HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE COMPLIANCE IN CG HEALTH CARE PROGRAMS

COMDTINST 6000.8
April 2024

THIS PAGE LEFT INTENTIONALLY BLANK

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7907
2703 Martin Luther King JR Ave SE
Washington, DC 20593-7907
Staff Symbol: CG-1K2
Phone: (202) 475-5165

COMDTINST 6000.8
30 APR 2024

COMMANDANT INSTRUCTION 6000.8

Subj: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE COMPLIANCE IN CG HEALTH CARE PROGRAMS

Ref: (a) Coast Guard Medical Manual, COMDTINST 6000.1 (series)
(b) 6 C.F.R Part 5, Subpart B - Privacy Act § 5.20- General Provisions
(c) Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996", August 21, 1996
(d) 45 C.F.R, Parts 160, 162, and 164 Subpart C
(e) The Privacy Act, 5 U.S.C. § 552a
(f) The Coast Guard Freedom of Information Act (FOIA) and Privacy Acts Manual, COMDTINST M5260.3 (series)
(g) Body Composition Standards Program, COMDTINST 1020.8 (series)
(h) Coast Guard Aviation Medicine Manual, COMDTINST M6410.3 (series)
(i) Physical Disability Evaluation System, COMDTINST M1850.2 (series)
(j) Coast Guard Periodic Health Assessment (PHA), COMDTINST 6150.3 (series)
(k) Telehealth, COMDTINST 6300.3 (series)
(l) Use of Imaging and Recording Devices in USCG Health Care Facilities, COMDTINST 6010.6A
(m) HIPAA Privacy Rule Compliance in Department of Defense (DoD) Health Care Programs, DoDI 6025.18
(n) Implementation of the HIPAA Privacy Rule in DoD Health Care Programs, DoDM-6025.18
(o) Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members, DoD Instruction-6490.08
(p) Comprehensive Health Surveillance, DoDD 6490.2
(q) Privacy Incident Handling Guidance, DHS Instruction Guide 047-01-008
(r) Privacy Incident Response, Notification, and Reporting Procedures for Personally Identifiable Information (PII), COMDTINST 5260.5 (series)
(s) Health, Safety, and Work-Life Service Center (HSWL SC) HIPAA Technical directive HSWLSCTD 2020-17 Health Insurance Portability and Accountability Act Procedural Guidance
(t) Coast Guard Occupational Medicine Manual, COMDTINST 6260.32 (series)
(u) Preventative Medicine and Population Health, COMDTINST 6000.7 (series)
(v) Command Notification Requirements to Dispel Stigmas in Providing Mental Health Care to Service Members, DoDI 6490.08

1. PURPOSE. This Instruction implements the policy in DoD Instruction (DoDI) 6025.18, the guidance in DoD Manual (DoDM) 6025.18, and the privacy regulations adopted under the Health Insurance Portability and Accountability Act (HIPAA). This Instruction integrates HIPAA compliance with related information privacy and security requirements, health information technology development, and associated procurement activities.

2. ACTION. This is Instruction applies to:

   a. All Coast Guard (CG) employees. Within the CG, the following are designated as covered entities under the HIPAA Privacy Rule: all CG health care plans and all CG health care providers that engage in electronic standard transactions and all CG employees when acting as HIPAA business associations.

   b. Non-CG government agencies and military heath system contractors that meet the definition of a business associate with respect to the protected health information (PHI) of a CG CE where the contract or other written arrangement makes this Instruction applicable.

3. AUTHORIZED RELEASE. Internet release is authorized.

4. DIRECTIVES AFFECTED. This is a new Commandant Instruction; the contents were derived from The Coast Guard Medical Manual, COMDTINST 6000.1 (series).

5. BACKGROUND.

   a. The Department of Health and Human Services (HHS) promulgated HIPAA regulations for protecting individuals' health information. The two HIPAA rules essential to the CG's protection, use, and disclosure of health information are the Privacy Rule and the Security Rule.

   b. HIPAA's Privacy Rule protects individually identifiable health information (called Protected Health Information (PHI)) that is held or transmitted by a covered entity (CE) or its business associate(s) (BA), in any form or media, whether electronic, paper, or oral. HIPAA CEs include health plans, health care clearinghouses, and health care providers that transmit PHI in electronic form. By virtue of the CG's participation in the TRICARE health plan and as a direct healthcare provider, the CG is a HIPAA CE subject to the provisions of the HIPAA Privacy Rule per Reference (d). For the purposes of this Instruction, the CG Health Services Program is considered the CE. The CG Healthcare Program includes all health services clinicians privileged by the COMDT (CG-1K) Professional Review Committee and other clinical and administrative personnel responsible for the provision of health services. Not all health-related programs affiliated with CG Health, Safety and Work-Life are CG covered entities. Examples of programs/providers that are not CG covered entities include but are not limited to: Sexual Assault and Prevention Response (SAPR), Substance Abuse Prevention Program (SAPP), or PSC Medical Examination Review Board.

   c. HIPAA's Security Rule operationalizes the protections contained in the Privacy Rule by addressing the administrative, physical, and technical controls that CEs must put in place to secure individuals' "electronic PHI" (e-PHI) per Reference (d).

d. This Instruction consolidates procedures from CG policy for HIPAA matters to a single source. HIPAA procedural guidance can be found in Health, Safety, and Work- Life Service Center (HSWL SC) HIPAA technical directive HSWLSCTD 2020-17 can be found at the following website: https://uscg.sharepoint-mil.us/sites/hswlsc/Shared%20Documents/Forms/AllItems.aspx

6. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide administrative guidance for Coast Guard personnel and is not intended nor does it impose legally-binding requirements on any party outside the Coast Guard.

7. MAJOR CHANGES. Creates separate HIPAA Instruction for implementation of the HIPAA Privacy Rule in the CG Health Program with significant updates to previous HIPAA policy in Chapter 13.G of Reference (a).

8. SCOPE AND AUTHORITIES. It is recommended the reader become familiar with the directives, publications and references noted throughout this Instruction.

9. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Commandant (CG-47) reviewed the development of this Instruction, and the general policies contained within it, and determined that this policy falls under the Department of Homeland Security (DHS) categorical exclusion A3. This Instruction will not result in any substantial change to existing environmental conditions or violation of any applicable federal, state, or local laws relating to the protection of the environment. It is the responsibility of the action proponent to evaluate all future specific actions resulting from this policy for compliance with the National Environmental Policy Act (NEPA), other applicable environmental mandates, and the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 (series).

10. DISTRIBUTION. Electronic distribution in the Directives System Library. Intranet/Pixel Dashboard: Directives Pubs, and Forms - PowerApps (appsplatform.us). If Internet released: Commandant Instructions (uscg.mil), Coast Guard Forms (uscg.mil) .

11. RECORDS MANAGEMENT CONSIDERATIONS. Records created as a result of this Instruction, regardless of format or media, must be managed in accordance with Records & Information Management Program Roles and Responsibilities, COMDTINST 5212.12 (series) and the records retention schedule located on the Records Resource Center Microsoft SharePoint site at: https://uscg.sharepoint-mil.us/sites/cg61/SitePages/CG-611-RIM.aspx .

12. ROLES AND RESPONSIBILITIES. Required agency personnel consist of the CG HIPAA Privacy Officer (CGHPO), the CG HIPAA Security Officer (CGHSO), HSWL SC HIPAA PO/SO and the CG Field HIPAA Privacy and Security Officers (FHPO/SO).

a. CG HIPAA Privacy Officer (CGHPO). 45 C.F.R. § 164.530(a) requires agencies to designate (1) a privacy official responsible for the development and implementation of HIPAA policies and procedures and (2) a contact person who is responsible for receiving complaints and providing further information about matters covered by the Notice of Privacy Practices (45 C.F.R. § 164.520(d)).Accordingly, the Chief, Office of Health Services, Commandant (CG-1K2) will designate an officer as the CGHPO, residing within Commandant (CG-1K2). As the HIPAA PO for the CG Health Care System, the incumbent will also serve as the CG Service Representative and Liaison to the Defense

Health Agency (DHA) Privacy Office. Responsibilities of the CGHPO are:

(1) Provide coordination between the CG, DHS and DHA Privacy Offices on all HIPAA-related issues.

(2) Maintain current knowledge of applicable Federal and State privacy laws, accreditation standards and CG regulations.

(3) Establish, modify and disseminate CG HIPAA policy.

(4) Serve as the CG HIPAA liaison to receive complaints and provide further information about matters covered by the notice required by the HIPAA Privacy Rule from HHS, Defense Health Agency (DHA), and Congress.

(5) Serve as the HQ HIPAA PO for Commandant (CG-1K).

b. CG HIPAA Security Officer (CGHSO). 45 C.F.R. § 164.308(a)(2) requires that the CG "identify the security official who is responsible for the development and implementation of the policies and procedures required by this Instruction for the CE." The CGHSO, designated by the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (CG-6), will serve as HIPAA SO for the CG Health Care system. Primary responsibilities:

(1) Ensure Health Care system compliance with systems security statutes and regulations.

(2) Verify security measures affecting PHI align health-related information with established system security policies.

c. HSWL SC HIPAA PO/SO. The Commanding Officer, HSWL SC, will designate a staff member as the HSWL SC PO/SO for the CG Medical Treatment Facility. Responsibilities of the HSWL SC HIPAA PO/SO are:

(1) Serve as the CG HIPAA liaison between the CGHPO, the CGHSO and CG commands and operational level HSWL support. This includes activities such as responding to and coordinating the resolution of complaints and providing guidance about matters covered by Reference (d), and all FHPOs.

(2) Will maintain a log of all FHPO, FHSO and a file of all letters of designation.

(3) Develop technical directive (TD) guidance for clinic practices to fulfill the HIPAA privacy and physical security regulation requirements. Establish and recognize best practices relative to the management of protected health information (PHI).

(4) Serve as a liaison to other POs.

(5) Serve as the point of contact for HIPAA privacy compliance, monitoring and assuring staff compliance with HIPAA training requirements. The officer will administer the databases that track data disclosures and complaints; conduct Privacy and Security risk assessments; participate in the HIPAA compliance quality assurance and improvement process; and report findings to the CGHPO/SO.

(6) Serve as the FHPO for the HSWL SC.

(7) Ensure all sites complete annual risk assessments.

d. FHPO/SO.

(1) Each clinic FHPO/SO will serve as the point of contact for their assigned treatment facility's Area of Responsibility. The FHPO/SO oversees activities related to the implementation and maintenance of local clinic HIPAA standard operating procedure (SOP) covering the access to and privacy of patient health information.

(2) Clinics will be evaluated on their privacy data protection as part of their triennial Healthcare Process Assessment Program (HPAP) survey with results included in the final HPAP report. Clinics will also be evaluated on a periodic basis to ensure they have adequate administrative and physical security. Records must be protected from viewing or inadvertent exposure by storing them in cabinets or other containers that, when unattended, are locked.

(3) Health Services Administrators are responsible for designating in writing the clinic FHPO/SO. A copy of this letter of designation will be forwarded to the HSWL SC HIPAA PO/SO. Whenever there is a change in the clinic FHPO/SO, the Health Services Administrator must designate another member as FHPO/SO and notify the HSWL SC HIPAA PO/SO of the change and provide a copy of the designation letter within 10 working days of the effective date of such letter.

e. Responsibilities of the clinic FHPO/SO are:

(1) Oversee, direct, monitor and ensure delivery of initial HIPAA training and orientation to all clinical staff. Ensure annual training, including DHS mandated training titled "Protecting Personal Information," is conducted in order to maintain workforce awareness and to introduce any changes to HIPAA privacy policies to the health care workforce. Ensure a mechanism is in place within all respective treatment facilities for receiving, documenting, tracking, and investigating all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions, and, when necessary, legal counsel and the Office of Privacy Management (CG-6P).

(2) Document disclosures of Protected Health Information (PHI).

(3) Understand the content of health information in its clinical, research and business context.

(4) Understand the decision-making processes that rely on health information. Identify and monitor the flow of information within the clinic and throughout the local health care network.

(5) Initiate, facilitate and promote activities to foster information privacy awareness within the organization and related entities.

(6) Serve as the advocate for the patient relative to the confidentiality and privacy of health

information.

(7) Conduct an annual internal assessment regarding clinic processes and procedures for the protection of personally identifiable information (PII) and PHI and develop a contingency plan for the inadvertent release of PII and PHI. Develop a contingency plan for the inadvertent release of PII and PHI that should include notifying the CG Privacy Officer via HQS-DG-M-CG-61-PII@uscg.mil as expeditiously as possible.

(8) Ensure adequate health record physical security provisions are required for the protection of PHI contained in CG health records, including both paper and electronic files.

13. GENERAL RULES ON USES OR DISCLOSURES OF PHI.

a. Permitted Uses and Disclosures. Except for uses or disclosures that require an authorization as listed in Paragraph 14 or that are prohibited under this paragraph a CG CE may use or disclose PHI for treatment, payment, or health care operations (TPO) described in Paragraph 16 without patient authorization, provided that such use or disclosure is consistent with other applicable requirements of this Instruction. Any questions regarding the use and disclosure of PHI can be directed to a HIPAA PO.

b. Prohibited Uses and Disclosures. Notwithstanding any other provision of this Instruction, a CG CE must not use or disclosure PHI which:

(1) The Privacy Act would prohibit the use or disclosure absent written consent from the individuals to whom the information relates.

(2) The special rules for substance abuse disorder program patient records would prohibit the use or disclosure absent a specific written consent from the individual to whom the information relates.

(3) The special rules for genetic information would prohibit the use or disclosure for health plan underwriting purposes.

14. USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION IS REQUIRED.

a. General Rule. The general rule is a CG CE may not use or disclose PHI without a valid authorization. When a CG CE obtains or receives a valid authorization for use or disclosure of PHI, any use or disclosure must be consistent with such authorization. The CG Health Care Program must not condition treatment, payment, or benefits eligibility on an individual granting an authorization, except in limited circumstances. The Authorization for Disclosure of Medical or Dental Information, DD Form 2870, fulfills the requirements for authorizing PHI documentation located at the following: DD Form 2870, "Authorization for Disclosure of Medical or Dental Information" (whs.mil).

b. Psychotherapy Notes. A CG CE must obtain authorization to use or disclose psychotherapy notes, except:

(1) To carry out the following treatment, payment, or health care operations:

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

(b) Use or disclosure to the CE for its own training programs through which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling.

(c) Use or disclosure by the CE to defend itself in a legal action or other proceeding brought by the individual whose PHI is used or disclosed. Uses or disclosures permitted under this paragraph include those to defend itself in the United States in a claim or action brough pursuant to Sections 2671-2680, Title 28, U.S.C., also known as the Military Claims Act, and arising from any alleged act or omission of the CE.

(2) A use or disclosure that is:

(a) For HHS to investigate the CE's compliance with privacy rules as required by law.

(b) For uses and disclosures required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(c) For health oversight activities with respect to the originator of psychotherapy notes.

(d) For the lawful activities of a coroner or medical examiner as required by law.

(e) To avert a serious and imminent threat to the health or safety of a person or the public, which may include a serious and imminent threat to military personnel or members of the public, or a serious imminent threat to a specific military mission or national security under circumstances that in turn create a serious and imminent threat to a person or the public.

c. Marketing. A CG CE must obtain an authorization for any use or disclosure of PHI for marketing, expect if the communication is in the form of:

(1) A face-to-face communication made by a CG CE to an individual; or

(2) A promotional gift of nominal value provided by the CG CE.

d. Sale. A CG CE may not sell an individual's PHI unless:

(1) The CG Privacy Office has determined, in writing, that such a sale is permitted by applicable DHS or DoD issuances or other applicable publications.

(2) The CG CE has obtained an authorization from everyone whose PHI is subject to such sale.

e. Valid Authorizations.

(1) A valid authorization must contain at least the following elements:

(a) description of the information to be used or disclosed that identifies the information

in a specific and meaningful fashion.

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

(c) The name or other specific identification of the person(s), or class of persons, to whom the CG CE may make the requested use or disclosure.

(d) A description of each purpose of the requested use or disclosure.

(e) An expiration date or an expiration event that relates to the individuals or the purpose of the use or disclosure.

f. An authorization is not valid if the document submitted has any of the following defects:

(1) The expiration date has passed, or the expiration event is known by the CG CE to have occurred.

(2) The authorization has not been filled out completely with respect to an element described by Paragraph 14, if applicable.

(3) The authorization is known by the CG CE to have been revoked.

(4) Any material information in the authorization is known by the CG CE to be false.

15. USES AND DISCLOSURES REQUIRING AN OPPORTUNITY FOR INDIVIDUAL TO AGREE OR OBJECT. A CG CE may use or disclose PHI when the individual is informed in advance of the use or disclosure and has the opportunity to agree to, prohibit, or restrict the disclosure, in accordance with the applicable requirements of this Instruction. The CG may orally inform the individual of, and obtain the individual's agreement or objection to, a use or disclosure permitted by this Instruction. If an individual objects, that objection must be documented by the CG CE and remain valid for the duration of the episode of care. A disclosure permitted by this Instruction must also be considered under the standards of the Privacy Act and CG Privacy Program issuances to determine whether the disclosure is also covered and permitted by such standards (CG-6P).

a. Uses and Disclosures for Facility Directories.

(1) Permitted Uses and Disclosure. Except when an objection is expressed in accordance with this paragraph, a covered health care provider may:

(a) Use the following PHI to maintain a directory of individuals in its facility:

1) The individual's name.

2) The individual's location in the covered health care providers facility.

3) The individual's condition described in general terms, that does not communicate specific medical information about the individual, such as "stable," "good," "fair," "serious," "critical," "conscious." "Semiconscious,"

and "unconscious."

4) The individual's religious affiliation for use by members of the clergy

(b) Use PHI for directory purposes of disclose for same purposes to:

1) Members of the clergy

2) Except for religious affiliation, to other persons who ask for the individual by name.

(2) Opportunity to Object. A covered health care provider must give an individual the opportunity to restrict or prohibit some or all the uses or disclosures permitted by this paragraph. If an individual objects, that objection must be documented by the CG CE and will remain valid for the duration of the episode of care.

(3) Emergency Circumstances:

(a) A covered health care provider may use or disclose some or all of an individual's PHI when an individual is incapacitated for emergency treatment is required. Disclosure of PHI is permitted by this section for the facility's directory if such disclosure is:

1) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider.

2) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgement.

3) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by this paragraph when it is practicable to do so.

b. Uses and Disclosures for Involvement in the Individual's Care and Notification purposes.

(1) Permitted Uses and Disclosures:

(a) A CG covered entity may in accordance with this section, disclose to a family member, other relative, close friend of the individual, or another person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(b) A CG covered entity may use or disclose PHI to notify or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes must be in accordance with this paragraph as applicable.

(2) Uses and Disclosures with the Individual Present. If the individual is present

for, or otherwise available prior to, a use or disclosure permitted by this paragraph, and has the capacity to make health care decisions, the CG covered entity may use or disclose the PHI if it:

(a) Obtains the individual's agreement.

(b) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

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

(3) Limited Uses and Disclosures When the Individual is Not Present:

(a) If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the CG CE may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes.

(b) The CG CE may use professional judgment and its experience with common practice and guidance from respective Service regulations to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

(4) Use and Disclosures for Disaster Relief Purposes. A CG CE may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by this paragraph. The requirements in Paragraphs this section apply to such uses and disclosures to the extent that the CG CE, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) Uses and Disclosures When the Individual Is Deceased:

(a) A CG covered entity may disclose a deceased individual's PHI to a family member or other person identified in this section if such family member or person was involved in the care or payment for health care of the individual before the individual's death. A permitted disclosure of the deceased individual's PHI under the preceding sentence is subject to the following limitations:

1) The disclosed PHI must be relevant to the person's involvement with the deceased individual.

2) Disclosure of the PHI does not conflict with any prior expressed preferences of the deceased individual known to the CG CE.

3) The CG CE may accept a request for disclosure of a deceased individual's PHI as a request submitted to CG through FOIA, and act upon such request in accordance with both FOIA and the HIPAA Privacy Rule.

16. USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED. A CG CE may use or disclose PHI without the written authorization of the individual, or the opportunity for the individual to agree or object. In situations covered by this paragraph, subject to the applicable requirements of this paragraph and subparagraphs. When the CG CE is required by this Instruction to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this Instruction, the CG CE's information and the individual's agreement may be given orally. In such cases, the CG CE must establish appropriate documentation of such oral communication. A disclosure permitted by this Instruction must also be considered under the standards of the Privacy Act and CG Privacy Program issuances to determine whether the disclosure is also covered and permitted by such standards (CG-6P).

a. Uses and Disclosures Required by Law.

(1) A CG CE may use or disclose PHI 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.

(2) A CG CE must meet the requirements described in this paragraph for uses and disclosures required by law.

b. Uses and Disclosures for Public Health Activities.

(1) Permitted Uses and Disclosures. A CG CE may use or disclose PHI for public health activities to:

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

(b) A public health authority or other government authority authorized by law to receive reports of child abuse or neglect.

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

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

2) Tracking FDA-regulated products.

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

4) Conducting post-marketing surveillance.

(d) A person who may have been exposed to a communicable disease or may otherwise, be at risk of contracting or spreading a disease or condition, if the CG CE or public health authority is authorized or required by law to notify such person as necessary in the conduct of a public health intervention or investigation.

(e) An employer, about an individual who is a member of the workforce of the employer, if:

1) The CG CE is a health care provider who provides health care to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury.

2) The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance.

3) The employer needs such findings in order to comply with its obligations in accordance with Parts 1904 through 1928 of Title 29, CFR, also known as the "Occupational Safety and Health Administration Regulations;" Parts 50 through 90 of Title 30, CFR, also known as the "Mine Safety and Health Administration Regulations;" or under State law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance.

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

(f) A school, about an individual who is a student or prospective student at the school, if:

1) The PHI that is disclosed is limited to proof of immunization.

2) The school is required by State or other law to have such proof of immunization prior to admitting the individual.

3) The CG CE obtains and documents the agreement to the disclosure from either:

a) A parent, guardian, or other person acting in loco parentis of the individual,

if the individual is an unemancipated minor; or

b) The individual if the individual is an adult or emancipated minor.

(2) Permitted Uses. If the CG CE is also a public health authority, the CG CE is permitted to use PHI in all cases for which it is permitted to disclose such information for public health activities as described in this paragraph.

(3) CG Administered Public Health Activities. Activities of the CG authorized by applicable CG issuances or other applicable publications to carry out functions identified in this section are included as public health activities for purposes of that paragraph.

c. Disclosures About Victims of Abuse, Neglect, or Domestic Violence.

(1) Permitted Disclosures. In addition to the authorities identified in this paragraph, a CG CE may disclose PHI about an individual whom the CG CE reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(a) When the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law.

(b) If the individual agrees to the disclosure; or

(c) When the disclosure is expressly authorized by statute or regulation, and:

1) The CG CE, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

2) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) Informing the Individual. A CG CE that makes a disclosure permitted by this paragraph must promptly inform the individual that such a report has been or will be made, except if:

(a) The CG CE, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(b) The CG CE would inform the individual's personal representative, but the CG CE reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the CG CE, in the exercise of

professional judgment.

d. Uses and Disclosures for Heath Oversight Activities.

(1) Permitted Disclosures. A CG CE may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(a) The health care system.

(b) Government benefits programs for which health information is relevant to beneficiary eligibility.

(c) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards.

(d) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) Exception to Health Oversight Activities. For the disclosures permitted in this paragraph, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity, and such investigation or other activity does not arise out of and is not directly related to:

(a) The receipt of health care.

(b) A claim for public benefits related to health.

(c) Qualification for, or receipt of, public benefits or services when an individual's health is integral to the claim for public benefits or services.

(3) Joint Activities or Investigations. Notwithstanding guidance in this paragraph, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of this paragraph.

(4) Permitted Uses. If a CG CE is also a health oversight agency, the CE may use PHI for health oversight activities as permitted by this paragraph.

(5) CG Health Oversight Activities:

(a) Any activity of the CG authorized by applicable CG issuances or other applicable publications to carry out health oversight functions is included as a health oversight agency for purposes of this paragraph. Under the provisions of Executive Order 13181, PHI concerning an individual discovered during health oversight activities will not be used against that individual in an unrelated civil, administrative, or criminal investigation of a non-health oversight matter, unless

the CG has authorized such use:

1) CG health oversight activities will seek and obtain approval for such uses from the CG Legal before such use is made.

2) In assessing whether PHI should be used under guidance in this paragraph, the CG will permit such use upon concluding that the balance of relevant factors weighs clearly in favor of its use (i.e., the CG Legal will permit disclosure if the public interest and the need for disclosure clearly outweigh the potential for injury to the individual, to the physician-patient relationship, and to the treatment services).

3) Upon the decision to use PHI under this paragraph, CG Legal, in determining the extent to which this information should be used, will impose appropriate safeguards against unauthorized use.

e. Uses and Disclosures for Judicial and Administrative Proceedings.

(1) Permitted Disclosures. The CG CE may disclose the protected health information during any judicial or administrative proceeding:

(a) In response to an order of a court or administrative tribunal, provided that the CE disclosed only the PHI expressly authorized by such order.

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

1) The CG CE received satisfactory assurances, as defined by 45 C.F.R. §164.512(e)(1)(iii) that the party seeking the information made reasonable efforts to ensure that the individual who is the subject of the protected health information has been given notice of the request; or

2) The CG received satisfactory assurances, as defined by 45 C.F.R. §164.512(e)(1)(iv), that the party seeking the information made reasonable efforts to secure a protective order that meets the requirements of Paragraph 16.

(c) A CG CE receives satisfactory assurances are considered received if the CG CE receives from such party a written statement and accompanying documentation demonstrating that:

1) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address). The notice included sufficient information about the litigation or proceeding for which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal.

2) The time for the individual to raise objections to the court or administrative tribunal has elapsed.

a) No objections were filed; or

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

(d) For purposes of this paragraph, a CG CE receives satisfactory assurances from a party seeking PHI if the CG CE receives from such party a written statement and accompanying documentation demonstrating that:

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

2) The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

(e) For the purposes of Paragraph 16.e.1, a qualified protective order concerning the PHI requested is an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that satisfies both of the following:

1) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested.

2) Requires the return to the CG CE or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

(f) Notwithstanding paragraph 16.e.1.b, A CG CE may disclose PHI in response to lawful process described in this paragraph without receiving satisfactory assurance if the CG CE makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of this paragraph or to seek a qualified protective order sufficient to meet the requirements of this paragraph.

(2) Relationship to Privacy Act Disclosures Pursuant to the Order of a Court of Competent Jurisdiction. Under Section 552a(b)(11) of the Privacy Act, a federal agency may disclose Privacy Act-protected information pursuant to the order of a court (i.e., an order that has been reviewed and approved by a judge) of competent jurisdiction. In certain cases, the authority to disclose PHI in response to an order of a court or administrative tribunal may be broader than the related authority under the Privacy Act. In such cases, other Privacy Act rules and procedures, such as the establishment of a routine use permitting disclosure, and where compulsory legal process is concerned, notification of the individual when the process becomes a matter of public record, may also apply. A disclosure of PHI must be in accordance with both this issuance and the Privacy Act and DHS Privacy Program issuances.

(3) Administrative of Judicial Proceedings in Relation to Court-Martial Procedures. Any order from a military judge in connection with any process under Chapter 47 of Title 10, U.S.C., also known and referred to in this issuance as the “Uniform Code of

Military Justice (UCMJ)," is an order covered by this Paragraph.

f. Disclosures for Law Enforcement Purposes. A CG CE may disclose PHI for a law enforcement purpose to a law enforcement official if the following conditions are met, as applicable.

(1) Permitted Disclosures: A CG CE may disclose PHI:

(a) As required by law to a law enforcement official as required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to reports of child abuse and neglect, or abuse, neglect, or domestic violence.

(b) In compliance with, and as limited by, the relevant requirements of:

1) A court order or court ordered warrant, or a subpoena or summons issued by a judicial officer.

2) A grand jury subpoena.

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

a) The information sought is relevant and material to a legitimate law enforcement inquiry.

b) The request is in writing, specific, and limited in scope to the extent reasonably practicable considering the purpose for which the information is sought.

c) De-identified information could not be reasonable use.

g. Uses and Disclosures About Decedents.

(1) Coroners and Medical Examiners:

(a) A CG CE may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A CG CE that also performs the duties of a coroner or medical examiner may use PHI for the purposes described in this paragraph. Any official of the DoD authorized to perform functions under the authority of the Armed Forces Medical Examiner System is a medical examiner under this paragraph.

(2) Funeral Directors. A CG CE may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties concerning the decedent. If necessary for funeral directors to carry out their duties, the CE may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

h. Uses and Disclosures for Cadaveric Organ, Eye, or Tissue Donation Purposes.

(1) A CG CE may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

i. Uses and Disclosures for Research Purposes.

(1) Permitted uses and disclosures. A CG CE may use or disclose PHI for research, regardless of the source of funding of the research, if the requirements of this paragraph are met.

(a) Board Approval of a Waiver of Authorization. A CG CE obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by Paragraph 14 for use or disclosure of PHI has been approved by either:

1) An Institutional Review Board (IRB) that:

a) In the case of research conducted or supported by a DoD Component, is established in accordance with Section 219.107 of Title 32, CFR, also known and referred to in this issuance as the "Common Rule;" or

b) In the case of research not conducted or supported by a DoD Component but conducted or supported by another federal agency, is established in accordance with the agency's regulation comparable to the Common Rule; or

2) A privacy board that:

a) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests, including a representative from the Office of Privacy Mgmt. (CG-6P).

b) Includes at least one member who is not affiliated with the CE, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities.

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

(b) Reviews Preparatory to Research. The CG CE obtains representations from the researcher that:

1) Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research.

2) No PHI is to be removed from the CE by the researcher during the review.

3) The PHI for which use, or access is sought is necessary for the research purposes.

(c) Research on Decedent's Information. The CG CE obtains from the researcher:

1) Representation that the use or disclosure sought is solely for research on the PHI of decedents.

2) Documentation, at the request of the CG CE, evidencing the death of such individuals.

3) Representation that the PHI for which use, or disclosure is sought is necessary for the research purposes.

(2) Documentation of Waiver Approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under the Board of Approval for Waiver Authorizations in this section, the documentation must include all of the following:

(a) Identification and Date of Action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved.

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

1) The use or disclosure of PHI involves no more than minimal risk to the privacy of the individuals, based on, at least, the presence of the following elements:

a) An adequate plan to protect the identifiers from improper use and disclosure.

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

c) Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by this issuance.

2) The research could not practicably be conducted without the waiver or alteration.

3) The research could not practicably be conducted without access to and use of the PHI.

(c) PHI Needed. A brief description of the PHI for which use, or access has been determined necessary by the IRB or privacy board, in accordance with this section.

(d) Review and Approval Procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures of an IRB or privacy board as set forth below:

1) An IRB must follow the requirements of the Common Rule; Subparts B, C, and D of Part 46 of Title 45, CFR, also known and referred to in this issuance as the "Protection of Human Subjects Regulation;" and DoDI 3216.02, including the normal review procedures or the expedited review procedures in Sections 219.108(b) and 219.110 of the Common Rule or comparable regulation of another federal agency.

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

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

4) The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

j. Uses and Disclosures to Avert Serious Threat to Health or Safety.

(1) Permitted Disclosures. A CG CE may, consistent with applicable law and standards of ethical conduct, use or disclose PHI if the CG CE, in good faith, believes the use or disclosure:

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

(b) Is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the CG CE reasonably believes may have caused serious physical harm to the victim. However, such a use or disclosure may not be made if such statement is made during treatment related to the propensity to commit the criminal conduct that is the basis for the disclosure, or in the course of counseling or therapy, or through a request by the individual to initiate or to be referred for such treatment, counseling, or therapy. In addition, any such disclosure must reveal only the statement by the individual and the PHI described in this

paragraph; or

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

(2) Presumption of Good Faith Belief. A CG CE that uses or discloses PHI pursuant to this paragraph is presumed to have acted in good faith regarding a belief described in this section if the belief is based upon the CE's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

k. Uses and Disclosures for Specialized Government Functions Including Certain Activities Related to Military Services' Personnel.

(1) Military Service Personnel. A CG CE (and a covered entity not part of or affiliated with the CE) may use and disclose the PHI of individuals who are Service members for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. Exceptions pertaining to disclosures to command authorities of PHI involving Service members seeking mental health services and substance abuse education services are outlined in this section. The definition of "Military Command Exception" can be found in Appendix B of this Instruction. In the event of a disagreement between a commander and a CE (including an affiliated health care provider) concerning disclosure of PHI, the CG will, before making its determination, seek the advice of the cognizant legal advisor or command counsel, or the cognizant HIPAA privacy officer designated under Paragraph 12, or both, as appropriate.

(2) Appropriate Military Command Authorities. For purposes of this paragraph, appropriate military command authorities are:

(a) All commanders who exercise authority over an individual who is a Service member, or other person designated by such a commander to receive PHI to carry out an activity under the commander's authority. In the case of a Reserve or National Guard commander who exercises authority over an individual member of the Reserve or National Guard, such commander may designate Reserve or National Guard members who are medical personnel to access, receive, use, or disclose PHI of an individual under the commander's authority for the purposes of this issuance; provided, however, that such designee's access to PHI in a health records system is subject to the terms and conditions applicable to the system or systems to which access is requested.

(b) The Secretary of Defense, the Secretary of the Military Department responsible for the Military Service of which the individual is a member, or the Secretary of the DHS in the case of a member of the Coast Guard when the Coast Guard is not operating as a service in the Department of the Navy.

(c) Any official delegated authority by a Secretary listed in this paragraph to take an action designed to ensure the proper execution of the military mission.

(3) Purposes for Which the PHI May Be Used or Disclosed. In accordance with this paragraph, the PHI of an individual who is a Service member may be used or disclosed to:

(a) Determine the member's fitness for duty, including but not limited to the member's compliance with standards and all other activities carried out under the authority of the CG Commandant, and similar requirements.

(b) 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.

(c) Inform the commander that one of the following notification standards pertaining to the delivery of mental health services is applicable:

1) If the presumption against disclosure is overcome.

2) If a CG CE determines that one of the notification standards applies, the CE must notify the commander personally or another person specifically designated by the commander for this purpose. The CE must disclose the minimum amount of information necessary to satisfy the purpose of the disclosure. In general, this will consist of the diagnosis, the treatment, impact on duty or mission, recommended duty restrictions, the prognosis, and ways the commander can support or assist the Service member's treatment.

(d) Report on casualties in any military operation or activity in accordance with applicable military regulations or procedures.

(e) Carry out any other activity necessary for the proper execution of the Military Service mission.

(4) Purposes for Which PHI May Not Be Used or Disclosed in the Case of Mental Health Services. DoDI 6490.08 creates a presumption that A CG CE may not notify a command authority when a Service member obtains mental health services, substance abuse education services, or both. Command notification is prohibited unless the presumption is overcome by one of the notification standards listed below:

(a) The use of military health system resources includes substance misuse education services and results of any drug testing incident to such mental health care services.

(b) Unless the presumption of confidentiality is overcome by one of the notification standards listed in Appendix B, there will be no Command notification.

(c) In making a disclosure pursuant to the notification standards, health care providers will provide the minimum amount of information to the commander concerned as required to address the exigent circumstance that overcomes the presumption of confidentiality.

(5) Uses and Disclosures for Workers Compensation. A CG CE may disclose PHI as

authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work- related injuries or illness without regard to fault.

17. SPECIAL RULES AND OTHER REQUIREMENTS RELATING TO USES AND DISCLOSURES OF PHI.

a. Minimum Necessary Rule.

(1) When using or disclosing PHI in any form or when requesting PHI from another CG CE or business associate, a CE or business associate must make "reasonable efforts" to limit the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(a) The minimum necessary rule does NOT apply to:

1) Disclosures to, or requests by, a health care provider for treatment.

2) Uses or disclosures made to the individual.

3) Uses or disclosures that are authorized by the individual pursuant to a valid authorization, signed by the patient or a personal representative designated by the patient, so long as the uses or disclosures are consistent with the authorization.

4) Disclosures to the HHS required under HIPAA for enforcement purposes.

5) Uses or disclosures that are required by Federal, state, or tribal laws, and regulations (unless prohibited by the Privacy Act of 1974).

6) 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.

7) Uses or disclosures that are required to comply with standard 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:

18. NOTICE OF PRIVACY PRACTICES (NOPP) FOR PHI.

a. All CG clinics will ensure that beneficiaries who receive care at or through the facility receive a Notice of Privacy Practices (NoPP) and sign a CG-5211B NoPP acknowledgement form that is permanently filed in the health record.

b. Patients have the right to inspect and obtain a copy of their PHI. A CG clinic may deny a patient's request for access under any of the following conditions:

(1) The PHI is psychotherapy notes.

(2) Information is compiled in reasonable anticipation of, or for use in civil, criminal, or administrative action or proceeding.

(3) The PHI is subject to the Clinical Laboratory Improvements Amendments (CLIA) of 1988 to the extent that access to the individual is prohibited by law.

(4) Quality assurance information that may not be disclosed under Section 1102 of Title 10, U.S.C., and Reference (m)

c. Any PHI that was provided from a source other than the CG CE under a promise of confidentiality. In certain situations, a patient may request the medical facility amend or supplement their PHI. Requests may be denied if the PHI is or was not:

(1) Created by the medical clinic.

(2) Part of a designated record set.

(3) Available for inspection. (e.g., signed out or in use by a healthcare provider, archived, electronic health record down or not accessible).

(4) Accounting for disclosures.

d. By law, the CG must be able to provide an accounting of disclosures to a patient upon request, IAW Reference (d):

(1) CG medical facilities must maintain a history of when and to whom disclosures of PHI are made for purposes other than TPO.

(2) Authorizations and restrictions from an individual 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.

(3) An individual has a right to receive an accounting of disclosures of PHI made in the six years prior to the date that the accounting is requested. Except for disclosures:

(a) To carry out treatment, payment, and health care operations.

(b) To individuals or their personal representative of PHI about them, (e.g., individual provides his/her command with a duty status documentation of fit or not fit for flying status Medical Recommendation for Flying Duty, (DD Form-2992) located at: DD Form 2992, "Medical Recommendation for Flying or Special Operational Duty" (whs.mil).

(c) When a signed authorization form (such as an Authorization for Disclosure of Medical or Dental Information, (DD Form-2870) allows for the disclosure.

(d) For the facility's directory, to persons involved in the individual's care, for disaster

relief or other notification purposes.

(e) For national security or intelligence purposes, such as disclosures to the Security Center (SECCEN).

(f) To correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody.

(g) As part of a limited data set.

(4) The accounting for each disclosure will include:

(a) The date of the disclosure.

(b) The name of the entity or person who received the PHI and, if known, the address of such entity or person.

(c) A brief description of the PHI disclosed.

(d) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such statement, a copy of a written request for disclosure.

(5) A single accounting of disclosure is permitted 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:

(a) The frequency, periodicity, or number of the disclosures made during the accounting period.

(b) The date of the last such disclosure during the accounting period.

(6) The clinic FHPOs will utilize an electronic disclosure-tracking database to log all PHI disclosures, authorizations, complaints, requests, and restrictions as stipulated IAW Reference (s).

(7) 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.

e. Responding to HIPAA complaints.

(1) Beneficiaries may file complaints regarding perceived misuse or disclosure of their PHI. This information includes demographics such as age, address, or e- mail, and relates to past, present, or future health information and related health care services.

(2) The clinic FHPO will submit an email to: D11-DG-CGHIPAAPRIVACYOFFICER@USCG.MIL on all complaints received by beneficiaries (e.g.: any patient who received care within CG CE). A designated individual at least quarterly will maintain this inbox. Outdated or emails no longer pertinent will be archived.

(3) Beneficiary complaints should be directed in writing to the local clinic FHPO. The complaint must include:

(a) Beneficiary's name, address, phone number, and clinic accessed for care.

(b) Date complaint submitted.

(c) Description of complaint and approximate date incident occurred; and,

(d) Facility and location where incident occurred.

(4) The clinic FHPO will prepare a summary of findings and forward to the CGHPO through the HSWL SC HIPAA PO via CG memorandum for endorsement.

(5) The clinic FHPO will reply to the complaining party within 30 days from the submission of the complaint to the HSWL SC HIPAA PO.

(6) Written documentation of the complaint and its disposition must be maintained by the activity receiving the inquiry or complaint. Each clinic is required to maintain appropriate documentation for a minimum of six years from the submission of the complaint:

(a) If anyone within the CG discovers evidence or circumstances which would suggest that a breach of security of a system containing PHI or of an unintentional disclosure of PHI may have occurred, the Health Services Administrator, clinic FHPO, and Office of Privacy Management (CG-6P) via HQS-DG-M-CG-61-PII, will be immediately notified.

(b) Complaints received at Commands other than treatment facilities:

1) Whenever possible, complaints received at Commands other than CG clinics, should be redirected to the appropriate local CG or DoD clinic FHPO for investigation and response.

2) Commands will notify the HSWL SC HIPAA PO and CGHPO by email of all complaints. The HSWL SC HIPAA PO and/or CGHPO will assist and advise the Command's investigating officer; coordinate the response with legal counsel, where necessary; and review the written response of the investigating officer. If necessary, the CGHPO will coordinate the response with the DHA Privacy Office.

f. Breaches and unauthorized uses and disclosures of PHI.

(1) The term 'breach' generally means the unauthorized acquisition, access, use, or

disclosure of PHI which compromises the security or privacy of such information. There are three exceptions to the definition of "breach":

(a) The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a CE or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.

(b) The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at a CE or business associate to another person authorized to access PHI at the CE or business associate, or organized health care arrangement in which the CE participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

(c) The final exception applies if the CE or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

(2) If anyone within the CG discovers evidence or circumstances which would suggest that a breach of security of a system containing PHI or of an unintentional disclosure of PHI may have occurred, the Health Services Administrator, clinic FHPO, and Office of Privacy Management (CG-6P) via HQS-DG-M-CG-61-PII, will be immediately notified.

(3) Procedures of the clinic HIPAA PO:

(a) Notify the HSWL SC HIPAA PO and CG HIPAA PO via email or telephonically. The CG HIPAA PO can provide further guidance on breach response procedures and will notify and communicate with the DHA Privacy Office, as necessary.

(b) Follow procedures outlined in HSWL SC HIPAA Procedural Guidance.

(c) Receive, document, and initiate an investigation of the incident.

(4) The clinic FHPO through the local command authority will provide notification of all individuals whose PHI may have been compromised within 10 business days of the conclusion of the investigation of the incident. This notification will identify or outline:

(a) The nature and scope of the incident and the circumstances surrounding the loss, theft, compromise, or disclosure of the PHI.

(b) Specific data that was involved.

(c) Actions taken by the local facility to remedy the vulnerability.

(d) Potential risks incurred by the affected individuals as a result of the disclosure, compromise, loss, or theft of PHI.

(e) Actions which the individuals can take to protect against potential harm; and,

(f) Resources for obtaining further information and/or a point of contact to address any further questions the individual may have related to the potential compromise of PHI.

(5) Final report. The clinic FHPO will submit to the CGHPO through HSWL SC HIPAA PO via CG memorandum containing a description of the findings of the investigation, efforts made to mitigate any harm resulting from the disclosure, and corrective actions take to remedy weakness of technical systems, or administrative policies or procedures which lead to the vulnerability.

(6) Lessons learned. The HSWL SC HIPAA PO will disseminate lessons learned from the incident to all clinics FHPOs and appropriate command authorities so that local systems, policies, and procedures can be reviewed and appropriate corrective action and/or training can be completed.

g. Electronic transmission of protected health information.

(1) CG messaging system. Messages should not contain PHI. This includes listing the name of the individual and any disease code (i.e., International Classification of Disease (ICD-10) or Common Procedural Terminology (CPT)) which is used to identify the disease or condition of the individual.

(2) Inpatient hospitalization messages. PHI will be sent utilizing the procedure described in Reference (a) utilizing the Inpatient Hospitalization System. Send only the minimum necessary information to accomplish the intended purpose of the use, disclosure, or request via e-mail to HQS-DG-HSWL Inpatient Hospitalization, as appropriate. This e-mail will only be viewed by limited command designated individuals at HQ and HSWL SC with a need to know. No other individuals will be included or copied on this e-mail, nor will the e-mail containing PHI be forwarded after the fact to unauthorized individuals. A designated individual at least quarterly will maintain this inbox. Outdated or emails no longer pertinent will be archived.

(3) Faxing protected health information. All faxes containing PHI must be securely sent utilizing a FAX coversheet.

(4) Disclaimer on protected health information sent electronically. The disclaimer statement below will be placed in the footer of a Fax Cover Sheet for the transmission of PHI and used at the end of an email containing PHI. The words “Protected Health Information” in bold should be placed at the beginning of the footer above this disclaimer as depicted below:

Protected Health Information
This document may contain information covered under the Privacy Act, 5 U.S.C. 552(a), and/or the Health Insurance Portability and Accountability Act of 1996 (PL 104-191) and its various implementing regulations and must be protected in accordance with those provisions. Health care information is personal and sensitive and must be treated accordingly. If this correspondence contains health care information, it is being provided to you after appropriate authorization from the patient or under circumstances that don't require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure, and confidential manner. Disclosure without additional patient consent or as permitted by law is prohibited. Unauthorized Disclosure or failure to maintain confidentiality subjects you to application of appropriate sanction. If you have received this correspondence in error, please notify the sender at once and destroy any copies you have made.

h. HIPAA training requirements.

(1) Reference (d) specifies the training requirement standards under HIPAA. All CG health care workforce members, or those members assigned to a specific unit that requires access to PHI, will complete designated training within 30 working days of reporting on duty and annually thereafter.

(2) Training will be completed by utilizing the web-based training courses stipulated in the HSWL SC HIPAA Procedural Guidance (HSWLSCTD). Members will forward the certificate of completion to the member's respective training officer.

(3) The local clinic FHPO will ensure compliance and report deficiencies to HSWL SC HIPAA PO.

(4) The HSWL SC HIPAA PO will track compliance to the training requirements.

i. Other CG members who utilize PHI.

(1) Other members of the CG may routinely or occasionally have access to or utilize PHI in the course of their duties. These members are not considered part of the health care workforce, or CE, and therefore, are not required by law and implementing regulations in Reference (d) to take HIPAA training. However, these individuals are required to complete the DHS mandated training titled "Protecting Personal Information," which is located on the Coast Guard e- learning site. It is also critical that these members are aware of the intent of HIPAA and maintain the privacy and confidentiality of PHI with which they are entrusted. To accomplish this objective, members assigned to the following organizations or performing duties in the following roles are recommended to complete appropriate HIPAA training: National Maritime Center (NMC).

(a) Coast Guard Headquarters Staff Personnel Who Process Appeals of NMC Decisions Involving PHI:

(b) The Medical Branch, Personnel Services Division of the Personnel Service Center.

(c) Special Needs Program staff.

(d) Command Drug and Alcohol Representatives/Substance Abuse Prevention Program (SAPP) staff; and,

(e) Others as deemed necessary by the CGHPO.

j. When PHI is released IAW the HIPAA command exception (Reference (m)) or other applicable exceptions, that PHI now falls under the protections of the Privacy Act (Reference (e)), and not HIPAA (Reference (d)).

19. BUSINESS ASSOCIATE AGREEMENTS (BAA).

a. HIPAA (Reference (d)) rules require that covered entities (CE) and business associates (BA) enter into contractual agreements to ensure PHI is safeguarded. All HSWL contracting officers will ensure that the 10 HIPAA BAA provisions are included in the BAA or MOU for all contracts where a BA will have access to CG PHI:

(1) Use or disclose PHI only as permitted or required this Instruction or as required by law.

(2) Use appropriate safeguards, and comply, where applicable, with the HIPAA Security Rule and other CG cybersecurity requirements with respect to electronic PHI, to prevent use or disclosure of the information other than allowed by this Instruction.

(3) Report to the CE any use or disclosure of PHI not allowed by this Instruction (or by the contract with the CE) of which the business associate becomes aware, this includes breaches.

(4) Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such PHI in accordance with the HIPAA Privacy Rule.

(5) Make available PHI in accordance with the access provisions for individual privacy rights regarding access to information in this Instruction and individual directions to transmit information to a person designated by the individual.

(6) Make available PHI for an amendment and incorporate any amendments to PHI.

(7) Make available the information required to provide an accounting of disclosures.

(8) To the extent the business associate is to carry out the CE's obligations under this Instruction, comply with the requirements of this Instruction that apply to the CE in the performance of such obligation.

(9) Make its internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by the business associate on behalf of, the CE available to the Secretary of HHS and to the Director, DHA, for purposes of

investigating or determining the CE's compliance with the HIPAA rules.

(10) Return or destroy, at the termination of the performance of the business associate's functions, all PHI received from, or created or received by the business associate on behalf of the CE that the business associate still maintains in any form. If such return or destruction is not feasible, the business associate must maintain compliance with this Instruction with respect to any retained copies of the information, and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. Any action taken should be appropriately documented.

b. Commandant (CG-1K) will be the signature authority for all CG BAAs. Commandant (CG-1K) reserves the right to delegate this authority as necessary.

c. Contractors and subcontractors are required to follow Homeland Security Acquisition Regulation (HSAR) provisions when handling Sensitive PII. Moreover, contractors and subcontractors must cooperate with DHS and exchange information as necessary to effectively report and manage a suspected or confirmed privacy incident, including risk assessment, mitigation, and notification in the case of a major privacy.

20. FORMS/REPORTS. None.

21. SECTION 508. This policy is created to adhere to accessibility guidelines and standards as promulgated by the U.S. Access Board with consideration of Information and Communications Technology (ICT) requirements. If accessibility modifications are needed for this artifact, please communicate with the Section 508 Program Management Office (PMO) at Section.508@uscg.mil. Concerns or complaints for non-compliance of policy and/or artifacts may be directed to the Section 508 PMO, the Civil Rights Directorate (https://www.uscg.mil/Resources/Civil-Rights/) for the Coast Guard, or to the U.S. Department of Homeland Security at accessibility@hq.dhs.gov.

22. REQUEST FOR CHANGES. Units and individuals may recommend changes via the chain of command to: HQS-DG-lst-CG-112@uscg.mil.

/DANA. L. THOMAS/
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Health,
Safety, & Work-Life

Appendix A. Glossary
Appendix B. Military Command Exception to the Health Insurance Portability and Accountability Act (HIPAA)

THIS PAGE LEFT INTENTIONALLY BLANK

Appendix A. Glossary

1. **DEFINITIONS.** Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

2. **Breach.** The term "Breach" can be used synonymously with the term "Privacy Incident." According to OMB, a breach is a type of incident. OMB M-17-12 further defines the appropriate reporting, handling, and notification procedures in the event a breach occurs. This guidance uses "privacy incident" and "breach" interchangeably. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

   a. A person other than an authorized user accesses or potentially accesses personally identifiable information; or

   b. An authorized user accesses or potentially accesses personally identifiable information for a purpose other than authorized.

3. **Business Associate (BA).**

   a. A person who, or entity, other than a member of the CG CE workforce, who performs functions or activities on behalf of, or provides certain services to, the CG CE that involve access by the BA to protected health information; or

   b. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of another BA.

4. **Business associate does not include**:

   a. A health care provider, with respect to disclosures by CG CE to the health care provider concerning the treatment of the individual.

   b. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

5. **CG Covered Entity.** A health plan or a healthcare provider within the Military Health System (MHS), for the Coast Guard specifically, the Healthcare Program, which transmits any health information in electronic form to carry out financial or administrative activities related to healthcare. The CG Healthcare Program includes all health services clinicians privileged by the COMDT (CG-1K) Professional Review Committee and other clinical and administrative personnel responsible for the provision of health services. Not all health-related programs affiliated with CG Health, Safety and Work-Life are CG CE's. Examples of programs/providers that are not CG CE's include but are not limited to: Sexual Assault and Prevention Response (SAPR), Substance Abuse Prevention Program (SAPP), or PSC Medical Examination Review Board.

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

7. **De-identification of PHI.** Health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

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

9. **Employment Records.** Records that include health information and are maintained by the CG; are about an individual who is (or seeks or sought to become) a member of the Uniformed Services, employee of the United States Government, employee of a CG contractor, or person with a comparable relationship to the CG.

10. **Health Care.** Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

11. **Health Care Operations:** Per Reference (d) are certain administrative, financial, legal and quality improvement activities of a CE that are necessary to run its business and to support the core functions of treatment and payment and include:

    a. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;

    b. Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;

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

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

    e. Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and

    f. Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other simplification rules,

customer service, or other provisions defined in Reference (d).

12. **Health Care Provider.** Any CG clinic, including sick bays and such facilities in a CG operational unit, or ship, and any other person or organization outside of such facilities' workforce who furnishes, bills, or is paid for health care in the normal course of business.

13. **Health Information.** Any information, including genetic information, in any form or medium, that: Is created or received by a health care provider, health plan, public health authority, employer, life insurer, or school or university. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

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

15. **HHS Breach.** A breach as defined in Section 164.402 of the HIPAA Breach Rule. The text of that HHS definition states: Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part [i.e. the HIPAA Privacy Rule] which compromises the security or privacy of the PHI.

    a. HHS breach excludes:

        (1) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CG CE or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

        (2) Any inadvertent disclosure by a person who is authorized to access PHI at a CG CE or business associate to another person authorized to access PHI at the same CG CE or business associate, or organized health care arrangement in which the CG CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted the HIPAA Privacy Rule.

        (3) A disclosure of PHI where a CG CE or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

        (4) Except as provided in this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under this issuance is presumed to be a breach unless the CG CE or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(b) The unauthorized person who used the PHI or to whom the disclosure was made;

(c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated.

16. **HIPAA Complaint.** A written statement submitted to a CG CE's HIPAA privacy officer or to the HHS Office for Civil Rights alleging that the CG CE has violated an individual's health information privacy rights or committed a violation of the HIPAA Privacy or Security Rule provisions.

17. **Law Enforcement Official.** An officer or employee of any agency or authority of the United States (including an officer, employee, or designated member of a Military Service, including the CG), a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: investigate or conduct an official inquiry into a potential violation of law, including the Uniform Code of Military Justice (UCMJ), or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law, including violations of the UCMJ.

18. **Notice of Privacy Practices (NoPP).** The notice of the CG Health Service's practices and procedures with respect to safeguarding the confidentiality, integrity, and availability of an individual's PHI, and the rights of individuals with respect to their PHI. The CG utilizes the Military Healthcare System NoPP.

19. **Payment.** The activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

20. **Protected Health Information (PHI).** Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a CG CE. Information which has been de-identified is not PHI. PHI is a subset of PII, with respect to living persons.

21. **Personally Identifiable Information (PII).** Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department. Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

22. **Privacy Incident.** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

    a. A person other than the authorized user accesses or potentially accesses [PII] or;

    b. An authorized user accesses or potentially accesses [PII] for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm.

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

24. **Public Health Authority.** An agency or authority of the United States, a State, territory, political subdivision of State or territory, Indian tribe, or person or entity acting under a grant of authority from or contract with such public agency, that is responsible for public health matters as part of its official mandate.

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

26. **Virtual Lifetime Electronic Record Health Information Exchange.** A set of programs that manages the electronic exchange of beneficiary health information among Department of Veterans' Affairs, DoD, CG, other federal agencies, and private partners.

27. **Workforce.** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a CG CE or business associate is under the direct control of the CG CE or business associate whether or not they are paid by the CG CE or business associate.

Appendix B. Military Command Exception to the Health Insurance Portability and Accountability Act (HIPAA)

1. The Health Insurance Portability and Accountability Act is a federal law that requires national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. HIPAA permits protected health information of service members to be disclosed under special circumstances. Under the Military Command Exception, a healthcare provider may disclose the PHI of service members for authorized activities to appropriate military command authorities. An appropriate military command authority includes commanders who exercise authority over the service member, or another person designated by a commander. The exception does not require healthcare providers to disclose PHI to commanders. It only permits the disclosure. If the disclosure is made, then only the minimum amount of information necessary should be provided. Furthermore, the exception does not permit a commander's direct access to a service member's electronic medical record, unless otherwise authorized by the service member or the HIPAA Privacy Rule.

2. Authorized activities for which PHI may be disclosed to a commander include but are not limited to fitness for duty determinations, fitness to perform a particular assignment, or the service member's ability to carry out any other activity essential for the military mission. Once PHI has been disclosed to military command authorities, it is no longer subject to HIPAA. However, it remains protected under the Privacy Act of 1974.

3. To dispel stigma around service members seeking mental health care or voluntary substance misuse education, Department of Defense Instruction 6490.08 was issued to balance patient confidentiality rights with the commander's need to make informed operational and risk management decisions. DoD healthcare providers are not permitted to notify a service member's commander when the member obtains these services unless certain conditions are met. However, if one of the below conditions or circumstances apply, the healthcare provider is required to notify the commander:

    a. **Harm to self**. The provider believes there is a serious risk of self-harm by the service member either as a result of the condition itself or medical treatment of the condition.

    b. **Harm to others**. The provider believes there is a serious risk of harm to others either as a result of the condition itself or medical treatment of the condition. This includes any disclosure concerning child abuse or domestic violence.

    c. **Harm to mission**. The provider believes there is a serious risk of harm to a specific military operational mission. Such serious risk may include disorders that significantly impact impulsivity, insight, reliability, and judgment.

    d. **Special personnel**. The service member is in the Personnel Reliability Program or is in a position that has been pre-identified by Service regulation or the command as having mission responsibilities of such potential sensitivity or urgency that normal notification standards would significantly risk mission accomplishment.

    e. **Inpatient care**. The service member is admitted or discharged from any inpatient mental health or substance abuse treatment facility, as these are considered critical points in

treatment and support nationally recognized patient safety standards.

f. **Acute medical conditions interfering with duty**. The service member is experiencing an acute mental health condition or is engaged in an acute medical treatment regimen that impairs the service member's ability to perform assigned duties.

g. **Substance misuse treatment program**. The service member has entered into, or is being discharged from, a formal outpatient or inpatient treatment program for the treatment of substance abuse or dependence.

h. **Command-directed mental health evaluation**. The mental health services are obtained as a result of a command-directed mental health evaluation.

i. **Other special circumstances**. The notification is based on other special circumstances in which proper execution of the military mission outweighs the interests served by avoiding notification, as determined on a case-by- case basis by a health care provider.

4. In making a disclosure pursuant to the circumstances described above, healthcare providers shall provide the minimum amount of information to satisfy the purpose of the disclosure. In general, this shall consist of: (1) 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; and (2) ways the command can support or assist the service member's treatment.

5. Commanders must protect the privacy of information provided pursuant to the Privacy Act. Information provided shall be restricted to personnel with a specific need to know; that is, access to the information must be necessary for the conduct of official duties. Such personnel shall also be accountable for protecting the information. Commanders must also reduce stigma through positive regard for those who seek mental health assistance to restore and maintain their mission readiness, just as they would view someone seeking treatment for any other medical issue.