Privacy Impact Assessment for the

United States Coast Guard Composite Health Care System

DHS/USCG/PIA-017

July 25, 2011

Contact Point
LT Mark Williams
United States Coast Guard
CG-1123 Medical Information Systems Division
(202) 475-5187

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Coast Guard (USCG) owns and operates the Composite Health Care System (CHCS), which is a fully integrated health care information system that connects USCG medical clinics to the computerized patient records of USCG members, other military personnel, and eligible family members. USCG is conducting this Privacy Impact Assessment (PIA) because CHCS collects and maintains Protected Health Information (PHI) and Personally Identifiable Information (PII).

Overview

The Composite Health Care System (CHCS) is owned and operated by the United States Coast Guard (USCG). CHCS is a fully integrated health care information system that connects USCG medical clinics to computerized patient records that are created and maintained for the purposes of providing health care services to patients. USCG medical clinic patients include USCG members; other military active duty, reserve, and retired personnel; and their eligible family members. CHCS is used by USCG health care providers and authorized staff at its medical clinics located throughout the United States and Puerto Rico.

CHCS Modules

CHCS is a modules-based application. Each module has menus and reports that health care providers and authorized staff can utilize for the purposes of providing health care services to patients. CHCS is comprised of the following seven core modules:

1. **Patient Appointment & Scheduling (PAS)** – PAS enables authorized staff to create provider profiles and make and track patient appointments for various services that may be performed at the medical clinic.
2. **Managed Care Program (MCP)** – MCP enables health care providers and authorized staff to document patient consults and referrals. MCP also allows for the documentation of patients who refuse treatment and/or leave against medical advice.
3. **Pharmacy (PHR)** – PHR enables health care providers, pharmacists, and other authorized staff to store, track, and control medications that are prescribed, dispensed, and administered on an inpatient and outpatient basis.
4. **Laboratory (LAB)** – LAB enables health care providers, phlebotomists, and other authorized staff to track the processing of laboratory orders, including collection methods and test results.
5. **Clinical (CLN)** – CLN enables health care providers, including physicians, nurses, and other clinical staff, to input information related to services that the patient receives during any visit at the medical clinic. This information includes medical history, current assessment, consults, orders, discharge instructions, and progress notes. Collectively, this information is the patient's treatment record. Health care providers may access CLN at a docked station or through portable electronic devices.
6. **Radiology (RAD)** – RAD enables health care providers, radiologists, and other authorized staff to track the processing of radiology orders, tests, results, and reports.

7. **Patient Administration (PAD)** – PAD enables authorized staff to perform a broad range of administrative system tasks that support the life cycle of the patient visit. The life cycle depends on the types of services that the patient receives. Generally, this cycle opens through the registration process and closes through the collection of payment for services. Included in PAD is the Medical Service Accounting function that supports the recording, collection, and tracking of costs for services rendered.

Reporting

CHCS also provides USCG medical clinics with administrative reports for internal business purposes, such as provider licensure, staff training, risk management, quality improvement, internal auditing, and other administrative activities. These reports are intended to assist management with evaluating and increasing overall productivity at the clinic and command level.

Links to Other Systems and Use of Social Security Numbers

CHCS' main interface is with the DoD Defense Eligibility Enrollment Reporting System (DEERS). DEERS is used to verify the identity and benefit eligibility of USCG members; other military active duty, reserve, and retired personnel; and their eligible family members. DEERS uses Social Security Numbers (SSNs) for personal identification and health care benefit eligibility determinations, as authorized by 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199.17 TRICARE Program; and, Executive Order 9397 (as amended, SSN). The Office of Management and Budget (OMB) has directed all federal agencies to reduce the use of SSNs and DoD has initiated the replacement of SSNs with alternative identification numbers. Until these alternative numbers are in place, USCG needs to continue to use SSNs in order to verify a patient's identification and eligibility to receive health care benefits.

In addition to DEERS, CHCS receives data through interfaces with other clinical systems. For example, CHCS interfaces with:

- DoD Pharmacy Data Transaction Service (PDTS), a global data repository that stores information about prescriptions for DoD beneficiaries;
- QUEST Diagnostics via the Lab Interoperability System (LIO), a patient lab delivery system for health care providers;
- Naval Ophthalmic Support & Training Activity (NOSTRA), a system that provides eyewear-related services to support the readiness of the Armed Forces; and
- TRICARE, the military health insurance provider.

Additional Privacy Protections

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides individuals with the right to privacy and security over their protected health information (PHI). As a fully integrated health care information system, CHCS creates and maintains PHI for the purposes of providing health care services. Accordingly, USCG provides its patients with a Military Health System Notice of Privacy Practices (MHS NOPP), which describes the individual's rights, and USCG's responsibilities, with respect to how PHI may be used and disclosed.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

CHCS collects the following demographic and medical information on the patient. When the patient is an eligible family member of a military member (sponsor), the demographic information of the sponsor is also collected for the purposes of verifying the family member's identification and eligibility to receive health care benefits.

- Name;
- Sponsor SSN (to verify eligibility with DoD DEERS);
- Sponsor rank/military level and status;
- Sponsor marital status;
- Date of birth;
- Patient addresses;
- Patient telephone numbers;
- Email addresses;
- Insurance information;
- Gender;
- Height and weight;
- Current symptoms; and
- All medical records including chronic/acute illnesses, vital statistics, laboratory test results, radiology test results, and previous health history including eyewear, prescriptions, medications, and allergies.

1.2 What are the sources of the information in the system?

Generally, CHCS collects most information directly from the patient or his/her legally designated representative as part of the patient registration process. This occurs during the patient's visit or call to the medical clinic. Patient identification and eligibility data is provided by DEERS, the official repository for such data.

CHCS receives demographic information from the patient; medical info can be collected from patient and the medical provider. Data comes to CHCS through interfaces with other clinical systems. For example, CHCS interfaces with the DoD Pharmacy Data Transaction Service (PDTS), a global data repository that stores information about prescriptions for DoD beneficiaries. CHCS interfaces with QUEST Diagnostics via the Lab Interoperability System

(LIO), which delivers patient lab results to providers. CHCS also interfaces with the Naval Ophthalmic Support & Training Activity (NOSTRA), which provides eyewear to support readiness of the Armed Forces.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information maintained in CHCS about the patient is collected to identify the patient, assure eligibility to receive health care, assist in determining the best course of treatment for that patient, and document diagnosis and treatment for future care.

1.4 How is the information collected?

USCG staff collects information directly from the patient or his/her legally designated representative during the patient registration process at the USCG medical clinic. DEERS is used to verify the identity and benefit eligibility of USCG members; other military active duty, reserve, and retired personnel; and their eligible family members.

1.5 How will the information be checked for accuracy?

Information comes directly from patients and their medical providers to ensure it is accurate when collected. Additionally, patients are able to correct their information in CHCS by contacting the registration staff at the USCG medical clinics where they initially provided their information. CHCS also has the capability of providing corrected or updated information back to the originating source.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

10 U.S.C. §§ 1071-1107, 14 U.S.C. § 93(a)(17), 44 U.S.C. § 3101, 29 CFR § 1630.14(d), and 45 CFR § 164.500–164.530 authorize the collection of information from individuals in order to receive treatment at a USCG medical clinic. Governing directives on the usage of SSNs can be found in: 10 U.S.C. §1095(k)(2) and E.O. 9397.

Additionally, the HIPAA provides individuals with the right to privacy and security over their protected health information (PHI). As a fully integrated health care information system, CHCS creates and maintains PHI for the purposes of providing health care services.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: The primary risk in collecting demographic and medical information of patients in CHCS is the possibility of information being improperly accessed, used, or shared beyond the reason for which it was collected.

Mitigation: CHCS mitigates these risks through internal and external controls. Internally, CHCS uses a role-based security system. Security keys allow users access to only those functions required for their official duties. The CHCS System Security Plan requires all users to obtain and pass proper training with a proficiency of 80% or better in order to gain access

to the system. Security clearance is also required. Externally, CHCS protects against the unauthorized access of information by employing confidentiality controls such as data encryption for the protection of data in transit and at rest. To maximize confidentiality and protection assurances, CHCS files are kept separately from general USCG personnel files. Finally, CHCS has the capability of generating audit trails to identify any misuse of the system.

Privacy Risk: More data than necessary may be collected from external sources via interfaces with other clinical systems.

Mitigation: All system-to-system interfaces are governed by a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or other contractual arrangement which has strict data usage clauses protecting any PHI or PII transferred. In order to minimize the collection of PII, these documents contain strict data usage and protection clauses.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

USCG uses the information collected and maintained in CHCS to facilitate and manage the delivery of patient care and reimbursement for services provided. The information is also used for management reporting.

2.2 What types of tools are used to analyze data and what types of data may be produced?

The clinical portion of CHCS allows for the aggregation of patient clinical data for management reports. These reports do not contain PII.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

CHCS uses some standard codes in patient records, most notably postal zip codes from the United States Post Office and diagnosis and treatment code sets which are standard across medical facilities.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: There is a risk that data collected for medical treatment could be used by USCG staff beyond the reason for which it was collected.

Mitigation: To maximize confidentiality and protection assurances, CHCS files are kept separately from general USCG personnel files. USCG does not mix CHCS data with other USCG databases. Additionally, CHCS uses role-based user accounts under which users access data on a need-to-know basis. All users are trained on the system and required to pass an exam on proper system use in order to gain access.

Privacy Risk: CHCS users may access, use, or disclose more information than necessary for treating patients.

Mitigation: When CHCS users disclose data to authorized individuals or entities, the Site Manager applies the Principle of Least Privilege. This privilege requires that each subject in CHCS be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this privilege limits the damage that can result from unauthorized access, use, or disclosure. The principle is applied in CHCS via system and application access control mechanisms, which assures that access is granted only to the data elements required for the user's official duties. The user's identity is authenticated through the use of unique user IDs and passwords, as well as verification questions, when needed. In addition, Site Managers are responsible for the following tasks:

- Supervise and review the activities of users with respect to the usage and enforcement of information system access controls;
- Review audit records for inappropriate activities in accordance with USCG procedures;
- Investigate any unusual information system-related activities;
- Periodically review changes to access authorizations; and
- Frequently review the activities of users with significant information system roles and responsibilities.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

CHCS is a repository for health data that supports the health care delivery processes and clinical business functions within the Military Health System (MHS). All data entered during the course of patient treatment is retained within the system. Please see Section 1.1 for a complete listing of data collected.

3.2 How long is information retained?

CHCS system operating data (non-PII) is retained for the life of the system. CHCS keeps PII for different periods of time depending on the status of USCG members, other military personnel, or their family members and the rules contained in the Information Life Cycle and Management Manual, COMDTINST M5212.12 (series).

Active Duty Personnel: Active Duty personnel medical files are retained at the active duty personnel's unit or healthcare facility at which the individual receives care for so long as the individual is assigned to the particular area. When active duty personnel are reassigned, the medical file is transferred to the new duty station upon reassignment. Upon separation or retirement, the medical file is sent to VA Record Management Center, 4300 Goodfellow Blvd, ST Louis, Mo 63115-1703. Data is destroyed 50 years from the date of latest document in record. (NC1-26-80-4, items 360a and 154a/b). Reappraisal of this schedule is pending.

Retired and Seperated Personnel: Retired personnel medical files are retained at the medical facility for a period of two years from the date of last activity. Upon separation or retirement, the medical file is sent to VA Record Management Center, 4300 Goodfellow Blvd, ST Louis, Mo 63115-1703. Destroy 50 years from the date of latest document in record. (NC1-26-80-4, items 360a and 154a/b). Reappraisal of this schedule is pending.

Family Members: Military personnel family members' medical files are transferred to NPRC-ANNEX, 1411 Boulder Blvd., Valmeyer, IL, 62295 four years from the date of last activity. They are destroyed 25 years from the date of the latest document in record. (AUTH: NC1-26-82-5, Item 2bl)

Reserve Personnel: Reservist personnel medical files are retained in custody of the reservist personnel's group, unit, or healthcare facility at which the individual receives care for so long as the individual is assigned to the particular area. When reservist personnel are reassigned, the medical file is transferred to the new reserve group, unit, or district commander upon reassignment.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention of CHCS data is currently under review. Department of Defense, Military Personnel Records Management Working Group (MPRMWG) – which includes Coast Guard Military personnel) has submitted a new Service Treatment Record (STR) records disposition schedule (SF115) to NARA; disposition pending.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: USCG may retain data in CHCS for longer than is required to provide medical care.

Mitigation: USCG retains different sets of data for different periods of time in order to minimize unnecessary retention. For example, records on USCG members and other military personnel are permanently retained for historical purposes, but records on their family members are not. Rather than apply one retention policy to all PII, USCG tracks whether the subjects of records are military personnel or their family members so that family member data is not unnecessarily retained.

Privacy Risk: There is a risk that users may not follow the retention schedules because they require manual action.

Mitigation: CHCS does not automatically transfer or purge data, so USCG staff must manually move data in order to adhere to retention schedule requirements. To ensure that this process is maintained, USCG has written rules for manually moving PII contained in the Information Life Cycle and Management Manual, COMDTINST M5212.12 (series). Additionally, users are trained to follow the retention schedules.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

CHCS does not share, send, or retrieve any data from other DHS components or elsewhere within USCG.

4.2 How is the information transmitted or disclosed?

Information from CHCS can only be transmitted electronically and may only be disclosed to authorized personnel and when provided appropriate access. Information may be shared with internal USCG components only if they are involved in facilitating access to the collection and distribution of health care related information. On a case-by-case basis, information in CHCS may be shared by individuals within DHS only if they have a need to know that specific information. For example, information may be shared if needed as part of an official USCG investigation.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: There is a possible risk of use of PII beyond its original purpose.

Mitigation: CHCS has no internal system interfaces and its patient data files are kept separate from other USCG files in order to prevent their use beyond medical purposes. All authorized CHCS users are trained on the appropriate access to CHCS and use and sharing of PII.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

There are no external organizations that have direct access to CHCS, but staff may transmit CHCS data to the following external organizations as permitted or required by law.

- **DoD:** DoD does not have direct access to CHCS. Information related to communicable diseases may be shared with DoD so that standards of care and immunization plans may be developed to ensure fitness for duty. This information may also assist DoD with ensuring uniformity and centralization of record keeping for all military personnel. CHCS sends data to two major DoD MHS medical data repositories. The first repository is the Executive Information and Decision Support (EIDS), which contains the patient appointment along with any associated laboratory or radiology test or prescription orders. The second repository is the TRICARE Management Activity (TMA) Center, which contains patient demographic information, along with the sponsor's name and SSN.

- **Veteran's Affairs and Public Health Service:** PII may be shared with Veteran's Affairs (VA), the Public Health Service (PHS), and DoD Contractors that provide medical treatment to USCG members; other military active duty, reserve, and retired personnel, and their eligible family members. Eligibility determinations, facilitation of care, coordination of cost sharing, and collaborative research activities between VA and DoD, can be accomplished through the exchange of military personnel PHI and PII. In addition, the reporting of certain diseases as required by law can be accomplished through data sharing with PHS. It also should be noted that immunization and disability records of USCG Medical and Dental Officers may be shared with PHS for duty and detail purposes.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of information among USCG, DoD, VA, and commercial laboratories is governed by the Privacy Act of 1974 and DHS/USCG-011 Military Personnel Health Records System of Records.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The Military Health System Virtual Private Network (MHS VPN) is used to encrypt all data transmissions with the Triple DES (Data Encryption Standard) algorithm and affix a data integrity checksum using the Secure Hash Algorithm (SHA-1). The MHS VPN appliances comply with all applicable federal standards and have been certified at Level 2 by the National Institute of Standards and Technology (NIST) in accordance with Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules*. All system-to-system interfaces are governed by a MOU, Memorandum of Agreement MOA, or other contractual arrangement which has strict data usage clauses protecting any PHI or PII transferred.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: USCG members; other military active duty, reserve, and retired personnel; and their eligible family members' information may be improperly used beyond the reason for which it was collected.

Mitigation: Access to CHCS is granted only to authorized users. The sharing of information among USCG, DoD, VA, and commercial laboratories is governed by a signed MOU, MOA, or other contractual arrangement which has strict data usage clauses protecting any PII or PHI transferred.

Privacy Risk: Individuals may be unaware of the transmittal of their information outside of USCG.

Mitigation: The primary systems with which CHCS shares information are major military health care databases that patients will have already interacted with directly to establish

their eligibility for care at military health facilities. Patients are further notified during clinic intake that their eligibility will be verified and they provide the information at that time. In cases of sharing public health data, providers notify the patients at the time data is shared.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

All patients are provided a copy of, or have ready access to, the MHS Notice of Privacy Practices (MHS NOPP). The MHS NOPP provides a comprehensive description, in ten different languages, of Medical Department Activity (MEDDAC) probable uses and disclosures of PHI, legal duties, and the patient's rights with respect to PHI. As patient's access care and services at MEDDAC, designated staff will make every attempt to obtain the patient's written acknowledgement of receipt of the MHS NOPP. The acknowledgement, an MHS NOPP sticker signed by the patient, will be retained in the patient's medical record. All information is collected at the consent of the patient and per HIPAA standards. Additional notice is provided as part of the Systems of Records Notice (SORN) DHS/USCG-011 - Military Personnel Health Records.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes, individuals have the right to decline to provide information. However, it is in the best interest of the patient to provide any and all insight to the providers and health service technicians in order to receive the best health care. If patients decline to provide information, they may be denied service if the medical condition is not an emergency.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No, individuals do not have the opportunity to consent to particular uses of the information they provide. Information is used in accordance with MHS policy. CHCS does not allow for a specific portion of information to be withheld from personnel authorized system access.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: Individuals may be unaware that CHCS is collecting and using their data.

Mitigation: This risk is primarily mitigated by the fact that individuals are present at the time of data collection and provide their data directly to staff at USCG medical clinics. In addition, they are given notification via the MHS NOPP, this PIA, and DHS/USCG-011 - Military Personnel Health Records System of Records Notice.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals have the right to access and/or obtain copies of their medical records in CHCS by contacting the administrative staff at the USCG medical clinic.

Individuals seeking notification of and access to any record contained in CHCS, or seeking to contest its content, may submit a request in writing to USCG, Commandant (CG-611), Attn: FOIA Coordinator, 2100 2nd St. SW, Washington, DC 20593-0001.

The FOIA Coordinator and/or other authorized USCG personnel who receive a request for any record contained in CHCS must conform to the Privacy Act regulations set forth in 6 CFR Part 5 by first verifying the requestor's identity, including full name, current address, and date and place of birth. The requestor must also sign the request. The signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, requestors may obtain additional information from the FOIA website[1] or 1-866-431-0486.

In addition, the requestor should explain the following:

- Why they believe the USCG medical clinic would have information on the person for which the record pertains;
- When they believe the records would have been created.
- If the request is seeking records pertaining to another living individual, a statement from that individual certifying his/her agreement for the requesting party to access and/or obtain copies of his/her records.

Without this bulleted information the USCG may not be able to conduct an effective search and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals can request correction to their information in CHCS using the same means by which they can access and/or obtain copies of their medical records, as described above. Requests for correction to clinical information are managed locally at each USCG medical clinic through quality assurance and various clinic review processes. Individuals also have the ability at anytime to update their demographic information in DEERS via USCG administrative staff, who may access and update DEERS through CHCS.

[1] Please access the following website to obtain forms necessary to complete a FOIA request http://www.dhs.gov/xfoia/editorial_0579.shtm.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals can contact the USCG medical clinic directly to receive instructions on how to submit requests to correct their information. Individuals are also given notification via the MHS NOPP, this PIA, and DHS/USCG-011 - Military Personnel Health Records System of Records Notice.

Military active duty, reserve, and retired personnel are automatically registered in DEERS; however, they must register their family members. Requests for corrections or updates to information in DEERS may be submitted to USCG administrative staff, who may access and update DEERS through CHCS. Requests for corrections or updates to information in DEERS may also be submitted online through TRICARE's website.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Not applicable.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: There is a risk that individuals may not be able to correct or access their records.

Mitigation: Although the easiest method for accessing and correcting medical records is by contacting the USCG medical clinic directly, individuals may also formally request access or correction by making a Privacy Act request.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

The MIS Project Officer (CG-1123), in conjunction with Clinic Administrators (CA) and System Administrators (SA), will ensure medical and administrative personnel assigned to Medical Treatment Facilities (MTF) and Independent Duty Health Service Technicians (IDHS) within their Area of Responsibility (AOR) complete all requirements prior to recommending access to the Electronic Health Record (EHR) or other MIS components. EHR access level is role-based and will be determined based on the individual's credentials, duty position and job description. Access to the Coast Guard Data Network (CGDN) is needed to use most MIS components. CGDN access is controlled by CG-63. To obtain CGDN access the requester must: Complete Automated Information System (AIS) Security Training, sign the data use agreements and complete the COAST GUARD Computer-User Test.

Clinic personnel may obtain the proper keys for the CHCS by first obtaining the "Clinic Administration Account Creation Form" from their local Clinic Administrator or approved System Administrator. The form must be completed in its entirety and then returned to the CA (or approved SA) for signature. Once approved the requesting personnel or the CA will contact

the USCG CHCS Helpdesk (1-866-851-2630) and provide them with the completed form via fax. Mandatory training will be implemented for anyone requesting access to specific keys. User have the option of attending training through a Virtual Classroom Training system (VCT), or users familiar with the system and their specific modules may request to take a Challenge assessment and test out of the required training. All users must complete the CGDN access requirements prior to requesting MIS access.

New Health & Safety employees/staff will be granted EHR Temporary Access until they complete required MIS training. This access will be issued for 30 days and will only be issued ONCE to each requested user. Any requests for additional temporary access must be submitted to CG-112 and provide adequate documentation as to why the member/employee could not complete the requirements in a timely manner. If the required training has not been completed within the 30 day period the user who is delinquent will find their access to CHCS terminated.

8.2 Will Department contractors have access to the system?

Yes, Department contractors that work within USCG medical clinics are granted access to CHCS and must comply with the same procedures discussed above for system access. Personnel Security establishes that all personnel involved in the access, design, development, operation, or maintenance of CHCS are properly investigated, cleared, authorized, and trained. Procedures are implemented at each USCG medical clinic to monitor personnel security policies of outside contractors in order to assure their ongoing compliance.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

CHCS users have an IT security training program. Continuous computer security awareness and training, in various forms, is utilized to elevate and sustain personnel awareness of proper operational and security related risks and procedures. Security training encompasses instruction on individual responsibilities under the Privacy Act of 1974 and specific guidance is provided to personnel who design, implement, use, or maintain CHCS resources. Training also includes annual instruction on personal duties and responsibilities under the privacy and security provisions of HIPAA.

Furthermore, CHCS users are trained that appropriate administrative action consistent with the site's policies will be taken against individuals found responsible for unauthorized disclosure of information in violation of HIPAA provisions. Individuals found responsible for unauthorized disclosure of sensitive information protected under the Privacy Act of 1974 and HIPAA may be faced with civil and/or criminal action.

All privacy and security awareness training is tracked to demonstrate compliance with this CHCS Security Policy. Tracking includes the training programs conducted for contractors and commercial health care providers.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

CHCS was previously accredited and certified following the DoD Instruction 5200.40, DoD Information *Technology Security Certification and Accreditation Process (DITSCAP)* dated Jan 20, 2006. In February 2009, the CHCS system received a full Authority To Operate (ATO) from TISCOM and USCG CG-6 Program Office. This ATO is valid through February 2, 2012.

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, Radio Frequency Identification (RFID), biometrics and other technology.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

CHCS is a DoD developed integrated hospital information system, which provides multi-functional support to medical ancillary services in an effort to provide better patient care and accountability.

9.2 What stage of development is the system in and what project development lifecycle was used?

CHCS is currently in the operational phase of its life cycle. CHCS entered into the System Development Life Cycle (SDLC) on June 22, 2006 at the Operations and Maintenance phase.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No, CHCS does not employ any technologies that compromise the privacy of the data transmitted and stored by the system.

Responsible Official

LT Mark Williams
United States Coast Guard
CG-1123 Medical Information Systems Division
Department of Homeland Security

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Military Health Systems Notice of Privacy Policy

HEALTH AFFAIRS

TRICARE

MILITARY HEALTH SYSTEM
NOTICE OF PRIVACY PRACTICES

Effective April 14, 2003

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions about this notice, please contact your local Military Treatment Facility (MTF) Privacy Officer or, if necessary, the TRICARE Management Activity (TMA) Privacy Officer at *www.tricare.osd.mil.*

This Notice of Privacy Practices is provided to you as a requirement of the Health Insurance Portability and Accountability Act (HIPAA). It describes how we may use or disclose your protected health information, with whom that information may be shared, and the safeguards we have in place to protect it. This notice also describes your rights to access and amend your protected health information. You have the right to approve or refuse the release of specific information outside of our system except when the release is required or authorized by law or regulation.

ACKNOWLEDGMENT OF RECEIPT OF THIS NOTICE

You will be asked to provide a signed acknowledgment of receipt of this notice. Our intent is to make you aware of the possible uses and disclosures of your protected health information and your privacy rights. The delivery of your health care services will in no way be conditioned upon your signed acknowledgment. If you decline to provide a signed acknowledgment, we will continue to provide your treatment, and will use and disclose your protected health information for treatment, payment, and health care operations when necessary.

WHO WILL FOLLOW THIS NOTICE

This notice describes the Military Health System (MHS) practices regarding your protected health information. For this notice, the MHS includes the following:

- Any Department of Defense (DoD) health plan
- Military Treatment Facilities (References to MTFs within this notice include both medical and dental treatment facilities and all providers/staff who operate under their auspices.)
- TRICARE Regional Offices
- Headquarters activities, such as the Surgeons General of the Military Departments and the TRICARE Management Activity

The MHS is part of an organized health care arrangement with the Coast Guard. The Coast Guard and its treatment facilities will also follow these practices.

OUR DUTIES TO YOU REGARDING PROTECTED HEALTH INFORMATION

"Protected health information" is individually identifiable health information. This information includes demographics, for example, age, address, e-mail address, and relates to your past, present, or future physical or mental health or condition and related health care services. The MHS is required by law to do the following:

- Make sure that your protected health information is kept private.
- Give you this notice of our legal duties and privacy practices related to the use and disclosure of your protected health information.
- Follow the terms of the notice currently in effect.
- Communicate any changes in the notice to you.

We reserve the right to change this notice. Its effective date is at the top of the first page and at the bottom of the last page. We reserve the right to make the revised or changed notice effective for health information we already have about you as well as any information we receive in the future. You may obtain a Notice of Privacy Practices by accessing your local MTF web site or TMA web site *www.tricare.osd.mil,* calling the local MTF Privacy Officer and requesting a copy be mailed to you, or asking for a copy at your next appointment.

HOW WE MAY USE OR DISCLOSE YOUR PROTECTED HEALTH INFORMATION

Following are examples of permitted uses and disclosures of your protected health information. These examples are not exhaustive.

Required Uses and Disclosures
By law, we must disclose your health information to you unless it has been determined by a competent medical authority that it would be harmful to you. We must also disclose health information to the Secretary of the Department of Health and Human Services (DHHS) for investigations or determinations of our compliance with laws on the protection of your health information.

Treatment
We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of your health care with a third party. For example, we would disclose your protected health information, as necessary, to a TRICARE contractor who provides care to you. We may disclose your protected health information from time-to-time to another MTF, physician, or health care provider (for example, a specialist, pharmacist, or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment. This includes pharmacists who may be provided information on other drugs you have been prescribed to identify potential interactions.

In emergencies, we will use and disclose your protected health information to provide the treatment you require.

Payment
Your protected health information will be used, as needed, to obtain payment for your health care services. This may include certain activities the MTF might undertake before it approves or pays for the health care services recommended for you such as determining eligibility or coverage for benefits, reviewing services provided to you for medical necessity, and undertaking utilization review activities. For example, obtaining approval for a hospital stay might require that your relevant protected health information be disclosed to obtain approval for the hospital admission.

Health Care Operations
We may use or disclose, as needed, your protected health information to support the daily activities related to health care. These activities include, but are not limited to, quality assessment activities, investigations, oversight or staff performance reviews, training of medical students, licensing, communications about a product or service, and conducting or arranging for other health care related activities.

For example, we may disclose your protected health information to medical school students seeing patients at the MTF. We may call you by name in the waiting room when your physician is ready to see you. We may use or disclose your protected health information, as necessary, to contact you to remind you of your appointment.

We will share your protected health information with third-party "business associates" who perform various activities (for example, billing, transcription services) for the MTF or any DoD health plan. The business associates will also be required to protect your health information.

We may use or disclose your protected health information, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that might interest you. For example, your name and address may be used to send you a newsletter about our MTF and the services we offer. We may also send you information about products or services that we believe might benefit you.

Required by Law
We may use or disclose your protected health information if law or regulation requires the use or disclosure.

Public Health
We may disclose your protected health information to a public health authority who is permitted by law to collect or receive the information. The disclosure may be necessary to do the following:

- Prevent or control disease, injury, or disability.
- Report births and deaths.
- Report child abuse or neglect.
- Report reactions to medications or problems with products.
- Notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.
- Notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect, or domestic violence.

Communicable Diseases
We may disclose your protected health information, if authorized by law, to a person who might have been exposed to a communicable disease or might otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight
We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. These health oversight agencies might include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and civil rights laws.

Food and Drug Administration
We may disclose your protected health information to a person or company required by the Food and Drug Administration to do the following:

- Report adverse events, product defects, or problems and biologic product deviations.
- Track products.
- Enable product recalls.
- Make repairs or replacements.
- Conduct post-marketing surveillance as required.

Legal Proceedings
We may disclose protected health information during any judicial or administrative proceeding, in response to a court order or administrative tribunal (if such a disclosure is expressly authorized), and in certain conditions in response to a subpoena, discovery request, or other lawful process.

Law Enforcement
We may disclose protected health information for law enforcement purposes, including the following:

- Responses to legal proceedings
- Information requests for identification and location
- Circumstances pertaining to victims of a crime
- Deaths suspected from criminal conduct
- Crimes occurring at an MTF site
- Medical emergencies (not on the MTF premises) believed to result from criminal conduct

Coroners, Funeral Directors, and Organ Donations
We may disclose protected health information to coroners or medical examiners for identification to determine the cause of death or for the performance of other duties authorized by law. We may also disclose protected health information to funeral directors as authorized by law. Protected health information may be used and disclosed for cadaveric organ, eye, or tissue donations.

Research
We may disclose your protected health information to researchers when authorized by law, for example, if their research has been approved by an institutional review board that has reviewed

the research proposal and established protocols to ensure the privacy of your protected health information.

Criminal Activity
Under applicable Federal and state laws, we may disclose your protected health information if we believe that its use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Military Activity and National Security
When the appropriate conditions apply, we may use or disclose protected health information of individuals who are Armed Forces personnel (1) for activities believed necessary by appropriate military command authorities to ensure the proper execution of the military mission including determination of fitness for duty; (2) for determination by the Department of Veterans Affairs (VA) of your eligibility for benefits; or (3) to a foreign military authority if you are a member of that foreign military service. We may also disclose your protected health information to authorized Federal officials for conducting national security and intelligence activities including protective services to the President or others.

Workers' Compensation
We may disclose your protected health information to comply with workers' compensation laws and other similar legally established programs.

Inmates
We may use or disclose your protected health information if you are an inmate of a correctional facility, and an MTF created or received your protected health information while providing care to you. This disclosure would be necessary (1) for the institution to provide you with health care, (2) for your health and safety or the health and safety of others, or (3) for the safety and security of the correctional institution.

Disclosures by the Health Plan
DoD health plans may also disclose your protected health information. Examples of these disclosures include verifying your eligibility for health care and for enrollment in various health plans and coordinating benefits for those who have other health insurance or are eligible for other government benefit programs. We may use or disclose your protected health information in appropriate DoD/VA sharing initiatives.

Parental Access
Some state laws concerning minors permit or require disclosure of protected health information to parents, guardians, and persons acting in a similar legal status. We will act consistently with the law of the state where the treatment is provided and will make disclosures following such laws.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION REQUIRING YOUR PERMISSION

In some circumstances, you have the opportunity to agree or object to the use or disclosure of all or part of your protected health information. Following are examples in which your agreement or objection is required.

MTF Directories
Unless you object, we will use and disclose in our MTF inpatient directory your name, the location at which you are receiving care, your condition (in general terms), and your religious affiliation. All of this information, except religious affiliation, will be disclosed to people who ask for you by name. Only members of the clergy will be told your religious affiliation.

Individuals Involved in Your Health Care
Unless you object, we may disclose to a member of your family, a relative, a close friend, or any other person you identify, your protected health information that directly relates to that person's involvement in your health care. We may also give information to someone who helps pay for your care. Additionally we may use or disclose protected health information to notify or assist in notifying a family member, personal representative, or any other person who is responsible for your care, of your location, general condition, or death. Finally, we may use or disclose your protected health information to an authorized public or private entity to assist in disaster relief efforts and coordinate uses and disclosures to family or other individuals involved in your health care.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

You may exercise the following rights by submitting a written request or electronic message to the MTF Privacy Officer. Depending on your request, you may also have rights under the Privacy Act of 1974. Your local MTF Privacy Officer can guide you in pursuing these options. Please be aware that the MTF might deny your request; however, you may seek a review of the denial.

Right to Inspect and Copy
You may inspect and obtain a copy of your protected health information that is contained in a "designated record set" for as long as we maintain the protected health information. A designated record set contains medical and billing records and any other records that the MTF uses for making decisions about you.

This right does not include inspection and copying of the following records: psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and protected health information that is subject to law that prohibits access to protected health information.

Right to Request Restrictions
You may ask us not to use or disclose any part of your protected health information for treatment, payment, or health care operations. Your request must be made in writing to the MTF Privacy Officer where you wish the restriction instituted. Restrictions are not transferable across

MTFs. If the restriction is to be throughout the MHS, the request may be made to the TMA Privacy Officer. In your request, you must tell us (1) what information you want restricted; (2) whether you want to restrict our use, disclosure, or both; (3) to whom you want the restriction to apply, for example, disclosures to your spouse; and (4) an expiration date.

If the MTF believes that the restriction is not in the best interest of either party, or the MTF cannot reasonably accommodate the request, the MTF is not required to agree. If the restriction is mutually agreed upon, we will not use or disclose your protected health information in violation of that restriction, unless it is needed to provide emergency treatment. You may revoke a previously agreed upon restriction, at any time, in writing.

Right to Request Confidential Communications
You may request that we communicate with you using alternative means or at an alternative location. We will not ask you the reason for your request. We will accommodate reasonable requests, when possible.

Right to Request Amendment
If you believe that the information we have about you is incorrect or incomplete, you may request an amendment to your protected health information as long as we maintain this information. While we will accept requests for amendment, we are not required to agree to the amendment.

Right to an Accounting of Disclosures
You may request that we provide you with an accounting of the disclosures we have made of your protected health information. This right applies to disclosures made for purposes other than treatment, payment, or health care operations as described in this Notice of Privacy Practices. The disclosure must have been made after April 14, 2003, and no more than 6 years from the date of request. This right excludes disclosures made to you, for an MTF directory, to family members or friends involved in your care, or for notification. The right to receive this information is subject to additional exceptions, restrictions, and limitations as described earlier in this notice.

Right to Obtain a Copy of this Notice
You may obtain a paper copy of this notice from your MTF or view it electronically at your local MTF web site or TMA web site at *www.tricare.osd.mil*.

FEDERAL PRIVACY LAWS

This MHS Notice of Privacy Practices is provided to you as a requirement of the Health Insurance Portability and Accountability Act (HIPAA). There are several other privacy laws that also apply including the Freedom of Information Act, the Privacy Act and the Alcohol, Drug Abuse, and Mental Health Administration Reorganization Act. These laws have not been superseded and have been taken into consideration in developing our policies and this notice of how we will use and disclose your protected health information.

COMPLAINTS

If you believe these privacy rights have been violated, you may file a written complaint with your local MTF Privacy Officer, the TMA Privacy Officer, or the Department of Health and Human Services. No retaliation will occur against you for filing a complaint.

CONTACT INFORMATION

You may contact your local MTF Privacy Officer or the TMA Privacy Officer for further information about the complaint process, or for further explanation of this document. The TMA Privacy Officer may be contacted at TRICARE Management Activity, Information Management, Technology and Reengineering Directorate, HIPAA Office, Five Skyline Place, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206, by phone at 1-888-DOD-HIPA (1-888-363-4472 – Toll Free from the continental United States)/TTY 877-535-6778. You may also email questions to hipaamail@tma.osd.mil. For additional information regarding your privacy rights visit the TRICARE Web site at http://www.tricare.osd.mil/hipaa/.

This notice is effective in its entirety as of April 14, 2003.