, MHS personnel shall not transmit sensitive information or PHI via the Internet/e-mail or other electronic means unless appropriate security controls (e.g., encryption, Public Key Infrastructure) are in place.

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on HIPAA Security

HIPAA Security Web Page

<http://www.tricare.mil/tma/privacy/hipaa-securityrule.aspx>

HIPAA Security Rule

45 CFR Parts 160, 162 & 164

DoD Health Information Security Regulation

DoD 8580.02-R, dated July 2007

ASD Memorandum

Disposition of Unclassified DoD Computer Hard Drives, dated June 4, 2001

ASD for Health Affairs Memorandum

MHS IA Policy Guidance and MHS IA Implementation Guides, dated February 12, 2010

POINT OF CONTACT

HIPAASecurity@tma.osd.mil

for HIPAA Security-related questions

FINAL HIPAA OMNIBUS RULE

Major Changes and Impacts

The January 25, 2013 release of the Final Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule by the Department of Health and Human Services (HHS) significantly modifies the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rules under HIPAA. TRICARE Management Activity (TMA) and the military medical departments will have to implement substantial “to-do” lists in order to comply with the new Omnibus Rule changes summarized below, and to survive the compliance deadlines of September 23, 2013 and September 22, 2014.

FAST FACTS

Modified the HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rules

Published at 78 Fed. Reg. 5566-5702, January 25, 2013

Compliance deadline of September 23, 2013, and a later deadline for conforming contract amendments

All Business Associate Agreements (BAA) in effect as of January 25, 2013, must be amended by September 22, 2014 or earlier, if they are renewed or amended in the interim

The TMA Privacy and Civil Liberties Office is developing an implementation strategy and project plan to address these changes

SUMMARY OF MAJOR CHANGES

BREACH RESPONSE

- The definition of breach is revised in a manner that will likely increase notifications to individuals and reporting to HHS
- Harm standard theoretically eliminated
- Now an actual or potential breach is presumed to be a breach unless the entity conducts a risk analysis and determines likelihood of access or use of the protected health information (PHI) to be very small
- Note: if encrypted or otherwise unavailable, not a breach under HIPAA/ Health Information Technology for Economic and Clinical Health Act (HITECH)

BUSINESS ASSOCIATE (BA) STATUS

HIPAA obligations apply directly to covered entities' (CE) business associates, including enforcement and penalties.

The definition of BA is expanded/clarified to include subcontractors, providers of transmission services with routine PHI access, and providers of personal health records.

BA must negotiate HIPAA-compliant BAAs with their subcontractors.

CIVIL PENALTIES

A new structure for setting and imposing civil money penalties was created, including an increase in the maximum penalty per violation at \$50,000 with an annual cap of \$1.5M for violations of an identical requirement or prohibition.

VIOLATION CATEGORY	EACH VIOLATION	MAXIMUM FINE
(A) Did Not Know	\$100 - \$50,000	\$1,500,000
(B) Reasonable Cause	\$1,000 - \$50,000	\$1,500,000
(C)(i) Willful Neglect-Corrected	\$10,000 - \$50,000	\$1,500,000
(C)(ii) Willful Neglect-Not Corrected	\$50,000	\$1,500,000



NOTICE OF PRIVACY PRACTICES (NOPP)

CEs must revise their NoPPs in accordance with the Final HIPAA Omnibus Rule.

The revised NoPPs must be made available to beneficiaries by the September 23, 2013 compliance date.

ELECTRONIC ACCESS TO PHI

Individuals have the right to receive an electronic copy of their PHI in designated record set maintained electronically in the form and format requested, if readily available, or as agreed.

Individual may designate another person to receive the electronic copy.

CEs may charge a reasonable, cost-based fee.

RESTRICTIONS ON DISCLOSURES OF SELF-PAID CARE

CE must agree to an individual's request for restrictions on disclosure, unless the disclosure is required by law, if the disclosure: is to a health plan; is for purposes of payment or health care operations; and pertains to a health care item or service paid for out-of-pocket in full.

RESEARCH AUTHORIZATIONS

Compound authorizations for conditioned and unconditioned research activities are permitted.

Authorizations are not required to be study-specific and thus may apply to future studies.

GENETIC INFORMATION

Health plans are prohibited from using or disclosing genetic information for underwriting purposes (i.e., health plan coverage and beneficiary cost sharing determinations).

Genetic information is defined broadly to include family history.

The definition of health information is clarified to expressly include genetic information.

PROOF OF IMMUNIZATION TO SCHOOLS

In states that require proof of immunization for school enrollment, CEs may disclose such proof without a written authorization if they obtain and document consent from a parent or legal guardian.

PHI STATUS AND DISCLOSURES AFTER DEATH

CEs may continue to make disclosures to family members or others involved in care or payment, unless the CE is aware that the individual had expressed a contrary preference.

PHI status continues for 50 years after death, after which HIPAA protections no longer apply.



RESOURCE

Final HIPAA Omnibus Rule
78 Federal Register, 5566-5702,
dated January 25, 2013

POINT OF CONTACT

PrivacyMail@tma.osd.mil for
HIPAA Privacy-related questions

BREACHES & COMPLAINTS

Prevention and Mitigation

Understanding what breaches and complaints are, why they occur, and how to prevent them will help to ensure you are able to survive in the Health Insurance Portability and Accountability Act (HIPAA) wilderness. Mishandled or misused personally identifiable information (PII) or protected health information (PHI) can result in a breach or HIPAA Privacy violation, but the tips on the next page can be a quick reference for methods to prevent breaches before they occur and for understanding how to mitigate breaches once they have been discovered. A critical element of breach and complaint management and prevention is the understanding of key definitions.

WHAT IS A BREACH?

UNDER THE PRIVACY ACT and as defined by DoD, a breach is the “actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected.”

UNDER HIPAA and as defined by the Department of Health and Human Services, a breach is the unauthorized acquisition, access, use, or disclosure of PHI which compromises the privacy or security of the PHI.

TRICARE MANAGEMENT ACTIVITY (TMA) PRIVACY CONTACTS

Identify your local privacy officer and ensure he or she is available as a resource to all staff members for relevant questions and concerns.

Linda Thomas,
Director, TMA Privacy and Civil Liberties Office, 703-681-7500
Linda.Thomas@tma.osd.mil

Rahwa Keleta,
HIPAA Compliance Manager,
TMA Privacy and Civil Liberties Office, 703-681-7500
Rahwa.Keleta@tma.osd.mil

WHAT IS A COMPLAINT?

HIPAA Privacy complaints typically result from an individual's belief that a covered entity has violated their health information privacy rights or such rights of another individual.

SUBSTANTIATED COMPLAINT:

A violation of the HIPAA Privacy and/or Security Rule has occurred.

UNSUBSTANTIATED COMPLAINT:

A violation of the HIPAA Privacy and/or Security Rule has not occurred.

POLICIES AND PROCEDURES

- Appropriate policies/procedures are critical in order to have an effective prevention and response management plan that includes: access, use, and disclosure of PII/PHI
- Safeguarding PII/PHI
- Breach reporting and complaint filing processes
- Documentation (communications, requests, findings)
- Mitigation and sanctions when PII/PHI is compromised
- HIPAA Privacy and Security training requirements

Awareness of the applicable privacy and security policies can be achieved when information is thoroughly disseminated to staff members and staff members are notified and trained appropriately on policy changes or updates.

BREACH PREVENTION TIPS

Secure hard copy documents containing PII/PHI (e.g., lock in a filing cabinet, desk, or office)

Log off when leaving your work station

Familiarize yourself with the TMA fax policy to prevent any unauthorized disclosure (i.e., check fax number, use a coversheet, and confirm receipt)

Encrypt e-mails containing PII/PHI when transmitting outside the network

Ensure there is no PII/PHI embedded or "hidden" in shared documents/files

Close the door and/or lower your voice when discussing PII/PHI

Access only the minimum necessary amount of PII/PHI you need for your position duties

Disclose PII/PHI only to authorized individuals with an official need for the information

Retrieve your documents from the printer promptly

Validate all contact information prior to sending postal mail

Protect your laptop at all times

The above tips can be used to avoid circumstances that lead to complaints.

BREACH REPORTING

When a loss, theft, or compromise of information occurs, the breach must be reported according to the local incident response team guidelines.

FOR TMA	FOR SERVICE COMPONENTS
Leadership: Immediately	Leadership: Immediately
TMA Privacy & Civil Liberties Office: Within 1 hr	US CERT: Within 1 hr
United States (US) Computer Emergency Readiness Team (CERT): Within 1 hr	DoD Component Sr. Privacy Officials: Within 24 hrs
Defense Privacy & Civil Liberties Office: Within 48 hrs*	TMA Privacy & Civil Liberties Office: Within 24 hrs
	Defense Privacy & Civil Liberties Office: Within 48 hrs

*TMA is responsible for reporting to the Defense Privacy & Civil Liberties Office

Note: If necessary, notify issuing banks (if government issued credit cards are involved); law enforcement; and all affected individuals within 10 working days of breach and identity discovery.

RESOURCES

Enclosed CD

Please see enclosed CD for detailed presentation on Breaches & Complaints

Breach Response Web Page

www.tricare.mil/tma/privacy/breach.aspx

HIPAA Privacy Web Page

www.tricare.mil/tma/privacy/hipaa-privacyrule.aspx

How to File a HIPAA Privacy Complaint

www.tricare.mil/tma/privacy/hipaa-PrivacyComplaint.aspx

POINTS OF CONTACT

PrivacyOfficerMail@tma.osd.mil
to report breaches and for breach-related questions

PrivacyMail@tma.osd.mil for HIPAA Privacy-related questions

HIPAASecurity@tma.osd.mil
for HIPAA Security-related questions

BREACH RESPONSE PROCESS

INCIDENT IDENTIFICATION	Examine all available information in order to determine if a breach has occurred
INCIDENT REPORTING	Disseminate information to the appropriate parties in a timely fashion
CONTAINMENT	Determine what actions can be taken immediately to limit the scope and magnitude of the breach
MITIGATION	Take actions to mitigate the harmful effects of the breach
ERADICATION	Remove the cause of the breach and mitigate all associated vulnerabilities
RECOVERY & FOLLOW-UP	Restore normal business operations and take measures to prevent future incidents

COMPLIANCE ENFORCEMENT

Enforcement of compliance should be reviewed and verified regularly.

- Include consequences and/or penalties for staff member non-compliance in your employee manual(s)
- Retraining and remedial training on the appropriate privacy policies
- Consider stiffer penalties such as suspension, revocation of access, and/or termination
- Enforce penalties consistently enough to deter breaches
- If the workforce sees little to no consequence for breaching PII/PHI, it may be less inclined to comply

TRAINING

Enforcement of staff training is essential to ensure compliance with the appropriate privacy and security policies. To do so:

- Confirm staff members are current with their annual privacy and HIPAA training
- Ensure staff members requiring remedial training have completed it
- Investigate whether job-specific training is available as needed and ensure your workforce is trained appropriately

HUMAN RESEARCH PROTECTION PROGRAM

Research Compliance

DoD supports and encourages research, including human subject research. All research protocols that include human subjects must be compliant with federal laws, federal regulations, and DoD policies intended to protect the subjects of the studies. The Human Research Protection Program (HRPP) provides guidance and enhances collaboration on research compliance issues. Research protocols are reviewed via the HRPP to determine if they meet the criteria for human subjects' research.

HRPP COMPLIANCE REVIEWS

The HRPP reviews compliance with:

- Department of Health and Human Services (HHS) Regulation, “Protection of Human Subjects,” 45 CFR 46, the “Common Rule”
- DoD Regulation, “Protection of Human Subjects,” 32 CFR 219
- DoD Instruction (DoDI) 3216.02, “Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research”

HRPP compliance reviews are required for research involving human subjects and all protocols must be submitted through IRBNet in order to obtain any type of review.

The Human Research Protection Official reviews studies approved by Institutional Review Boards (IRB) with federal-wide assurance from HHS and agreement with TRICARE Management Activity (TMA) attesting to its understanding of and adherence to DoD-specific protections, and includes:

- Initial review of approved protocols
- Requests to modify previously approved protocols
- Requests to continue a study beyond the expiration date of a previous approval

The HRPP office reviews protocols to determine if they meet the criteria for human subjects research and if so, conducts reviews to determine whether the research is exempt from IRB review. If exempt, the HRPP office reinforces the understanding that “exempt” protocols must still adhere to the ethical standards set forth in the Common Rule and other applicable regulations by continuing to monitor exempt protocols until completion of the study.

HRPP TRANSITION

HRPP transitioned in mid-2011 from Defense Health Cost Assessment and Program Evaluation to the TMA Privacy and Civil Liberties Office.

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on HIPAA Research and Data Sharing

HRPP Web Site

<http://www.tricare.mil/tma/privacy/hrpp/default.aspx>

Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research

DoDI 3216.02

POINT OF CONTACT

TMA_HRPP@tma.osd.mil for HRPP-related questions

DATA SHARING

Requesting Access to Data Managed by TMA

The TRICARE Management Activity (TMA) Privacy and Civil Liberties Office (Privacy Office) receives various types of data sharing requests for Military Health System (MHS) data owned or managed by TMA. Examples of these data sharing requests are summarized below. Under its Data Sharing Program, the TMA Privacy Office reviews each request for compliance with applicable federal and DoD regulatory requirements. Applicants for MHS data must comply with all applicable standards and safeguard the integrity of the data received.

DATA SHARING AGREEMENT (DSA) PROGRAM

The purpose of a **DSA** is to:

- Identify the type of data owned and/or managed by TMA that is required to meet a specific data request
- Ensure compliance with applicable DoD regulations and privacy laws
- Set forth permissible uses and disclosures in accordance with regulatory requirements
- Document the agreed upon responsibilities of the Applicant/Recipient and Government Sponsor
- Provide clear terms and conditions for approving the data request

DATA SHARING AGREEMENT APPLICATION (DSAA) – An application designed to assist in reviewing a data request for compliance with applicable regulatory requirements.

The DSA team reviews DSAs upon submission and considers the following reviews (as applicable):

- Data Request Templates (DRT), which is a listing of data elements requested for research studies
- Status of Human Research Protection Program (HRPP) review
- TMA Privacy Board review
- Defense Health Cost Assessment and Program Evaluation (DHCAPE) TMA survey program review
- System security verification review
- Health Insurance Portability and Accountability Act (HIPAA) minimum necessary standard review
- Confirmation that business associate agreement language is included in underlying project documentation
- Privacy Act compliance review

Once all compliance reviews are completed and the DSAA is approved by the TMA Privacy Office, one of the following DSAs will be executed based on the type of data requested:

- DSA for de-identified data
- DSA for personally identifiable information (PII), excluding protected health information (PHI)
- DSA for limited data set (LDS), known as a Data Use Agreement
- DSA for PHI

DSAA MUST BE INITIATED BY THE FOLLOWING:

Applicant – the individual who will provide primary oversight and responsibility for the handling of the requested data.

- For contract-driven requests, must be employee of prime contractor
- For projects with more than one prime contractor, must be completed by each prime contracting organization that will have custody of the requested data

Government Sponsor – the point of contact within TMA or the respective Armed Service who assumes responsibility for the contract, grant, project, or Cooperative Research and Development Agreement.

Requests for data managed by TMA are reviewed for compliance with various data sharing requirements and must be submitted through a DSAA.

RESEARCH DATA SHARING STREAMLINING INITIATIVES

Streamlining measures are currently underway to prepare some multi-service markets for their DoD IRBs to take on the responsibility of conducting the required HIPAA Privacy Rule reviews and generating appropriate HIPAA compliant documentation.

THE FOUR PROPOSED STREAMLINING MEASURES ARE:

1. Create uniform MHS-wide HIPAA Privacy Rule Review templates
2. Develop agreements with select multi-service markets and set conditions under which TMA Privacy Board review may no longer be required
3. Alleviate the current requirement for government personnel seeking data for research purposes to submit a DSAA
4. Maintain the DSAA requirement for research-related contractors, however, where multi-service market agreements are in place with TMA, no longer require TMA Privacy Board review and accept DSAs from research foundations/organizations exclusively conducting research within the multi-service market

TMA PRIVACY BOARD

The TMA Privacy Board reviews research related data requests for PHI for compliance with the HIPAA Privacy Rule.

There are four types of Privacy Board reviews:

1. Required Representations for Research on Decedent's Information – use or disclosure of PHI solely for research on decedents
2. Required Representations for Review Preparatory to Research
 - a. Use or disclosure of PHI solely for preparing a research protocol or similar purpose
 - b. Researchers agree not to remove PHI from TMA during review
3. Studies that must obtain HIPAA Authorizations
4. Studies that require a Waiver of Authorization or an Altered Authorization



RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on HIPAA Research and Data Sharing

DSA Web Page

<http://www.tricare.mil/tma/privacy/duas.aspx>

TMA Privacy Board Web Page

<http://www.tricare.mil/tma/privacy/privacyboard.aspx>

DoD Health Information Privacy Regulation

DoD 6025.18-R,
dated January 2003

DoD Health Information Security Regulation

DoD 8580.02-R,
dated July 2007

POINTS OF CONTACT

TMAPrivacyBoard@tma.osd.mil
for TMA Privacy Board questions

PrivacyMail@tma.osd.mil for
HIPAA Privacy-related questions

INTEGRATED ELECTRONIC HEALTH RECORD

The Way Ahead

In February 2011, the Deputy Secretary of Veterans Affairs, the Deputy Secretary of Defense, and the Vice Chairman of the Joint Chiefs of Staff agreed to an approach for joint development of an integrated Electronic Health Record (iEHR) system to integrate healthcare capability and enhance and streamline the care and benefits provided to our Service members, Veterans, and their beneficiaries. The iEHR solution will create a seamless healthcare record for each Service member, from swearing-in through final honors the iEHR solution will promote health information exchange to the DoD and Department of Veterans Affairs (VA) population.

THE ROLE OF THE INTERAGENCY PROGRAM OFFICE (IPO)

The IPO serves as the single point of accountability for the VA and DoD for:

- iEHR
- Virtual Lifetime Electronic Record (VLER) Health
- Full health information interoperability between VA and DoD

iEHR PROJECT SCOPE

Health Information Technology services provided for a combined beneficiary population of more than 18 million beneficiaries, 440,300 practitioners, and 1,864 medical facilities (including hospitals and medical and dental clinics), and it is projected to grow to ultimately include more than 30 million users.

IEHR EXPECTED BUSINESS BENEFITS

POPULATION HEALTH <i>Improve the overall health of the population</i>	Enhanced patient safety and care Better availability of individual/ population health measures Access to longitudinal patient data for research
PATIENT & PROVIDER SATISFACTION <i>Enhance the patient and provider experience</i>	Better care transfers from DoD to VA Improved user interface design and reduced errors Efficient workflows Improved diagnostic accuracy
COST EFFICIENCY <i>Make the cost of healthcare sustainable</i>	Decreased total cost of care through more efficient care delivery More effective gathering of information Decreased information technology costs
MEDICAL READINESS <i>Maximize medical readiness for our military</i>	Timely access to Individual Medical Readiness (IMR) data Timely access to computable IMR data

IEHR BUSINESS NEEDS

Integrate DoD/VA medical records and applications

- Different formats of patient information (paper/electronic)
- Consolidate scattered data and information
- Avoid fragmented medical records prevent a logical or longitudinal health record
- Modernize VA/DoD healthcare legacy systems to improve delivery of quality of care

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on iEHR

POINT OF CONTACT

PrivacyMail@tma.osd.mil for privacy questions related to emerging technologies

VIRTUAL LIFETIME ELECTRONIC RECORD

Incremental Rollout

The Virtual Lifetime Electronic Record (VLER) is DoD's standardized capability to electronically exchange information amongst members of a network that is either defined or dynamically created. Data is transmitted using standardized formats agreed to by participants in the eHealth Exchange (formerly the Nationwide Health Information Network). VLER and the integrated Electronic Health Record (iEHR) are intertwined, and privacy implications are associated with both initiatives. Privacy subject matter experts need to ensure the survival of privacy requirements during the VLER development.

WHAT IS THE VLER?

- VLER is DoD's standardized capability to electronically exchange information amongst members of a network including other federal agencies such as the Department of Veterans Affairs (VA) and private providers
- Exchanged data will include health, benefits, and administrative data
- Extracts health and demographic data from a base system, Armed Forces Health Longitudinal Technology Application (AHLTA), which links to records from military treatment facilities (MTF)

FOUR PRODUCTION SITES:

San Diego, California
Tidewater area of Virginia
Spokane, Washington
Puget Sound, Washington

- Data is transmitted using standardized formats agreed to by participants in the eHealth Exchange

UPCOMING SOFTWARE UPDATES

ELIGIBILITY EXPANSION – VLER data sharing expanded to include non-active duty beneficiaries such as family members.

OPT OUT – Some beneficiaries will have the choice to not share data with network participants.

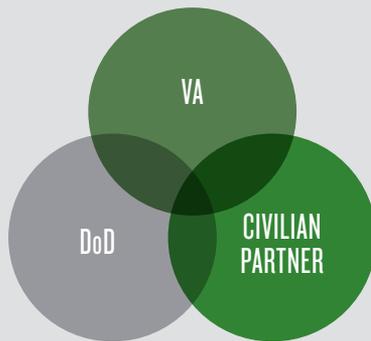
SOCIAL SECURITY ADMINISTRATION (SSA) DEFERRED PATIENT DISCOVERY – Document exchange initiated by SSA with consent form review process.

PERFORMANCE ENHANCEMENTS
Optimization of VLER adapter code to include fan-out to allow parallel queries to all external partners, as well as real-time display update of the communication status. This will increase the speed of data exchange.

“...I’m asking both departments to work together to define and build a seamless system of integration with a simple goal: When a member of the Armed Forces separates from the military, he or she will no longer have to walk paperwork from a DOD duty station to a local V.A. health center. Their electronic records will transition along with them and remain with them forever.”

—President Barack Obama
April 9, 2009

VLER: DATA EXCHANGE OVERLAPS



RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on VLER

**VLER Capability Area 1
Concept of Operations v 2.0**
dated April 8, 2011

POINT OF CONTACT

PrivacyMail@tma.osd.mil for privacy questions related to emerging technologies

MILITARY COMMAND EXCEPTION

Disclosing PHI of Armed Forces Personnel

In accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and applicable DoD issuances, a DoD covered entity (CE) may use or disclose the protected health information (PHI) of Armed Forces members for activities deemed “necessary by appropriate military command authorities to assure the proper execution of the military mission.” This military command exception to HIPAA confidentiality protections defines when DoD providers may (1) disclose PHI of Service members to military commanders or (2) use PHI for military commanders’ purposes such as evaluating fitness for duty. If the specific requirements of this military command exception are satisfied, patient authorization is not required for such uses or disclosures.

What follows is a summary of how the military command exception applies to DoD CEs. The military command exception as stated in 45 CFR 164.512(k)(1)(i) also applies to CEs outside of DoD, such as non-government hospitals and other healthcare providers. Those entities, however, are not subject to the DoD issuances referenced on the next page.

MILITARY COMMAND AUTHORITY

Commander with authority over a member of the Armed Forces

Other person designated by such commander

Designee of an appropriate Secretary or another official delegated authority by such Secretary

WHAT IS “NECESSARY TO ASSURE PROPER EXECUTION OF THE MILITARY MISSION”?

Under paragraph C7.11.1.3 of DoD 6025.18-R, “DoD Health Information Privacy Regulation,” January 24, 2003, the military purposes for which PHI may be used or disclosed include:

1. Determining the member’s fitness for duty, including but not limited to compliance with:
 - DoD Directive 1308.1, “DoD Physical Fitness and Body Fat Program,” June 30, 2004;
 - DoD Instruction 1332.38, “Physical Disability Evaluation,” November 14, 1996 (incorporating Change 2, April 10, 2013); and,
 - DoD Instruction 5210.42, “Nuclear Weapons Personnel Reliability Program (PRP),” July 16, 2012
2. Determining the member’s fitness to perform any particular mission, assignment, order, or duty, including any actions required as a precondition to performance
3. Carrying out comprehensive health surveillance activities in compliance with DoD Directive 6490.02E, “Comprehensive Health Surveillance,” February 8, 2012
4. Reporting on casualties in connection with a military operation or activity in accordance with applicable military regulations or procedures
5. Carrying out other activities necessary to the proper execution of the Armed Forces’ mission



MILITARY COMMAND AUTHORITIES

Appropriate military command authorities include commanders who exercise authority over a member of the Armed Forces, or other person designated by such a commander to receive PHI to carry out an activity under that commander's authority.

Other appropriate authorities include any official designated for this purpose by the Secretary of Defense, the Secretary of the applicable Military Department, or the Secretary of Homeland Security (for Coast Guard activities not under the Navy).

DISCLOSURE ACCOUNTING

Disclosures to military commanders must be tracked for disclosure accounting purposes. See paragraph C13.2.3 of DoD 6025.18-R for guidance. Tracking is best accomplished by recording military command exception disclosures in the Protected Health Information Management Tool (PHIMT) at the time those disclosures are made.

Visit <http://www.tricare.mil/tma/privacy/ProtectedHealthInformationManagementTool.aspx>.

MEDICAL APPOINTMENT NOTIFICATION

Command authorities and/or their designees may require notification of medical appointments for Armed Forces personnel for purposes related to the execution of the military mission, such as fitness for duty determinations or assignment coverage. Medical appointment notifications include treatment reminders (physicals, immunizations, laboratory, etc.) and notifications of missed and cancelled appointments.

The military command exception applies only to disclosures of Armed Forces personnel PHI. PHI of family members or other categories of beneficiaries is never shared with military command authorities without a HIPAA-compliant authorization.

MENTAL HEALTH AND/ OR SUBSTANCE MISUSE DISCLOSURES

To foster DoD's culture of support in the provision of mental health care and voluntarily sought substance abuse education to military personnel, DoD Instruction 6490.08, "Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members," August 17, 2011, provides guidance regarding command notification requirements.

CEs shall not notify a Service member's commander when the member obtains mental health care or substance abuse education services, unless a certain condition or circumstance is met. See Enclosure 2, paragraph 3.b. of DoDI 6490.08.

In contrast to the HIPAA Privacy Rule, the Alcohol, Drug Abuse, and Mental Health Administration (ADAMHA) Reorganization Act regulations broadly permit "interchange of that information within the Armed Forces;" however, the disclosure of PHI must satisfy both ADAMHA and the HIPAA Privacy Rule. Therefore, it is not sufficient that a disclosure by a military treatment facility (MTF) provider to a commander is a permitted "interchange . . . within the Armed Forces." The disclosure must separately comply with the HIPAA military command exception.

DODI 6490.08: DISCLOSURE OF PHI RELATING TO MENTAL HEALTH CARE OR SUBSTANCE ABUSE TREATMENT

Command notification by CEs is not permitted for Service member self and medical referrals for mental health care or substance misuse education unless the disclosure is authorized under subparagraphs 1.b.(1) through 1.b.(9) of Enclosure 2. If one of those provisions applies, then notification is required.

Notifications shall generally consist of the diagnosis; a description of the treatment prescribed or planned impact on duty or mission, recommended duty restrictions, and the prognosis.

MINIMUM NECESSARY RULE

When disclosing PHI to military commanders, CEs must make reasonable efforts to limit the disclosure to the “minimum necessary” to accomplish the intended purpose. See paragraph C8.2 of DoD 6025.18-R. Additionally, disclosures of PHI should only be made to command authorities with an official need for the information.

Under DoDI 6490.08, required mental health or substance misuse disclosures to military commanders should, in general, consist of the diagnosis; a description of the treatment prescribed or planned; impact on duty or mission; recommended duty restrictions; the prognosis; any applicable duty limitations; and implications for the safety of self or others.

The Minimum Necessary Rule states that a CE should limit the use or disclosure of PHI to the “minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”

THE PRIVACY ACT OF 1974

Military commanders who receive PHI have special responsibilities to safeguard the information and limit any further disclosure in accordance with the Privacy Act of 1974 and the DoD Privacy Program as now or hereafter in effect. The current DoD Privacy Program is set forth in DoD 5400.11-R.



RECOMMENDED MTF POLICIES AND PROCEDURES

The following policies and procedures are recommended regarding the disclosure of Armed Forces members' PHI to appropriate military command authorities:

1. Designate person(s) at an MTF with authority to release PHI to commanders
2. Maintain documentation of commanders and other designees to whom Service members' PHI may be disclosed
3. Train personnel on circumstances where PHI disclosures to military command authorities are and are not appropriate
4. Implement measures to ensure only the minimum necessary PHI is disclosed (e.g., a clinical summary rather than the entire medical record)
5. Educate personnel on use of PHIMT to comply with disclosure accounting requirements

POINT OF CONTACT

PrivacyMail@tma.osd.mil for questions regarding the HIPAA Privacy Rule and the Military Command Exception



RESOURCES

DoD Health Information Privacy Regulation

DoD 6025.18-R,
dated January 2003

DoD Privacy Program

DoD 5400.11-R,
dated May 14, 2007

Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members

DoDI 6490.08,
dated August 17, 2011

HIPAA Privacy Web Page

<http://www.tricare.mil/tma/privacy/hipaa-privacyrule.aspx>

TMA Privacy Military Command Exception Web Page

<http://www.tricare.mil/tma/privacy/Military-Command-Exception.aspx>

HIPAA AUDITS

Audits under HITECH

The American Recovery and Reinvestment Act of 2009, in Section 13411 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, requires the Department of Health and Human Services (HHS) to provide for periodic audits to ensure covered entities (CE) and business associates (BA) are complying with criteria associated with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and Breach Notification standards. CEs and BAs can survive the loss of contracts, civil and criminal investigation, fines, and other penalties associated with this audit program by conducting robust reviews and assessments, mapping the movement of protected health information within their organizations, and complying with HHS guidance.

TOP PRIVACY AND SECURITY PROBLEMS

PRIVACY RULE	SECURITY RULE
Policies and procedures	User activity monitoring
Complaints	Contingency planning
Privacy training	Authentication/integrity
Mitigation of known harmful effects on non-compliance	Media reuse and destruction

GETTING READY FOR AN AUDIT

Ensure you have the documentation required by the HIPAA Privacy and Security Rules:

- Mapping of information security controls to the HIPAA Security Rule and DoD 8580.02-R standards, as well as required and addressable implementation specifications
- Copy of a risk assessment conducted within the past 12 months, and resulting risk management plan
- Written continuity of operations plan

Review HITECH Omnibus Final Rule and the changes it makes to the HIPAA Privacy and Security Rules to determine how it impacts your organization's internal compliance procedures and processes.

If you are a military treatment facility, ensure you have documented how your organization handles access to or amendment of individual's health information, alternative communications, restrictions on disclosures, and accounting of disclosures.

Ensure your workforce is appropriately trained in HIPAA Privacy and Security matters applicable to your organization/facility and its duties.

GOALS OF HITECH AUDIT PROGRAM

Ensure CEs and BAs are complying with HIPAA Privacy and Security Rules and Breach Notification standards

Spur CEs and BAs to assess and calibrate their privacy and security protections

Permit Office for Civil Rights to develop best practices and guidance targeted to meeting observed compliance challenges

Provide for overall improvement in CE and BA compliance with HIPAA standards

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on HIPAA Audits

DoD Health Information Privacy Regulation

DoD 6025.18-R, dated
January 2003

DoD Health Information Security Regulation

DoD 8580.02-R, dated July 2007

POINT OF CONTACT

PrivacyMail@tma.osd.mil for
HIPAA audit-related questions

HIPAA TRANSACTIONS, CODE SETS & IDENTIFIERS

HIPAA Compliance

Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification provisions required Department of Health and Human Services (HHS) to establish national standards for electronic healthcare transactions, code sets, and identifiers. National standards for HIPAA transactions, code sets, and identifiers improve the effectiveness and efficiency of the health care industry in general, by simplifying the administration of the system and enabling the efficient electronic transmission of certain health information.

While the TRICARE Management Activity (TMA) Privacy and Civil Liberties Office supports Military Health System compliance with HIPAA and other federal privacy and security laws, TMA's Information Management Division oversees compliance with HIPAA transactions, code sets, and identifier regulations, and HIPAA Certificates of Creditable Coverage for portability. Regulations for HIPAA transactions, code sets, and identifiers mandate the electronic standards that must be used when conducting named and adopted administrative healthcare transactions such as enrollment in a health plan, eligibility checking, referrals, and claims processing. HIPAA mandated

identifiers include the Employer Identifier, the National Provider Identifier, and the upcoming Health Plan Identifier. These identifiers are used within HIPAA transactions to identify employers, providers, and health plans.

HIPAA also mandates the use of certain code sets within the HIPAA transactions. For example, ICD-10 (the International Classification of Diseases, 10th Edition, Clinical Modification/Procedure Coding System) is a code set required by HIPAA.



WHICH COVERED ENTITIES NEED TO COMPLY?

Providers (e.g., military treatment facilities, civilian clinics, hospitals, individual and group provider practices)

Health Plans (e.g., TRICARE, Blue Cross/Blue Shield)

Clearinghouses (e.g., ePremise, Emdeon)

Business associates of the CEs (e.g., Defense Enrollment Eligibility Reporting System/ Defense Manpower Data Center, Managed Care Support Contractors)

RESOURCES

HIPAA Web site

<http://www.tricare.mil/tma/hipaa/hipaageneralinformation.aspx>

POINT OF CONTACT

HIPAAMail@tma.osd.mil for questions related to HIPAA Transactions, Code Sets, and Identifiers

HEALTH INFORMATION PRIVACY & SECURITY TRAINING

FOR MORE INFORMATION

703-681-7500 / www.tricare.mil/tma/privacy

