OFFICE OF INSPECTOR GENERAL

United States Coast Guard Safeguards For Protected Health Information Need Improvement

Homeland Security

May 7, 2015

OIG-15-87

DHS OIG HIGHLIGHTS

United States Coast Guard Safeguards For Protected Health Information Need Improvement

May 7, 2015

Why We Did This

We evaluated United States Coast Guard (USCG) safeguards for the protected health information it maintains. Our objectives were to determine whether the USCG's plans and activities instill a culture of privacy and whether it ensures compliance with the *Privacy Act of 1974,* as amended, the *Health Insurance Portability and Accountability Act of 1996,* and related laws and regulations.

What We Recommend

USCG faces challenges in protecting privacy data. We are making five recommendations to the USCG which, if implemented, should reduce the risks to privacy data.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The USCG has made progress in developing a culture of privacy. Separately, the USCG Privacy Office and *Health Insurance Portability and Accountability Act* (HIPAA) Office are working to meet requirements of pertinent legislation, regulations, directives, and guidance. These offices ensure their staff annually receive mandatory privacy training, which helps embed shared attitudes, values, goals, and practices for complying with requirements to properly handle sensitive personally identifiable information and protected health information (privacy data). Also, USCG has completed required privacy and security documentation for managing its information technology systems containing privacy data.

However, USCG faces challenges in protecting privacy data effectively because it lacks a strong organizational approach to resolving privacy issues. Specifically:

- USCG Privacy and HIPAA officials do not formally communicate to improve privacy oversight and incident reporting, thereby limiting USCG's ability to assess and mitigate the risks of future privacy or HIPAA breaches.
- USCG does not have consistent instructions for managing and securing the health records, potentially exposing USCG personnel and their families to loss of privacy or identity theft.
- USCG clinics have not completed contingency planning to safeguard privacy data from loss in case of disaster.
- USCG clinics lack processes to periodically review physical security, placing privacy data at unnecessary risk.
- USCG has not assessed the merchant mariner credentialing program and processes to identify and reduce risk to merchant mariners' privacy data managed throughout its geographically dispersed program operations.

USCG Response

The agency concurred with all of our recommendations. A copy of the agency's comments on a draft of this report is included at appendix C.

Table of Contents

Appendixes

Abbreviations

CFR	Code of Federal Regulations
CHCS	United States Coast Guard Composite Health Care System
COOP	Continuity of Operations Plan
DHS	Department of Homeland Security
HHS	Department of Health and Human Services
HIPAA	*Health Insurance Portability and Accountability Act of 1996*
IT	information technology
MMLD	Merchant Mariner Licensing and Documentation
NARA	National Archives and Records Administration
NMC	National Maritime Center
OIG	Office of Inspector General
OMB	Office of Management and Budget
PHI	protected health information
PIA	privacy impact assessment
PII	personally identifiable information
SPII	sensitive personally identifiable information
SORN	system of records notice
USCG	United States Coast Guard

Background

Since 1790, the United States Coast Guard (USCG) has protected the maritime domain, the environment, and U.S. economic interests—in the Nation's ports and waterways, along the coast, on international waters, or in any maritime region—to support national security. To accomplish this mission, USCG's employees and contractors may collect, use, maintain, and process sensitive personally identifiable information (SPII) and protected health information (PHI) on a daily basis.

The USCG operates 42 health clinics and 150 sick bays geographically dispersed throughout the United States and Puerto Rico. These clinics provide health care services to military active duty, reserve, and retired personnel, as well as eligible family members. Also, the clinics maintain paper and electronic health records generated from approximately 300,000 clinic visits per year.[1] Health records containing SPII and PHI (privacy data) consist of clinical, immunological, pharmacological, and radiological reports, and other logs.[2] USCG clinics use the United States Coast Guard Composite Health Care System (CHCS) for computerized management of these patient records.

In addition, the USCG National Maritime Center (NMC) collects privacy data to process credentials each year for merchant mariners, who are U.S. citizens and legal residents serving on or operating U.S. registered marine vessels in 195 countries. The NMC maintains paper and electronic records on more than 2.4 million merchant mariners around the world. These records contain sensitive biographical, medical, professional, and security information. Also, 19 geographically dispersed examination centers maintain records containing privacy data as part of assisting merchant mariners with submitting new or updated credential applications.[3] The Merchant Mariner Licensing and Documentation (MMLD) System tracks privacy data related to merchant mariner service, training, credentials, and qualifications for operating commercial vessels.

The *Privacy Act of 1974*, as amended (*Privacy Act*), imposes various requirements on each agency whenever it collects, uses, maintains, or disseminates information that is retrieved by the name of the individual or by some number, symbol, or other identifier. The Department of Homeland Security (DHS) defines personally identifiable information (PII) as any information that permits the identity of an individual to be inferred directly or indirectly, including any information that can be linked to that individual,

[1] A USCG health record is the chronological medical and dental record of an individual.
[2] For this report, we use privacy data to refer to sensitive personally identifiable information (SPII) or protected health information (PHI).
[3] There are 17 regional examination centers and 2 examination monitoring units that collect privacy data when they perform functions, such as receiving and screening credential applications, administering USCG examinations, overseeing course examinations, and facilitating credential submissions.

regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, employee, or contractor to the Department. DHS defines SPII as a particular type of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. The *Health Insurance Portability and Accountability Act of 1996* (*HIPAA*) *Privacy Rule* defines PHI as any individually identifiable health information, held or transmitted in any form or media whether electronic, paper, or oral, where there is a reasonable basis to believe that the information can be used to identify the individual.

On June 5, 2009, the DHS Deputy Secretary issued a "Memorandum Designation of Component Privacy Officers," directing each of its 10 components to designate a senior-level Federal employee as a full-time Privacy Officer. As of December 2014, the USCG Privacy Officer had three staff members dedicated to privacy issues (Privacy Office). (See appendix F for a complete list of duties.) This Office reports to the Assistant Commandant for Command, Control, Computers, and Information Technology. The Privacy Office is responsible for:

- overseeing USCG's implementation of Federal privacy law and regulations. (We confirmed that USCG is working to ensure that it meets legislation, regulations, directives, and guidance listed in appendix D.)
- conducting privacy assessments on systems of record, including USCG information technology (IT) systems and other activities for attendant privacy impacts, as required by *DHS Instruction 047-01-001, Privacy Policy and Compliance*. (See appendix E for our analysis of the status of USCG IT systems containing PII.)
- reporting on privacy activities and accomplishments.[4]
- addressing complaints, incidents, and managing records retention schedules.
- providing mandatory annual privacy training developed by the DHS Privacy Office, as well as advanced or supplementary training, as needed.

The HIPAA Privacy and Security Rules require that a covered entity designate a Privacy Official and a Security Official. USCG has designated a single senior-level officer who is responsible for the development and implementation of both privacy and security policies for the USCG Health Care System. (See appendix G for a complete list of this official's duties.) This official reports upward to the Assistant Commandant for Human Resources. The HIPAA Official is responsible for:

[4] OMB Memorandum M-14-04, "Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," (Nov. 18, 2013).

- serving as representative for the USCG Health Care System,[5]
- providing support for establishing, modifying, and disseminating USCG HIPAA policy,
- coordinating with the Defense Health Agency on all HIPAA related issues,
- serving as the liaison to receive inquiries or complaints from patients or beneficiaries, and
- collaborating with the Health, Safety, and Work-Life Service Center Privacy and Security Official, Regional Practice Privacy and Security Officials, and the Clinic Privacy and Security Officials (comprising the HIPAA Office) who serve as points of contact for their respective treatment facilities.

[5] *HIPAA* standards apply to "covered entities." USCG clinics, as part of the USCG Health Care Program, are covered entities.

Results of Audit

We evaluated the safeguards for sensitive personally identifiable information and protected health information (privacy data) maintained by USCG. Our objectives were to determine whether the USCG's plans and activities instill a culture of privacy and whether the USCG ensures compliance with the *Privacy Act of 1974*, as amended, the *Health Insurance Portability and Accountability Act of 1996*, and other privacy and security laws and regulations. The USCG designated a Privacy Officer as well as a Health Insurance Portability and Accountability Act Privacy and Security Official. These officials, among other functions, are responsible for ensuring compliance with Federal privacy laws and policies and for preparing reports and documentation on the USCG's privacy activities. For example, USCG has privacy and security documentation on how it manages its information technology systems that contain privacy data.

The USCG has made progress in developing a culture of privacy. Separately, the USCG Privacy Officer and Health Insurance Portability and Accountability Act Official are working to ensure that they are meeting the requirements of pertinent legislation, regulations, directives, and guidance. These Offices ensure that USCG provides mandatory privacy training annually for USCG staff. The respective training helps to embed shared attitudes, values, goals, and practices for complying with the requirements for properly handling privacy data.

However, USCG faces challenges in protecting privacy data effectively because it has not placed a priority on a strong organizational approach to resolving privacy issues. Specifically:

- USCG Privacy Officer and HIPAA Privacy and Security Official do not have formal communications or regular meetings, which are necessary for improving privacy oversight and incident reporting. Lacking such coordination, USCG is limiting its ability to assess risks and mitigate potential for privacy or HIPAA breaches.
- USCG does not have consistent instructions for managing and securing health records. Without updated instructions for records retention and disposal, USCG personnel and their families may be exposed to loss of privacy or identify theft.
- USCG clinics have not completed contingency planning for safeguarding privacy data from loss in case of an emergency or disaster.
- USCG clinics lack a process for periodically reviewing physical security to mitigate risks to privacy data.
- USCG has not conducted an assessment of the merchant mariner credentialing program and processes to identify and reduce privacy risk. Without improving accountability and internal controls, USCG is not

adequately protecting merchant mariner's privacy data throughout its geographically dispersed program operations.

We are making five recommendations to the USCG, which if implemented, should reduce the risks to privacy data.

USCG Progress in Developing a Culture of Privacy

USCG has made progress in developing a culture of privacy. Separately, the USCG Privacy Office and HIPAA Office are working to ensure that they are meeting the requirements of pertinent legislation, regulations, directives, and guidance (see appendix D). Specifically, these offices ensure that USCG provides mandatory privacy training for USCG staff. Their respective annual privacy training helps to embed shared attitudes, values, goals, and practices for complying with the requirements for proper handling of privacy data. The USCG Chief Information Officer identified 19 IT systems that require documentation regarding how they comply with privacy laws. (See appendix E for our analysis of the status of USCG IT systems that contain SPII.)

USCG Provision of Mandatory Privacy and HIPAA Training

Both USCG Privacy Office and the HIPAA Office have responsibility for enhancing the culture of privacy and assuring that Federal requirements for handling privacy data are met. Regular training is a key element of developing and maintaining an effective privacy culture.

The DHS Privacy Office requires that all employees complete annual DHS privacy training entitled "Privacy at DHS: Protecting Personal Information." This training meets Office of Management and Budget Memorandum (OMB) M-07-16 mandatory training requirements. The USCG Privacy Office oversees this training for USCG employees. For 2014, the DHS Privacy Office confirmed that USCG employees took this training. Also, the USCG Privacy Office conducted supplementary training over the last 2 years through two privacy awareness forums with the USCG Information System Security Officers and the Office of Regulations to convey best practices for safeguarding PII.

The USCG HIPAA Office directs all USCG health care workforce members to complete annual training, entitled "Privacy Act and HIPAA Core Training." This training meets the *HIPAA Privacy Rule*. The USCG HIPAA Office coordinates with the Defense Health Agency to use the Military Health System's Training Portal, MHS Learn, which pertains to military organizations.[6] Although we were unable to confirm training from the Military Portal, we verified that staff at the clinics we visited had taken this training.

Status of USCG for IT Systems that Contain Privacy Data

The USCG has completed key documentation for its 19 IT systems that contain privacy data as required. The *E-Government Act of 2002* requires agencies to

[6] The Department of Defense established the Defense Health Agency to manage the activities of the Military Health System. Previously, these activities were managed by TRICARE Management Activity, which was disestablished on the same date.

conduct a privacy impact assessment (PIA) for all new or substantially changed information systems that collect, maintain, or disseminate privacy and personal information. A PIA is used to identify and mitigate privacy risks at the beginning of and throughout the development life cycle of a program or system. In addition, the *Privacy Act* requires Federal agencies to issue a system of records notice (SORN) for publication in the *Federal Register* when PII is maintained by a Federal agency in a system of records and the information is retrieved by a personal identifier. The SORN identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally, and how the PII can be accessed and corrected.

USCG has published 19 PIAs and 36 associated SORNs that are available on the DHS Privacy Office's public website. We reviewed each document, the types of PII that are shared through access agreements, and retention periods for the PII. We also confirmed the accuracy, submission, and approval status of this documentation in various databases, including Trusted Agent FISMA, DHS Information Assurance Compliance System, *Federal Register*, the DHS Privacy Office, and USCG Privacy Office. (See appendix E for our analysis.)

Of the authorized IT systems containing privacy data, USCG has only two IT systems that contain PHI. These are the CHCS and MMLD. The CHCS is part of USCG's vision for an integrated health care IT system. As of December 2014, CHCS connects USCG clinics to its computerized records of patients. The MMLD is used to manage applications for, and issuance of, credentials to merchant mariners. Figure 1 describes these systems, the privacy data that may be collected in them, and internet links to associated PIAs and SORNs publicly available on the DHS Privacy Office website.

Figure 1. USCG Composite Health Care System (CHCS) and Merchant Mariner Licensing and Documentation (MMLD) System

Name and Purpose of System	Data That May Be Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
United States Coast Guard Composite Health Care System (CHCS) connects USCG clinics to its computerized patient records.	Name, sponsor Social Security number, date of birth, sponsor marital status, patient address, patient telephone number, email address, insurance information, gender, height and weight, current symptoms, medical records including chronic/acute illnesses, vital statistics, laboratory test results, radiology test results, previous health history including eyewear, prescriptions, medications, and allergies	DHS/USCG/PIA-017 - United States Coast Guard Composite Health Care System, July 25, 2011	DHS/USCG-011 - Military Personnel Health Records, December 19, 2008 73 FR 77773
Merchant Mariner Licensing and Documentation (MMLD) System tracks merchant mariner service, training, credentials, and qualifications related to operation of commercial vessels.	Name, Social Security number, date and place of birth, country of citizenship, mailing address, telephone number, home and work, email address, MMLD identification number, medical limitations, seaman's biometrics (photographs, fingerprint records, physical characteristics), information related to narcotics, driving while under the influence, and conviction records, next of kin's name, mailing address, phone number and email address, character references, including full name, address, and telephone number	DHS/USCG/PIA-020 - Merchant Mariner Licensing and Documentation System (MMLDS), March 1, 2011	DHS/USCG-030 - Merchant Seamen's Records, June 25, 2009 74 FR 30308

Source: DHS Privacy Office and USCG Compliance Documentation.

USCG Faces Challenges in Protecting Privacy Data

USCG has made progress in identifying its privacy data. However, it faces challenges in protecting privacy data effectively because it has not placed a priority on a strong organizational approach to resolving privacy issues. Specifically:

- USCG does not have formal communications, such as regular meetings, between its respective Privacy and HIPAA Offices which are necessary for improving privacy oversight and incident reporting. Without such coordination, USCG is limiting its ability to assess risks and mitigate potential privacy or HIPAA breaches.
- USCG does not have consistent instructions for managing and securing health records. Without updated instructions for records retention and disposal, USCG may expose personnel and their families to loss of privacy or identify theft.
- USCG clinics have not completed contingency planning for protecting privacy data from loss in case of emergency or disaster.
- USCG clinics do not have a process for periodically reviewing physical security to mitigate risks to privacy data.
- USCG has not conducted an assessment of the merchant mariner credentialing program and processes to identify and reduce privacy risk.

Without improving accountability and internal controls, USCG is not adequately protecting merchant mariners' privacy data throughout its geographically dispersed program operations.

USCG Privacy and HIPAA Offices Do Not Formally Communicate on Privacy Oversight and Reporting

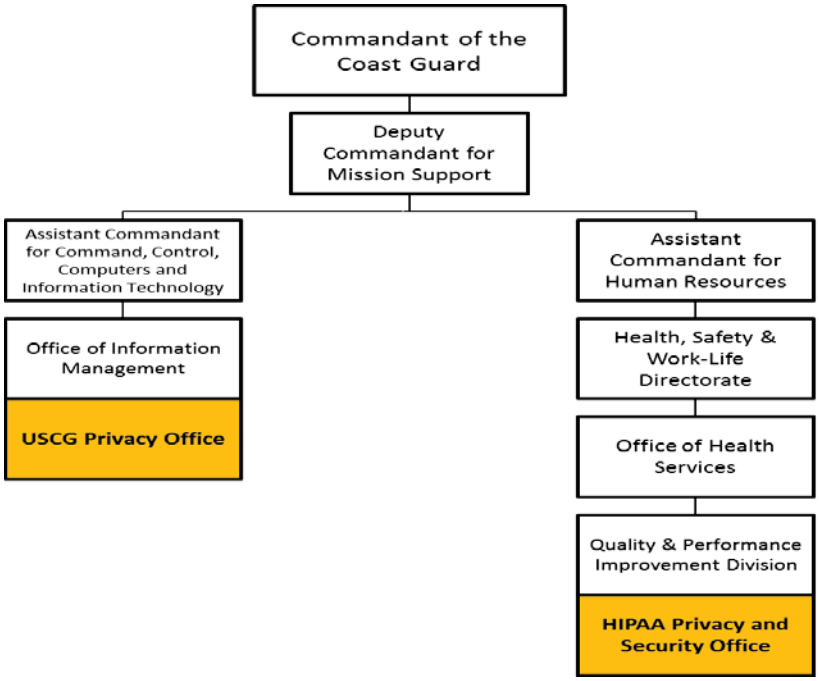
The USCG Privacy Office and the HIPAA Office do not have formal communications, or regular meetings, to ensure effective privacy oversight and reporting. USCG has established procedures for some offices to communicate across reporting lines to jointly address pertinent topics, such as the USCG Web Advisory Board or the USCG Headquarters Permanent Continuity of Operations Working Group Charter.

However, no formal communications have been established between the Privacy Office and the HIPAA Office, creating gaps in privacy oversight and reporting. For example, the DHS *Privacy Incident Handling Guidance* requires that the USCG Privacy Office report potential or confirmed PII incidents to the DHS Privacy Office.[7] In contrast, *HIPAA Breach Notification Rule* requires that USCG HIPAA Office report PHI notifications to the Department of Health and Human Services (HHS) Office of Civil Rights.[8] Because these USCG Offices have different reporting requirements and operate in separate structures within USCG, there is no centralized record of all privacy breaches. These Offices also have not developed a strategy to reduce such breaches.

To illustrate, these two USCG Offices are in different organizational command structures that require upward reporting. Each Office has stovepiped operations and lines of communications. There has been no lateral sharing of pertinent information. The Privacy Officer reports to the Assistant Commandant for Command, Control, Computers and Information Technology, while the HIPAA Official reports through its command structure to the Assistant Commandant for Human Resources. Figure 2 shows the two different organizational chains of command for the Privacy Office and the HIPAA Office.

[7] Privacy incidents are defined as the loss of control; a compromise; or a situation in which people other than authorized users have access or potential access to PII in usable form, whether physical or electronic, or in which authorized users access PII for an unauthorized purpose.
[8] Department of Health and Human Services, Office for Civil Rights enforces the *HIPAA Privacy Rule*, the *HIPAA Security Rule*, the *HIPAA Breach Notification Rule*, and the *Patient Safety Rule*.

Figure 2. Different Reporting Structures for the USCG Privacy Office and HIPAA Office



Source: OIG-developed based on USCG information.

Sharing and coordinating information for privacy oversight and reporting is useful for preventing or resolving privacy violations. Formal communications are also necessary for conducting risk assessments, establishing and verifying records retention, as well as improving the overall privacy culture. Without such coordination, USCG is limiting its ability to assess risks, and remediate privacy or HIPAA breaches. However, as of December 2014, USCG had not established procedures for formal communications to improve privacy oversight.

USCG Clinics Do Not Have Consistent Instructions for Health Records Retention and Disposal

USCG clinics do not have consistent guidance on managing and securing health records. The 42 clinics and 150 geographically dispersed sick bays manage approximately 200,000 medical and 100,000 dental visits annually, which require health services personnel to regularly create, use, maintain, transfer, and dispose of records containing privacy data. Without updating instructions for retention and disposal of these sensitive documents containing PII and PHI, USCG may expose personnel and their families to loss of privacy or identify theft.

There are two USCG manuals that provide records management instructions, but they have conflicting information. The *USCG Information and Life Cycle*

Management Manual (Life Cycle Manual) COMDTINST M5212.12A (406 pages) provides instructions, such as when clinics should retain and dispose of health records. Also, clinics should follow the Coast Guard *Medical Manual* (Medical Manual) COMDTINST M6000.1E (966 pages), Chapter 4, Health Records and Forms, for instructions pertaining to health records.[9]

However, these two manuals have records series that are difficult to cross-reference and have inconsistent retention periods.[10] Also, we identified a number of areas where the instructions are conflicting, incomplete, or unclear. For example:

- The Medical Manual instructs the clinics to dispose of "all health record documents" in accordance with the *Information and Life Cycle Management Manual*, COMDTINST M5212.12A. However, the Medical Manual's definition of "health records" as medical and dental records limits the instruction to only those record series addressed in the Life Cycle Manual's SSIC 6150 Health and Medical Records.
- The Medical Manual provides no instructions for the disposal of patient records that are listed in the Life Cycle Manual SSIC 6200 Preventative Medicine (vaccinations, case records, tests, and logs).
- The Life Cycle Manual is unclear whether the disposition of Immunology Tests and Logs includes Human Immunodeficiency Virus logs that are maintained by the clinics we evaluated.
- The Life Cycle Manual provides instructions to either "dispose" of or "destroy" records, but does not explain the difference. Figure 3 provides detailed examples of conflicting instructions.

[9] After our field work period, USCG released the current *Medical Manual COMDTINST M6000.1F* on August 22, 2014.

[10] 36 Code of Federal Regulations (CFR) Sec. 1220.18 defines a records series as file units or documents arranged according to a filing or classification system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access and use.

Figure 3. Examples of Conflicting, Incomplete, or Unclear Instructions

Type of USCG Health Record	USCG Medical Manual (April 29, 2011)	USCG Life Cycle Manual (June 15, 2011) or NARA's Approved Changes (June 7, 2013)
Controlled Substance Prescriptions	Chapter 10. C. Page 2, "Maintain all prescriptions on file, including all prescription logs related to chart prescribing, for **3 years**, after which they may be destroyed by shredding"	NARA's Approved Changes to Life Cycle Manual, 2-15, SSIC 6570 Pharmacy, Controlled Substances Prescriptions, "Destroy when **6 years** old."
Official Health and Dental Record	Chapter 4. A. Page 9, "follow the disposition instruction" (However, this Manual does not identify where to find the disposition instruction.)	Life Cycle Manual, II-6-3, SSIC 6150 Health and Medical Records, "Handle in accordance with Chapter 4 of Medical Manual."
Military Dependent Clinical Records	Chapter 4. D. Page 4, terminate **4** "**years** after the last record entry" However, this Manual does not explain whether "terminate" means that the record should be destroyed.	Life Cycle Manual, II-6-4, SSIC 6150 Health and Medical Records, "Transfer to NPRC … 4 years after last activity. Destroy **25 years** from the date of the latest document in record."
Health Service Log	Chapter 9. C. Page 18, serves "as a complete and **permanent** historical record."	NARA's Approved Changes, 2-14, SSIC 6150 Health and Medical Records, "Destroy after **6 years**."
Pathology Tests and Logs	No guidance is listed. However, the users might not realize that they need to follow instructions in the other Manual.	NARA's Approved Changes, 2-15, SSIC 6200 Preventive Medicine, "Destroy when **15 years**."
Biological Monitoring (Spore Testing)	Chapter 13. J. Page 16, "Regardless of the system used, document spore monitoring, including identification test date, test results, and operator, and maintain the records for **2 years**."	No guidance is listed. However, the users might not realize that they need to follow instructions in the other Manual.

Sources: USCG Medical Manual, USCG Information and Life Cycle Management Manual, and National Archives and Records Administration's (NARA) Approved Changes.

USCG recognized that the Life Cycle Manual and Medical Manual contained a number of disparate record series with varying retention dates for the same types of records. On March 10, 2014, USCG Office of Health Services issued a directive to the clinics that no medical records and related documents shall be destroyed. All records are to be retained pending further direction because USCG is in the process of revising the disposition and management policies for Coast Guard Medical Records. However, as of December 2014, USCG had not completed needed revisions of both Manuals. Nor had USCG identified which instructions should be followed. Therefore, USCG continued to lack consistent policies across its enterprise-wide health service infrastructure.

Without updated instructions for records retention and disposal, USCG may expose personnel and their family members to loss of privacy or identity theft. Also, maintaining records past archival or disposal dates increases the amount of privacy data that needs to be protected and imposes unnecessary storage costs on the taxpayer.

USCG Clinics Do Not Have Complete Contingency Planning

USCG does not have complete contingency planning for protecting privacy data in electronic and paper health records at any of its 42 clinics. Contingency plans include policies and procedures for responding to emergencies or other

occurrences (for example, fire, vandalism, system failure, and natural disaster) that can damage systems containing electronic and paper PHI.

Contingency Planning for Electronic Records

Electronic health records must meet standards and guidelines for contingency planning. Specifically, the *HIPAA Security Rule, Standard: Contingency Plan* (HIPAA contingency plan) requires clinics to establish and implement policies and procedures for responding to an emergency or other event that may damage PHI records. Also, the National Institute of Standards and Technology provides guidelines for implementing the following five elements of a HIPAA contingency plan, as shown in figure 4.[11]

Figure 4. The Five Elements of the HIPAA Contingency Plan for Electronic PHI

HIPAA Contingency Plan Element	Description
Data Backup Plan	"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."
Emergency Mode Operation Plan	"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."
Disaster Recovery Plan	"Establish (and implement as needed) procedures to restore any loss of data."
Testing and Revision Procedures	"Implement procedures for periodic testing and revision of contingency plans."
Applications and Data Criticality Analysis	"Assess the relative criticality of specific applications and data in support of other contingency plan components."

Sources: HIPAA Security Rule and National Institute of Standards and Technology Special Publication 800-66 Rev. 1.

USCG's CHCS Continuity of Operations Plan (COOP) dated December 2008 has addressed all five elements for electronic health data. In particular, USCG's level of criticality of the data is a key factor in deciding how PHI should be handled in case of a disaster or emergency. The COOP requires that each clinic identify its own level of criticality for both electronic and hard copy health data. In contrast, CHCS System Security Plan dated January 21, 2009, established a single assessment of the criticality for all clinic applications and safeguards for electronic data. Specifically, the CHCS Plan establishes the criticality level for each of the objectives of confidentiality, integrity, and availability for clinics as moderate, which we believe is too generic given each unique clinic environment.

[11] National Institute of Standards and Technology Special Publication 800-66 Rev. 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule*, October 2008.

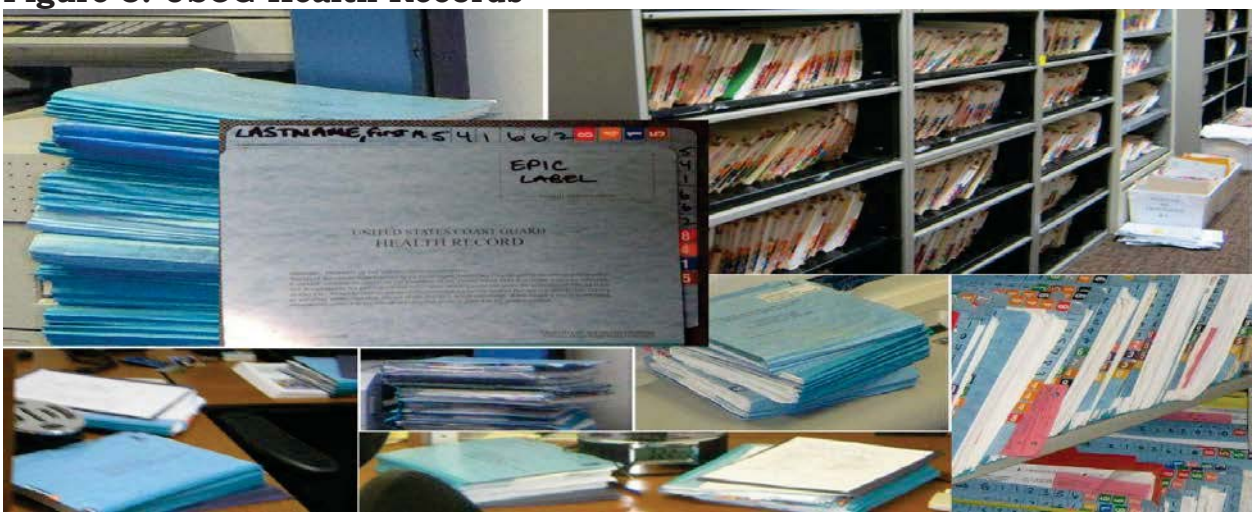
Further, the CHCS System Security Plan did not consider the system as a "Chief Privacy Officer Privacy Sensitive System," although it contains data that require heightened protection, such as: mental health visits, suspected spousal or child abuse, suspected rape, sensitive injury cases, sequestered for legal action, and family advocacy cases. In contrast, according to the CHCS privacy threshold analysis dated January 30, 2009, the DHS Privacy Office classified this system as a "privacy sensitive system," which requires a higher level of security for clinic data. However, as of December 2014, USCG had not updated privacy documentation to resolve this discrepancy.

Contingency Planning for Hard Copy Records Management

USCG contingency planning for hard copy privacy data was incomplete at the clinics. Specifically, the CHCS COOP requires that each clinic conduct its own assessment on how it will protect hard copy privacy data given its unique environment and requirements. Each clinic needs to identify its essential business functions, best solutions for continuing patient care and safety, priorities for protecting and recovering documents and health records, and physical safeguards which should be implemented to mitigate risks. However, as of December 2014, none of the 42 clinics had filed its individual assessment on protecting hard copy privacy data in the DHS Information Assurance Compliance System, as required.

Also, as of December 2014, only three of the nine judgmentally selected clinics that we evaluated had provided us with established procedures for safeguarding privacy data during disasters in accordance with the CHCS COOP. According to the Medical Manual, clinic administrators are responsible for developing a disaster preparedness plan to address the protection of hard copy privacy data in correspondence, reports, and records specific to their respective facilities. Figure 5 shows health records from various facilities that we evaluated that could be damaged or lost by a disaster.

Figure 5. USCG Health Records



Source: Office of Inspector General (OIG).

USCG still has not completed contingency planning for hard copy health records even though one clinic was destroyed during Hurricane Katrina in August 2005. Without complete contingency planning, the USCG has not fully minimized the risks of losing privacy data in a disaster. For example, figure 6 shows how flooding can damage facilities and records.

Figure 6. Examples of Flood Damage to Facilities and Records

Source: DHS and NARA.

Recovering and salvaging damaged health records after a disaster can be costly. Using industry estimates, we calculated that the recovery of just 7,500 records is approximately $1.41 million.[12] The addition of legal fees, identity protection, and credit reporting for 7,500 breached records could total more than $62 million. These expenses increase exponentially with a greater volume of records stored at a facility.

[12] According to the Ponemon Institute, the average cost to recover and salvage a record is $188 per record and an average of $8,369 in legal fees, identity protection, and credit reporting for each affected individual.

USCG Clinics Do Not Mitigate Physical Security Risks to Privacy Data

USCG clinics do not have an established process for periodically reviewing physical security to mitigate risks to privacy data. The *Coast Guard Freedom of Information and Privacy Acts Manual* COMDTINST M5260.3, Chapter 15, Section D, Safeguarding Personal Information requires that each area where privacy data are maintained shall have adequate administrative and physical security. This Manual requires that records be protected from viewing or inadvertent exposure by storing them in cabinets or other containers that, when unattended, are locked. However, USCG did not adequately address physical security risks at all nine clinics that we judgmentally selected for inspection. Figure 7 illustrates some of our observations while we were at the clinics.

Figure 7. Physical Security Risks at Various Clinics

Source: OIG.

Figure 7 illustrates access to rooms where health records were stored in cabinets that remained unlocked. We found this same condition at all nine clinics that we evaluated. Also, these clinics had open reception areas with low counters that afforded access to health records to be filed. While in the reception areas, we were able to overhear medical conversations among clinical staff, as well as from patients checking in at the front desk. At four of the nine clinics, we noticed gaps or breakage in ceiling tiles above the file cabinets where hard copy privacy data were stored. Some ceiling tiles showed evidence of water leakage. At two clinics, we observed unattended work stations that had computer screens displaying unprotected PHI.

As of December 2014, clinics had not established a process for periodic review of physical security for health records, nor resolved the physical security issues

that we identified during our inspections. The Medical Manual requires clinics to perform quality improvement studies regarding issues such as dental exam room configuration, medical record tracking, and patient data verification. However, the Medical Manual does not require these studies to include a review of physical security for privacy data. Without sufficient review of physical safeguards, the USCG may be placing privacy data at unnecessary risk.

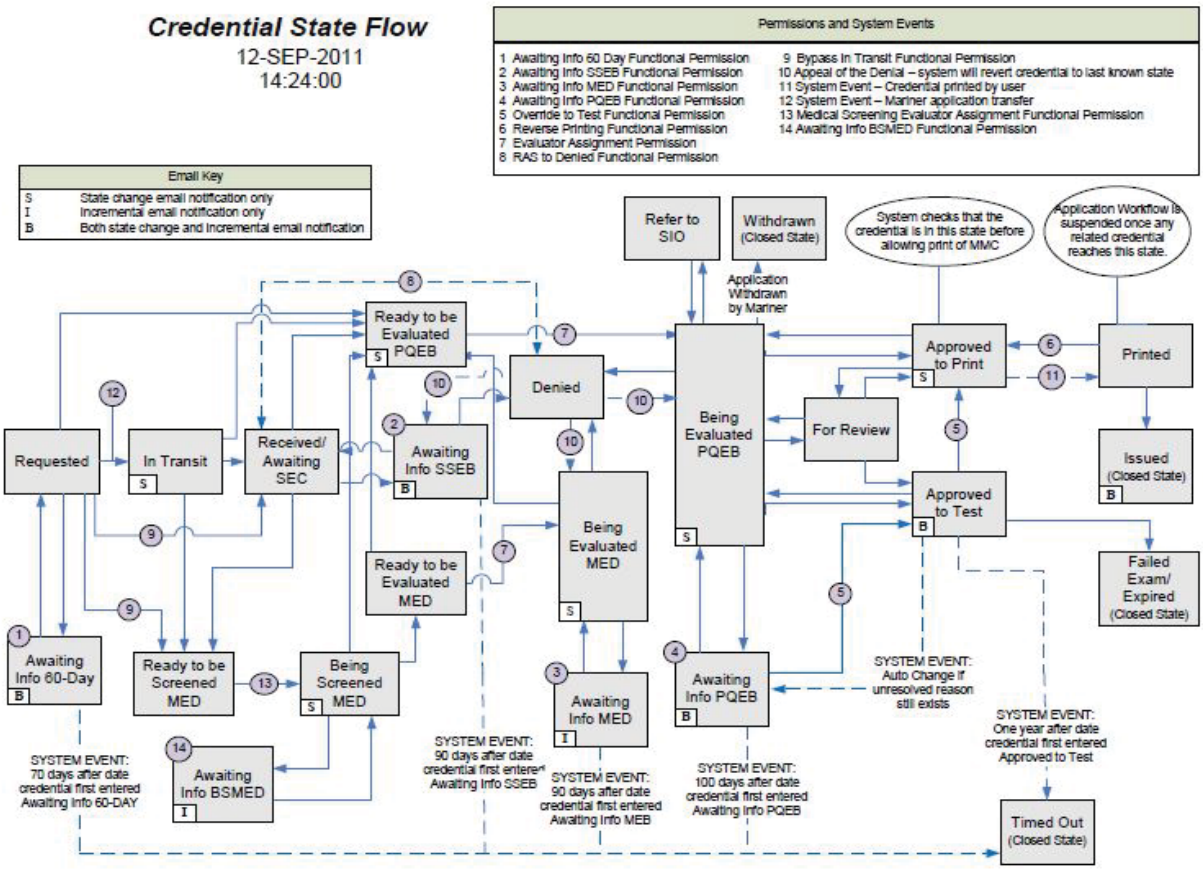
USCG Has Not Conducted Risk Assessments for Merchant Mariner Credentialing Program and Processes

NMC's mission is to issue credentials to merchant mariners. Without such credentials, fully compliant with current regulations, merchant mariners are not allowed to work. However, USCG has not conducted an assessment of the credentialing program and processes to identify and analyze risks, establish accountability for resources and records, and determine ways to minimize privacy risks.

During our visits with NMC and at a judgmentally selected sample of regional examination centers, we identified a number of areas where a risk assessment would help NMC to adapt to evolving demands, new priorities, shifting environments, and changing risks.

First, NMC has not met the current demand for credentials. To produce a credential, NMC must follow a complex process using both paper and electronic information, which includes biographical, medical, professional, and security data. Each day, NMC processes 262 applications, takes 998 phone calls, sends 1,300 emails, and reviews 193 applications for safety and suitability to produce 250 credentials related to operation of commercial vessels. However, the current process for NMC to complete a credential is not fast enough to overtake the growing backlog of credential applications. Figure 8 shows the flow of the credentialing process.

Figure 8. Merchant Mariner Credentialing Flow Chart



Source: USCG NMC.

Second, NMC had to address new priorities starting March 2014. Specifically, NMC must process new applications and convert all legacy credentials that have been issued for separate licenses into a newly designed and consolidated passport-type credential. Full implementation of new regulations must be completed by March 2019.

Third, NMC has not expedited operational processes by implementing new technology. In 2010, the USCG began developing an electronic application, the Merchant Mariner Security Electronic Application System. As of December 2014, this application is still not functional. Also, the Merchant Mariner Licensing and Documentation (MMLD) System remains limited to tracking evidence of merchant mariner capabilities related to the operation of commercial vessels. Therefore, NMC's processing of credentials is predominately a paper-based operation.

Fourth, NMC does not have consistent instructions on records retention and disposal to minimize risks to merchant mariner records. Presently, NMC has conflicting instructions regarding the short-term storage of supporting

documentation for completed credentials (supporting files). According to the PIA for the MMLD System, NMC must hold supporting files related to the issuance of credentials on site for 1 year past the last activity with the file. In contrast, according to the SORN for Merchant Seaman's Records, NMC must hold these supporting files on site for 5 years past the last activity with the file. Thereafter, NMC transports files "past the last activity" to the Federal Records Center for long-term storage. As of December 2014, USCG had not updated privacy compliance documentation to resolve this discrepancy.

Lastly, NMC has inadequate physical storage capacity for active records. Presently, merchant mariner files exceeding NMC's physical capacity (100,000 records) are sent to and retrieved from the Federal Records Center, which serves as short-term storage. The ongoing transportation of paper records to and from NMC has increased their risk of being mislabeled, mishandled, misplaced, or lost. USCG reported three or four incidents per year involving misplaced or lost merchant mariner credential applications. These incidents resulted from a high volume of transport and retrieval of files for several reasons:

- Each week, the 19 geographically dispersed examination centers transport files to NMC. Incoming records are combined with information that is either at NMC's central records room or at the Federal Records Center to produce a completed merchant mariner file. Therefore, completing a merchant mariner file may require transfer of stored files back to NMC for final processing before it can be stored again.
- Every year, NMC recalls an additional 30,000 records from the Federal Records Center to add or change information about a merchant mariner.
- When a merchant mariner appeals a credentialing decision, NMC may need to recall particular files from the Federal Records Center.

Figure 9 depicts the volume of merchant mariner files in active storage at NMC, as well as files being boxed for offsite storage.

Figure 9. NMC Central File Room

Source: OIG.

Senior leadership has the overall responsibility for implementing and maintaining an effective internal control system to address the various credentialing program and records management issues. The USCG Privacy Office has responsibilities according to *DHS Instruction Number 047-01-001: Privacy Policy and Compliance*. This Instruction requires an ongoing review of IT systems, programs, information sharing, and other activities to identify privacy impacts. This Instruction would entail conducting a risk assessment and incorporating safeguards to protect merchant mariner's privacy data throughout the credentialing process. However, as of December 2014, NMC had not completed a risk assessment and incorporated pertinent safeguards.

Without senior leadership and USCG Privacy Office conducting a risk assessment as a basis for improvements in the accountability, internal controls, policies, and procedures to protect privacy data throughout its geographically dispersed program operations, USCG will continue to expose merchant mariners' privacy data to unmitigated risks. Presently, the NMC maintains records on more than 2.4 million merchant mariners. The livelihoods of these merchant mariners around the world depend on having current and timely credentials. Protecting their privacy data is of paramount importance.

Recommendations

Recommendation 1. We recommend that the Vice Commandant of the Coast Guard establish a formal mechanism to ensure communication between the USCG Privacy Officer and the HIPAA Privacy and Security Official for enhanced privacy oversight and reporting.

Recommendation 2. We recommend that the Vice Commandant of the Coast Guard ensure consistent instructions for managing the health records retention and disposal.

Recommendation 3. We recommend that the Vice Commandant of the Coast Guard prepare a plan of action and milestones to ensure that USCG has complete contingency planning for safeguarding privacy data in the event of emergency or disaster.

Recommendation 4. We recommend that the Vice Commandant of the Coast Guard prepare a plan of action and milestones to periodically review physical safeguards to mitigate risks to SPII and PHI at clinics.

Recommendation 5. We recommend that the Vice Commandant of the Coast Guard prepare a plan of action and milestones to improve internal controls for the merchant mariner credentialing program and processes to ensure protection of privacy data.

United States Coast Guard Comments

The USCG concurred with all of the recommendations in a draft report provided for its review and comment. According to USCG management's comments, which are included in their entirety in appendix C, measures have been identified and milestones established for ensuring that privacy data are managed properly and appropriately protected.

OIG Analysis of the United States Coast Guard Comments

We consider USCG's plan of action and milestones to be responsive to the recommendations. These recommendations are considered open and unresolved until USCG provides documentation that it has completed corrective actions.

Appendix A

Transmittal to Action Official

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

May 7, 2015

TO: Vice Admiral Peter V. Neffenger
Vice Commandant of the Coast Guard
United States Coast Guard

FROM: Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *United States Coast Guard Safeguards for Protected Health Information Need Improvement*

Attached for your action is our final report, *United States Coast Guard Safeguards for Protected Health Information Need Improvement.* We incorporated the formal comments from the United States Coast Guard in the final report.

The report contains five recommendations aimed at improving privacy management. Your office concurred with all five recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 5 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations,* within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Marj Leaming, Director, Systems Privacy Division, at (202) 254-4172.

Attachment

Appendix B

Scope and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296), by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

Our objectives were to determine whether the USCG's plans and activities instill a culture of privacy that protects SPII and PHI and ensures compliance with the *Privacy Act of 1974*, as amended, the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), and other privacy and security laws and regulations. As background, we reviewed USCG's responsibilities for privacy protection, USCG guidance related to field and clinic operations, testimonies, compliance documentation, records management, training, and field program management. We confirmed that the USCG Privacy Office and HIPAA Office, separately, have worked to ensure that they are meeting the requirements of pertinent legislation, regulations, directives, and guidance (see appendix D). USCG has privacy and security documentation for its IT systems that contain privacy data (see appendix E).

As part of our initial fieldwork, we interviewed USCG's Privacy Officer, HIPAA Privacy and Security Official, and 96 managers and employees. We evaluated health records management, contingency planning, and physical security risks at nine judgmentally selected clinics located in California, Connecticut, Louisiana, Maryland, New Jersey, and Virginia. We identified the need for privacy controls in the processing of credentials by five regional examination centers located in California, Louisiana, Maryland, Massachusetts, and New York, as well as the National Maritime Center. We interviewed staff at the Operations Systems Center for Merchant Mariner Licensing and Documentation System and the United States Coast Guard Composite Health Care System.

After May 2014, we reviewed DHS and USCG websites for posting records instructions, documentation, or procedures that would relate to our recommendations. We also conducted telephone interviews and follow-up activities in October, November, and December 2014 with USCG management. We verified that the initial conditions described in this report still existed. Specifically, USCG management had not taken corrective action to coordinate Privacy Office and HIPAA Office oversight; ensure consistent privacy documentation and records instructions; conduct risk assessments; or address

clinic contingency planning and physical security. The effect of not implementing appropriate safeguards could result in serious consequences.

We conducted this performance audit between May 2013 and December 2014 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix C

United States Coast Guard Comments to the Draft Report

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

Commandant
United States Coast Guard

2703 Martin Luther King, Jr. Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-8
Phone: (202) 372-3533
Fax: (202) 372-4960

5730
APR 17 2015

MEMORANDUM

From: T. A. Sokalzuk
COMDT (CG-8)

Reply to Attn of: Audit Manager
Mark Kulwicki
(202) 372-3533

To: Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

Subj: DHS OIG DRAFT REPORT: UNITED STATES COAST GUARD SAFEGUARDS FOR POTECTED HEALTH INFORMATION NEEDS IMPROVEMENT

Ref: (a) OIG Project No. 12-032-ITA-USCG of March 2015

1. This memorandum transmits the Coast Guard's response to the draft report identified in reference (a).

2. The Coast Guard concurs with all the recommendations listed in the draft report. Our response in enclosure (1) demonstrates that the Coast Guard has measures in place and under development to ensure that Protected Health Information (PHI) is managed properly and information is appropriately protected.

3. If you have any questions, my point of contact is Mr. Mark Kulwicki who can be reached at 202-372-3533.

Enclosure: (1) USCG Response to OIG Draft Report PHI

USCG STATEMENT ON DHS OIG DRAFT REPORT: UNITED STATES COAST GUARD SAFEGUARDS FOR PROTECTED HEALTH INFORMATION NEEDS IMPROVEMENT
OIG Project No. 12-032-ITA-USCG

OIG Recommendation #1: Establish a formal mechanism to ensure communication between the USCG Privacy Officer and the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Official for enhanced privacy oversight and reporting.

Response: Concur. The Management Programs and Policy Division (CG-611) and the Office of Health Services (CG-112) have established monthly meetings between the Coast Guard Privacy Officer and the HIPAA Privacy and Security Official for enhanced privacy oversight and reporting. Estimated completion date is May 1, 2015.

OIG Recommendation #2: Ensure consistent instructions for the managing the health records retention and disposal.

Response: Concur. The Coast Guard released the Disposition of Health Records, COMDTINST 6150.4 on September 16, 2014 – This Instruction describes policy for the Coast Guard community regarding the life cycle management of health records for active duty and reserve members, dependents, retirees, and civilian employees upon separation or retiring. This Instruction aligns Coast Guard policy with Service Treatment Record (STR) and Non-Service Treatment Record (NSTR) Life Cycle Management, DoDI 6040.45 (released in October 28, 2010) - "The STR and NSTR shall be disposed in compliance with applicable National Archives and Records Administration (NARA) disposition schedules.

Disposition as defined by the Office of the Under Secretary of Defense (OUSD) Personnel & Readiness (P&R), SF 115, Submission for scheduling with NARA, (N-330-10-3) (Dated 2/18/2010) (see attached). The Coast Guard will revise the Medical Manual and Life Cycle Management Manual to reflect the content of the SF-115 – "The Armed Forces Military Service Treatment Record (STR) will be destroyed/deleted 100 years after the Date of Separation of the member form the Armed Services."

Additionally, the Coast Guard will issue joint message to all Coast Guard members (ALCOAST) to state that the Health, Safety, and Work-life Service Center (HSWL SC) will follow disposition guidance in accordance with the SF-115 disposition. Estimated completion date for all updates and release is August 1, 2015.

OIG Recommendation #3: Prepare a plan of action and milestone to ensure that USCG has complete contingency planning for safeguarding privacy data in the event of emergency or disaster.

Response: Concur. The Coast Guard will revise the Coast Guard's Composite Health Care System (CHCS) System Security Plan dated January 21, 2009 to provide an

Enclosure (1)

assessment of the criticality for each individual clinic application. This will improve the criticality level for each of the objectives of confidentiality, integrity and availability for each clinic (since they have unique environments).

The Coast Guard will also revise the Coast Guard's CHCS System Security Plan to consider the system as a Chief Privacy Officer Privacy Sensitive System. Privacy documentation will be updated to resolve this discrepancy. Estimated completion date is December 1, 2015.

OIG Recommendation #4: Prepare a plan of action and milestone to periodically review physical safeguards to mitigate risks to sensitive personally identifiable information (SPII) and PHI at clinics.

Response: Concur. HSWL SC will ensure that each clinic conducts its own assessment on how it will protect hard copy privacy data given its unique environment and requirements. Each clinic will identify its essential business functions, best solutions for continuing patient care and safety, priorities for protecting and recovering documents and health records, and physical safeguards which should be implemented to mitigate risks. This information will be incorporated in Healthcare Process Assessment Program (HPAP) or Accreditation Association for Ambulatory Health Care (AAAHC) reviews.

HSWL SC will ensure that each clinic develops a disaster preparedness plan to address the protection of hard copy privacy data in correspondence, reports, and records specific to their respective facilities. This information will be incorporated in HPAP or AAAHC reviews.

HSWL SC will evaluate each clinic 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. This information will be incorporated in HPAP or AAAHC reviews.

The Coast Guard will revise the Medical Manual to include a review of physical security for privacy data. Estimated completion date for all action is February 1, 2016.

OIG Recommendation #5: Prepare a plan of action and milestones to improve internal controls for the merchant mariner credentialing program and processes to ensure protection of privacy data.

Response: Concur. The Coast Guard National Maritime Center (NMC) and the Coast Guard Chief Privacy Officer will prepare a plan of action to improve internal controls for the merchant mariners credentialing program. Coast Guard will identify essential business functions, best solutions for protecting privacy data and physical safeguards which should be implemented to mitigate any risks.

Enclosure (1)

NMC and Coast Guard Chief Privacy Officer will evaluate the credentialing program on a periodic basis to ensure they have adequate administrative and physical security controls. The Coast Guard will revise the Systems of Record Notice (SORN) for retention of merchant mariner's credentials. Estimated completion date is February 1, 2016.

Enclosure (1)

Appendix D

Legislation, Regulations, Directives, and Guidance

We reviewed USCG activities in relation to each of the following legislation, regulations, directives, and guidance. We confirmed that the USCG Privacy Office and HIPAA Office are working to ensure that they meet the respective requirements. Public internet sites are also provided below.

LEGISLATION

Privacy Act of 1974, *as amended*, 5 U.S.C. § 552a.
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title5/pdf/USCODE-2011-title5-partI-chap5-subchapII-sec552a.pdf

E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899.
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, et seq.
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, 121 Stat. 266. http://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf

Homeland Security Act of 2002, *as amended*, Public Law 107-296, 116 Stat. 2135.
http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf

Paperwork Reduction Act of 1995, 44 U.S.C. § 3501, et seq.
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapI-sec3501.pdf

REGULATIONS, DIRECTIVES, AND GUIDANCE

36 CFR § 1220.18, *What definitions apply to the regulations in Subchapter B?* (July 01, 2012)
http://www.gpo.gov/fdsys/pkg/CFR-2012-title36-vol3/pdf/CFR-2012-title36-vol3-sec1220-18.pdf

***HIPAA Security Rule*, 45 CFR §164.308 (a)(7)(i)**, *Standard: Contingency Plan* (October 1, 2012). http://www.gpo.gov/fdsys/pkg/CFR-2012-title45-vol1/pdf/CFR-2012-title45-vol1-sec164-308.pdf

OMB M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007). http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

OMB M-14-04: *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (November 18, 2013).
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

REGULATIONS, DIRECTIVES, AND GUIDANCE

DHS Directive Number 047-01: *Privacy Policy and Compliance* (July 7, 2011). (No External Link Available)

DHS Instruction Number 047-01-001: *Privacy Policy and Compliance* (July 25, 2011). (No External Link Available)

DHS Memorandum: *Designation of Component Privacy Officers* (June 5, 2009). (No External Link Available)

DHS Privacy Office Privacy Policy Guidance Memorandum Number 2008-02: *DHS Policy Regarding Privacy Impact Assessments* (December 30, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (March 2012). http://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf

DHS Privacy Office: *Guide to Implementing Privacy* Version 1.0 (June 2010). http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf

Privacy Incident Handling Guidance (January 26, 2012). http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

DHS Privacy Office: *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

System of Records Notice Official Guidance. http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf

DHS Sensitive Systems Policy Directive 4300A*, Version 10.0* (May 20, 2013). (No External Link Available)

NIST SP 800-66 Rev. 1*: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (October 2008). http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

NIST SP 800-34 Rev.1: *Contingency Planning Guide for Federal Information Systems* (May 2010). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905266

NIST SP 800-88: *Guidelines for Media Sanitization* (September 2006). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50819

Federal CIO Council, Privacy Committee: *Best Practices: Elements of a Federal Privacy Program Version 1.0* (June 2010). http://energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf

USCG DOCUMENTS

Coast Guard Medical Manual, COMDTINST M6000.1E (April 2011).
http://www.uscg.mil/pacarea/pac13/docs/CIM_6000_1E.pdf

USCG Message to AIG, Subject: *Public Health Emergency Management Within The Coast Guard (CG)* (March 5, 2010)
http://www.uscg.mil/hq/cg1/cg112/cg1121/docs/aig/2010/aig03.05.pdf

National Archives and Records Administration's Approved Changes to Information and Life Cycle Management Manual, COMDTINST M5212.12A (updated June 7, 2013).
http://www.uscg.mil/records/docs/NewNARA.pdf

USCG Commandant Instruction M6230.9: Coast Guard Human Immunodeficiency Virus Program (June 25, 2008) http://www.uscg.mil/directives/cim/6000-6999/CIM_6230_9.PDF

Quality Improvement Implementation Guide, Exercise 23, Subject: *Laboratory Policy & Procedure Manual* (updated December 2008)
http://www.uscg.mil/hq/cg1/cg112/cg1122/docs/qiig/QIIG_23.doc

Commandant Instruction M5260.3, Subject: *The Coast Guard Freedom of Information (FOIA) and Privacy Acts Manual, Chapter 15, Section D, Safeguarding Personal Information* (June 14, 1996). http://www.uscg.mil/directives/cim/5000-5999/CIM_5260_3.pdf

Commandant Instruction M3010.13B, Subject: *Contingency Preparedness Planning Manual, Volume III – Exercises* (June 06, 2011). http://www.uscg.mil/directives/cim/3000-3999/CIM_3010_13B.pdf

Commandant Instruction 3010.19D, Subject: *Coast Guard After Action Program (CGAAP)* (January 12, 2015). http://www.uscg.mil/directives/ci/3000-3999/CI_3010_19D.pdf

National Incident Management System Training Program (September 2011)
http://www.fema.gov/pdf/emergency/nims/nims_training_program.pdf

USCG Message to AIG, Subject: *Coast Guard Medical Records Disposition Update* (March 10, 2014).
http://www.uscg.mil/hq/cg1/cg112/cg1121/docs/aig/2014/R%20101345Z%20MAR%2014.pdf

Appendix E

USCG Systems and Associated Privacy Impact Assessments and System of Records Notices

Privacy protections must be incorporated during the development and operation of systems and programs that affect privacy. DHS components are to conduct a privacy impact assessment (PIA) of all systems that collect, use, maintain, or disseminate PII, according to the *E-Government Act of 2002.* PIAs must be conducted for all new or substantially changed information systems that collect, maintain, or disseminate PII. The *Privacy Act of 1974* requires a system of records notice (SORN) to inform the public about what PII is being collected, why it is being collected, how long it is being retained, and how it will be used, shared, accessed, and corrected.

Below is our analysis of the status of USCG IT Systems that contain PII. We reviewed each of the documents, the types of PII that are shared through access agreements, and the retention periods for the PII. We confirmed the accuracy, submission, and approval status in Trusted Agent FISMA, DHS Information Assurance Compliance System, *Federal Register,* the DHS Privacy Office, and USCG Privacy Office. The following table lists USCG systems and related internet links to the associated 19 PIAs and 36 SORNs.

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
United States Coast Guard Composite Health Care System (CHCS) is an integrated health care information system that connects USCG medical clinics to computerized patient records. USCG medical clinics provide health care services to military active duty, reserve, retired personnel, and eligible family.	DHS/USCG/PIA-017 - United States Coast Guard Composite Health Care System, July 25, 2011	DHS/USCG-011 - Military Personnel Health Records, 73 FR 77773 (December 19, 2008)
Merchant Mariner Licensing and Documentation (MMLD) System manages the issuance of credentials to Merchant Mariners and processing of their applications. The MMLD tracks merchant mariner service, training, credentials, and qualifications related to operation commercial vessels.	DHS/USCG/PIA-015 - Merchant Mariner Licensing and Documentation System (MMLD), March 1, 2011	DHS/USCG-030 - Merchant Seamen's Records, 74 FR 30308 (June 25, 2009)

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
United States Coast Guard Homeport Internet Portal serves as an enterprise portal that combines secure information dissemination, advanced collaboration, and provides a public-facing interface for internal Coast Guard processes. It is an operational mission replacement for the current legacy internet system (www.uscg.mil).	DHS/USCG/PIA-001(b) – United States Coast Guard Homeport Update, November 16, 2012 DHS/USCG/PIA-001(a) - United States Coast Guard Homeport (USCGH) Update, October 17, 2008 DHS/USCG/PIA-001 - United States Coast Guard Homeport (USCGH), May 9, 2006	DHS/CG 060 Homeport, 74 FR 57692 (November 9, 2009)
United States Coast Guard "Biometrics at Sea" collects biometric information from persons reasonably suspected of violations of U.S. law who are interdicted at sea or as a result of at-sea interdictions.	DHS/USCG/PIA-002(c) - United States Coast Guard "Biometrics at Sea", July 12, 2011 DHS/USCG/PIA-002(b) - United States Coast Guard "Biometrics at Sea", March 14, 2008 DHS/USCG/PIA-002(a) - United States Coast Guard "Biometrics at Sea" Mona Passage Proof of Concept Update, May 15, 2007 DHS/USCG/PIA-002(a) - United States Coast Guard "Biometrics at Sea" Mona Passage Proof of Concept, November 3, 2006	DHS/USVISIT-0012 – DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007)

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
United States Coast Guard Law Enforcement Information Data Base (LEIDB) Pathfinder archives text messages prepared for law enforcement, counter terrorism, maritime security, maritime safety, or other Coast Guard missions for historical analysis, watch lists, link analysis, and trend analysis.	DHS/USCG/PIA-004 - United States Coast Guard Law Enforcement Information Data Base (LEIDB)/Pathfinder, March 31, 2008	DHS/USCG-062 - Law Enforcement Information Data Base (LEIDB)/Pathfinder, 73 FR 56930 (September 30, 2008)
United States Coast Guard Maritime Awareness Global Network (MAGNET) collects information on people, places, and things with maritime environment activity information for sharing and correlation of data to establish Maritime Domain Awareness.	DHS/USCG/PIA-005 - United States Coast Guard Maritime Awareness Global Network (MAGNET), April 11, 2008	DHS/USCG-061 Maritime Awareness Global Network (MAGNET), 73 FR 28143 (May 15, 2008)
Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System to add the Notice of Arrival on the Outer Continental Shelf expands Notice of Arrival requirements to vessels, establishes Notice of Departure requirements for certain vessels, with the modifications to electronically collected information for notice of arrivals and notice of departures.	DHS/USCG/PIA-006(a) - Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System to add the Notice of Arrival on the Outer Continental Shelf Update, June 3, 2009 DHS/USCG/PIA-006 – Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System Notice of Proposed Rulemaking, November 19, 2008	DHS/USCG-013 - Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305 (June 25, 2009) DHS/USCG-029 - Notice of Arrival and Departure, 73 FR 75442 (December 11, 2008) DHS/USCG-061 Maritime Awareness Global Network (MAGNET), 73 FR 28143 (May 15, 2008)

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
National Pollution Funds Center – Pollution Response Funding, Liability, and Compensation System (NPFCPRFLCS) is used for the management of funds and recovery of costs involved with damages resulting from an oil spill under the *Oil Pollution Act.*	DHS/USCG/PIA-007 - National Pollution Funds Center – Pollution Response Funding, Liability, and Compensation System (NPFC PRFLACS), June 17, 2009	None Applicable
Marine Information for Safety and Law Enforcement (MISLE) is used by USCG personnel to schedule and record operational activities such as vessel boarding, facility inspections, marine casualty investigations, pollution response actions, law enforcement actions, and search-and-rescue operations.	DHS/USCG/PIA-008 - Marine Information for Safety and Law Enforcement (MISLE), September 3, 2009	DHS/USCG-013 - Marine Information for Safety and Law Enforcement (MISLE), 74 FR 30305 (June 25, 2009)
Core Accounting Suite is a financial suite of applications hosted by the USCG Finance Center as an integrated financial and asset management system used by the USCG, the Transportation Security Administration, and the Domestic Nuclear Detection Office. *Chief Financial Officer Tools* provides web-based tools to assist with budget tracking. *Core Accounting System* administers accounts receivable, assets, property, inventory, accounts payable, purchasing, and the general ledger. *Financial Procurement Desktop* is an enterprise-wide accounting and procurement system. *Contract Information Management System* provides information to the Financial Procurement Desktop, Workflow *Image Network System* provides imaging and document processing for the Core Accounting System, and *Sunflower Asset Management* is a property management system used by the Transportation Security Administration.	DHS/USCG/PIA-009 - Core Accounting Suite, September 18, 2009	DHS/ALL-007 - Department of Homeland Security Accounts Payable System of Records, 73 FR 61880 (October 17, 2008) DHS/ALL-008 - Department of Homeland Security Accounts Receivable System of Records, 73 FR 61885 (October 17, 2008) DHS/ALL-010 - Department of Homeland Security Asset Management Records, 73 FR 63181 (October 23, 2008)

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
Case Matter Management Tracking System Functions as a repository for all information for cases and matters across all legal practices areas within the USCG Office of Chief Counsel. The database is used to track information for parties and entities, docketing, financial estimates, with an integrated document management system.	DHS/USCG/PIA-010 - Case Matter Management Tracking System, September 25, 2009	DHS/USCG-008 - Courts Martial Case File, 73 FR 64961 (October 31, 2008) DHS/USCG-010 - Physical Disability Evaluation System Files, 73 FR 77768 (December 19, 2008) DHS/USCG-011 - Military Personnel Health Records, 73 FR 77773 (December 19, 2008) DHS/USCG-014 - Military Pay and Personnel, 73 FR 77743 (December 19, 2008) DHS/USCG-015 - Legal Assistance Case Files, 73 FR 75455 (December 11, 2008)
Boating Accident Report Database (BARD) is a database for boating accident report data submitted by state and territorial reporting authorities. Information in the system includes vessel information, environmental conditions, description of the accident, casualty information, and property ownership information.	DHS/USCG/PIA-011 - Boating Accident Report Database (BARD), November 12, 2009	None Applicable

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
Recruit Analysis and Tracking System gathers and distributes recruiting leads, tracks recruit progression, prepares accession forms, processes reservations for enlisted and officer candidates, manages mission plans and reports on quality, quantity, and diversity statistics for recruiting. Information collected on recruits varies, with increased information collected as a recruit progresses through the process.	DHS/USCG/PIA-012 - Recruit Analysis and Tracking System, November 30, 2009	DHS/USCG-027 Recruiting Files, 76 FR 49494 (August 10, 2011)
Academy Information System (AIS) maintains information for the USCG Academy on cadets, prior cadets, faculty, and staff. This system processes transactional data for cadet military program records. Further, the system manages applicant data to facilitate admissions to the Academy.	DHS/USCG/PIA-013 - Academy Information System (AIS), January 26, 2010	DHS/USCG-014 - Military Pay and Personnel, 73 FR 77743 (December 19, 2008)
Security and Safety Computer Network is composed of major applications to support physical access control, identity verification, security camera monitoring, and key tracking for USCG Headquarters.	DHS/USCG/PIA-014 - Security and Safety Computer Network, June 16, 2010	DHS/ALL-010 - Department of Homeland Security Asset Management Records, 73 FR 63181 (October 23, 2008) DHS/ALL-023 - Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010) DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010)

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
Transportation Worker Identification Credential (TWIC) Reader Requirements for U.S. Coast Guard would require owners or operators of vessels and facilities that meet certain risk factors to use, as an access control measure, electronic readers that work in combination with the Transportation Worker Identification Credential.	DHS/USCG/PIA-019 – Transportation Worker Identification Credential (TWIC) Reader Requirements for U.S. Coast Guard, March 25, 2013	DHS/TSA-002 Transportation Security Threat Assessment System, 75 FR 28046 (May 19, 2010)
Interagency Operations Center (IOC) Watchkeeper system was developed to improve tactical decision making, situational awareness, operations monitoring and processing, and joint planning in a coordinated interagency environment.	DHS/USCG/PIA-020 – Interagency Operations Center (IOC) Watchkeeper, January 4, 2013	DHS/USCG-029 Notice of Arrival and Departure, 76 FR 69749 (November 9, 2011) DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012)
College Board Recruitment Plus (CBRP) describes the USCG Academy use of the software application *Recruitment PLUS* from College Board. The system collects and stores prospective applicant biographical and educational data and facilitates tracking of the application process.	DHS/USCG/PIA-016 - College Board Recruitment Plus (CBRP), April 1, 2011	DHS/ALL-003 - Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008) DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS), , 74 FR 49882 (September 29, 2009) DHS/USCG-027 - Recruiting Files, 76 FR 49494 (August 10, 2011)

Name and Purpose for PII Collected	Privacy Impact Assessment(s)	System of Records Notice(s)
Coast Guard Business Intelligence (CGBI) provides data analysis and reporting across all 11 USCG mission areas as a business intelligence and mission support tool to assess USCG activities, performance, capabilities, and readiness. The system does not directly collect information and receives data from other USCG systems. The system receives information from the Merchant Mariner License and Documentation System (MMLD), Marine Information for Safety and Law Enforcement, Homeport, Recruiting Analysis and Tracking System, and Boating Accident Report Database Additional information is obtained from *Shipboard Arrival Notification System* containing ship arrival information, *Shore Asset Management* providing details on shore assets including personnel, and *Integrated Aids to Navigation Information System* containing navigational aid information.	DHS/USCG/PIA-018 - Coast Guard Business Intelligence (CGBI), April 17, 2012	DHS/USCG-013 Marine Information for Safety and Law Enforcement, 74 FR 30305 (June 25, 2009) DHS/USCG-027 Recruiting Files, 76 FR 49494 (August 10, 2011) DHS/USCG-029 Notice of Arrival and Departure, 76 FR 69749 (November 9, 2011) DHS/USCG-030 Merchant Seaman's Records, 74 FR 30308 (June 25, 2009) DHS/USCG-060 Homeport, 74 FR 57692 (November 9, 2009) DHS/ALL-002 DHS Mailing and Other Lists, 73 FR 56930 (September 30, 2008) DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records, 73 FR 63172 (October 23, 2008)

Source: DHS Privacy Office website as of the period covered by the audit.

Appendix F

Component-Level Privacy Officer Designation and Duties

COMPONENTS REQUIRED TO DESIGNATE PRIVACY OFFICERS
▪ United States Coast Guard ▪ Federal Emergency Management Agency ▪ National Protection and Programs Directorate ▪ Office of Intelligence and Analysis ▪ Science & Technology Directorate ▪ Transportation Security Administration ▪ U.S. Citizenship and Immigration Services ▪ U.S. Customs and Border Protection ▪ U.S. Immigration and Customs Enforcement ▪ United States Secret Service

Source: DHS Designation Memorandum, June 5, 2009.

COMPONENT PRIVACY OFFICER DUTIES
Maintain an ongoing review of component IT systems, technologies, rulemakings, programs, pilot projects, information sharing, and other activities to identify collections and uses of PII and any other attendant privacy impacts.
Coordinate with system and program managers, together with the DHS Privacy Officer and component counsel to complete required privacy compliance documentation.
Review component policies and directives to ensure compliance with DHS privacy policy, privacy laws applicable to DHS, and Federal Government-wide privacy policies.
Oversee component implementation of DHS privacy policy.
Provide the DHS Privacy Officer all component information necessary to meet the Department's responsibilities for reporting to Congress or OMB on DHS activities that involve PII or otherwise impact privacy.
Oversee component's implementation of procedures and guidance issued by the DHS Privacy Officer for handling suspected and confirmed privacy incidents; notify the DHS Privacy Officer and other Department offices of such incidents as component procedures dictate; ensure that privacy incidents have been properly mitigated; and recommend that the DHS Privacy Officer close privacy incidents upon mitigation.
Process privacy complaints from organizations, DHS employees, and other individuals, whether received directly or by referral from the DHS Privacy Officer.
Oversee component privacy training and provide educational materials, consistent with mandatory and supplementary training developed by the DHS Privacy Officer.
Maintain an ongoing review of component data collection forms, whether electronic or paper-based, to ensure compliance with the Privacy Act Statements and implementation of regulations and guidelines.
Review component record retention schedules for paper or electronic records that contain PII to ensure privacy interests are considered in the establishment of component record disposition policies.
Advise component on information sharing activities that involve the disclosure or receipt of PII and participate in the review of Information Sharing Access Agreements.
Document and implement procedures for identifying, processing, tracking, and reporting on Privacy Act Amendment requests.

Source: DHS Instruction Number 047-01-001.

Appendix G

HIPAA Privacy and Security Official Duties

COMPONENT HIPAA PRIVACY OFFICIAL DUTIES
Personnel Designations. A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice. Notice of privacy practices, Right to notice. Except as provided by paragraph (a)(2) or (3) of 45 CFR § 164.520, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. Uses and disclosures of protected health information: General rules. Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Right to an accounting of disclosures of protected health information. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested. Access to protected health information. Right of access. An individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set. Amendment of protected health information. Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set. Notice shall be provided to the (HHS) Secretary by covered entities of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals, then such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved. Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been accessed, acquired, or disclosed during such breach. *Privacy Policies and Procedures*. A covered entity must develop and implement written privacy policies and procedures that are designed to comply with the standards, implementation specifications, or other requirements of this subpart (Privacy Rule). *Training*. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart (Privacy Rule), as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

Documentation and Record Retention. A covered entity must retain the documentation required by 45 CFR § 164.530(j)(1) (Privacy Rule) for six years from the date of its creation or the date when it last was in effect, whichever is later.

Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity.

COMPONENT HIPAA SECURITY OFFICIAL DUTIES

Security Personnel. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart (Security Rule) for the entity.

Risk Analysis. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Risk Management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Contingency Plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Policies and Procedures and Documentation Requirements. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart (Security Rule).

Sources: 45 CFR §§164.306-316 and §§164.502-534, Department of Health and Human Services.

Appendix H

Major Contributors to This Report

Marj Leaming, Director
Eun Suk Lee, Privacy Audit Manager
Kevin Mullinix, Privacy Analyst
Christopher Browning, Program Analyst
Thomas Rohrback, Referencer

Appendix I

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commandant of the Coast Guard
USCG Audit Liaison Officer
Chief Privacy Officer
USCG Privacy Officer
USCG HIPAA Privacy and Security Official

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Senator Al Franken, Chairman, Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law
Representative Bennie G. Thompson, Ranking Member, House Committee on Homeland Security
Representative Jason Chaffetz, Chairman, House Committee on Oversight and Government Reform
Representative Duncan Hunter, Chairman, Subcommittee on Committee on Coast Guard and Maritime Transportation, Transportation and Infrastructure Committee

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305