

## **QUALITY IMPROVEMENT IMPLEMENTATION GUIDE**

### **EXERCISE 44, 9/2009**

SUBJECT: Disclosure and accounting of protected health information (PHI).

REFERENCES: DoD 6025.18-R, DoD Health Information Privacy Regulation  
TMA Privacy Office Policy Guidance found at <http://www.tricare.mil/tmaprivacy>  
Code of Federal Regulations (CFR), Title 45, Section 164

PURPOSE: To assist in developing effective local policies and procedures for appropriate disclosure of protected health information and proper accounting thereof.

#### DISCUSSION:

##### 1. Authorizations for Use or Disclosure

- a. **Authorization Required: General Rule.** Except as otherwise permitted or required by 45 CFR 164.512, a covered entity (CE) may not use or disclose protected health information without an authorization that is valid per paragraph 1.b. 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. A DD Form 2870, "Authorization for Disclosure of Medical or Dental Information", fulfills the requirements detailed in paragraphs b and c below.
- b. **Valid Authorizations.** A valid authorization shall contain at least the following elements:
  - i. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
  - ii. The name or other specific identification of the person(s) authorized to make the requested use or disclosure.
  - iii. The name or other specific identification of the person(s) to whom the CE may make the requested use or disclosure.
  - iv. 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.
  - v. 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.
  - vi. 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.

- c. 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:
  - i. The individual's right to revoke the authorization in writing, and either:
    1. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
    2. The information in subparagraph 1.c.i.1. is included in the notice.
  - ii. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
    1. The CE may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or
    2. The consequences to the individual of a refusal to sign the authorization when the CE can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
  - iii. 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.
2. Minimum Necessary: The minimum amount of PHI that is reasonably needed to achieve the purpose of a requested use, disclosure or request for PHI. A CE must make a reasonable effort to limit its use, disclosure of, and requests for PHI to the minimum necessary in order to accomplish the intended purpose of the use, disclosure, or request. The CE must also make a reasonable effort to limit access to PHI to those in its workforce who need access based on their role in the organization.
  - a. The minimum necessary rule does **not** apply to:
    - i. Uses, disclosures to, or requests by a healthcare provider for treatment purposes.
    - ii. Uses or disclosures made to the individual (patient).
    - iii. Uses or disclosures that are authorized by the individual pursuant to a valid authorization, signed by the patient or a personal representative, so long as the uses or disclosures are consistent with the authorization.
    - iv. Uses or disclosures that are required by state or other law, statutes, and regulations (unless prohibited by the Privacy Act of 1974).
    - v. Uses or disclosures for purposes of training medical residents, medical students, nursing students and other medical trainees as part of their medical training program. If required, the entire medical record may be requested and/or

disclosed for training purposes.

- vi. Uses or disclosures which are required to comply with standard Health Insurance Portability and Accountability Act (HIPAA) transactions (however, the minimum necessary standard applies to the “optional” data elements which may be included in these transactions) or other HIPAA Administrative Simplification Regulations.
  - vii. Disclosures to the Secretary of Health and Human Services (HHS) required under HIPAA for enforcement purposes.
- b. Reasonable Reliance: Under certain circumstances, the Privacy Rule permits a CE to rely on the judgment of the part requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:
- i. A public official or agency for a disclosure permitted under the Privacy Rule.
  - ii. Another covered entity.
  - iii. A professional who is a workforce member or business associate of the covered entity holding the information for the purpose of providing professional services to the CE.

However, regardless of these circumstances, the CE always retains the right to exercise discretion in making its own determinations regarding the application of the minimum necessary standard regarding the use, disclosure and requests for PHI.

3. The Privacy Rule of HIPAA of 1996 requires a CE to maintain a history of when and to whom disclosures of PHI are made for purposes other than treatment, payment and healthcare operations (TPO). CG Health Services is considered a single CE and no clinic is a CE unto itself; therefore it is imperative that a central database, the Protected Health Information Management Tool (PHIMT), be used to accurately account for all disclosures and to effectively manage requests made by all CG medical/dental facilities on each patient. By law, the CG must be able to provide an accounting of those disclosures to an individual upon request. Authorizations and Restrictions from an individual to a CE are included in the information that is required for tracking purposes. The HIPAA Rule suggests that disclosures for the purpose of appointment reminders, such as for upcoming, missed, or cancelled appointments, can be treated as disclosures for purposes of treatment.
- a. An individual has a right to receive an accounting of disclosures of PHI made by a CE in the 6 years prior to the date that the accounting is requested. An accounting of disclosures is **not** needed for the following:
    - i. To carry out treatment, payment and healthcare operations;
    - ii. To individuals or their personal representative of PHI about them, (e.g. individual provides his/her command with a duty status chit or up/down chit

(CG-6020));

- iii. When a signed authorization form (such as a DD Form 2870) allows for the disclosure;
  - iv. For the facility's directory, to persons involved in the individual's care, for disaster relief or other notification purposes;
  - v. For national security or intelligence purposes, such as disclosures to the Security Center (SECCEN);
  - vi. To correctional institutions or law enforcement officials; or,
  - vii. As part of a limited data set.
- b. The accounting for each disclosure shall include:
- i. The date of the disclosure.
  - ii. The name of the entity or person who received the PHI and, if known, the address of such entity or person.
  - iii. A brief description of the PHI disclosed.
  - iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.
- c. Multiple Disclosure Accounting  
A CE may provide one accounting of disclosure if multiple disclosures of PHI to the same person or entity are made for a single purpose. This single accounting may be utilized only for disclosures that occur on a set periodic basis such as medical boards or binnacle lists containing PHI to a commander or the commander's designee(s). The disclosure accounting must include:
- i. All the elements as outlined in paragraph 3.b.
  - ii. The frequency, periodicity, or number of the disclosures made during the accounting period.
  - iii. The date of the last such disclosure during the accounting period.
- d. To comply with the requirements for disclosures, the TRICARE Management Activity (TMA) provides the Protected Health Information Management Tool (PHIMT), an electronic disclosure-tracking database. The PHIMT stores information about all disclosures, authorizations, and restrictions that are made for a particular patient. PHIMT has a functionality built into it that can provide an accounting of disclosures, if necessary.

- e. A CG clinic must provide an accounting of disclosures within 60 days of the request. If the clinic cannot honor an accounting of disclosures within the 60-day period, it must provide information to the requestor as to the reason for the delay and expected completion date. The clinic may extend the time to provide the accounting by no more than 30 days. Only one extension is permitted per request.
4. Disclosure of PHI to Special Programs. Paragraph 3.a.iii explains that disclosures made through the execution of a valid authorization are exempt from the accounting requirement. For certain special programs, such as the CG Academy cadet training program, TRACEN Cape May recruit training program, or other such training programs, it may prove useful to incorporate form [CG-6026 “Authorization for Disclosure of Protected Health Information to Special Programs”](#), into the member’s application or orientation materials for the disclosure of PHI necessary for the proper conduct of the training program.
    - a. Through the use of a valid authorization, CG clinics may disclose PHI for purposes outlined in the authorization itself. By obtaining an individual’s signed authorization, the responsibility to account for these disclosures no longer exists (see para 3.a.iii. above).
    - b. Use of this special programs authorization is intended for military and statutory programs where the release of medical information is required by military authorities to monitor and assess an individual’s fitness for participation in the specific program. Incorporating this language into consent forms and the regulations or directives that govern these programs serves as a means of reducing the disclosure accounting requirements of HIPAA.
    - c. The special programs authorization differs from DD Form 2870, Dec 2003, “Authorization for Disclosure of Medical or Dental Information”, in several ways. First DD Form 2870 is for use in authorizing the release of information for personal use, insurance, continued medical care, school, legal, retirement/separation, and other similar personal reasons. Second, the failure to sign or future revocation of this authorization will prevent the release of the PHI. This is not the case with the special programs authorization. Failure to sign or future revocation of this authorization will **not** prevent the release of the information in accordance with authorized procedures.
    - d. The use of this voluntary authorization form allows and authorizes CG clinics to disclose information in accordance with the authorization and not account for the disclosure as the individual has been given notice and authorized the disclosures throughout the period of their participation in the designated program.
  5. PHI Disclosure and the Military Mission. The cornerstone of HIPAA Privacy is the protection of health information. The implementation of the rule standards cannot compromise the provision of quality healthcare or the military mission. 45 CFR 164.512 states that “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 (PHI) 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.”
    - a. Appropriate Military Command Authorities include the following:

- i. All Commanders who exercise authority (in the individual's chain of command) over an individual who is a member of the Armed Forces, or other person designated by such a Commander to receive PHI in order to carry out an activity under the authority of the Commander.
  - ii. The Secretary of Homeland Security when the Coast Guard is not operating as a service in the Department of the Navy.
  - iii. Any official delegated authority by the Secretary of Homeland Security to take an action designed to ensure the proper execution of the military mission.
- b. Activities or purposes that qualify under this stipulation:
- i. To determine the member's fitness for duty, including but not limited to the member's compliance with standards and all activities carried out under the authority of COMDTINST M1020.8(series), "Coast Guard Weight and Body Fat Standards Program Manual", COMDTINST M6000.1(series), "Medical Manual", COMDTINST M6410.3, "Coast Guard Aviation Medicine Manual", COMDTINST M1850.2(series), "Physical Disability Evaluation System", , COMDTINST 6150.3(series), "Periodic Health Assessment (PHA)", and similar requirements.
  - ii. 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.
  - iii. To carry out activities under the authority of COMDTINST 6000.1(series), Chapter 12, "Occupational Medical Surveillance and Evaluation Program (OMSEP)" and DoD Directive 6490.2, "Joint Medical Surveillance".
  - iv. To report on casualties in any military operation or activity in accordance with applicable military regulations or procedures.
  - v. To carry out any other activity necessary to the proper execution of the mission of the Armed Forces.
- c. Accounting for Disclosures to Command Authorities: Coast Guard clinics are required to account for disclosures made to command authorities using the PHIMT. If the member of the Armed Forces voluntarily gives his health information to a command authority, this is not an accountable disclosure and therefore the clinic is not required to account for it.

**ACTION:** Local HIPAA Privacy and Security Officials will develop and maintain policies and procedures for authorizations of the use and disclosure of PHI, the minimum necessary rule, establishing a workflow and accounting for disclosures using the PHIMT, and the disclosure of PHI for the military mission.

1. Policies and procedures for the minimum necessary rule shall include the following:
  - a. Identify the persons or classes of persons within the CE who require access to PHI in order to perform their specific job duties.
  - b. Identify the categories or types of PHI needed, and the conditions appropriate to such access.
  - c. Establish standard protocols for routine or recurring requests and disclosures, such as health service referrals.
  - d. Require the case-by-case review of non-routine request for, and disclosure of PHI.
  - e. Identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes. The Privacy Rule does not require that a justification be provided of each distinct health record.
  
2. Policies and procedures for the disclosure of PHI for the military mission shall include the following:
  - a. Establish an approved roster of commanders and other persons who may access PHI on the commander's behalf. It is highly recommended that the Coast Guard Security Center (SECCEN) is approved by the commander to be listed on this roster.
  - b. Develop screening criteria for requests that will ensure only the minimum amount of information necessary is released. For example, there may be cases where a clinical summary is needed rather than the entire medical record.
  - c. Establish policy designating who is authorized to release PHI.
  - d. Ensure personnel are trained on what information or combination of information may be considered PHI.
  - e. Establish PHIMT procedure for an accounting of disclosure; train personnel to local policy and procedures.