



HEALTH AFFAIRS



TRICARE
Management
Activity

Privacy Essentials: Uses and Disclosures

Quarterly Training 2007

TMA Privacy Office



Objectives (1 of 2)

- Upon completion of this module, you should be able to:
 - Define use and disclosure
 - Explain how to document disclosures in Protected Health Information Management Tool (PHIMT)
 - Explain legal and regulatory requirements
 - Describe minimum necessary rule in use and disclosure
 - Describe how to de-identify PHI and what the identifiers are
 - Identify the 14 Permitted uses for disclosure

Uses and Disclosures

Objectives (2 of 2)

- Upon completion of this module, you should be able to:
 - Identify when PHI can be released to the Department of Veterans Affairs (DVA)
 - Explain patient safety rules and other uses and disclosures
 - Define authorizations to disclose
 - Explain 42 CFR Part 2 vs. DoD 6025.18-R

Uses and Disclosures

Use and Disclosure Defined

- **Use** is the sharing of information within an entity
- **Disclosure** is the sharing or release of PHI in any manner outside the covered entity
- HIPAA requires the use and disclosure of PHI in three instances only:
 - TPO
 - To the individual when requested
 - To the HHS Secretary to determine compliance
- Other uses and disclosures are permitted subject to the requirements of the Rule (without the patient's opportunity to agree or object)

Documentation of Disclosures

- Disclosures are documented in the PHIMT
- The PHIMT is a web-based application that assists in complying with the HIPAA Privacy disclosure accounting requirement
 - Centrally managed application that is accessed via the Internet
 - Allows the MHS to
 - Track disclosures across the organization, and
 - Provide organization-wide accounting of disclosures
- PHIMT allows users to document disclosures and streamline the disclosure process
- A general rule is disclosures with an authorization do not have to be accounted for
 - Exceptions include certain marketing and fund raising activities
 - Disclosures to Commanders must be accounted for

DoD Health Information Privacy Regulation 6025-18R (1 of 3)

- Implements HIPAA requirements throughout DoD
 - A covered entity (including a covered entity not part of or affiliated with the DoD) may use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure proper execution of the military mission

DoD Health Information Privacy Regulation 6025-18R (2 of 3)

■ Appropriate Military Command Authorities

- All Commanders who exercise authority over an individual who is a member of the Armed Forces
- A person designated by a Commander to receive PHI
- The Secretary of Defense
- The Secretary of the Military Department for the Armed Forces for which the individual is a member
- The Secretary of Homeland Security has command authority of a member of the Coast Guard

DoD Health Information Privacy Regulation 6025-18R (3 of 3)

- Purposes for which PHI may be used or disclosed to the military commander to:
 - Determine member's fitness for duty
 - Determine member's fitness to perform mission, assignment, order, or duty, including compliance with any actions required as a pre-condition to performance of such mission, assignment, order or duty
 - Carry out any other activity necessary to the proper execution of the mission of the Armed Forces
 - Minimum Necessary still applies

Uses and Disclosures

Service Requirements

■ Air Force

- Air Force Instruction 41-210
- Air Force Instruction 41-217
 - Patient Administration Functions
 - Health Information Assurance for Military Treatment Facilities

■ Navy

- SECNAV Instruction 5211.5E
- Department of Navy Privacy Act Program

■ Army

- Army Regulation 40-66
 - Medical Record Administration and Health Care Documentation

Minimum Necessary Requirement

- All uses and disclosures of information are limited by the 'need-to-know' standard
- Only the amount of information reasonably necessary to achieve the purpose of the release is permitted

De-Identified Health Information

- You may use PHI to create de-identified health information
- De-identified health information is not subject to regulation
- Two methods to verify de-identification of information:
 - Expert in statistical analysis and de-identification of information must analyze the information and attest that it does not contain elements that would identify an individual or aid in the identification of an individual when combined with other available data. The method of analysis and results must be documented
 - Remove the listed identifiers associated with the individual, relatives, employers or household members and any other information that might identify the individual

Identifiers (1 of 3)

- Names
- Geographic subdivisions smaller than a state (e.g. street address, city, county, precinct, zip code)
- All dates (except year) (e.g. birth date, admission date, date of death etc.)
- All dates and numbers (including year) that indicate a persons age if over 89
- Telephone and fax numbers
- Email address
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- URLs

Uses and Disclosures

Identifiers (2 of 3)

- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Uses and Disclosures

Identifiers (3 of 3)

- Any other unique identifying number or characteristic except an assigned code that meets HIPAA requirements
- Codes assigned to aide in re-identification may not use information related to individual or allow a person to identify the individual
- You must not use or disclose code for any other purpose
- You must not disclose the re-identification mechanism

Limited Data Set (1 of 2)

- A CE may use or disclose a limited data set that meets the following requirements:
 - Limited Data Set
 - Permitted Purposes for Uses and Disclosures
- Limited Data Set
 - PHI that excludes the direct identifiers of the individual or of relatives, employers, or household members of the individual
 - A CE may use PHI to create a limited data set that meets the requirements or disclose PHI only to a BA for such purpose, whether or not the limited data set is to be used by the CE

Limited Data Set (2 of 2)

■ Exclusions:

- Names
- Postal address information
- Telephone numbers
- Fax numbers
- E-mail addresses
- Vehicle Identification numbers and serial numbers, including license plate numbers
- Device identifiers
- Web Universal Resource Locators (URL)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images

Permitted Uses & Disclosures (1 of 4)

- A CE may use and disclose a limited data set for the purposes of research, public health, or health care operations
- There are 14 categories of permitted uses and disclosures of PHI that do not require that we give the individual the opportunity to agree or object
- Some examples:
 - Avert serious threat to health or safety
 - Specialized government functions/military provisions
 - Judicial and administrative proceedings
 - Victims of abuse, neglect or domestic violence
 - Law enforcement purposes

Permitted Uses & Disclosures (2 of 4)

- You may use and disclose PHI for TPO :
 - For your own TPO activities without a patient authorization
 - To another provider for use in treating an individual without a patient authorization
 - To another CE to aide in payment activities without a patient authorization
 - To another DoD CE for use in health care operations without a patient authorization because they are both members of a single OHCA
 - For some but not all healthcare operation activities to a non-OHCA member if both have an established relationship with the individual

Permitted Uses & Disclosures (3 of 4)

- Those health care operations including but not limited to:
 - Quality Assurance (QA) and improvement activities
 - Population based activities relating to improving health or reducing costs
 - Protocol development
 - Case management and care coordination
 - Providing information about treatment alternatives
 - Competence or qualification reviews of health care professionals

Permitted Uses & Disclosures (4 of 4)

- Evaluating provider or practitioner performance
- Health plan performance
- Training programs for health care providers
- Training of non-health care professionals
- Accreditation, certification, licensing, or credentialing activities
- Health care fraud and abuse detection or compliance

Other Uses and Disclosures

Other Uses and Disclosures

Objectives

- Upon completion of this module, you should be able to:
 - Define the other uses and disclosures

Other Uses and Disclosures- Business Associates

■ BAs will:

- Use and disclose PHI only for purposes permitted by the contract or HIPAA
- Use appropriate safeguards to prevent use or disclosure of the PHI other than as permitted by the contract
- Report to the CE any use or disclosure of the information not provided for by its contract

Other Uses and Disclosures Workforce

- Workforce members or BAs may disclose PHI to the proper authorities or their attorney if they believe the CE is:
 - Engaged in unlawful activity
 - Violating professional or clinical standards
 - Potentially endangering patients, workers or the public through care, services or conditions
- Workforce members who are victims of a crime may disclose to law enforcement officers those elements of the suspect's PHI that identify the suspect

Other Uses and Disclosures- Patient Safety (1 of 2)

- Patient Safety and Quality Improvement Act of 2005 (P.L. 109-41)
- Purpose: Improve patient safety and reduce the incidence of events that adversely effect patient safety
- Enables providers to contract voluntarily and at their own cost with HHS certified Patient Safety Organizations (PSOs) to:
 - Identify and analyze threats to patient safety
 - Change health care structures and processes to improve health outcomes without fear that data will be disclosed or used in legal or administrative proceedings against them

Other Uses and Disclosures- Patient Safety (2 of 2)

- “Patient safety work products” resulting from providers working with PSOs are treated as confidential and privileged
- HIPAA still applies

Other Uses and Disclosures - Psychotherapy

Notes (1 of 2)

- Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the content 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
- The disclosure must be accounted for in PHIMT

Other Uses and Disclosures-Psychotherapy

Notes (2 of 2)

- Authorization is required, except for:
 - TPO carried out by the:
 - Originator of the psychotherapy notes
 - Covered entity for training
 - Covered entity to defend itself in a legal action
 - Uses and disclosures that are:
 - Required by the Secretary of HHS
 - Required by law
 - For healthcare oversight activities
 - About decedents to coroners and medical examiners
 - To avert a serious and imminent threat

Other Uses and Disclosures

- Incidental use or disclosure is permitted if you already comply with all of the minimum necessary requirements and have established appropriate administrative, physical, and technical safeguards to protect the privacy of PHI
- Incidental uses and disclosures include:
 - Overheard conversations among providers or with patients
 - Sign in sheets and calling patient names in waiting rooms
 - Paging patients in the facility
 - Posting patient names by doors
 - Maintaining a chart by patient's bed
 - Discussing patient's condition during rounds

Other Uses and Disclosures MOA

- Memorandums of Agreement (MOAs) are an integral part of the data process
- MOAs are established between government agency's to allow for sharing of MHS data
- The agreements:
 - Delineate the confidentiality of the Privacy Act and DoD's data use policies and procedures
 - Inform data users of these requirements and serve as a means of obtaining their agreement to abide by these requirements
 - Are a control mechanism through which DoD can track the location of its data and the reason for the release of the data

Other Uses and Disclosures - DUA (1 of 5)

- DUAs are an integral part of the data use approval process
- DUAs are established between a DoD and a non-DoD entity, including contractors, researchers, etc
- The agreements:
 - Delineate the confidentiality of the Privacy Act and DoD's data use policies and procedures
 - Inform data users of these requirements and are a means of obtaining their agreement to abide by these requirements
 - Are a control mechanism through which DoD can track the location of its data and the reason for the release of the data

Other Uses and Disclosures - DUA (2 of 5)

- DoD has developed a number of standard DUAs, all of which are designed to ensure that:
 - Requesters use DoD data only for the purposes cited in the request
 - Requesters will not release DoD data to other organizations without prior written DoD approval
 - Requesters will take reasonable steps to implement appropriate procedural, administrative, technical, and physical safeguards to prevent unauthorized use
 - Requesters do not publish any information that identifies individual beneficiaries or providers, or permits the identity of a beneficiary or provider to be deduced
 - A limit is established on the period of time a requester may retain DoD data before the data must be destroyed

Other Uses and Disclosures - DUA (3 of 5)

- A CE may use or disclose a limited data set if the CE obtains satisfactory assurance, in the form of a DUA, that the limited data set recipient shall only use or disclose the PHI information for intended purposes
- The DUA does not authorize the limited data set recipient to further disclose the information in a manner that would violate this agreement
 - Establish who is permitted to use or receive the limited data set
 - Use appropriate safeguards to prevent use or disclosure of information other than as provided for by the DUA

Other Uses and Disclosures - DUA (4 of 5)

- The limited data set recipient shall
 - Not use or further disclose the information other than permitted by the DUA or as required by law
 - Report to the CE any use or disclosure of the information not provided for by is DUA of which it becomes aware
 - Ensure that any agents, including subcontractors, 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
 - Not identify the information or contact the individuals

Other Uses and Disclosures - DUA (5 of 5)

■ Compliance

- A CE is not in compliance with the standards if the CE 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
 - An exception to this is if the CE took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful
 - Discontinue disclosure of PHI to the recipient
 - Report problem to the Secretary of HHS

Other Uses and Disclosures

Other Uses and Disclosures

- Both DUAs and MOAs include BAA language
- Those organizations which hold a DUA or MOA are subject to the rules of BA as put forth in HIPAA

Other Uses and Disclosures - Media

- HIPAA does not expressly prohibit disclosure of patient information to the media
 - TMA requires that hospitals must adopt policies that prohibit disclosure of information other than patient condition and location to the media without patient authorization
- If the media does get involved, the patient must sign an authorization form
- CE should have a central release authority (single site) for media, VIP, etc

Other Uses and Disclosures - Media Activities

- Activities that involve the media could include:
 - Drafting of a detailed statement by the hospital (which goes beyond the one-word condition) that is approved by the patient or their legal representative
 - Taking photographs of patients
 - Interviewing patients
- Next of kin or guardians must sign when a person is unable to do so in their own right (incapacitated, minors)

Other Uses and Disclosures - Media Patient Access

- Media should not contact patients directly. If media does get involved, appropriate hospital staff should be present at all times
- Hospitals should consider denying access if it's determined that a patient's medical condition could be aggravated or that patient care could be interfered with
- A hospital representative should accompany media at all times and should deny access to certain areas of the hospital (such as operating rooms, maternity, pediatrics, emergency rooms, etc.)

Other Uses and Disclosures - Public Record

- “Public Record” cases are those cases where certain situations are reportable to public authorities (such as Department of Health and Human Services (DHHS)), law enforcement or public health authorities
- “Public Record” cases are no different than other patients, so a hospital should handle their privacy rights in the same way all patients are dealt with – even under HIPAA
- Celebrities and public officials are no different than any other patient and should be treated as such

Other Uses and Disclosures - Public Directories and the Clergy

- Health Care facilities may maintain directories of current patients with the following information:
 - Name
 - Location in facility
 - Condition in general terms
 - Religious affiliation
- Except for religious affiliation, the information may be disclosed to anyone who asks for the individual by name
 - Religious affiliation may be disclosed only to member of the clergy

Other Uses and Disclosures - Public Directories Condition

- Only one-word condition description should be made
 - Undetermined: Patient awaiting physician and assessment or when unknown
 - Good: Vital signs are stable and within normal limits Patient is conscious and indicators are excellent
 - Fair: Vital signs are stable and within normal limits Indicators are favorable
 - Serious: Vital signs may be unstable and not within normal limits Patient is acutely ill and indicators are questionable
 - Critical: Vital signs are unstable and not within normal limits Patient may be unconscious and indicators are unfavorable

Other Uses and Disclosures - Public Directories Location

- The patient's location (room number) may be included in the patient directory to facilitate visits by family and friends and deliveries of cards and flowers, etc.
 - However, as part of your policy, the patient's location should not be given out to the media
 - Keep in mind, a patient can elect not to be included in the patient directory and that request should be honored
 - Caution should be exercised to ensure that the location given is not generally known or associated with a particular specialty of care that could confirm a diagnosis

Other Uses and Disclosures - Public Directories Restrictions

- Patient must have prior opportunity to agree or object to being included on the public directory
 - Oral agreement or objection is allowed
- In an emergency situation or if a patient is unable to agree or object, use professional judgment
 - Provide opportunity to agree or object as soon as possible

Other Uses and Disclosures - Provider and Patient Communication

- Providers may remind patients of appointments, test result availability, and prescriptions through:
 - Answering machines
 - Mailings
 - Messages with family members or others answering the phone
- The minimum necessary rule applies

Other Uses and Disclosures - Sharing with Family Members

- Sharing is allowed with family members if:
 - An individual does not object, an MTF may disclose limited information to family members or others regarding the individual's care when:
 - An individual is present and agrees or does not object when given the opportunity
 - An individual is not present, the provider may use their professional judgment as to the best interest of the individual

DoD/DVA Sharing

When Can PHI be Provided to VHA?

(1 of 4)

- HIPAA Privacy Rule states that “a covered entity may disclose protected health information for treatment activities of a health care provider”
 - Sharing of PHI between DoD and VHA for the purpose of treatment can be accomplished at the point where a decision is made to seek care for an individual in the VHA
- HIPAA Privacy Rule defines treatment as “the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another”

Disclosure of PHI for Determining Benefits

(2 of 4)

- PHI may be disclosed to the DVA when an individual who is a member of the armed forces upon separation or discharge of the individual from military service for the purposes of the determination by DVA of the individuals eligibility for or entitlement to benefits
- DVA may use and disclose PHI to components of the Department that determine eligibility for or entitlement to, or that provide, benefits
- PHI can be shared when an individual signs a valid HIPAA-compliant authorization granting permission to a CE to share their data with another specified CE

Veteran's Support/Service Organizations Receiving PHI (3 of 4)

- DoD requires a HIPAA compliant authorization form to be initiated by the individual service member prior to information being provided to non-government groups
- Veterans Support/Service organizations often request PHI of hospitalized service members to help these individuals identify and apply for DVA benefits they are entitled to receive
 - Disabled American Veterans (DAV)
 - Veterans of Foreign Wars (VFW)
- These groups have no direct right to receive PHI without an authorization from the individual

Required By Law Provision (4 of 4)

- “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”
- A TMA determination would need to be made to determine whether the sharing in question falls within the scope of the provided authority

Authorizations

Authorizations

Authorization

- An authorization is not required for disclosures made under TPO
- CEs cannot condition the provision of treatment, payment, enrollment or eligibility upon an authorization
- Individuals have the right to request a restriction of the use of their PHI
- PHIMT can be used to manage authorizations and the right to request restrictions

Authorizations

Elements of Valid Authorizations

- Description of the information to be used or disclosed
- Name of person(s) authorized to make the request
- Name of person(s) to whom the requested use or disclosure may be made
- An expiration date or an expiration event
- Statement of the patient's right to revoke authorization, exceptions to this right and how the patient may revoke the authorization
- Statements that information used or disclosed may be subject to re-disclosure by the recipient and thereby no longer protected under HIPAA
- Signature of the patient and date
- If signed by a patient representative, a description of the representative's authority is required

Authorization at Request of MTF

- In addition to the minimum elements for valid authorization, include:
 - Statement that neither treatment, payment, enrollment nor eligibility will be conditioned upon authorization
 - Description of each purpose of the requested use or disclosure
 - Statement that patient may inspect or copy PHI to be used or disclosed
 - Indication of whether use or disclosure of requested information will result in direct or indirect remuneration to the CE from the third party

Authorization to Disclose Medical or Dental Information (DD Form 2870)

- An authorization is a written document, signed by the patient, that specifically allows the covered entity to disclose PHI with patient's permission
- Guidelines regarding use of this form are contained in DoD Regulation 6025.18-R
- This form can also be accessed through the PHIMT



42 CFR – Drug and Alcohol Treatment

42 CFR Part 2 vs. DoD 6025.18-R

42 CFR – Drug and Alcohol Treatment

- General Rule
- Substance abuse treatment programs must comply with both rules
- When disclosures are permitted
- Part 2 Consent and Privacy Rule Authorization
 - A CE may not disclose any information (except for bona fide medical emergencies, information in de-identified form for certain listed limited purposes, or if ordered by a court of competent jurisdiction) unless the patient has signed an authorization

42 CFR Part 2 vs. DoD 6025.18-R

General Rules (1 of 4)

- Two laws enacted in the early 1970's (one for alcohol, one for drugs)
- Guarantee strict confidentiality of information about persons receiving alcohol and drug prevention and treatment services
- Regulations implementing the statutes are found at 42 CFR Part 2. The present version of those regulations was promulgated in 1987 and amended in 1995

42 CFR Part 2 vs. DoD 6025.18-R

General Rules (2 of 4)

- DoD requires substance abuse treatment programs to comply with the Public Health Service, Department of Health and Human Services (HHS), Confidentiality of Alcohol and Drug Patient Records (42 CFR Part 2) and the Department of Defense Health Information Privacy Regulation (DoD 6025.18-R)

General Rules (3 of 4)

- 42 CFR Part 2: Public Health Service, HHS, Confidentiality of alcohol and drug abuse patient records
 - Programs may not use or disclose any information about any patient unless patient has consented in writing (on a form that meets the requirements established by the regulations) or unless another very limited exception specified in the regulation applies
 - Any disclosure must be limited to the information necessary to carry out the purpose of the disclosure

General Rules (4 of 4)

■ DoD Health Information Privacy Regulation

- The Privacy Regulation permits uses and disclosures for “treatment, payment, and health care operations” as well as certain other disclosures without the individuals authorization
- Disclosures not otherwise specifically permitted or required by the Privacy Regulation must have an authorization that meets certain requirements
- With certain exceptions, the Privacy Regulation generally requires that uses and disclosures of PHI be the minimum necessary for the intended purpose of the use or disclosure

Presentation Summary

- You should now be able to:
 - Define use and disclosure
 - Explain how to document disclosures in Protected Health Information Management Tool (PHIMT)
 - Explain legal and regulatory requirements
 - Describe minimum necessary rule in use and disclosure
 - Describe how to de-identify PHI and what the identifiers are
 - Identify the 14 Permitted uses for disclosure
 - Identify when PHI can be released to the Department of Veterans Affairs (DVA)

Presentation Summary

- You should now be able to:
 - Explain patient safety rules and other uses and disclosures
 - Define authorizations to disclose
 - Explain 42 CFR Part 2 vs. DoD 6025.18-R

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- DoD 8580.X-R, DoD Health Information Security Regulation (Draft)
- <http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm>
- <http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm> to subscribe to the TMA Privacy Office E-News
- <https://hipaasupport.tricare.osd.mil> for tool related questions
- Privacymail@tma.osd.mil for subject matter questions
- Service HIPAA Representatives