Report No. DODIG-2018-109

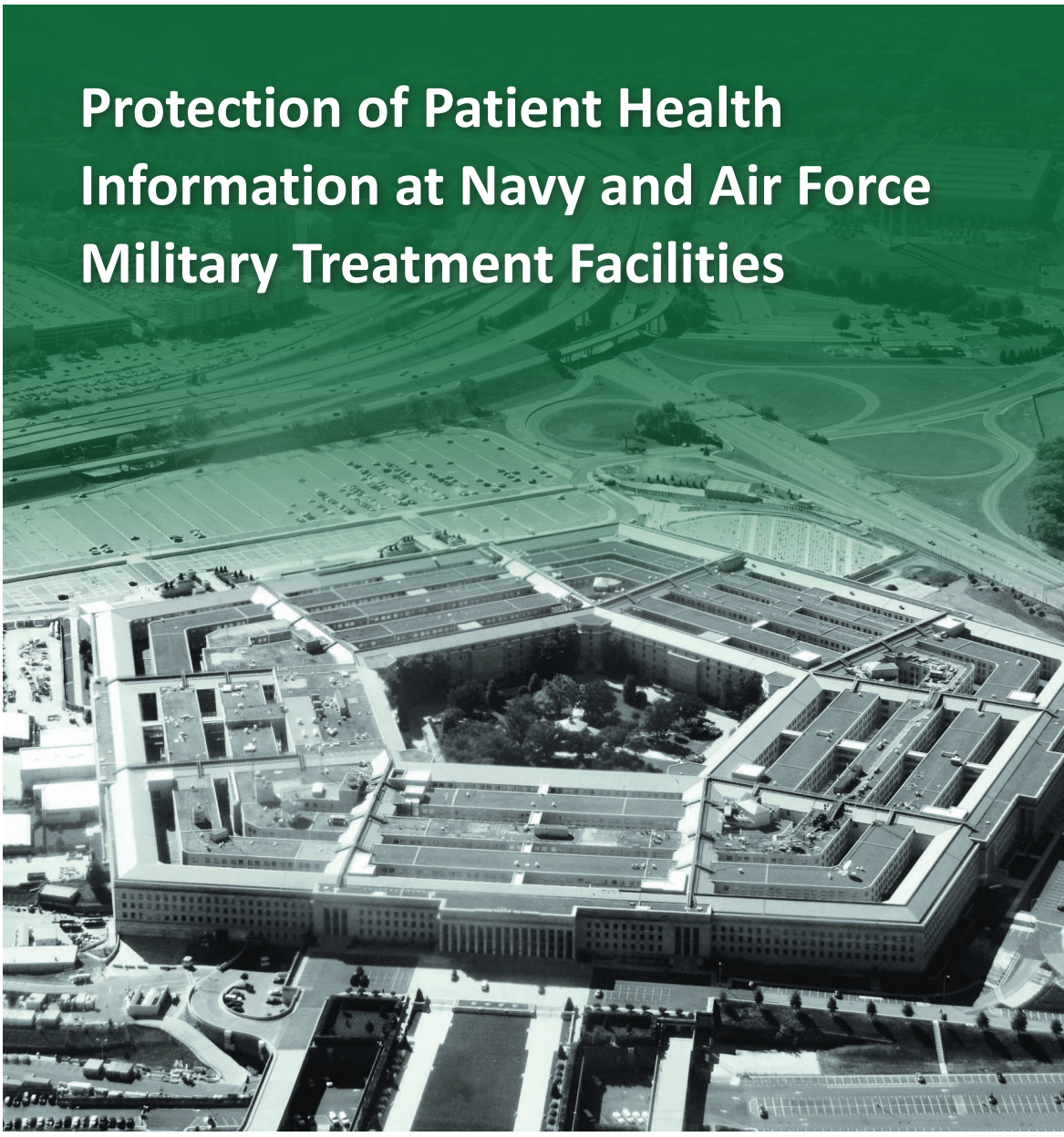
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

MAY 2, 2018

Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities

May 2, 2018

Objective

We determined whether the Departments of the Navy and Air Force designed and implemented effective security protocols to protect electronic health records (EHRs) and individually identifiable health information (patient health information [PHI]) from unauthorized access and disclosure.[1] This report is the second in a series of reports on security protocols used by the Military Departments for protecting EHR and PHI systems. The first report (DODIG-2017-085) identified that the Defense Health Agency (DHA) and the Army did not consistently implement effective security protocols to protect systems that stored, processed, and transmitted PHI.

Background

We visited three Navy facilities—Naval Hospital Camp Pendleton, Camp Pendleton, California; San Diego Naval Medical Center, San Diego, California; and the U.S. Naval Ship (USNS) Mercy, San Diego, California; and two Air Force facilities, the 436th Medical Group, Dover, Delaware; and Wright-Patterson Medical Center, Dayton, Ohio. We reviewed 17 information systems at the 5 locations: 3 DoD EHR systems, 3 modified EHR systems used aboard the USNS Mercy, 2 DHA-owned systems, and 9 Service-specific systems.

[1] An EHR is a digital patient-centered record that provides real-time information containing medical and treatment histories of patients and comprehensive information related to the patient's care.
For this report, "effective" means that security controls were implemented and operated as defined by Federal and DoD system security requirements.

Findings

Officials from the DHA, Navy, and Air Force did not consistently implement security protocols to protect systems that stored, processed, and transmitted EHRs and PHI at the locations tested. Specifically, we identified issues at the Naval Hospital Camp Pendleton; San Diego Naval Medical Center; USNS Mercy; 436th Medical Group; and Wright-Patterson Medical Center related to:

- accessing networks using multifactor authentication;
- configuring passwords to meet DoD length and complexity requirements;
- mitigating known network vulnerabilities;
- ~~(FOUO)~~ [redacted] and [redacted];
- granting users access based on the user's assigned duties;
- configuring systems to lock automatically after 15 minutes of inactivity;
- reviewing system activity reports to identify unusual or suspicious activities and access;
- developing standard operating procedures to manage system access;
- implementing adequate physical security protocols to protect electronic and paper records containing PHI from unauthorized access;
- maintaining an inventory of all Service-specific systems operating that stored, processed, and transmitted PHI; and
- developing or maintaining privacy impact assessments.

Officials from the DHA, Navy, and Air Force did not consistently implement security protocols to protect systems that stored, processed, and transmitted EHRs and PHI for a variety of reasons including lack of resources and guidance, system incompatibility, and vendor limitations.

Results in Brief

Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities

Findings (cont'd)

Without well-defined, effectively implemented system security protocols, the DHA, Navy, and Air Force compromised the integrity, confidentiality, and availability of PHI. In addition, ineffective administrative, technical, and physical security protocols that result in a violation of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 could cost the MTFs up to $1.5 million per year in penalties for each category of violation.[2]

Recommendations

We recommend that the Director, DHA, configure the DoD EHR systems and other DHA-owned systems that process, store, and transmit PHI to lock automatically after 15 minutes of inactivity.

We recommend, among other actions, that the Surgeons General for the Departments of the Navy and Air Force, in coordination with the Navy Bureau of Medicine and Surgery and the Air Force Medical Service:

- assess whether the systemic issues identified in this report exist at other Service-specific MTFs; and
- develop and implement an oversight plan to verify that MTFs enforce the use of Common Access Cards and configure passwords that meet DoD password complexity requirements to access systems that process, store, and transmit PHI.

We also recommend, among other actions, that the MTF Chief Information Officers:

- develop a plan of action and milestones and take appropriate steps to mitigate known network vulnerabilities in a timely manner;
- implement procedures to grant access to systems that process, store, and transmit PHI based on roles that align with user responsibilities;

Recommendations (cont'd)

- configure all systems that contain PHI to lock automatically after 15 minutes of inactivity; and
- ~~(FOUO)~~ [redacted] and [redacted] for systems that process, store, and transmit PHI.

Management Comments and Our Response

The DHA Director agreed that the DHA could potentially configure systems to lock automatically after a defined period of inactivity, but did not provide assurance that the DHA would configure its systems that process, store, and transmit PHI to lock automatically after 15 minutes of inactivity.

The Navy Executive Director, Navy Bureau of Medicine and Surgery, agreed with all recommendations for the Navy Bureau of Medicine and Surgery and the Naval Hospital Camp Pendleton. The Executive Director also agreed with 10 recommendations for the Naval Medical Center San Diego and disagreed with one recommendation. However, recommendations for the Navy Bureau of Medicine and Surgery, Naval Hospital Camp Pendleton, and the Naval Medical Center San Diego are unresolved, and require additional comments.

In addition, the Air Force Surgeon General agreed with all 15 recommendations addressed to his office and the Air Force MTFs; however, one recommendation is unresolved and requires additional comments. Furthermore, the Military Sealift Command Chief of Staff agreed with nine recommendations, partially agreed with two, and disagreed with one recommendation for the USNS Mercy. However, the Chief of Staff identified additional controls and alternative actions that the USNS Mercy would implement that resolved all recommendations. Please see the Recommendations Table on the next page.

[2] HIPAA requires covered entities to implement administrative, technical, and physical safeguards to protect the integrity and confidentiality of PHI from unauthorized use or disclosure.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, Defense Health Agency	5		
Surgeon General, Department of the Navy	2.a, 2.b, 2.c, 2.d		
Surgeon General, Department of the Air Force		2.a, 2.b, 2.c, 2.d	
Chief Information Officer, U.S. Navy Bureau of Medicine and Surgery	2.a, 2.b, 2.c, 2.d		
Chief Information Officer, U.S. Air Force Medical Service		2.a, 2.b, 2.c, 2.d	
Commander, 436th Medical Group		3	
Commander, Naval Hospital Camp Pendleton	3		
Commander, Naval Medical Center San Diego	3		
Commander, U.S. Naval Ship Mercy		3, 4, 6	
Commander, Wright-Patterson Medical Center		3	
Chief Information Officer, 436th Medical Group		1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 1.h, 1.i	
Chief Information Officer, Naval Hospital Camp Pendleton		1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 1.h, 1.i, 4	
Chief Information Officer, Naval Medical Center San Diego	1.e, 1.f, 1.i	1.a, 1.b, 1.c, 1.d, 1.g, 1.h, 4	
Chief Information Officer, U.S. Naval Ship Mercy		1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 1.h, 1.i, 4	
Chief Information Officer, Wright-Patterson Medical Center	4	1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 1.h, 1.i	

Please provide Management Comments by June 1, 2018.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

May 2, 2018

MEMORANDUM FOR DIRECTOR, DEFENSE HEALTH AGENCY
SURGEON GENERAL, DEPARTMENT OF THE NAVY
SURGEON GENERAL, DEPARTMENT OF THE AIR FORCE
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE
NAVAL INSPECTOR GENERAL

SUBJECT: Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities
(Report No. DODIG-2018-109)

We are providing this report for your review and comment. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on the draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Executive Director, Navy Bureau of Medicine and Surgery, addressed all the specifics of Recommendations 1.a–1.i and 4 for Naval Hospital Camp Pendleton; and Recommendations 1.a, 1.b, 1.c, 1.d, 1.g, and 1.h for Naval Medical Center San Diego. In addition, comments from the Air Force Surgeon General addressed all specifics of Recommendations 1.a–1.i, 2.a–2.d, and 3. Furthermore, comments from the Chief of Staff, Military Sealift Command, addressed all the specifics of Recommendations 1.a–1.i, 3, 4, and 6. Therefore, those recommendations are resolved.

However, comments from the Director, Defense Health Agency only partially addressed Recommendation 5. Comments from the Executive Director, Navy Bureau of Medicine and Surgery, only partially addressed Recommendations 1.e, 1.f, and 1.i for Naval Medical Center San Diego; Recommendations 2.a–2.d for the Surgeon General of the Navy and Navy Bureau of Medicine and Surgery; and Recommendation 3 for Naval Hospital Camp Pendleton and Naval Medical Center San Diego. Comments from the Air Force Surgeon General only partially addressed Recommendation 4 for the Wright-Patterson Medical Center. Therefore, those recommendations are unresolved. We request that the Director, Defense Health Agency; Air Force Surgeon General; and the Executive Director provide additional comments on the recommendations by June 1, 2018.

Please send a PDF file containing your comments to audcso@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

cc:
Assistant Secretary of Defense for Health Affairs
Commander, Military Sealift Command

Contents


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Introduction

Objective

The audit objective was to determine whether the Departments of the Navy and the Air Force designed and implemented effective security protocols to protect electronic health records (EHRs) and individually identifiable health information (patient health information [PHI]) from unauthorized access and disclosure.[3] We issued a prior report on the Defense Health Agency (DHA) and the Army security protocols for protecting systems that processed, stored, and transmitted PHI.[4]

For this audit, we focused on Navy and Air Force medical centers, hospitals, and clinics. We selected a nonstatistical sample of 3 of the 81 Navy military treatment facilities (MTF) and 2 of the 84 Air Force MTFs to visit within the scope of this audit. The MTFs are facilities established to provide medical and dental care to eligible individuals. At the five locations, we reviewed: three DoD EHR systems, three modified EHR systems used aboard the U.S. Naval Ship (USNS) Mercy, two DHA-owned systems, and nine Service-specific information systems. See Appendix A for a discussion on the scope and methodology, and prior audit coverage.[5]

Background

An EHR is a digital patient-centered record that provides real-time information containing medical and treatment histories of patients and comprehensive information related to the patient's care. EHRs allow health care providers, including primary care physicians, specialists, laboratories, radiologists, clinics, and emergency rooms, to share and access PHI at any time. PHI is medical information obtained by medical personnel that states the physical or mental health or condition of a patient.

On August 21, 1996, Congress passed Public Law 104-191, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA)," which requires covered entities to implement administrative, technical, and physical safeguards to protect the integrity and confidentiality of PHI from unauthorized use or disclosure.[6] HIPAA includes provisions for securing PHI to provide patient's assurance on

[3] For this report, "effective" means that security controls were implemented and operated as defined by Federal and DoD system security requirements.

[4] Report DODIG-2017-085, "Protection of Electronic Patient Health Information at Army Military Treatment Facilities," July 6, 2017.

[5] Service-specific systems are systems used by the Navy and the Air Force.

[6] Covered entities, as defined by HIPAA, are health plans, health care clearinghouses, and health care providers who electronically transmit health-related information for transactions covered by Department of Health and Human Services standards.

the integrity, confidentiality, and availability of their personal information. Entities could be fined up to $1.5 million a year per violation category if they violate the HIPAA provisions.[7] Ensuring compliance with HIPAA standards requires a combined effort from the Assistant Secretary of Defense for Health Affairs as well as the Military Services and Other Defense Organizations.

DoD Responsibilities for Protecting Health Information

The Assistant Secretary of Defense for Health Affairs develops policies, procedures, and standards to manage the DoD Military Health System (MHS), which includes transferring and securing medical records and ensuring privacy of medical, health, and other sensitive information. The DoD MHS provides medical and dental services to about 9.4 million beneficiaries at 673 MTFs, including 55 military hospitals and 373 military medical clinics worldwide. The DHA supports the delivery of health services to MHS beneficiaries and manages 56 systems that process, store, or transmit PHI. Additionally, the DHA manages the following DoD EHR systems and modified EHR systems used by health care providers to capture in- and out-patient information.

- The Armed Forces Health Longitudinal Technology Application (AHLTA). A medical and dental record management system used to access patient conditions, prescriptions, and diagnostic test results.
- The AHLTA – Theater (AHLTA-T). An application used by deployed medical staff to document clinical care.
- The Composite Health Care System (CHCS). An outpatient care system used to track appointments, order laboratory tests, authorize radiology procedures, and prescribe medications.
- The Theater Medical Information Program CHCS Cache System (TC2). A system used by deployed medical personnel to document inpatient healthcare and ordered services, and view patient results. The TC2 includes limited CHCS functionality.
- The Clinical Information System/Essentris Inpatient System (Essentris). An inpatient care system used to capture bedside point-of-care data such as real-time heart and fetal monitoring.
- The Maritime Medical Module. Ships use the Maritime Medical Module to store and process data and continuously monitor the medical environment and health of personnel who live and work on the ship.

[7] 42 U.S. Code § 1320d-5 describes four categories related to HIPAA violations that covered entities (1) were unaware of, (2) not willfully neglected and the violation was due to reasonable cause, (3) willfully neglected but addressed in a timely manner, and (4) willfully neglected and did not address in a timely manner.

The DoD is in the process of replacing the three EHR systems (AHLTA, the CHCS, and Essentris) with MHS GENESIS, which will provide a single health record service for service members, veterans, and their families. MHS GENESIS integrates inpatient and outpatient care to provide complete medical and dental information from the point of injury to the MTF. Once fielded, the DHA will manage MHS GENESIS. However, the MTFs will continue to use AHLTA, the CHCS, and Essentris for at least a year after the MHS GENESIS is fully deployed. MHS GENESIS will not be fully deployed at all the MTFs until FY 2022.

Public Law 114-328, the National Defense Authorization Act for Fiscal Year 2017, Section 702, provides the DHA additional responsibilities for administering and securing systems and PHI data beginning October 1, 2018. Specifically, Section 702 requires the DHA to manage information technology, budget, policies and procedures, health care administration and management, and military medical construction for the DoD EHR systems at all MTFs.

Service Commands' Role in Protecting Health Information

The Navy Bureau of Medicine and Surgery (BUMED) and the Air Force Medical Service (AFMS), under the leadership of their respective Surgeon General, provide oversight of and guidance to the MTFs. BUMED develops policy and manages resources for about 63,000 Navy and Marine Corps military, civilian, and contractor personnel performing medical care. BUMED provides oversight of the Department of the Navy's medical operations, research and development, and educational programs. AFMS provides full medical readiness of the services used to support operations, and delivers health care to 2.6 million patients at 76 military installations worldwide. The USNS Mercy is under the command of the Military Sealift Command, which provides ocean transportation to the DoD. However, the Military Sealift Command is not responsible for protecting PHI and securing the systems used aboard the USNS Mercy. The DHA and the Navy share those responsibilities.

MTFs and Systems Reviewed

The Navy and Air Force MTFs use DoD EHR systems, modified EHR systems, DHA-owned systems, and other Service-specific systems to process, store, and transmit PHI. The USNS Mercy uses modified EHR systems when the ship is afloat to document medical and surgical services to deployed military personnel and civilians. For this audit, we visited five Navy and Air Force medical centers, hospitals, and clinics. Specifically, we visited the Naval Hospital Camp Pendleton, California (NHCP); Naval Medical Center San Diego, California (NMC San Diego); USNS Mercy in San Diego, California; the 436th Medical Group, Dover Air Force Base, Dover, Delaware (Dover Clinic); and Wright-Patterson Medical

Center, Dayton, Ohio (WPMC). In addition to the three EHR systems and three modified EHR systems, the five MTFs used two other DHA-owned systems and nine Service-specific systems to process, store, and transmit PHI. The systems we reviewed at each MTF are as follows (See Appendix A for system descriptions).

NHCP

- McKesson Cardiology
- Parata System Suite
- PeerVue

NMC San Diego

- Audio Metric Database System
- Blood Management Blood Bank/Transfusion Service (BMBB/TS)
- Health Artifact and Imaging Management Solution (HAIMS)

USNS Mercy

- Carestream Picture Archiving and Communication System (Carestream)

Dover Clinic

- Health Artifact and Imaging Management Solution
- Picture Archiving and Communication System (PACS)

WPMC

- Draeger Innovian Anesthesia (Innovian)
- Epiphany Electrocardiogram Management
- Nuclear Medicine Information System

Guidance on Protecting PHI

Federal and DoD guidance prescribes requirements to protect systems that process, store, and transmit PHI as follows.

- The *Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, August 21, 1996, Section 1173 (d)(2)*. HIPAA requires covered entities to implement administrative, technical, and physical safeguards to protect the integrity and confidentiality of PHI from unauthorized use or disclosure.
- *DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Healthcare Programs," August 12, 2015*. DoD Instruction 8580.02 implements information security requirements by establishing policy and assigning responsibilities for covered entities to protect PHI that is created, received, maintained, or transmitted electronically.

- *DoD Instruction 6025.18, "Privacy of Individually Identifiable Health Information in DoD Health Care Programs," December 2, 2009*. DoD Instruction 6025.18 requires covered entities to protect PHI.
- *National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013*. National Institute of Standards and Technology Special Publication 800-53 provides guidelines for selecting security controls used by organizations and information systems that support executive agencies of the U.S. Government to meet Federal Information Processing Standard Publication 200 requirements.[8] The guidelines apply to all components of an information system that process, store, or transmit Federal information.

Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[9] We identified an internal control weakness related to protecting systems that process, store, and transmit PHI. Specifically, DHA, Navy, and Air Force officials did not consistently implement technical, physical, and administrative protocols to protect DoD EHR systems, modified EHR systems, and Service-specific systems from unauthorized access and disclosure. We will provide a copy of the report to the senior official at the DHA, BUMED, AFMS, and the MTFs who is responsible for internal controls.

[8] Federal Information Processing Standard Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006.

[9] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

DHA, Navy, and Air Force Security Protocols for Systems Containing PHI Were Not Effective

Officials from the DHA, Navy, and Air Force did not consistently implement security protocols to protect systems that processed, stored, and transmitted EHRs and PHI.[10] Specifically, the officials did not consistently require users to use a Common Access Card (CAC) to access the three DoD EHR systems, one modified EHR, and seven Service-specific systems (three Navy and four Air Force). The officials did not consistently require users to use a CAC for system access because system administrators determined the CAC software was incompatible with older system software or did not disable the password function for AHLTA. In addition, the DHA, Navy, and Air Force officials did not consistently comply with the DoD password complexity requirements for Essentris, one modified EHR, and six Service-specific systems (three Navy and three Air Force) because system limitations or vendor requirements did not allow system administrators to change password configurations to meet DoD length and complexity requirements.

Moreover, system and network administrators at the five MTFs did not:

- consistently mitigate known vulnerabilities affecting the Navy and Air Force networks at the five MTFs because they lacked resources such as tools and staff to address the vulnerabilities as systems and devices were connected to the networks;
- ~~(FOUO)~~ [redacted] for four Service-specific systems (two Navy and two Air Force) because [redacted] were used instead of [redacted] or the servers did not support using [redacted];
- grant users access to three DoD EHR systems, two modified EHR systems, two DHA-owned systems, and eight Service-specific systems (five Navy and three Air Force) based on the user's assigned duties because they did not consistently develop and implement standard operating procedures (SOPs) to grant, elevate, and deactivate user access or require written justification to obtain and elevate system access privileges;

[10] Navy and Air Force officials include BUMED, AFMS, MTF Chief Information Officers, and the MTF information assurance managers and officers.

- configure three DoD EHR systems, three modified EHR systems, and six Service-specific systems (three Navy and three Air Force) to lock automatically after 15 minutes of inactivity because they stated that only the vendors were able to change the configuration settings or they relied on network configuration settings to automatically lock users for inactivity; or
- consistently review system activity reports to identify unusual or suspicious activities and access for three DoD EHR systems, three modified EHR systems, one DHA-owned system, and eight Service-specific systems (four Navy and four Air Force) because they performed this task only when a security incident occurred.

Furthermore, officials at the Dover Clinic and aboard the USNS Mercy did not implement adequate physical security controls to protect electronic and paper records containing PHI from unauthorized access because they did not properly secure communications equipment or record when medical records were accessed.

Additionally, officials from BUMED, AFMS, and the MTFs were not aware of all Service-specific systems operating on their networks that processed, stored, and transmitted PHI. Specifically, the officials were unaware that systems were operating on their networks because BUMED and AFMS did not require the MTFs to identify and report systems that contained PHI and the MTFs did not maintain an inventory of systems that contained PHI. The Chief Information Officers (CIOs) for the DHA, BUMED, and AFMS did not develop and maintain privacy impact assessments (PIAs) for two DoD EHR systems and six Service-specific systems (three Navy and three Air Force). According to DHA officials, existing processes to complete and approve the assessments were delayed as agencies transitioned to the DoD's risk management framework (an integrated DoD-wide decision-making process for managing cyber risk).[11]

Without well-defined, effectively implemented system security protocols, the DHA, Navy, and Air Force compromised the integrity, confidentiality, and availability of PHI. Security protocols, when not applied or ineffective, increase the risk of successful cyber attacks; system and data breaches; data loss and manipulation; and unauthorized disclosures of PHI. In addition, ineffective administrative, technical, and physical security protocols that result in a HIPAA violation could cost the MTFs up to $1.5 million per year in penalties for each category of violation.

[11] DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014 (Incorporating Change 2, July 28, 2017).

System Security Protocols Were Ineffective or Not Implemented

The DHA, Navy, and Air Force security protocols for its systems that processed, stored, and transmitted PHI did not protect against unauthorized access to, or unauthorized disclosure of, the data. Specifically, the DHA, Navy, and Air Force system and network administrators did not:

- require the use of CACs to access 11 of the 17 systems reviewed;
- configure passwords to meet DoD password complexity requirements for 8 of the 17 systems reviewed;
- consistently mitigate known network vulnerabilities at all five MTFs visited;
- ~~(FOUO)~~ protect [redacted] and [redacted] for 4 of the 17 systems reviewed at NHCP, WPMC, and aboard the USNS Mercy;
- grant user access to 15 of the 17 systems reviewed based on the user's assigned responsibilities;
- configure 12 of the 17 systems reviewed to lock automatically after 15 minutes of inactivity in accordance with DoD requirements;
- consistently review system activity reports to identify unusual or suspicious activities and access for 15 of the 17 systems reviewed; or
- protect electronic records that contained PHI from unauthorized physical access at two of the five MTFs visited.

CAC Usage Was Not Consistently Enforced

Officials for the DHA, Navy, and Air Force did not consistently enforce CAC usage to access the three DoD EHR systems, one modified EHR system, and seven Service-specific systems. Although the PIAs for the three DoD EHR systems identified that the systems used CACs; officials for the DHA, Navy, and Air Force did not require CAC use. DoD Instruction 8520.03 requires DoD Components to require the use of CACs to access all DoD networks and systems to comply with two-factor authentication requirements.[12] Authentication is a process that verifies

Officials for the DHA, Navy, and Air Force did not consistently enforce CAC usage to access the three DoD EHR systems, one modified EHR system, and seven service-specific systems.

[12] DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011.

the identity of a user and is a prerequisite to allowing access to an information system. Two-factor authentication is based on using something in a user's possession such as a token, and entering something known only to the user, such as a personal identification number.[13]

Officials for the DHA, Navy, and Air Force considered single-factor authentication, such as a user name and password, more efficient to access PHI while providing bedside care; however, single-factor authentication is less stringent and presents a greater risk of compromise. The DHA and MTF CIOs did not enforce CAC usage on AHLTA because MTF officials stated that the CAC software was incompatible with the CHCS and Essentris. Additionally, the system administrators stated that users accessed AHLTA with a user name and password because the CHCS did not support using a CAC to access the system.[14]

In addition, BUMED did not require the Navy MTF CIOs to configure the TC2, a modified EHR, and Carestream aboard the USNS Mercy; the Audio Metric Database System at NMC San Diego; and McKesson Cardiology at NHCP to authenticate using CACs. Instead, the TC2, Carestream, the Audio Metric Database System, and McKesson Cardiology users accessed the systems using single-factor authentication. System administrators stated that they did not configure the Audio Metric Database System, Carestream, McKesson Cardiology, and the TC2 to authenticate using CACs because the CAC software was incompatible with the older systems.[15] Furthermore, AFMS and Air Force MTF CIOs did not require system administrators to configure Epiphany Electrocardiogram Management, Innovian, the Nuclear Medicine Information System, and PACS to authenticate using CACs because:

- neither the Nuclear Medicine Information System nor PACS supported the use of multifactor authentication;
- system administrators stated that using CACs to access Innovian during surgical procedures disrupted the flow of data to monitor vital signs and the distribution of anesthesia levels; and
- system administrators for Epiphany Electrocardiogram Management made addressing system operational issues a higher priority than configuring the system to use a CAC.

DoD Instruction 8520.03 allows the use of single-factor authentication if the DHA obtains a waiver. However, the DHA did not obtain waivers exempting the use of CACs for AHLTA, the CHCS, and Essentris users. On October 8, 2013,

[13] A token authenticates a user's identity.

[14] The CHCS provides the overall infrastructure for AHLTA. To access the CHCS, users must enter a user name and password. Because users could access AHLTA through the CHCS, the MTFs allowed users to also access AHLTA using a user name and password.

[15] During the audit, the USNS Mercy implemented the use of CACs in November 2017 to access Carestream.

the CHCS program manager requested an extension until September 2014 to comply with the MHS's requirement for using CACs. The DHA officials stated that developers continued to work on a solution to use CACs for the CHCS, but the system still did not support CAC usage and the DHA officials did not request and obtain a waiver exempting its use as of September 2017.

In DODIG-2017-085 report, we recommended that the DHA enforce the use of CACs for AHLTA, the CHCS, and Essentris. The DHA Director stated that the DHA would coordinate with the Service Surgeons General to enforce CAC usage for AHLTA and Essentris. Additionally, the DHA Director stated that the DHA was continuing to test solutions for using CACs to access the CHCS. We agreed with the DHA Director's planned actions and will close the recommendation once we verify that the DHA has implemented a CAC solution for the CHCS and that the Service Surgeons General are enforcing the use of CACs to access AHLTA and Essentris. Therefore, we did not make a similar recommendation to the DHA in this report. The CIOs for BUMED, AFMS, and the Navy and Air Force MTFs should either configure the use of CACs to access systems that process, store, and transmit PHI, or obtain a waiver that exempts the systems from using CACs.

System Passwords Did Not Meet Complexity Requirements

The DHA, Navy, and Air Force system administrators did not configure system passwords for Essentris, one modified EHR system, and six Service-specific systems to meet DoD complexity requirements when they were unable to use CACs to access those systems. The Defense Information Systems Agency Security Technical Implementation Guide on Application Security requires system passwords to be at least 15 characters in length.[16] When user names and passwords are used to access DoD systems, the DoD requires the following combination, at a minimum, as part of the 15-character password complexity requirement.

- one lowercase letter;
- one uppercase letter;
- one number; and
- one symbol.

~~(FOUO)~~ At NMC San Diego, system administrators configured [redacted] to require only an [redacted] password. Although the [redacted] system administrator changed the system configuration during the audit to meet the 15-character password length requirement, he stated that only the [redacted] vendor could configure the system to meet DoD complexity requirements. As the system owner for [redacted], the DHA is responsible for configuring the password to meet

[16] Application Security and Development Security Technical Implementation Guide, Release 4, April 28, 2017.

~~(FOUO)~~ DoD requirements. In the DODIG-2017-085 report, we recommended that the DHA configure passwords for [redacted] to meet DoD complexity requirements. The DHA Director stated that the DHA would coordinate with the Services and the MTFs to enforce password complexity policies. We agree with the DHA Director's planned actions and will close the recommendation when we obtain documentation, such as system configuration settings, that show the DHA configured [redacted] to meet DoD password complexity requirements. Therefore, we did not make a similar recommendation to the DHA in this report.

~~(FOUO)~~ In addition, the system administrators for the Audio Metric Database System at NMC San Diego did not configure the system to require a specific password length because system limitations restricted those actions. System administrators configured [redacted] at NHCP to require passwords that met [redacted] password complexity requirements, but they stated that only the vendor could configure the system to meet the 15-character password length requirement. A system administrator configured the [redacted] aboard the USNS Mercy to require only an [redacted] password that met [redacted] complexity requirements although the system was capable of using passwords up to 20 characters. The system administrator stated that he did not configure the [redacted] to meet DoD standards because he was not allowed to change password complexity requirements. However, the system administrator did not request the DHA to change the password complexity configuration settings for the [redacted]. The system administrator stated that he planned to implement CAC authentication for the [redacted], but could not provide a timeframe for implementing that solution.

~~(FOUO)~~ System administrators configured [redacted] at WPMC to require only a [redacted] password that met [redacted] complexity requirements, but they did not configure the [redacted] to require a specific password length or to meet specific complexity requirements. Additionally, system administrators configured [redacted] to require only a [redacted] password. The WPMC CIO stated that he made a management decision to decrease cybersecurity as a priority after a contractual lapse reduced staffing in the information technology department. As a result, the CIO did not require WPMC system administrators to configure the systems to meet DoD password complexity requirements. At the Dover Clinic, system administrators configured [redacted] to require only a [redacted] password with [redacted] complexity requirements because of technical

The WPMC CIO stated that he made a management decision to decrease cybersecurity as a priority after a contractual lapse reduced staffing.

(FOUO) limitations that affected the server hosting [redacted]. Documentation from the Dover Clinic identified that the server supported passwords with a minimum of [redacted] that could meet only [redacted] complexity requirements.

Computer hackers have at their disposal countless programs that are designed to exploit weak passwords and gain unauthorized access to information technology systems. The exploitative programs use common words and phrases and personal information associated with specific users, randomly generate potential words based on the dictionary, or use a combination of various methods and programs to repeatedly attempt to gain access to sensitive, password protected information. A longer, more complex password decreases the ability of hackers to conduct a successful cyber attack to obtain a system password. The CIOs for BUMED, AFMS, and the MTFs for the Navy and Air Force should ensure system administrators configure passwords for systems that process, store, and transmit PHI to meet DoD length and complexity requirements.

Network Vulnerabilities Were Not Consistently Mitigated

(FOUO) Network administrators at the five MTFs did not consistently mitigate known network vulnerabilities. In addition, the CIOs for the MTFs did not develop plans of action and milestones (POA&M) to mitigate vulnerabilities affecting their networks. Chairman of the Joint Chiefs of Staff Manual 6510.02 [redacted][17] Information assurance vulnerability alerts, which are issued by U.S. Cyber Command, are notifications generated when vulnerabilities may result in an immediate and potentially severe threat to DoD systems and information that require corrective actions based on the severity of the risk.

(FOUO) At the Dover Clinic, a June 21, 2017, scan revealed that 342 of the 1,430 vulnerabilities identified on a May 10, 2017, network scan remained unmitigated.[18] The 342 vulnerabilities consisted of 34 critical and 308 high vulnerabilities.[19] For example, a [redacted] vulnerability identified in May 2017 could allow attackers to [redacted]. The information assurance vulnerability alert required components to mitigate the vulnerability or develop a POA&M by June 1, 2017; however, the Dover Clinic had not mitigated the vulnerability by our review on June 21, 2017.

[17] Chairman of the Joint Chiefs of Staff Manual 6510.02, "Information Assurance Vulnerability Management (IAVM) Program," November 5, 2013.

[18] The scans we obtained identified all unmitigated vulnerabilities at a specific point in time, regardless of the date when the vulnerability was first identified, that could be used to exploit network security at the five MTFs.

[19] Critical vulnerabilities, if exploited, would likely result in privileged access to servers and information systems and, therefore, require immediate patches. High vulnerabilities, if exploited, could result in obtaining elevated privileges, significant data loss, or network downtime.

~~(FOUO)~~ Another unmitigated [redacted] vulnerability initially identified in September 2015 could allow attackers to [redacted].[20] Although the associated information assurance vulnerability alert required DoD Components to mitigate the vulnerability or develop a POA&M by October 1, 2015, the Dover Clinic still had neither mitigated the vulnerability nor developed a POA&M in June 2017. Dover Clinic officials stated that they did not have automated software programs to patch vulnerabilities; therefore, they installed patches to mitigate vulnerabilities manually. According to Dover Clinic network administrators, other Air Force commands had responsibility for scanning the MTF networks for vulnerabilities while the MTFs had responsibility for mitigating them. However, the network administrators stated that the Air Force did not provide the MTFs with tools to automate the process. Therefore, system administrators had to address the 342 unmitigated vulnerabilities manually, which indicates that the manual process was not effective to mitigate those vulnerabilities timely.

~~(FOUO)~~ At the NHCP, a May 7, 2017, scan revealed that 36,925 of the 36,926 vulnerabilities identified on an April 22, 2017, network scan remained unmitigated. The 36,925 vulnerabilities included 27 critical and 85 high vulnerabilities. For example, one of the unmitigated vulnerabilities identified in March 2017 could allow attackers to compromise [redacted]. Although the associated information assurance vulnerability alert required DoD Components to mitigate the vulnerability or include it in a POA&M by April 6, 2017, the NHCP had neither mitigated the vulnerability nor included it in a POA&M. Another unmitigated [redacted] vulnerability initially identified in April 2015 could allow an attacker to [redacted]. The NHCP was required to mitigate this vulnerability or develop a POA&M by May 7, 2015. The NHCP still has not mitigated vulnerabilities more than 2-years old after notification. The Information Systems Security Manager, who was new to the position, stated he was evaluating how to address the vulnerabilities previously unmitigated by his predecessor.

~~(FOUO)~~ At the NMC San Diego, a May 5, 2017, scan revealed that 372 of the 470 vulnerabilities identified on a March 2017 network scan remained unmitigated. The 372 vulnerabilities included 157 Category I vulnerabilities and 182 Category II vulnerabilities.[21] A vulnerability identified in March 2017 could [redacted]. DoD Components were required to mitigate the vulnerability or develop a POA&M by April 13, 2017; however,

[20] Denial of service results in preventing authorized access to resources or delaying time-critical operations from occurring.

[21] Category I vulnerabilities, if exploited, would directly and immediately result in loss of confidentiality, availability, or integrity of data. Category II vulnerabilities, if exploited, could potentially result in the loss of confidentiality, availability, or integrity of data.

(FOUO) NMC San Diego did not mitigate the vulnerability. Additionally, an unmitigated vulnerability identified in March 2016 could allow an attacker to [redacted]. The associated information assurance vulnerability alert, which did not specify a mitigation date, required DoD Components to mitigate the vulnerability or include it in a POA&M. The NMC San Diego CIO accepted the risk of not mitigating the vulnerability; however, the DHA neither agreed to nor approved the acceptance of risk.[22]

(FOUO) Aboard the USNS Mercy, a September 13, 2017, scan revealed that 212 of the 223 vulnerabilities identified on an August 14, 2017, network scan remained unmitigated. The 212 vulnerabilities included two critical and three high vulnerabilities. For example, one of the unmitigated [redacted] vulnerabilities identified in March 2017 could allow an attacker to [redacted]. The associated information assurance vulnerability alert required DoD Components to mitigate the vulnerability or include it in a POA&M by April 6, 2017. Network administrators aboard the USNS Mercy stated that they focused on mitigating only critical or high vulnerabilities because those vulnerabilities directly affected their ability to maintain network authorization. Therefore, the network administrators focused on those types of vulnerabilities first.

(FOUO) At the WPMC, a July 7, 2017, scan revealed that 2,389 of the 2,629 vulnerabilities identified on a June 6, 2017, network scan remained unmitigated. The 2,389 vulnerabilities included 174 critical vulnerabilities and 1,049 high vulnerabilities. WPMC identified a [redacted] vulnerability in June 2017 that [redacted]. DoD Components were required to mitigate the vulnerability or develop a POA&M by July 6, 2017; however, this vulnerability was neither mitigated nor included in a POA&M. Additionally, an unmitigated vulnerability identified in September 2014 could allow an attacker to [redacted]. Although the associated information assurance vulnerability alert required DoD Components to mitigate the vulnerability or include it in a POA&M by October 16, 2014, WPMC had neither mitigated the vulnerability nor included it in a POA&M. The CIO made network security a lower priority after the WPMC information technology contract lapsed in November 2016 and, therefore, did not prioritize resources and actions to mitigate known vulnerabilities. However, the CIO did not have an explanation for not mitigating the vulnerabilities that existed before the contract lapsed.

[22] DHA must agree to and approve an MTF CIO's decision to accept risk when the MTF operates on a DHA Medical Community of Interest network. NMC San Diego was in the process of transitioning to the DHA's network and, therefore, required DHA approval.

Although the five MTFs had vulnerability management programs that identified and mitigated some vulnerabilities, the MTF CIOs did not meet the program's expectations to manage risk when they allowed vulnerabilities to remain unmitigated on their networks and systems, many of which existed for more than three years. Without a rigorous and systematic process to patch vulnerabilities in a timely manner, the MTF CIOs increased their risk that cyber attacks or other malicious actions could exploit the vulnerabilities. As a result, PHI could be compromised through cyber attacks that are designed to exploit those weaknesses. The MTF CIOs should develop POA&Ms and take appropriate and timely steps to mitigate known network vulnerabilities. In addition, the commanders for NHCP, NMC San Diego, Dover Clinic, WPMC, and USNS Mercy should review the performance of their CIOs. Furthermore, the commanders should consider administrative action, as appropriate, against their CIOs for not following Federal and DoD guidance for protecting PHI to include not mitigating known vulnerabilities in a timely manner; not developing POA&Ms for unmitigated vulnerabilities; and not formally accepting risks for unmitigated vulnerabilities.

Although the five MTFs had vulnerability management programs that identified and mitigated some vulnerabilities, the MTF CIOs did not meet the program's expectations to manage risk.

Data Was Not Consistently Protected

~~(FOUO)~~ MTF officials did not consistently [redacted] for four Service-specific systems that contained PHI. DoD Instruction 8580.02 requires the use of [redacted] to protect PHI.[23] System administrators for [redacted] aboard the USNS Mercy; [redacted] at NHCP; and [redacted] at WPMC stated that they did not [redacted] on the servers because the servers did not support [redacted].[24] In addition, system administrators for [redacted] stated they did not [redacted] at WPMC because they relied on network boundary defenses such as firewalls and anti-virus software to protect the data. Without [redacted], the MTFs increased the risk that PHI is compromised if existing security controls, which they relied on to protect the information, were breached.

[23] DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Healthcare Programs," August 12, 2015.

[24] [redacted] systems, including printers, fax machines, or scanners.

~~(FOUO)~~ Furthermore, system administrators for [redacted] did not [redacted] at WPMC because they believed PHI [redacted] did not require [redacted]. Likewise, system administrators for [redacted] did not [redacted] at NHCP because the vendor configured the system to use an [redacted]. During the audit, system administrators for [redacted] began using a [redacted] in August 2017 to [redacted] PHI [redacted]. The CIOs for NHCP, USNS Mercy, and WPMC should upgrade the servers and [redacted] PHI data stored on or transmitted across the Navy and Air Force networks.

User Roles and Privileges Did Not Always Align With User Responsibilities

Navy and Air Force system administrators did not consistently grant user access, based on defined roles that aligned with user responsibilities, to the three DoD EHR systems, two modified EHR systems, two DHA-owned systems, and eight Service-specific systems. The CIOs and system administrators at the MTFs stated that they used access request forms to document the need for system access. However, system administrators did not consistently require written justification as a condition to obtain and elevate system access privileges. National Institute of Standards and Technology Special Publication 800-53 and DoD Instruction 8530.01 requires system access to be granted based on the principle of least privilege.[25] Least privilege is a security objective requiring users to have only the access needed to perform their official duties. We selected a statistical sample of users from the three DoD EHR systems, three modified EHR systems, two DHA-owned systems, and nine Service-specific systems to validate whether user roles and privileges aligned with their responsibilities. Appendix B lists the systems and types of access-related issues we identified for the 17 systems at the five MTFs.

System administrators did not consistently require written justification as a condition to obtain and elevate system access privileges.

At the Dover Clinic, we tested user access to AHLTA, the CHCS, HAIMS, and PACS. We did not identify problems in how the system administrator managed access to AHLTA; however, we identified 90 instances where system administrators did not effectively manage user access to the CHCS, HAIMS, and PACS. For example, system administrators for the CHCS, HAIMS, and PACS did not provide access request

[25] National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013; and DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016.

forms for 40 users. In addition, although the system administrators provided access request forms for 19 users, 18 of the forms did not include a reason why the users needed access to the systems, and one form for a CHCS user did not match the user's role designated in the system. Therefore, we could not determine whether access was granted based on assigned duties. System administrators provided various reasons why they did not provide the forms, such as the age of the accounts. The 59 users should not have continued access to the systems without completed and approved access request forms that identify specific access privileges that align with the user's responsibilities. System administrators for the CHCS did not align system access according to responsibilities for one user. The CHCS system administrators also granted elevated privileges for eight users without receiving written justification and five users remained active in the system although the users had not accessed the system in more than 35 days. The Defense Information Systems Agency Security Technical Implementation Guide on Application Security requires accounts to be disabled after 35 days of inactivity.

Furthermore, 17 PACS users at the Dover Clinic shared access to a system administrator account, which allowed the 17 users the ability to create, modify, and disable user accounts. DoD Instruction 8580.02 requires system access based on individual and unique accounts to identify and monitor user activity. The 17 users also had the ability to modify user passwords in addition to scanning images to a compact disc. System administrator privileges provide users with the ability to create, modify, and disable user accounts, in addition to the ability to perform functions that could, whether intentional or not, change system security or system functionality. The system administrator stated that PACS only allowed system administrators to scan and store the images to external storage devices. To reduce potential impacts to patient care, the system administrator stated that he provided the 17 users with system administrator privileges in PACS although the users did not need that level of access.

At the NHCP, we tested user access to AHLTA, the CHCS, Essentris, McKesson Cardiology, the Parata System Suite, and PeerVue. We identified 219 instances where system administrators did not effectively manage user access to those systems. Specifically, system administrators for the CHCS, Essentris, McKesson Cardiology, and the Parata System Suite did not provide access request forms for 151 users and they could not verify whether access was granted based on assigned duties. The 151 users should not have continued access to the systems without completed and approved access request forms that identify specific access privileges that align with the user's responsibilities. System administrators for the CHCS did not align system access according to responsibilities for one user. Additionally, system administrators for AHLTA, the CHCS, and PeerVue also did

not deactivate eight users from the systems in a timely manner. For example, two CHCS users last accessed the system in March 2016; however, as of May 2017, system administrators had not deactivated their accounts. The system administrators did not have an explanation why they had not taken the required actions. Automatically disabling system and user accounts within required timeframes limits the potential for unauthorized access and malicious actions that could jeopardize patient health care. Lastly, system administrators for AHLTA, the CHCS, Essentris, and Parata System Suite granted elevated privileges for 59 users without receiving written justification.

At NMC San Diego, we tested user access to AHLTA, the Audio Metric Database System, the BMBB/TS, the CHCS, Essentris, and HAIMS. We identified 120 instances where system administrators did not effectively manage user access to AHLTA, the Audio Metric Database System, the BMBB/TS, the CHCS, Essentris, and HAIMS. For example, system administrators for AHLTA, the Audio Metric Database System, the BMBB/TS, the CHCS, Essentris, and HAIMS did not provide access request forms for 46 users and could not verify whether access was granted based on assigned duties. In addition, although the system administrators provided access request forms for seven users, two forms did not include a reason why the users needed access to the systems, and five forms for Essentris users did not match their role in the system. Therefore, the 53 users should not have continued access to the systems without completed and approved access request forms that identify specific access privileges that align with the user's responsibilities. In addition, we identified 18 instances where system administrators for the CHCS and the Audio Metric Database System granted users additional access outside of their assigned duties. Furthermore, system administrators for AHLTA, the Audio Metric Database System, the CHCS, and Essentris granted elevated privileges for 48 users without receiving written justification. Lastly, system administrators allowed one Audio Metric Database System user to retain access to the system, although the user's access to the system should have expired in July 2016 based on the access request form. Granting access based on least privilege decreases the risk of users performing actions that could compromise the privacy or integrity of PHI data or the systems and network on which the data resides.

Aboard the USNS Mercy, we tested user access to AHLTA-T, the Maritime Medical Module, and the TC2. We did not identify problems in how the system administrators managed access to AHLTA-T. However, we identified seven instances where system administrators did not effectively manage user access to the Maritime Medical Module and the TC2. Specifically, system administrators for the Maritime Medical Module did not provide access request forms for six users and did not develop a formal process for aligning system access with user responsibilities. Instead, they relied on their collective knowledge of user

responsibilities to assign roles in the system. In addition, the system administrator for the TC2 granted elevated privileges for one user without receiving written justification. Although Carestream was included in the audit scope, we did not test access management because the system administrator was the only user with access to the system.

At the WPMC, we tested user access to AHLTA, the CHCS, Epiphany Electrocardiogram Management, Essentris, Innovian, and the Nuclear Medicine Information System. We did not identify problems in how the system administrator managed access to the Nuclear Medicine Information System. However, we identified 136 instances where system administrators did not effectively manage user access to AHLTA, the CHCS, Epiphany Electrocardiogram Management, Essentris, and Innovian. Specifically, system administrators for AHLTA, the CHCS, Essentris, Epiphany Electrocardiogram Management, and Innovian did not provide access request forms or provided incomplete forms for 61 users and could not show whether access was granted based on assigned duties. In addition, although the system administrators provided access request forms for 20 users, the forms did not include a reason why the users needed access to the systems. Therefore, the 81 users should not have continued access to the systems without completed and approved access request forms that identify specific access privileges that align with the user's responsibilities. System administrators for the CHCS, Essentris, and Innovian also did not timely deactivate 20 users from their systems. For example, one Innovian user last accessed the system on March 10, 2017, but as of August 28, 2017, the account was still active. Furthermore, AHLTA, the CHCS, Essentris, and Epiphany Electrocardiogram Management system administrators granted elevated privileges for 28 users without written justification. Lastly, system administrators for the CHCS and Essentris granted seven users access that did not align with their assigned responsibilities.

Account management problems existed at the five MTFs because system administrators did not consistently develop and implement SOPs to grant, elevate, and deactivate user access to the three DoD EHR systems, three modified EHR systems, one DHA-owned system, and nine Service-specific systems.[26] DoD Instruction 8580.02 requires DoD entities to implement policies and procedures for granting and modifying access to PHI. System administrators stated that they considered documented procedures unnecessary; and instead they relied on verbal discussions to manage system access. SOPs are written, detailed instructions that document a repetitive activity to uniformly perform specific functions and serve as a vital tool to transfer knowledge. Table 1 lists, by location, the systems without SOPs for managing user access.

[26] System administrators at NHCP developed procedures to manage access to McKesson Cardiology.

Table 1. Systems Without Written Procedures for Managing System Access

System Name	Systems Without Procedures for Granting Access (By MTF)					Systems Without Procedures for Deactivating Access (By MTF)				
	Dover Clinic	NHCP	NMC San Deigo	USNS Mercy	WPMC	Dover Clinic	NHCP	NMC San Diego	USNS Mercy	WPMC
AHLTA	X	X	X		X	X	X	X		X
AHLTA-T									X	
Audio Metric Database System			X					X		
Carestream				X					X	
CHCS	X	X			X		X	X		X
Epiphany Electrocardiogram Management					X					X
Essentris		X	X		X		X	X		
HAIMS	X									
Innovian					X					
Maritime Medical Module				X					X	
McKesson Cardiology		X					X			
Nuclear Medicine Information System					X					X
PACS	X					X				
Parata System Suite		X					X			
PeerVue		X					X			
TC2				X					X	

Source: The DoD OIG.

An effective account management process includes procedures for granting, elevating, and deactivating user access to increase the likelihood that only authorized users can obtain access to Navy and Air Force networks and systems. Limiting access to PHI based on roles that aligns with a user's assigned duties reduces the risk of intentional and unintentional disclosure of sensitive information. The MTF CIOs should require written justification for obtaining access to all systems that process, store, and transmit PHI. In addition, the MTF CIOs should develop and maintain access request forms for all users of

systems that process, store, and transmit PHI, and verify, at least annually, the continued need for system access. Furthermore, the MTF CIOs should develop and maintain SOPs that address processes for granting access, assigning and elevating privileges, and deactivating user access.

Systems Were Not Configured to Lock Automatically After Extended Periods of Inactivity

System administrators at the five MTFs did not configure the three DoD EHR systems, three modified EHR systems, and six Service-specific systems that contained PHI to lock automatically after 15 minutes of inactivity. The Defense Information System Agency Security Technical Implementation Guide for Application Security and Development requires systems to lock automatically for nonprivileged users after no more than 15 minutes of inactivity. A nonprivileged user is not authorized to perform security-related functions. Table 2 identifies systems that took longer than 15 minutes to lock automatically and those that were not configured to lock automatically.

Table 2. Automatic Lockout Settings for Inactivity in Minutes

System Name	MTF				
	Dover Clinic	NHCP	NMC San Diego	USNS Mercy	WPMC
AHLTA	30	30	30		30
AHLTA-T				30	
Audio Metric Database System			NC*		
Carestream				NC+	
CHCS	15	1,666	166		20
Essentris		NC	NC		15
Innovian					NC
Maritime Medical Module				20	
McKesson Cardiology		NC			
Nuclear Medicine Information System					NC
PACS	20				
TC2				1,666	

Note: Gray cells indicate the system was not used at the MTF.
*NC (not configured) indicates the system was not configured to lock automatically.
+Carestream system administrator configured the system to lock after 10 minutes of inactivity after the site visit.
Source: The DoD OIG.

The system administrators did not configure the following systems to lock automatically after 15 minutes of inactivity because they relied on network configuration settings to meet the requirement:

- the Audio Metric Database System at NMC San Diego;
- the McKesson Cardiology and PeerVue at NHCP; and
- the Innovian and the Nuclear Medicine Information System at WPMC.

At the three MTFs, system administrators stated that the network locked automatically after 15 minutes of inactivity. Although the networks locked after 15 minutes of inactivity, the Defense Information System Agency Security Technical Implementation Guide for Application Security and Development requires **networks and systems** [emphasis added] to lock automatically after 15 minutes of inactivity. At NHCP, NMC San Diego, Dover Clinic, and WPMC, the DHA configured AHLTA to lock automatically after 30 minutes of inactivity; and aboard the USNS Mercy, the DHA configured AHLTA-T to lock automatically after 30 minutes of inactivity. At the five MTFs, system administrators could not configure AHLTA and AHLTA-T to lock after 15 minutes of inactivity because only DHA system administrators had the ability to make configuration changes as the systems' owner. However, none of the MTF system administrators requested the DHA to change the configuration settings to meet DoD requirements.

The CHCS system administrators at NHCP and NMC San Diego purposely did not configure the systems to lock automatically after 15 minutes of inactivity to allow additional time for users to perform assigned duties. Essentris system administrators at NHCP and NMC San Diego stated that they did not configure 28 and 256 terminals, respectively, to lock automatically because they believed the medical and dental operating rooms and non-clinical administrative areas where the terminals were located were exempt from this requirement based on BUMED guidance. BUMED guidance exempts systems used in operating and treatment rooms from the 15-minute requirement; and allows instead 4 hours of inactivity before automatically locking.[27] Although BUMED guidance extended the period of inactivity before systems locked automatically for specific mission requirements, it did not eliminate the requirement. Without providing justification for their actions, the PACS system administrators at the Dover Clinic and the TC2 system administrators aboard the USNS Mercy overrode system default settings that would have locked users after 15 minutes of inactivity. The administrators stated that they instead relied on the network configurations automatically locking out users after 15 minutes of inactivity. Although the

[27] BUMED Memorandum, "Exception to Policy, Request to Exceed Standard 15-Minute System Timeout Setting," November 15, 2011.

network lockout mitigated some risk, unless the network and systems are configured to lock simultaneously, the PHI will be exposed if users log into the network and leave the workstation unattended. Automatically locking systems and user accounts within DoD required timeframes limits the potential for unauthorized access to PHI and prevents malicious actions, such as patient records manipulation, which could jeopardize patient care. The Director, DHA, and the MTF CIOs should configure all systems used to process, store, and transmit PHI to lock automatically after 15 minutes of inactivity.

System Activity Was Not Consistently Reviewed

System administrators did not consistently review activity reports to assess user activity, failed login attempts, and possible data exfiltration attempts for:

- three DoD EHR systems,
- three modified EHR systems, and
- nine Service-specific systems.

DoD Instruction 8580.02 requires DoD Components to perform regular system activity reviews to protect PHI; however, the MTF CIOs only reviewed the reports for the following systems if a security incident occurred:

- AHLTA,
- AHLTA-T,
- Carestream,
- CHCS,
- Epiphany Electrocardiogram Management,
- Essentris,
- Innovian,
- Maritime Medical Module,
- McKesson Cardiology,
- Nuclear Medicine Information System,
- PACS,
- Parata System Suite,
- PeerVue, and
- TC2.

System administrators at the Dover Clinic reviewed HAIMS activity reports to monitor successful login attempts and user activity, but their reviews did not include failed log-in attempts because the HAIMS vendor did not configure the system to record that information. In addition, system administrators for HAIMS

at NMC San Diego did not review system activity because they did not configure the system to generate system activity reports. National Institute of Standards and Technology Special Publication 800-66 requires audit logs to include descriptions of user activity, and all login and data exfiltration attempts.[28] When properly configured, audit logs provide automated and chronological records of system activity. Regularly reviewing the logs can identify unauthorized access attempts and provide forensic evidence to aid in investigating and identifying malicious behavior. If system activity is not reviewed on a regular basis, PHI could be compromised without detection. The MTF CIOs should appropriately configure and regularly review system activity reports to identify user and system activity anomalies.

Physical Access to PHI Was Not Consistently Controlled

Navy and Air Force officials did not consistently implement physical access controls to limit unauthorized access to, or disclosure of, PHI. Specifically, Air Force officials at the Dover Clinic used a fax machine to transmit PHI in an unsecured area of the optometry department. Air Force officials at the Dover Clinic did not secure a fax machine in the optometry department because contractual requirements delayed their ability to install a permanent glass partition to separate the waiting area and general office space. DoD Instruction 8580.02 requires authorized users of health information to protect terminals, workstations, and other devices containing or processing PHI from unauthorized access. Unsecured and unattended PHI enables visitors, patients, and unauthorized staff to review or remove sensitive PHI, which could compromise a patient's privacy. During the audit, Dover Clinic officials relocated the fax machine behind locked doors in the optometry department to limit the risk of unauthorized access to PHI.

Officials aboard the USNS Mercy controlled access to the PHI records room by posting a guard at the office that stores paper medical records; however, they did not use physical access logs to record the identity of personnel accessing the records. Physical access logs document both physical access to the room and the removal of a patient's medical record from the room. National Institute of Standards and Technology Special Publication 800-53 requires agencies to maintain physical access logs to record the identity and time a person enters a facility. Likewise, HIPAA security rules require organizations to identify and maintain a

[28] System activity reports are generated from audit logs that record system activity, such as system access and user activities, in a given period.
National Institute of Standards and Technology Special Publication 800-66, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule," October 2008.

record of when health information is accessed. HIPAA security rules are intended to protect a patient's medical record from unauthorized disclosure and access. Although officials aboard the USNS Mercy controlled access to the health records office and required personnel to enter a combination to the door, personnel were not required to sign a log when they accessed individual paper medical records.[29]

In addition to documenting access, physical access logs also serve as a starting point for investigating security incidents that involve compromised medical records. Without physical access logs, it would be difficult to identify persons of interest tied to a potential security incident. The Commander, USNS Mercy should implement physical access controls to identify and record the names of personnel who access a patient's paper medical records, and the times those records were accessed; and should regularly, at least monthly, reconcile the logs against the list of authorized personnel with access to the area.

BUMED, AFMS, and MTFs Could Not Account for Systems Containing PHI

The CIOs for BUMED, AFMS, and the five MTFs were not aware of all Service-specific systems used at Navy and Air Force MTFs that processed, stored, or transmitted PHI. National Institute of Standards and Technology Special Publication 800-66 requires organizations to identify and account for all information systems that contain PHI. Instead of maintaining a system inventory, the MTF CIOs relied on the collective knowledge of system and network administrators to account for systems containing PHI.

Instead of maintaining a system inventory, the MTF CIOs relied on the collective knowledge of system and network administrators to account for systems containing PHI.

The DHA is replacing AHLTA, the CHCS, and Essentris with the MHS GENESIS. After several delays, the MHS GENESIS was fielded at Fairchild Air Force Base, Spokane, Washington, in February 2017; Naval Hospital Oak Harbor, Washington, in July 2017; and Naval Hospital Bremerton, Washington, in September 2017. The Navy and Air Force were unaware of the specific systems used at the MTFs, which could present challenges for the MHS GENESIS team when it implements interface controls between Service-specific systems and the new

[29] An authorized holder of official information determines if an individual requires access to specific information to perform official duties.

EHR system. A complete inventory of systems containing PHI is needed to avoid further delaying the DoD's transition to the MHS GENESIS, incurring additional costs to develop system interfaces, and implementing security protocols needed to protect the sensitive information. Accountability of all systems used to process, store, and transmit PHI is critical to the Navy and Air Force's ability to secure the systems and minimize security breaches and other incidents that could potentially compromise sensitive health-related data. The CIOs for BUMED, AFMS, and the MTFs should identify all systems used to process, store, and transmit PHI; should develop a baseline of systems used at each MTF; and should regularly, at least annually, validate the accuracy of the inventory of systems.

PIAs Were Not Updated or Did Not Exist

The CIOs for the DHA, BUMED, and AFMS did not maintain PIAs for nine systems: two DoD EHR systems, one modified EHR system, two DHA-owned systems, and four Service-specific systems. DoD Instruction 5400.16 requires a PIA, which documents privacy risks affecting all systems that collect, maintain, and disseminate personally identifiable information.[30] The Instruction also requires system owners to review and update the assessments every 3 years. Table 3 lists the system, the date of the PIA, and the date when the assessment expired.

Table 3. Systems With Expired PIAs

System	PIA Approval Date	PIA Expiration Date
AHLTA	October 10, 2013	October 10, 2016
Audio Metric Database System	NS*	NS
BMBB/TS	September 10, 2014	September 10, 2017
CHCS	August 7, 2013	August 7, 2016
HAIMS	September 9, 2013	September 9, 2016
Innovian	May 2, 2013	May 2, 2016
PACS	September 10, 2014	September 10, 2017
Parata System Suite	August 20, 2014	August 20, 2017

*NS (not signed) indicates the approving CIO did not sign the system's PIA.
Note: Data current as of October 2017.
Source: The DoD OIG.

[30] DoD Instruction 5400.16, "DoD Privacy Impact Assessment Guidance," July 14, 2015.

The DHA CIO stated that the DHA did not review and approve all PIAs in a timely manner because its workload increased since the DHA began transitioning to the DoD's enterprise-wide process for managing cybersecurity risk.[31] In DODIG-2017-085 report, we recommended that the DHA implement procedures to verify that PIAs are developed for all systems that process, store, and transmit PHI. The DHA Director stated that the DHA had procedures for developing PIAs. However, the DHA Director's planned actions were insufficient to verify that PIAs were maintained to meet DoD requirements. We will close the recommendation once the DHA provides written procedures that include a process to verify that PIAs are completed and regularly maintained for all systems that contain PHI. Because the previous recommendation is still open, we did not make a similar recommendation to the DHA in this report.

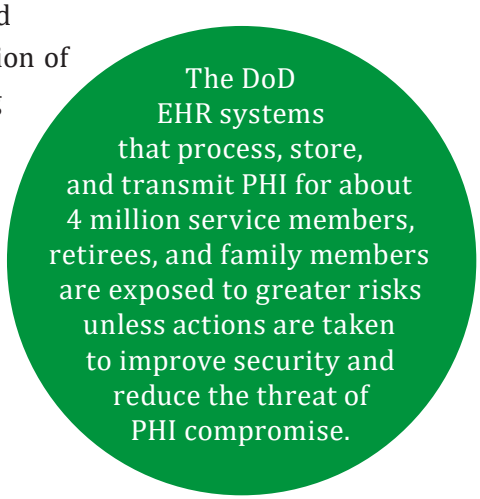
The Deputy CIO for BUMED stated a program management office for each system is responsible for completing and updating PIAs, but also acknowledged that BUMED did not verify the PIAs were completed or updated timely. The BUMED CIO stated that he did not develop a PIA for PeerVue and the Nuclear Medicine Information System because he thought the systems were included in the PIA for PACS. However, the PIA for PACS did not include either PeerVue or the Nuclear Medicine Information System. The AFMS HIPAA Privacy Office manager stated that AFMS began to transition oversight responsibilities for completing and updating PIAs to the DHA in October 2016 and expected to complete the transition in 2020. According to the DHA PIA team leader, the DHA provided minimal oversight of Air Force PIAs. Maintaining a current PIA improves a system owner's ability to protect sensitive information and document protocols and processes needed to mitigate potential privacy risks. The BUMED and AFMS CIOs should develop and implement procedures to validate that PIAs are completed and regularly updated for all systems that process, store, and transmit PHI.

Increased Risk of Unauthorized Disclosures of PHI

~~(FOUO)~~ The DHA, BUMED, AFMS, and Navy and Air Force MTFs did not protect DoD and Service-specific systems and databases that process, store, and transmit PHI from unauthorized access. Under HIPAA, the DHA, BUMED, AFMS, and Navy and Air Force MTFs are required to implement security protocols to protect the confidentiality, integrity, and availability of PHI. Security protocols such as using two-factor authentication, complex passwords, and [redacted] decreases

[31] DoD Instruction 8510.01 requires DoD Components to transition information systems that collect, maintain, and disseminate personally identifiable information to the integrated DoD-wide decision-making process by April 2018.

~~(FOUO)~~ the risk of unauthorized access to, and disclosure of, PHI. In addition, timely mitigation of known vulnerabilities and regular monitoring of system activity decreases the risk that cyber attackers could exploit known system and network weaknesses. Furthermore, limiting PHI access to users with a mission need reduces the risk of both intentional and unintentional disclosures of sensitive information. However, the DHA, BUMED, AFMS, and Navy and Air Force MTFs did not consistently implement security protocols or, when implemented, they were ineffective in consistently protecting PHI against compromise. As such, the DoD EHR systems that process, store, and transmit PHI for about 4 million service members, retirees, and family members are exposed to greater risks unless actions are taken to improve security and reduce the threat of PHI compromise.



Since January 25, 2016, health care providers, health plans, and health care business associates reported 405 data breaches to the Secretary of the Department of Health and Human Services.[32] The breaches, which affected more than 17 million individuals, resulted from hacking incidents, data loss, theft, improper disposal of data, and unauthorized access.[33] Of the 405 data breaches, 24 were the result of compromised EHR systems at health care provider facilities.[34] Security protocols, when not applied or ineffective, increase the risk of cyberattacks, system and data breaches, data loss or manipulation, and unauthorized disclosures of PHI, which could affect system availability, data integrity, and the confidentiality of PHI. Additionally, ineffective administrative, technical, and physical security protocols that result in a HIPAA violation could cost the MTFs up to $1.5 million per year in penalties for each category of violation.

Furthermore, the lack of a comprehensive and accurate inventory of all Service-specific systems that process, store, and transmit PHI presents the MHS with unnecessary challenges that could further delay the DoD's transition to the MHS GENESIS or increase implementation costs. A complete accounting of all Service-specific systems is needed to design and implement appropriate and secure system interfaces between the MHS GENESIS and Service-specific systems to avoid costly security and architecture changes once the system is fielded. A complete

[32] A health care business associate is an organization that helps covered entities carry out its health care activities and functions.

[33] Breaches that affect 500 individuals or more must be reported to the Secretary of the Department of Health and Human Services.

[34] Other locations of breached information included network servers, e-mails, laptops, portable electronic devices, desktop computers, and paper.

and accurate inventory of Service-specific systems is also essential to the Navy and Air Force's ability to secure the systems and minimize security breaches and other incidents that could potentially compromise PHI. We believe the systemic weaknesses we found across the five MTFs may indicate that similar weaknesses exist at other Navy and Air Force MTFs.

The Surgeons General for the Departments of the Navy and Air Force, in coordination with BUMED and AFMS, should assess whether the systemic issues identified in this report exist at other Service-specific MTFs, and should develop and implement an oversight plan to verify that MTFs used CACs and passwords that met DoD complexity requirements to access systems; completed and updated PIAs; and developed a baseline and regularly validated the inventory of systems used to process, store, and transmit PHI at the Service-specific MTFs.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Chief Information Officers for Naval Hospital Camp Pendleton, Naval Medical Center San Diego, U.S. Naval Ship Mercy, the 436th Medical Group, and Wright-Patterson Medical Center:

a. Implement appropriate configuration changes to enforce the use of a Common Access Card to access all systems that process, store, and transmit patient health information, or obtain a waiver that exempts the systems from using Common Access Cards.

Navy Comments

The Deputy Assistant Secretary of the Navy (Military Manpower and Personnel) endorsed all comments from the Executive Director, BUMED, who responded for the NHCP and NMC San Diego CIOs. The Executive Director agreed, stating that the NHCP requires a CAC to access all of the systems on its network.[35] The Executive Director stated that the NHCP only approves the use of usernames and passwords on a case-by-case basis, but for no more than 24 hours. For NMC San Diego, he stated that the MTF uses CACs to access systems that support CAC usage and single factor authentication to access systems that do not. The Executive Director also stated that the DHA was developing an enterprise-wide POA&M for the CHCS to ensure CAC use, which he expects to be completed in spring 2018.

[35] The BUMED Executive Director specifically responded for the Assistant Chief of Staff, Naval Medicine West (NHCP and NMC San Diego), Assistant Deputy Chief for Information Management and Technology, BUMED, and the Privacy Program Office, BUMED.

Our Response

Comments from the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation for the NHCP once they provide details explaining the basis for allowing a 24-hour use of usernames and passwords. We will close the recommendation for NMC San Diego once they provide details of waivers for systems that do not support the use of CACs.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, partially agreed, stating that the CIO did not have administrative privileges to modify access to systems. The Chief of Staff stated that the USNS Mercy had a memorandum with NMC San Diego to obtain information technology support for all medical applications. However, the Chief of Staff provided an alternative course of action, stating that the USNS Mercy CIO would work with BUMED to configure systems, including the CHCS and Carestream, to use a CAC by April 15, 2018. In addition, the Chief of Staff stated that the USNS Mercy CIO would submit a request for configuration changes to enable CAC usage for systems in which the Space and Naval Warfare Systems Center Atlantic is the program manager, to include AHLTA-T, the Maritime Medical Modules, and TC2.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation (such as updated system configuration settings) that show BUMED and the Space and Naval Warfare Systems Center Atlantic enabled their systems to use CACs and that the USNS Mercy enforced the use of CACs.

b. Configure passwords for all systems that process, store, and transmit patient health information to meet DoD length and complexity requirements.

Navy Comments

~~(FOUO)~~ The Executive Director, BUMED, responding for the NHCP and NMC San Diego CIOs, agreed, but stated that [redacted] did not allow the Navy to meet DoD password requirements. He stated that the Naval Medical Logistics Command was procuring an updated version of [redacted] that will require a CAC to access the system. The Executive Director stated that the updated version should be delivered in fall 2018. For NMC San Diego, the Executive Director stated that the MTF configured [redacted] to meet password complexity requirements. However, he also stated that the Navy was working with vendors to meet the password requirements for other systems that did not meet DoD requirements.

Our Response

~~(FOUO)~~ Comments from the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once the NHCP provides documentation showing it fielded the updated version of [redacted], and NMC San Diego provides documentation showing that [redacted] and the other systems have been configured to meet DoD password requirements.

Military Sealift Command Comments

~~(FOUO)~~ The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that the CIO would configure [redacted], and [redacted] to use 15-character passwords until the systems are configured to require a CAC for access or the DHA obtains an exemption waiver. He stated that the passwords would include uppercase and lowercase letters, symbols, and numbers.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation (such as system configuration settings) that show the USNS Mercy configured systems to meet DoD password length requirements.

c. Develop a plan of action and milestones and take appropriate steps to mitigate known network vulnerabilities in a timely manner.

Navy Comments

The Executive Director, BUMED, responding for the NHCP and NMC San Diego CIOs, agreed, stating that NHCP developed POA&Ms supporting its network authority to operate and that the Information Systems Security Manager monitors the POA&Ms daily. The Executive Director also stated that a Mitigation and Remediation Support team assisted the MTF's efforts to mitigate vulnerabilities between May and June 2017 and that a Continuous Risk Management team inspected the NHCP in July 2017. The Executive Director stated that NMC San Diego developed POA&Ms when it transitioned to the Risk Management Framework.

Our Response

Comments from the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain vulnerability scan results that show that the NHCP and NMC San Diego mitigated known vulnerabilities and approved POA&Ms for vulnerabilities that the MTFs could not mitigate in a timely manner.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that the USNS Mercy and the Military Sealift Command developed a POA&M to obtain an authority to operate on the Non-secure Internet Protocol Router Network.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain the POA&M that allowed the USNS Mercy to obtain an authority to operate on the Non-secure Internet Protocol Router Network and vulnerability scan results and the most recent POA&M that show that the USNS Mercy mitigated known vulnerabilities.

d. Require written justification for obtaining access to all systems that process, store, and transmit patient health information and implement procedures to grant access to the systems based on roles that align with user responsibilities.

Navy Comments

The Executive Director, BUMED, responding for the NHCP and NMC San Diego CIOs, agreed, stating that the NHCP developed and used procedures to manage user access, including an access request form that the MTF modified during the DoD OIG visit. The Executive Director stated that the form required departmental and supervisory approval of specific user roles requested by the user. For systems not managed by the NHCP Information Management Department, the Executive Director stated that the MTF would work with other organizations to ensure those systems were included on the access request forms. He also stated that the NHCP implemented an annual process to verify the need for continued access. For NMC San Diego, the Executive Director stated that the MTF assigned user access to AHLTA, the CHCS, and Essentris based on the user's position. However, he stated that a formal process did not exist to assign user roles to clinical staff; therefore, NMC San Diego would work with BUMED to formalize a policy.

Our Response

Comments from the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain approved procedures to manage access, and documentation (such as a recently approved access request form) that shows supervisory approval as justification granting specific roles access to systems that process, store, and transmit PHI.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that all personnel assigned to the USNS Mercy completed access request forms to obtain system access. The Chief of Staff stated that the USNS Mercy CIO would revise its procedures to ensure the access request form identified different levels of access based on clinical and patient care needs. In addition, he stated that revised procedures would describe the requirement for obtaining system access through the presentation of an individual identifier and password. Furthermore, the Chief of Staff stated that supervisors would sign the forms and keep them on file until personnel leave the ship to enable the CIO to validate the need for access. He stated that the CIO would revise the procedures and begin maintaining access request forms by April 15, 2018.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once the USNS Mercy provides the revised and approved procedures for managing access.

e. Configure all systems that process, store, and transmit patient health information to lock automatically after 15 minutes of inactivity.

Navy Comments

The Executive Director, BUMED, responding for the NHCP CIO, agreed, stating that the servers for AHLTA and the CHCS reside at NMC San Diego and that the system administrator at NMC San Diego submitted a request to the DHA to configure the system to lock automatically after 15 minutes of inactivity. The Executive Director stated that the CHCS and Essentris locked automatically after 15 and 5 minutes of inactivity, respectively, but acknowledged that McKesson Cardiology could not lock automatically after 15 minutes. He stated that the Naval Logistics Command was procuring a newer version of McKesson Cardiology in fall 2018 that would allow the Navy to comply with the requirement. In addition, the Executive Director stated that PeerVue locked automatically based on the settings of the computers running the system. He added that all computers on the NHCP network locked automatically after 15 minutes of inactivity except for the computers in the operating rooms, which locked automatically after 4 hours.

The Executive Director, responding for the NMC San Diego, disagreed, stating that configuring systems or the network to lock automatically after 15 minutes of inactivity impeded the MTF's ability to provide safe and effective patient care. The Executive Director stated that NMC San Diego would submit a waiver to the DHA requesting an exemption while continuing to address the issue with its Program Office.

Our Response

For the NHCP, the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain the policy from NHCP that exempts computers from locking automatically after periods greater than 15 minutes and documentation showing the systems locked automatically after no more than 15 minutes of inactivity.

For NMC San Diego, the Executive Director partially addressed the recommendation; therefore, the recommendation is unresolved. We recognize the criticality of providing patient care and recognize it may not be practical to lock automatically all systems after 15 minutes of inactivity in specific areas, such as operating rooms. However, in other areas where real-time patient care does not occur, the systems should lock automatically to prevent the disclosure or compromise of PHI. NMC San Diego should provide additional comments describing how it will implement the recommendation, or provide an approved waiver exempting the MTF from locking systems automatically after 15 minutes of inactivity.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that the CIO would validate that AHLTA-T, Carestream, the Maritime Medical Module, and TC2 were configured to lock automatically after 15 minutes of inactivity by April 15, 2018.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation (such as configuration settings) that shows the USNS Mercy configured AHLTA-T, Carestream, the Maritime Medical Module, and TC2 to lock automatically after 15 minutes of inactivity.

f. Appropriately configure and regularly review system audit reports and logs to identify user and system activity anomalies.

Navy Comments

The Executive Director, BUMED, responding for the NHCP and NMC San Diego CIOs, agreed, stating that the NHCP uses multiple systems to monitor and log system reports that identify anomalous system and user activity. The Executive Director stated that NMC San Diego's Information Management Department did not have sufficient staff or tools to review all reports. However, he stated that NMC San Diego would explore options to enable the MTF's administrators to review and address issues.

Our Response

For the NHCP, the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation showing that the systems record required events and user activities, and NHCP reviews those reports.

For NMC San Diego, the Executive Director partially addressed the recommendation; therefore, the recommendation is unresolved. The Executive Director did not describe how and when NMC San Diego would resolve resource limitations preventing the MTF from reviewing reports. Therefore, the Navy should provide additional comments that describe NMC San Diego's solutions to monitor system reports, and identify and address anomalous activity.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that the CIO would revise and implement procedures addressing anomalies. Specifically, he stated that the CIO would begin implementing monthly audits and submitting reports to the USNS Mercy Commander by April 15, 2018.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain revised procedures from the USNS Mercy, and examples of the monthly reports submitted to the USNS Mercy Commander.

g. Develop and maintain standard operating procedures for granting access, assigning and elevating privileges, and deactivating user access.

Navy Comments

The Executive Director, BUMED, responding for the NHCP and NMC San Diego CIOs, agreed, stating that NHCP developed and used procedures to manage user access, which include using an access request form that the MTF modified during the DoD OIG visit. He also stated that NHCP implemented an annual process to verify the need for continued system access. The Executive Director stated that NMC San Diego would work with the Medical Executive Committee and the Chief Medical Informatics Officer to develop appropriate procedures.

Our Response

Comments from the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain approved procedures from NHCP and NMC San Diego for managing access to all systems that process, store, and transmit PHI.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that the CIO would revise procedures for granting access, assigning and elevating privileges, and revoking access by April 15, 2018.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain revised and approved procedures for managing system access from the USNS Mercy.

h. Review and identify all systems used to process, store, and transmit patient health information, develop a baseline of systems used at each military treatment facility, and regularly, at least annually, validate the accuracy of the inventory of systems.

Navy Comments

The Executive Director, BUMED, responding for the NHCP and NMC San Diego CIOs, agreed, stating that the NHCP maintains a comprehensive list of systems that process, store, and transmit PHI in the System Center Configuration Monitor and in other systems. The Executive Director also stated that the NHCP inventories the systems annually. The Executive Director stated that NMC San Diego completed and documented a comprehensive inventory of systems while obtaining its authority to operate under the Risk Management Framework process.

Our Response

Comments from the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain the baseline of systems for the NHCP and NMC San Diego, and procedures describing their process for validating system inventories.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that the USNS Mercy had a list of systems that contained PHI. The Chief of Staff stated that the USNS Mercy Commander would validate the inventory annually.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain the baseline of systems for the USNS Mercy, and procedures describing the process for annually validating system inventories.

i. Develop and maintain access request forms for all users of systems that process, store, and transmit patient health information, and verify, at least annually, the continued need for system access.

Navy Comments

The Executive Director, BUMED, responding for the NHCP and NMC San Diego CIOs, agreed, stating that NHCP developed and used procedures to manage user access, to include an access request form that the MTF modified during the DoD OIG visit. He stated that the NHCP implemented an annual process to verify the need for continued access. The Executive Director stated that NMC San Diego developed an electronic process for submitting access request forms for NMC San Diego staff and would expand the process in the future to cover non-NMC San Diego staff.

Our Response

For the NHCP, the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain the revised and approved procedures for managing system access for the NHCP.

For NMC San Diego, the Executive Director partially addressed the recommendation; therefore, the recommendation is unresolved. The Executive Director did not describe whether NMC San Diego would regularly verify the need for continued user access. Therefore, the Navy should provide additional comments to clarify its plans for verifying system access at NMC San Diego.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, partially agreed, stating that the USNS Mercy maintained access request forms. The Chief of Staff stated that the USNS Mercy CIO would revise procedures to remove users who transfer from the ship, and would conduct audits of authorized users against the ship's manning roster within 30-days of returning from deployments, and monthly, to account for personnel with access to its systems.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We agree that removing users who transfer from the ship, and conducting audits of authorized users against the ship's manning roster within 30-days of returning from deployments would allow the USNS Mercy to improve management of user access to systems that maintain PHI. We will close this recommendation once we obtain the revised and approved procedures for managing access to systems for the USNS Mercy, and documentation, such as audit results for removing user access after returning from deployments.

Air Force Comments

The Air Force Surgeon General, responding for the Dover Clinic and WPMC CIOs, agreed, stating that his office would use Air Force Medical Support Agency and Air Force Medical Operations Agency assets to coordinate with the Dover Clinic and WPMC Commanders and CIOs to accomplish Recommendations 1.d, 1.e, 1.f, 1.g, 1.h, and 1.i in 90 days and Recommendations 1.a, 1.b, 1.c, and 1.f in 180 days. The Surgeon General stated that his office would validate the completion of actions in 240 days.

Our Response

Comments from the Air Force Surgeon General addressed all specifics of the recommendations; therefore, the recommendations are resolved. We will close the recommendations once we obtain documentation of the specific corrective actions the Dover Clinic and WPMC took to address each recommendation.

Recommendation 2

We recommend that the Surgeons General for the Departments of the Navy and Air Force, in coordination with Chief Information Officers for the U.S. Navy Bureau of Medicine and Surgery and the U.S. Air Force Medical Service, assess whether the systemic issues identified in this report exist at other Service-specific military treatment facilities, and develop and implement an oversight plan to:

a. **Verify that military treatment facilities enforce the use of Common Access Cards to access systems that process, store, and transmit patient health information, or obtain a waiver that exempts the systems from using Common Access Cards.**

b. **Verify that military treatment facilities configure passwords for systems that process, store, and transmit patient health information to meet DoD length and complexity requirements.**

c. **Develop a baseline of systems used at each military treatment facility, and regularly, at least annually, validate the accuracy of the inventory of systems.**

d. **Verify that privacy impact assessments are developed and updated for all systems that process, store, and transmit patient health information.**

Navy Comments

The Executive Director, BUMED, responding for the Surgeon General for the Department of the Navy, agreed, stating that BUMED would comply with the requested actions for Recommendations 2.a and 2.b by June 1, 2018; Recommendation 2.c by October 1, 2018, and annually thereafter; and Recommendation 2.d by October 1, 2018. The Executive Director recommended that the Surgeon General and BUMED include the need for meeting DoD password requirements in a POA&M and in its Management Internal Control Program. He stated that BUMED routinely validates the accuracy of its system inventories annually through data calls, the governance process, and DoD Information Technology Portfolio Repository reviews. The Executive Director also stated that BUMED evaluates existing and new information systems collecting, storing, or transmitting PHI through the governance process. He stated that if discrepancies are discovered, the systems managers are directed to initiate a PIA.

Our Response

Comments from the Executive Director partially addressed the recommendations; therefore, the recommendations are unresolved. The Executive Director did not describe the actions BUMED will take to address each recommendation. We agree that including the need to meet DoD password requirements should be included in a POA&M, as a POA&M will provide details explaining when and how BUMED would meet DoD password requirements. However, we disagree that BUMED routinely validates the accuracy of its system inventory because we were unable to obtain an inventory during the audit. Therefore, BUMED should provide additional comments to clarify the actions it will take to address each recommendation.

Air Force Comments

The Air Force Surgeon General agreed, stating that his office, in coordination with the AFMS Chief Technology Officer, will correct the issues discussed in this report at the identified MTFs; assess whether the issues identified in this report exist at other Air Force MTFs; and develop and implement a corrective action plan that addresses the recommendations. With respect to Recommendation 2.d, the Surgeon General stated that the DHA is responsible for providing written procedures for completing privacy act assessments because AFMS transitioned oversight responsibility to the DHA in October 2016. The Surgeon General also stated that AFMS would comply with the requested actions for Recommendations 2.a, 2.b, and 2.d by November 1, 2018, and Recommendation 2.c by June 1, 2018.[36] Furthermore, the Surgeon General stated that his office will conduct data calls at the remaining MTFs to confirm or deny discrepancies and to convey Federal and DoD guidance requirements to protect systems that process, store, and transmit PHI.

Our Response

Comments from the Air Force Surgeon General addressed all specifics of the recommendations; therefore, the recommendations are resolved. We will close the recommendations once we obtain documentation of the specific corrective actions the Air Force took to address each recommendation.

[36] AFMS transitioned oversight responsibilities to the DHA in October 2016. Therefore, the DHA is responsible for providing written procedures that include a process for verifying that PIAs are completed regularly for all systems.

Recommendation 3

We recommend that the Commanders, 436th Medical Group, Naval Hospital Camp Pendleton, Naval Medical Center San Diego, U.S. Naval Ship Mercy, and Wright-Patterson Medical Center review the performance of their Chief Information Officers and consider administrative action, as appropriate, for not following Federal and DoD guidance for protecting patient health information to include:

- **not mitigating known vulnerabilities in a timely manner;**
- **not developing plans of action and milestones for unmitigated vulnerabilities; and**
- **not formally accepting risks for unmitigated vulnerabilities.**

Navy Comments

The Executive Director, BUMED, responding for the NHCP and NMC San Diego Commanders, agreed, but stated that the NHCP and NMC San Diego CIOs did not have the resources to consistently meet their requirements. The Executive Director also stated that the NHCP shifted staff to support cybersecurity requirements while NMC San Diego was hiring additional staff to address resource issues.

Our Response

Comments from the Executive Director partially addressed the recommendation; therefore, the recommendation is unresolved. We recognize resource constraints may limit the ability of CIOs to perform their responsibilities and that the NHCP and NMC San Diego are taking action to address those resource constraints. However, the Executive Director did not address whether the MTF commanders would review the performance of their CIOs with respect to the protection of PHI. Therefore, the Navy should provide additional comments describing how MTF commanders plan to review the performance of NHCP and NMC San Diego CIOs.

Air Force Comments

The Air Force Surgeon General, responding for the Dover Clinic and WPMC Commanders, stated that his office would use Air Force Medical Support Agency and Air Force Medical Operations Agency assets to coordinate with the MTF commanders to accomplish the recommendation in 90 days. In addition, the Air Force Surgeon General stated that his office would validate that the Dover Clinic and WPMC Commanders implemented the recommendation in 240 days.

Our Response

Comments from the Air Force Surgeon General addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation (such as performance plans for CIOs) showing how the MTF commanders will review the CIO's performance at the Dover Clinic and WPMC.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy Commander, disagreed, stating that the CIO during the DoD OIG audit was no longer assigned to the MTF. The Chief of Staff stated that the USNS Mercy implemented a process that provides checks and balances to ensure oversight and accountability of the USNS Mercy's information management and information technology program.

Our Response

Although the Chief of Staff disagreed, implementing a process to ensure oversight and accountability of the USNS Mercy's information management and information technology program meets the intent of the recommendation. Therefore, the recommendation is resolved and we will close the recommendation once the USNS Mercy Commander provides documentation outlining the process used to improve oversight and accountability of the CIO's performance.

Recommendation 4

~~(FOUO)~~ We recommend that the Chief Information Officers for Naval Hospital Camp Pendleton, U.S. Naval Ship Mercy, and Wright-Patterson Medical Center [redacted] and [redacted] for systems that process, store, and transmit patient health information.

Navy Comments

~~(FOUO)~~ The Executive Director, BUMED, responding for the NHCP CIO, agreed, stating that all systems on the NHCP network used [redacted], which prevents access to the hard drives from outside the network. The Executive Director stated that requirements for a newer version of [redacted] software would use a [redacted] hard drive, or support the use of [redacted] and [redacted].

Our Response

~~(FOUO)~~ Comments from the Executive Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once the Navy acquires and uses a version of [redacted] that [redacted] and [redacted], and provides documentation showing configuration settings that support [redacted].

Air Force Comments

~~(FOUO)~~ The Air Force Surgeon General, responding for the WPMC CIO, stated that his office would use Air Force Medical Support Agency and Air Force Medical Operations Agency assets to coordinate with the WPMC Commander and CIO to accomplish the recommendation in 180 days. In addition, the Surgeon General stated that his office would validate that the WPMC CIO [redacted] in 240 days.

Our Response

~~(FOUO)~~ Comments from the Air Force Surgeon General partially addressed the recommendation; therefore, the recommendation is unresolved. The Air Force Surgeon General did not describe the actions the WPMC CIO would [redacted] for [redacted] or [redacted] for [redacted]. The Air Force Surgeon General should provide additional comments that clarify how the WPMC CIO will [redacted] PHI.

Military Sealift Command Comments

~~(FOUO)~~ The Military Sealift Command Chief of Staff, responding for the USNS Mercy CIO, agreed, stating that the CIO would submit a request to NMC San Diego to [redacted] data for [redacted] by April 15, 2018. The Chief of Staff also stated that the MTF was coordinating with the Navy Medical Logistics Command to modify [redacted] or replace the system entirely.

Our Response

~~(FOUO)~~ Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation from the USNS Mercy (such as configuration settings) that show [redacted], or [redacted] data for the replacement system.

Recommendation 5

We recommend that the Director, Defense Health Agency, configure the Armed Forces Health Longitudinal Technology Application, the Composite Health Care System, the Clinical Information System/Essentris Inpatient System, and all other Defense Health Agency-owned systems that process, store, and transmit patient health information to lock automatically after 15 minutes of inactivity.

DHA Comments

The DHA Director agreed, stating that the DHA **could potentially** [emphasis added] lock systems after a defined period of inactivity for AHLTA, the CHCS, and Essentris after coordinating with the Military Services, the functional community, commercial vendors, and the Defense Information Systems Agency (stakeholders). The Director also stated that the DHA would coordinate with its stakeholders to configure other DHA-owned systems that process, store, and transmit PHI to lock automatically after 15 minutes of inactivity.

Our Response

Comments from the DHA Director partially addressed the recommendation; therefore, the recommendation is unresolved. The Director stated that the DHA **could potentially** [emphasis added] lock systems after a defined period of inactivity. Use of the words "could potentially" does not provide assurance that the DHA would configure AHLTA, the CHCS, Essentris, and other DHA-owned systems that process, store, and transmit PHI to lock automatically after 15 minutes of inactivity. Therefore, the DHA should provide additional comments to clarify whether it will configure DHA-owned systems to lock automatically after 15 minutes of inactivity.

Recommendation 6

We recommend that the Commander, U.S. Naval Ship Mercy, implement physical access controls to identify and record the names of personnel and the times when personnel accessed a patient's paper medical records, and regularly, at least monthly, reconcile the logs against the list of authorized personnel with access to the area.

Military Sealift Command Comments

The Military Sealift Command Chief of Staff, responding for the USNS Mercy Commander, agreed, stating that the USNS Mercy CIO will develop procedures that address physical security and health record information access. He stated that the USNS Mercy would comply with a two-lock system for the access door and the file cabinets that store the health records. In addition, the Chief of Staff stated that the USNS Mercy would use health records custody cards to account for records that were accessed, would require staff to sign out and sign in all health records requested, and would reconcile the health records on a monthly basis against the record sign-in/sign-out log.

Our Response

Comments from the Chief of Staff addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain the approved physical access procedures from the USNS Mercy Commander and documentation supporting the monthly reconciliations of the logs against the access lists.

Appendix A

Scope and Methodology

We conducted this performance audit from April 2017 through January 2018 in accordance with 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 on our audit objective. We believe the evidence provides a reasonable basis for our findings and conclusions based on the audit objective.

To understand the process used to protect PHI, we interviewed officials from the DHA, AFMS, BUMED, and select Navy and Air Force MTFs. We also interviewed system owners, CIOs, system administrators, developers, and users to identify specific protocols implemented to protect systems that process, store, and transmit PHI.

We reviewed Federal laws and DoD policies, including Navy and Air Force guidance on complying with HIPAA security rules and implementing system security protocols. We selected a nonstatistical sample of 5 of the 165 Navy and Air Force MTFs to visit within the scope of this audit. Specifically, we visited:

- NHCP, California;
- NMC San Diego in San Diego, California;
- USNS Mercy in San Diego, California;
- Dover Clinic at Dover Air Force Base in Dover, Delaware; and
- WPMC at Wright-Patterson Air Force Base in Dayton, Ohio.

At the five MTFs, we reviewed whether the DHA, Navy, and Air Force assessed security risks and tested the suitability and effectiveness of implemented system security protocols to protect the three DoD EHR systems, three modified EHR systems, two DHA-owned systems, and nine Service-specific systems from unauthorized access and disclosure of PHI. We selected two medical centers, one hospital, one clinic, and one hospital ship to incorporate different types of Navy and Air Force medical facilities in the audit scope. Table 4 describes the EHR systems, modified EHR systems, DHA-owned systems, and Navy and Air Force-specific systems used at each MTF that were included in the audit scope.

Table 4. List of Systems Used at Each MTF Visited

System Name (Owner)	System Description	Systems Used at the MTFs Visited				
		Dover Clinic	NHCP	NMC San Diego	USNS Mercy	WPMC
AHLTA (DHA)	Used to access patient conditions, prescriptions, and diagnostic test results.	X	X	X		X
AHLTA-T (DHA)	Used by deployed medical staff to document clinical care.				X	
Audio Metric Database System (Navy)	Used by audiologists to obtain data from medical devices to diagnose patient hearing problems.			X		
BMBB/TS (DHA)	Used to collect and maintain blood records, blood orders, and patient information to support blood transfusions.			X		
Carestream Picture Archiving and Communication System (Carestream) (Navy)	Used to access cardiovascular records.				X	
CHCS (DHA)	Used to track appointments, order laboratory tests, authorize radiology procedures, and prescribe medications.	X	X	X		X
Innovian (Air Force)	Used by anesthesiologists to record and manage anesthesia vital signs in the operating room.					X
Epiphany Electrocardiogram Management (Air Force)	Used to import, manage, and export diagnostic test results.					X
Essentris (DHA)	Used to capture bedside point-of-care data such as real-time heart and fetal monitoring.	X	X	X		X
HAIMS (DHA)	Used to access radiographs, clinical photographs, audio files, videos, and scanned documents.	X		X		
McKesson Cardiology (Navy)	Used to record the results of electrocardiograms, stress tests, and other heart-related tests.		X			
Maritime Medical Module (DHA)	Used aboard ships to store and process data and continuously monitor the medical environment and health of personnel who live and work on the ship.				X	

System Name (Owner)	System Description	Systems Used at the MTFs Visited				
		Dover Clinic	NHCP	NMC San Diego	USNS Mercy	WPMC
Nuclear Medicine Information System (Air Force)	Used to monitor the receipt and distribution of radioactive material to patients.					X
Parata System Suite (Navy)	Used to manage prescription barcode scanning and electronic imaging.		X			
PeerVue (Navy)	Used to prioritize orders for ultrasounds and magnetic resonance imaging tests.		X			
PACS (Air Force)	Used by radiologists to access radiology exam images regardless of their physical location.	X				
TC2 (DHA)	Used by deployed medical personnel to document inpatient healthcare and ordered services, and view patient results. The TC2 includes limited CHCS functionality.				X	

Source: The DoD OIG.

We randomly selected 814 of 25,223 users from the 3 DoD EHR systems, 3 modified EHR systems, 2 DHA-owned systems, and 9 Service-specific systems to validate whether the users were authorized to access PHI. The 814 users were the sum of the users randomly selected for testing across the 17 systems reviewed. We selected up to 45 users per testing, based on our control testing methodology. If there were no exceptions the control test passed and we concluded with 90 percent confidence that the error rate in the population is less than or equal to 5 percent. If we identified one or more exceptions, the control test failed and, therefore, we could not conclude with 90 percent confidence that the error rate in the population was less than or equal to 5 percent. Table 5 identifies the universe of users per system at each MTF visited, the sample size selected for testing user access, and the number of access-related issues identified per system.

Table 5. Universe and Sample Size per System at Each MTF Visited

MTF	System Name	Universe	Sample Size	Number of Errors Identified*
Dover Clinic	AHLTA	207	39	0
	CHCS	471	43	52
	HAIMS	137	33	4
	PACS	25	17	34
	Totals	**840**	**132**	**90**
NHCP	AHLTA	1,211	45	3
	CHCS	1,543	44	83
	Essentris	973	44	68
	McKesson Cardiology	142	33	33
	Parata System Suite	68	30	31
	PeerVue	484	43	1
	Totals	**4,421**	**239**	**219**
NMC San Diego	AHLTA	3,747	45	9
	Audio Metric Database System	14	14	17
	BMBB/TS	34	18	18
	CHCS	1,221	45	54
	Essentris	2,462	45	14
	HAIMS	3,747	45	8
	Totals	**11,225**	**212**	**120**
USNS Mercy	AHLTA-T	12	12	0
	Carestream PACS	1	1	0
	Maritime Medical Module	6	6	6
	TC2	1,078	44	1
	Totals	**1,097**	**63**	**7**

MTF	System Name	Universe	Sample Size	Number of Errors Identified*
WPMC	AHLTA	2,354	45	7
	CHCS	3,316	45	67
	Epiphany Electrocardiogram Management	10	10	8
	Essentris	1,923	44	41
	Innovian	30	17	13
	Nuclear Medicine Information System	7	7	0
	Totals	**7,640**	**168**	**136**
Grand Total		**25,223**	**814**	**572**

* Multiple access control issues identified on systems at MTFs visited. See Appendix B for specific issues identified.
Source: The DoD OIG.

We also verified whether the users' roles and privileges aligned with assigned responsibilities and identified whether system administrators deactivated or terminated system access when it was no longer required. We tested security protocols for the three EHR systems, three modified EHR systems, two DHA-owned systems, and nine Service-specific systems related to:

- boundary defense;
- use of encryption for data stored on systems (at rest) and data transmitted across the network (in transit);
- administering and managing system access and authentication;
- protecting PHI from unauthorized modification and deletion;
- audit logging;
- security incident handling and response; and
- system maintenance.

Aboard the USNS Mercy, we also tested security protocols to limit and restrict physical access to rooms containing paper medical records.

Use of Computer-Processed Data

We used computer-processed data from DoD EHR systems, modified EHR systems, DHA-owned systems, and the Service-specific systems to generate user lists at each MTF visited. System administrators provided extracts of active and inactive users from the systems in Microsoft Excel spreadsheets and Adobe Acrobat documents. We used the documentation to compile a universe of users at the Dover Clinic, NHCP, NMC San Diego, WPMC, and aboard the USNS Mercy. To assess the reliability of the data, we selected a sample of users and compared the data to information obtained from testing users' access to the DoD EHR systems, modified EHR systems, DHA-owned systems, and Service-specific systems.

The system-generated user data were not sufficiently reliable to determine whether users were authorized to access the systems. Specifically, we identified instances where system administrators did not obtain written justification for granting and elevating access privileges to the DoD EHR systems, modified EHR systems, DHA-owned systems, and Service-specific systems. In addition, system administrators did not consistently deactivate users that no longer required access to the systems. As reported in our findings, we used the data only to generate a sample of users to validate system access and privileges; and developed recommendations for implementing controls to grant access to users based on a demonstrated need for access that aligned with documented responsibilities of the users.

In addition, network administrators provided vulnerability scan results in Microsoft Excel spreadsheets. We used the documentation to identify unmitigated vulnerabilities on the Navy and Air Force networks at specified periods. To test the reliability of the scan results, we searched U.S. Cyber Command's website for information assurance vulnerability management notices, which provide details on vulnerabilities such as the severity of the vulnerability, mitigation dates, and potential solutions for mitigating the vulnerability. Because the vulnerabilities from the network scans identified associated information assurance vulnerability alerts, we determined that the scan results were sufficiently reliable to identify unmitigated vulnerabilities affecting the security posture of the networks used to process, store, and transmit PHI at the Navy and Air Force MTFs.

Use of Technical Assistance

The DoD OIG Quantitative Methods Division provided assistance in developing the random sampling methodology that we used to select DoD EHR system, modified EHR system, DHA-owned system, and Service-specific system users.

Prior Coverage

During the last 5 years, the DoD OIG, the Government Accountability Office (GAO), and the Naval Audit Service issued six reports discussing DoD EHRs. GAO reports are accessible from https://www.gao.gov. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/. Naval Audit Service reports are not available over the Internet.

GAO

GAO-15-530, "Electronic Health Records: Outcome-Oriented Metrics and Goals Needed to Gauge DoD's and Veterans Affairs' Progress in Achieving Interoperability," August 2015

> The GAO identified that the DoD and the Department of Veterans Affairs took actions to increase interoperability between their EHR systems with guidance from the Interagency Program Office. The GAO reported that the Interagency Program Office provided a technical approach for the departments to achieve interoperability between systems. However, the GAO also reported that the DoD and Department of Veterans Affairs would not meet their deadline to deploy modernized EHR software by December 31, 2016.

GAO-16-184T, "Electronic Health Records: Veterans Affairs and DoD Need to Establish Goals and Metrics for Their Interoperability Efforts," October 27, 2015

> The GAO reported that the Interagency Program Office was focused on identifying more meaningful metrics such as quality of a user's experience and improvements in health outcome, but had not defined a timeframe for completing those metrics and incorporating them into guidance.

DoD OIG

~~(FOUO)~~ DODIG-2017-085, "Protection of Electronic Patient Health Information at Army Military Treatment Facilities," July 6, 2017

> The DoD OIG identified that the DHA, the U.S. Army Medical Command, and three Army MTFs did not consistently implement effective security protocols to protect systems that processed, stored, and transmitted PHI. The DoD OIG identified systemic weaknesses in the Army and the DHA's efforts to:
>
> - configure systems to use CACs or passwords that met DoD complexity requirements;
> - take appropriate and timely actions to mitigate known vulnerabilities affecting Army networks;

- consistently review system activity reports to identify unusual or suspicious activities and access; and
- implement procedures to grant system access based on roles that aligned with assigned user responsibilities.

DODIG-2016-094, "Audit of the DoD Healthcare Management System Modernization Program," May 31, 2016

The DoD OIG identified that the execution schedule for the DoD Healthcare Management System Modernization Program may not be realistic for meeting the required initial operational capability date of December 2016.

DODIG-2014-097, "Audit of the Transfer of DoD Service Treatment Records to the Department of Veteran Affairs," July 31, 2014

The DoD OIG identified that 77 percent of the 96,224 records transferred by the Army were not timely and 28 percent were incomplete. In addition, 35 percent of the 45,912 records transferred by the Air Force were not timely, and 11 percent were incomplete; 46 percent of the 3,217 records transferred by the Navy were not timely.

Navy

N2016-0013, "Managing Personally Identifiable Information at Naval Medical Center, Portsmouth and Naval Hospital, Jacksonville," December 29, 2015

The Naval Audit Service identified that the Department of the Navy East Coast commands' internal controls to dispose of medical treatment equipment containing personally identifiable information were ineffective. The Naval Audit Service found that personnel across four departments were unaware of the timeframe to report a breach, did not follow proper procedures for documenting the disposal of equipment containing PHI, and did not properly mark the classification or encrypt e-mails containing PHI.

Appendix B

Summary of Access Control Problems at the Five MTFs Visited

At the five MTFs, we assessed their processes for granting, elevating access privileges, and deactivating inactive users. Table 6 identifies the types of access-related problems we identified at the Dover Clinic, NHCP, NMC San Diego, USNS Mercy, and WPMC.

Table 6. Access Control Problems at MTFs Visited

System Name	Missing or Incomplete Access Request Forms	No Justification for Elevated Privileges	Inactive Users with System Access	Shared System Administrator Accounts	System Roles Did Not Align With User Duties
Dover Clinic					
CHCS	38	8	5		1
HAIMS	4				
PACS	17			17	
Totals	**59**	**8**	**5**	**17**	**1**
NHCP					
AHLTA		2	1		
CHCS	44	32	6		1
Essentris	44	24			
McKesson Cardiology	33				
Parata System Suite	30	1			
PeerVue			1		
Totals	**151**	**59**	**8**		**1**
NMC San Diego					
AHLTA		9			
Audio Metric Database System	9	5	1		2

System Name	Missing or Incomplete Access Request Forms	No Justification for Elevated Privileges	Inactive Users with System Access	Shared System Administrator Accounts	System Roles Did Not Align With User Duties
BMBB/TS	18				
CHCS	8	30			16
Essentris	10	4			
HAIMS	8				
Totals	**53**	**48**	**1**		**18**
USNS Mercy					
Maritime Medical Module	6				
TC2		1			
Totals	**6**	**1**			
WPMC					
AHLTA	4	3			
CHCS	34	16	13		4
Epiphany Electrocardiogram Management	6	2			
Essentris	27	7	4		3
Innovian	10		3		
Totals	**81**	**28**	**20**		**7**

Source: The DoD OIG.

Management Comments

Defense Health Agency

DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

MAR - 1 2018

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Draft Report for Audit of Securing Navy and Air Force Electronic Health Records (D2017-D000RC-0113.000)

Thank you for the opportunity to review and comment on the Department of Defense Inspector General Draft Report, "Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities." Overall, we concur with the report's findings and conclusions.

My specific comment to recommendation five is attached. Please feel free to direct any comments on this topic to [redacted] at [redacted] or via email at [redacted].

for R. C. BONO
VADM, MC, USN
Director

Attachment:
As stated

Defense Health Agency (cont'd)

Final Report Reference

DoD Inspector General *Audit of Securing Navy and Air Force Electronic Health Records (D2017-D000RC-0113.000)*
"Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities"
DEFENSE HEALTH AGENCY COMMENTS TO THE RECOMMENDATIONS

Recommendation 5 (page 30)
We recommend that the Director, Defense Health Agency, configure the Armed Forces Health Longitudinal Technology Application, the Composite Health Care System, the Clinical Information System/Essentris Inpatient System, and all other Defense Health Agency owned systems that process, store, and transmit patient health information to lock automatically after 15 minutes of inactivity.

Recommendation 5 on page 44

DHA Response: DHA concurs with this recommendation regarding systems automatically locking after 15 minutes of inactivity for AHLTA, CHCS, and Essentris. DHA could potentially implement a specific inactivity lockdown threshold for AHLTA, CHCS, and Essentris after coordination with the Services, the functional community, the appropriate commercial vendors, and the Defense Information Security Agency (DISA). DHA will evaluate which other DHA-owned systems process, store, and transmit patient health information. DHA will coordinate with DISA, the Services, the functional community, and the appropriate commercial vendors to work towards compliance.

2

Surgeon General for the Department of the Air Force

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON DC

March 11, 2018

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: HQ USAF/SG
1780 Air Force Pentagon
Washington, DC 20330-1780

SUBJECT: Response to DoD Office of Inspector General Draft Report, "Protection of Patient Health Information at Navy and Air Force Medical Treatment Facilities" Recommendations (Project No. D2017-D000RC-0113.000)

The Air Force Surgeon General in coordination with the Air Force Medical Service (AFMS) Chief Technology Officer (CTO) will correct issues identified in this report at the identified facilities, assess all other Air Force military treatment facilities, and develop and implement an oversight correction plan as outlined in the following recommendations:

DoD IG Recommendation 2:

That the Surgeon General for the Department of the Air Force, in coordination with Chief Information Officer U.S. Air Force Medical Service, assess whether the systemic issues identified in this report exist at other Service-specific military treatment facilities, and develop and implement an oversight plan to:

a. Verify that military treatment facilities enforce the use of Common Access Cards (CAC) to access systems that process, store, and transmit patient health information, or obtain a waiver that exempts the systems from using CAC.

Concur. AFMS will comply by 1 November 2018.

b. Verify that military treatment facilities configure passwords for systems that process, store, and transmit patient health information to meet DoD length and complexity requirements.

Concur. AFMS will comply by 1 November 2018.

c. Develop a baseline of systems used at each military treatment facility, and regularly, at least annually, validate the accuracy of the inventory of systems.

Concur. AFMS will comply by 1 June 2018.

d. Verify that privacy impact assessments (PIAs) are developed and updated for all systems that process, store, and transmit patient health information.

Surgeon General for the Department of the Air Force (cont'd)

Concur. However, The Defense Health Agency (DHA) is responsible for providing written procedures that include a process to verify that PIAs are completed regularly for all systems as the AFMS transitioned oversight responsibilities to DHA in October 2016. AFMS will comply by 1 November 2018.

We will invoke Air Force Medical Support Agency and Air Force Medical Operations Agency assets to engage Commanders and Chief Information Officers at Dover and Wright Patterson AFB to accomplish recommendations at 90/180/240 day milestones. We will also conduct data calls at remaining MTFs to confirm/deny discrepancies and to convey Federal and DoD Guidance requirements to protect systems that process, store, and transmit PHI.

Management	90-Day	180-Day	240-Day
CIOs, Dover/Wright-Patterson AFB	1.d, 1.e, 1.f, 1.g, 1.h, 1.i	1.a, 1.b, 1.c, 1.f,	Validation of Accomplished Recommendations and Internal Controls
AF/SG	2.c	2.a, 2.b, 2.d	
436th & 88th MDG/CCs	3		
CIOs, Wright-Patterson AFB		4	

The AF/SG point of contact is [redacted], AFMS CTO, who may be reached at [redacted] or by e-mail at [redacted].

MARK A. EDIGER
Lieutenant General, USAF, MC, CFS
Surgeon General

Attachment:
AF/SG Request for Security Markings

Navy Bureau of Medicine and Surgery

DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
(MANPOWER AND RESERVE AFFAIRS)
1000 NAVY PENTAGON
WASHINGTON, D.C. 20350-1000

MAR 15 2018

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities

The Department of the Navy (DON) appreciates the opportunity to provide responses to the report concerning "Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities." Attached is the Navy Bureau of Medicine and Surgery response to recommendations requiring comment. The Military Sealift Command submitted their response separately. My point of contact for this matter is [redacted] who may be reached at [redacted] or [redacted].

Juliet M. Beyler
Deputy Assistant Secretary of the Navy
(Military Manpower & Personnel)

Attachments:
As stated

Navy Bureau of Medicine and Surgery (cont'd)

DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH VA 22042

IN REPLY REFER TO
7500
Ser M6/18UM60014
14 MAR 2018

From: Chief, Bureau of Medicine and Surgery
To: Naval Audit Service, Assistant Auditor General for Research, Development, Acquisition, and Logistics Audits

Subj: NAVY INSPECTOR GENERAL AUDIT: PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES, (D2017-D000RC-0113)

Ref: (a) Signed Draft Report – Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities, (D2017-D000RC-0113)

Encl: (1) Bureau of Medicine and Surgery, Chief Information Officer response.
(2) Navy Medicine West consolidated response.
(3) Bureau of Medicine and Surgery, Privacy Program Office response.

1. Bureau of Medicine and Surgery (BUMED) provides enclosures (1) though (3) in response to recommendations 1a through 1i, 2a thru 2d, and 4 of reference (a) and concurs with agreed timelines outlined in the responses.

2. BUMED supports the responses for recommendation 1e. The responses from both Commands are correct. The independent responses support their respective business practices for healthcare delivery.

3. My point of contact is [redacted] who may be reached at [redacted], or e-mail at [redacted].

M. P. MALANOSKI
Executive Director

Navy Bureau of Medicine and Surgery (cont'd)

From: Assistant Deputy Chief for Information Management & Technology, Bureau of Medicine and Surgery
To: Chief, Bureau of Medicine and Surgery

Subj: RESPONSE: DOD OFFICE OF INSPECTOR GENERAL DRAFT REPORT, "PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES"

1. Recommendation 2:
We recommend that the Surgeons General for the Departments of the Navy and Air Force, in coordination with Chief Information Officers for the U.S. Navy Bureau of Medicine and Surgery and the U.S. Air Force Medical Service, assess whether the systemic issues identified in this report exist at other Service-specific military treatment facilities, and develop and implement an oversight plan to:

a. Verify that military treatment facilities enforce the use of Common Access Cards to access systems that process, store, and transmit patient health information, or obtain a waiver that exempts the systems from using Common Access Cards.

Concur: BUMED will comply by June 1, 2018

b. Verify that military treatment facilities configure passwords for systems that process, store, and transmit patient health information to meet DoD length and complexity requirements.

Concur: BUMED will comply by June 1, 2018

c. Develop a baseline of systems used at each military treatment facility, and regularly, at least annually, validate the accuracy of the inventory of systems.

Concur: BUMED will comply by October 1, 2018 and annually thereafter.

d. Verify that privacy impact assessments are developed and updated for all systems that process, store, and transmit patient health information.

Concur: BUMED will comply by October 1, 2018.

2. Point of Contact: [redacted], [redacted] or [redacted]

Enclosure (1)

Navy Bureau of Medicine and Surgery (cont'd)

From: Assistant Chief of Staff, Naval Medicine West
To: Chief Information Officer, U.S. Navy Bureau of Medicine and Surgery

Subj: RESPONSE: DOD OFFICE OF INSPECTOR GENERAL DRAFT REPORT, "PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES"

Naval Hospital Camp Pendleton Response:

Encl: (1) Screenshot of [redacted] password requirements
(2) NHCP POAM
(3) NHCP IMD Account Request Form V2.0
(4) NHCP SAAR-N OPNAV 5239/14

1. Recommendation 1

a. Concur. All computer systems on the NHCP network are PKI/CAC enforced to ensure systems are accessed by authorized users via two-form authentication. All username and password requests for computer systems are given on a day to day basis for no longer than 24 hours, which is set at the time of approval.

b. Concur. [redacted] is the current version of the software that was procured in 2013 with no support to meet the password complexity requirements. Enclosure (1) is a screenshot of the current password requirements for [redacted]. Naval Medical Logistics Command (NMLC) is procuring the newest version of [redacted] software that will require CAC authentication; estimated time of delivery is Fall 2018.

c. Concur. A plan of action and milestones (POAM) has been implemented to mitigate any known vulnerabilities. Enclosure (2) is a snapshot of the POAM located on the secured NHCP Cybersecurity Division share drive. Also, NHCP's Authority-to-Operate (ATO) POAM are located and updated in eMASS; https://emass-dha.csd.disa.mil/. Both POAMs will be monitored and managed by the Cybersecurity Division's Information Systems Security Manager (ISSM) and Information System Security Officers (ISSO) on a daily basis once reported by the Assured Compliance Assessment Solution (ACAS) scanning server. Additionally, NHCP has been inspected by the Continuous Risk Management Team from 24 July 2017 to 28 July 2017. The Mitigation and Remediation Support (MARS) team has conducted a site assist visit from 22 May 2017 to 06 June 2017 to aid in the mitigation of vulnerabilities on the NHCP network. NHCP was granted an ATO-C on 06 October 2017 which expires on 03 April 2018.

d. Concur. The NHCP Information Management Department (MID) Clinical Information Systems (CIS) division created and uses a Standard Operating Procedure (SOP) for creating accounts for all users of systems that process, store, and transmit PHI. They have also implemented annual checks to verify access needs as per the SOP. NHCP has an account creation form, Enclosure (3), that was modified during the DoD IG Audit to include credentialing department's approval, and requesting user's department head approval and signature to the user roles requested by the user. The following systems are included in the

Enclosure (2)

Navy Bureau of Medicine and Surgery (cont'd)

Subj: RESPONSE: DOD OFFICE OF INSPECTOR GENERAL DRAFT REPORT, "PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES"

account creation form: PACS, ESSENTRIS, CHCS, and AHLTA. Additionally, the SAAR-N form was modified to include PACS, ESSENTRIS, CHCS, and AHLTA on the requested systems access; Enclosure (4). This form is also signed by the requesting user's department head. Will work with CNIO and CMIO to create an account/access request form for systems not administered by MID.

e. Concur: NHCP's AHLTA and CHCS servers reside within NMC San Diego's network. The AHLTA system administrator at NMC San Diego has submitted a change request to DHA to modify the AHLTA timeout requirement for 15 minutes. All CHCS users have been configured for a maximum timeout of 900 seconds or 15 minutes. ESSENTRIS by design is already defaulted to 300 seconds or five (5) minutes timeout with the exception of four (4) status board computers. McKesson Cardiology 13 is not configurable for the 15 minute timeout. NMLC is procuring the newest version of McKesson Cardiology software that will comply with automatic lockout rule of 15 minutes; estimated time of delivery is Fall 2018. PeerVue is configured to use the computer PKI login requirements for authentication and the timeout requirement depends on the computers timeout settings. All computers on the NHCP network are set for the 15 minute timeout with the exception of operatories where the four (4) hour exception applies.

f. Concur. NHCP MID uses multiple systems to properly monitor and log system reports; these systems are used to identify user and system activity anomalies. The systems employed at NHCP include: HBSS, ACAS, Splunk SYSlogger, Varonis, ForeScout NAC, and the computer event logs which are configured at the time of baseline imaging.

g. Concur. See 1.d.

h. Concur. NHCP MID maintains a comprehensive inventory of all systems. All systems that process, store, and transmit PHI are inventoried and identifiable via System Center Configuration Monitor (SCCM), Splunk SYSlogger, ForeScout NAC and ACAS. The locations of these systems are maintained regularly by MID. All computer systems are inventoried on an annual basis to comply with BUMED and NMLC requirements.

i. Concur. See 1.d.

2. Recommendation 3

Concur. NHCP agrees, however the cite CIO does not have the resources to and enterprise level support to consistently meet this requirement. To address this issue, NHCP has shifted staffing to assist with Cybersecurity.

3. Recommendation 4

Concur. All computer systems located on the NHCP network are [redacted] with [redacted]

Enclosure (2)

Navy Bureau of Medicine and Surgery (cont'd)

Subj: RESPONSE: DOD OFFICE OF INSPECTOR GENERAL DRAFT REPORT, "PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES"

[redacted], which prevents the hard drives from being accessed outside of the NHCP network. Additionally, systems are secured with Host Based Security System (HBSS).. The proposed requirements for the [redacted] software replacement will have a [redacted] hard drive to mitigate the [redacted] requirement and/or support [redacted] and [redacted].

4. Point of contact: [redacted], or [redacted].

Naval Medical Center San Diego Response:

1. Recommendation 1

a. Concur: CAC usage is enforced by IMD with all systems that support CAC usage. Single-factor credentials were only utilized with systems that could not physically support CAC-centric login credentials. A POAM for CHCS is currently being worked at the DHA Enterprise level for CHCS CAC Login with ETR of Spring 2018.

b. Concur: CHCS and AHLTA were compliant systems and the [redacted] system has been changed to meet password complexity requirements as directed. At this time; however, there are several systems which are not able to support this requirement and we are working with the respective vendors to make them compliant.

c. Concur: This issue was addressed as part of our ATO conditions as we moved to the new Risk Management Frame work Cybersecurity process.

d. Concur: CHCS, AHLTA and Essentris access is based upon a staff member's ability to show network access has already been granted. Members are assigned roles as per their assignment/ positions (i.e., Physician, Nurse or Corpsman). To our understanding, no formalized process within BUMED to determine which roles are assigned to clinical staff. We will work with the CMIO in conjunction with the Medical Executive committee to formalize a local policy.

e. Do Not Concur: Based on input from clinical staff, a 15 minute lock time was deemed to be an impediment to providing safe and effective patient care. In high acuity areas such as the Emergency Department and operating room environment, a 15 minute lockout during stressful, time critical situations is contrary to the tenants of patient safety. To address this issue, NMCSD will submit a waiver request or a System Change Request (SCR) to the DHA. The NMCSD ITMD, CMIO and MEC committee will address this issue with the Program office.

f. Concur: IMD does not have sufficient staffing or tools to review all system activity reports on all systems. IMD will continue to look for automated tools that will allow system administrators to readily review the thousands of entries generated by said reports and will address with DHA

Enclosure (2)

Navy Bureau of Medicine and Surgery (cont'd)

Subj: RESPONSE: DOD OFFICE OF INSPECTOR GENERAL DRAFT REPORT, "PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES"

as well.

g. Concur: As these decisions should be part of a clinical process review, we are working with the Medical Executive Committee and CMIO to develop relevant policy and process to support this requirement.

h. Concur: As part of our recent ATO process change to Risk Management Framework, NMCSD was tasked and completed a comprehensive document that listed all relevant systems as directed by this paragraph.
i. Concur: NMCSD has developed an electronic SAAR-N submission process for all internal staff members. NMCSD will roll this process out to include external users in the near future.

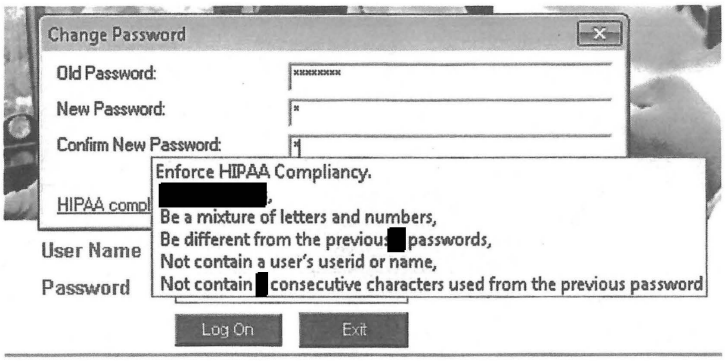
2. Recommendation 3

Concur: NMCSD agrees, however the site CIO does not have the resources to and enterprise level support to consistently meet this requirement. To address these issues, NMCSD is hiring new Cybersecurity staff.

3. Point of contact: [redacted] or [redacted].

Enclosure (2)

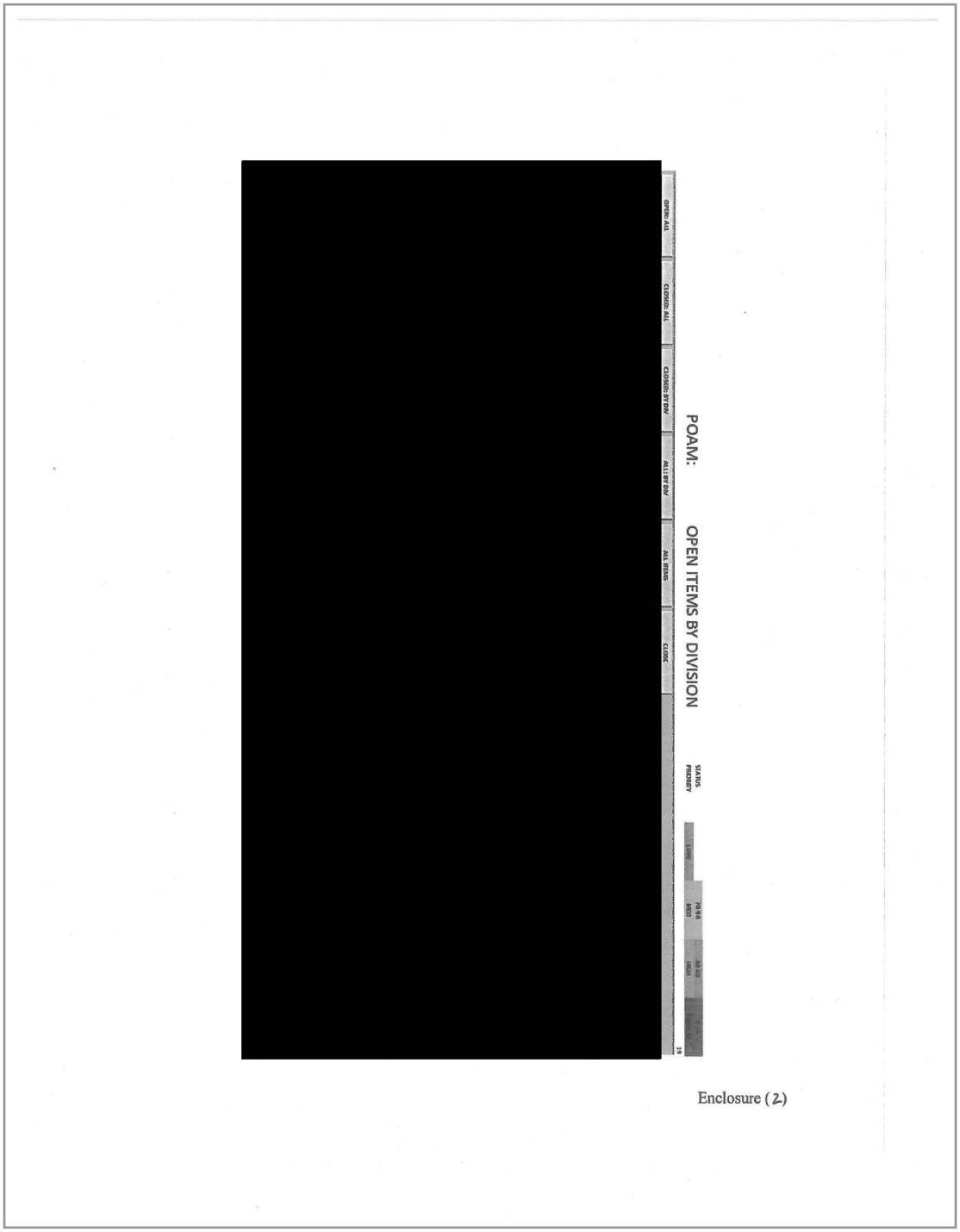
Navy Bureau of Medicine and Surgery (cont'd)



Note: Those password requirements are not enforced within the management

Enclosure (1)

Navy Bureau of Medicine and Surgery (cont'd)



Navy Bureau of Medicine and Surgery (cont'd)

NHCP INFORMATION MANAGEMENT DEPARTMENT

PERSONAL DATA – PRIVACY ACT OF 1974 (PL 93-579)
Account will be deactivated after 30 days of inactivity
Highlighted Fields must be filled out in order for form to be processed*

THIS SECTION TO BE COMPLETED BY THE USER/CUSTOMER (Incomplete forms delays the process)

LAST NAME:	FIRST NAME:	MI:	GENDER	Full SSN #:	DOB:
				- -	/ /

PRIMARY ASSIGNED CLINIC/LOCATION (i.e. CP Radiology, 13 Area, etc..) SECONDARY CLINIC:	POSITION/TITLE/ROLE:
WORK TELEPHONE #:	RANK/GRADE: / PRD: / / / Former Command:
GOVERNMENT EMAIL ONLY: (mail.mil/usmc.mil)	FORMER NAME:

Certificate Required — **REQUIRED TRAINING AND FORMS FOR EACH ACCOUNT[S]** — Certificate Required

~Network: Cyber Awareness (JKO) training: https://jkodirect.iten.mil/Atlas2/page/login/Login.jsf > Current Version
- SAAR-N Form (MUST BE COMPLETED BY USER AND SIGNED BY SECURITY ON PART 3 OF FORM) Location: 4th Floor—Room: 4156

~ HIPAA Training can be completed at portal Website: https://jkodirect.iten.mil/Atlas2/page/login/ > Course #: DHA-US001
- Questions? Contact Education & Training at (760)725-1408 / Location: 4th Floor

~ CHCS Managed Care Program I & II > https://jko.iten.mil/mhs > Course #: DHA-US003 & DHA-US004 > Not Required for Privileged Providers or IDCs.
- In-Patient personnel and/or Nurses: Only if Requiring Scheduling Keys/Menus.

THIS SECTION TO BE COMPLETED BY YOUR DEPARTMENT-HEAD/CLINIC SUPERVISOR

Default Clinic Location:_____ Request to: ☐ New Check-In ☐ Re-Activate account ☐ Dept. Transfer

Identify Clinical Systems Needed:	User Role:	Other Roles:
☐ AHLTA	☐ Provider	☐ Medical Student
☐ CHCS	- Specialty:_____	- Specialty:_____
☐ ESSENTRIS	☐ IDC (Must submit Page 13)	☐ PSI
☐ HAIMS	☐ Nurse	☐ Resident: [Circle One: 1st—2nd—3rd—4th YEAR]
☐ McKesson/Dinpacs-Radiology/PeerVue	☐ Corpsman	☐ Reservist
☐ Dinpacs—Cardiology	☐ Clerk/MSA	☐ TAD - Date(s):_____
☐ Laboratory Access Type:_____	☐ Administrative	☐ Other:_____
☐ Radiology Access Type:_____	Type:_____	
☐ Pharmacy Access Type:_____		

Department-Head/Supervisor Signature:
DH/Supervisor Name (Print):_____
Signature:_____
Date Signed:_____

** Dinpacs/McKesson access > Please check-in at the Radiology Department**

CREDENTIALING OFFICE USE ONLY: (Privileged Providers, Residents, Nurses ONLY!) > Medical Services—4th Floor—RM: 4171

Credentialing Office Use Only:

☐ Privileged / Expiration:_____
☐ DEA#_____
☐ License#:_____
☐ NPI #:_____
☐ Nurse
[x] Provider Specialty Code:_____

NHCP Credentialing:
Hours: 0700-1130 / 1300—1600
T: (760) 719-3621 / 3185 / 3621

Greenside Credentialing:
(Off Site)
T: (760) 725-3213
POC: Jesus Cerritos

Credentialing Signature:
MSS Staff - Name (Print):_____
Signature:_____
Date Signed:____/____/____

I hereby, acknowledge that I am responsible for the password I will/have receive(d) and that I will not divulge it to any other person. If it is found that I have willingly divulged my clinical systems username and password, my clinical systems accounts will be locked/deleted pending a review by Department Head/Supervisor, Chief Information Officer and the Commanding Officer. In compliance with the ADP Security procedures, it is imperative that each user set the initial VERIFY code immediately. VERIFY Codes/Passwords are secure to each individual user and are not to be written and not to be shared with ANYONE. Proof of valid HIPAA Training at MHS Learn portal, DoD IAA Training and DoD PII Training from NKO/JKO websites are mandatory per direction of BUMED and DON MTF Commanding Officer. Users who do not comply with these security procedures are subject to deactivation from any Medical system.

Privacy Act Statement
This document may contain information covered under the Privacy Act, 5 USC 522(a), and/or the Health Insurance Portability and Accountability Act (PL104-191) and its various implementing regulations and must be protected in accordance with those provisions.

USER'S SIGNATURE:_____ DATE:_____/_____/_____

SEE REVERSE SIDE FOR ADDITIONAL

ENCLOSURE (3-1)

Navy Bureau of Medicine and Surgery (cont'd)

THIS SECTION TO BE COMPLETED BY NETWORKING DEPARTMENT

By signing below, I acknowledge that the customer has presented their SAAR-N form (Completed) and Cyber Awareness certificate for access to Naval Hospital Camp Pendleton's networking system.

Name of Network Staff (Print):_____

Date Account Created/Verified:_____/_____/_____ Signature of Network Staff:_____

THIS SECTION TO BE COMPLETED BY CLINICAL SYSTEMS ADMINISTRATORS

AHLTA/CHCS

CHCS Managed Care I & II Presented: ☐YES ☐NO (Only if needed)

HIPAA Certificate Presented: ☐YES ☐NO

Date Account(s) Created:_____/_____/_____ Administrator Name (Print):_____

Administrator Signature: _____

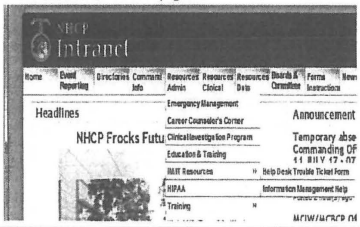
HAIMS

In order to gain HAIMS access via AHLTA. An account is required to be created via the following link:

https://balboa.haims.mhsi.health.mil/Login/Default.aspx?ReturnUrl=%2fdefault.aspx

- Save the username provided and then submit an IMD/MID trouble ticket via the NHCP intranet page at:

https://cpen-vm-s3.nmed.ds.med.navy.mil/ > > > > > > > > > >



Instructions are provided via the following link:

https://cpen-vm-spwas/dfa/mid/cls/default.aspx

or

- Can be picked up at MID by one of AHLTA/CHCS Administrators

  MID > Room: 2506

ENCLOSURE (7-2)

Navy Bureau of Medicine and Surgery (cont'd)

FOR OFFICIAL USE ONLY WHEN FILLED

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

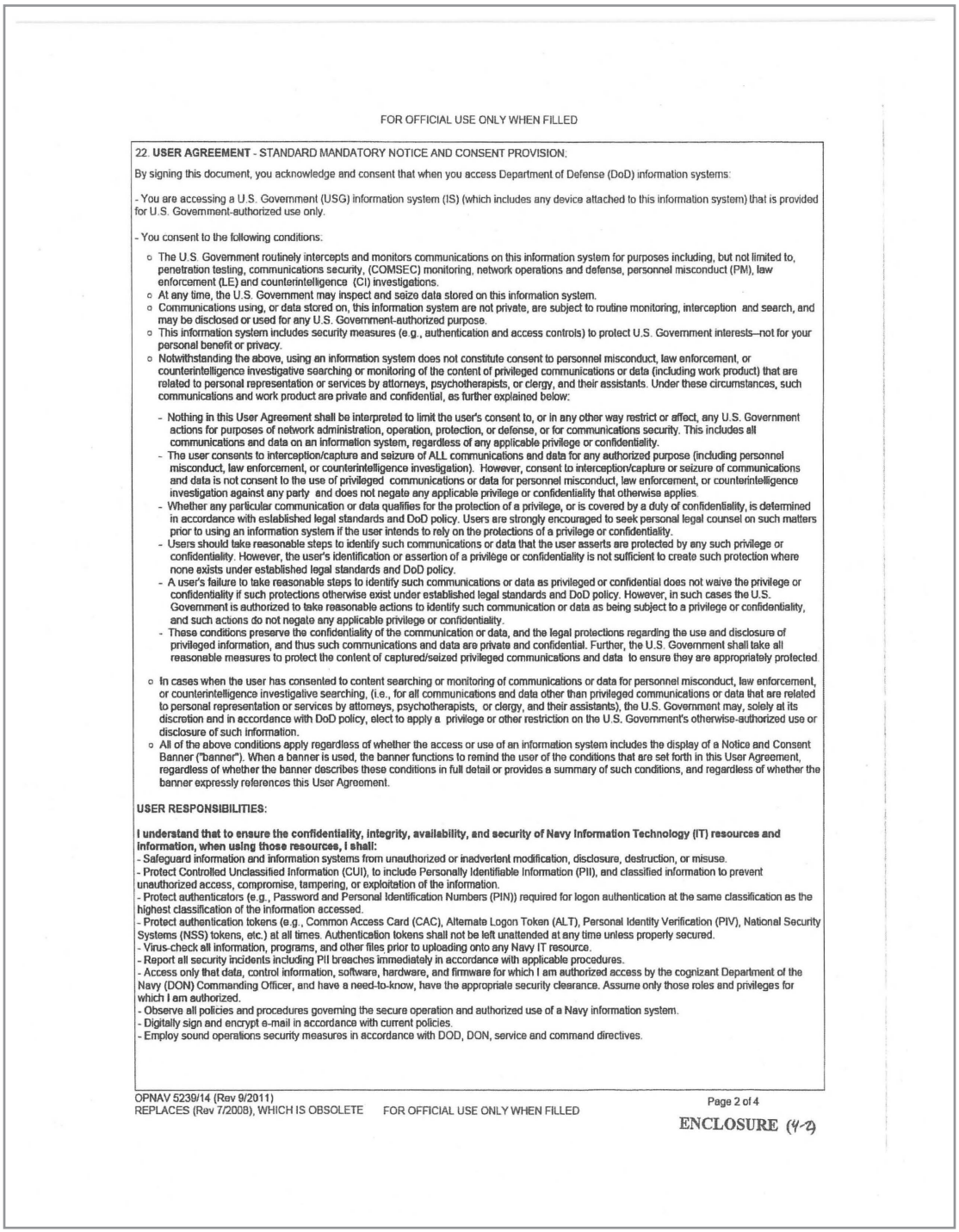
AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; and System of Records Notice: NM0500-2 Program Management and Locator System.
PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.
ROUNTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: ☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID _____	DATE *(DDMMMYYYY)*:
SYSTEM NAME *(Platform or Application)*:	LOCATION *(Physical Location of System)*:
PART I ***(To be completed by Requester)***	
1. NAME *(Last, First, Middle Initial)*:	2. ORGANIZATION: US Navy
3. OFFICE SYMBOL/DEPARTMENT:	4. PHONE *(DSN and Commercial)*: DSN: COM:
5. OFFICIAL E-MAIL ADDRESS:	6. JOB TITLE AND GRADE/RANK:
7. OFFICIAL MAILING ADDRESS:	8. CITIZENSHIP: ☐ US ☐ FN ☐ LN ☐ Other _____ / 9. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR
10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS *(Complete as required for user or functional level access.)*. ☒ I have completed Annual IA Awareness Training.	DATE *(DDMMMYYYY)*:
PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 14a).	
11. JUSTIFICATION FOR ACCESS: [ ] Access to computer via NHCP Network [ ] Access to CHCS/AHLTA Clinical System [ ] Access to Essentris Clinical System [ ] Access to the McKesson PACS System [ ] Others - please specify _____	
12. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED ☐ PRIVILEGED	12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form. / DATE SIGNED *(DDMMMYYYY)*:
13. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED ☐ CLASSIFIED *(Specify Category)*: _____ ☐ OTHER: _____	
14. VERIFICATION OF NEED TO KNOW: I certify that this user requires access as requested. ☒	14a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date)*:
15. SUPERVISOR'S ORGANIZATION/DEPARTMENT:	15a. SUPERVISOR'S E-MAIL ADDRESS: / 15b. PHONE NUMBER:
16. SUPERVISOR'S NAME *(Print Name)*:	16a. SUPERVISOR'S SIGNATURE / 16b. DATE *(DDMMMYYYY)*:
17. SIGNATURE OF INFORMATION OWNER/OPR:	17a. PHONE NUMBER: / 17b. DATE *(DDMMMYYYY)*:
18. SIGNATURE OF IAM OR APPOINTEE:	19. ORGANIZATION/DEPARTMENT: / 20. PHONE NUMBER: / 21. DATE *(DDMMMYYYY)*:

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED Page 1 of 1

ENCLOSURE (4-1)

Navy Bureau of Medicine and Surgery (cont'd)



FOR OFFICIAL USE ONLY WHEN FILLED

22. **USER AGREEMENT** - STANDARD MANDATORY NOTICE AND CONSENT PROVISION:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:

  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security, (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and seize data stored on this information system.
  - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception and search, and may be disclosed or used for any U.S. Government-authorized purpose.
  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

    - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
    - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
    - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
    - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
    - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
    - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

  - In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
  - All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

USER RESPONSIBILITIES:

I understand that to ensure the confidentiality, integrity, availability, and security of Navy Information Technology (IT) resources and information, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
- Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.
- Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.
- Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents including PII breaches immediately in accordance with applicable procedures.
- Access only that data, control information, software, hardware, and firmware for which I am authorized access by the cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.
- Observe all policies and procedures governing the secure operation and authorized use of a Navy information system.
- Digitally sign and encrypt e-mail in accordance with current policies.
- Employ sound operations security measures in accordance with DOD, DON, service and command directives.

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED

Page 2 of 4

ENCLOSURE (4-2)

Navy Bureau of Medicine and Surgery (cont'd)

FOR OFFICIAL USE ONLY WHEN FILLED

(Block 22 Cont)

I further understand that, when using Navy IT resources, I shall not:
- Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g., .com).
- Bypass, stress, or test IA or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
- Relocate or change equipment or the network connectivity of equipment without authorization from the Local IA Authority (i.e., person responsible for the overall implementation of IA at the command level).
- Use personally owned hardware, software, shareware, or public domain software without written authorization from the Local IA Authority.
- Upload/download executable files (e.g., exe, .com, .vbs, or .bat) onto Navy IT resources without the written approval of the Local IA Authority.
- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
- Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information and PII, and other uses that are incompatible with public service.
- Place data onto Navy IT resources possessing insufficient security controls to protect that data at the required classification (e.g., Secret onto Unclassified).

23. NAME *(Last, First, Middle Initial)*:	24. USER SIGNATURE:	25. DATE SIGNED *(DDMMMYYYY)*:

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

26. TYPE OF INVESTIGATION:		26a. DATE OF INVESTIGATION *(DDMMMYYYY)*:	
26b. CLEARANCE LEVEL:		26c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☐ LEVEL III	
27. VERIFIED BY *(Print name)*:	28. SECURITY MANAGER TELEPHONE NUMBER:	29. SECURITY MANAGER SIGNATURE:	30. DATE *(DDMMMYYYY)*:

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

31. TITLE:	31a. SYSTEM:	31b. ACCOUNT CODE:
	31c. DOMAIN:	
	31d. SERVER:	
	31e. APPLICATION:	
	31h. DATASETS:	
	31f. DIRECTORIES:	
	31g. FILES:	
32. DATE PROCESSED *(DDMMMYYYY)*:	32a. PROCESSED BY:	32b. DATE *(DDMMMYYYY)*:
33. DATE REVALIDATED *(DDMMMYYYY)*:	33a. REVALIDATED BY:	33b. DATE *(DDMMMYYYY)*:

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED

Page 3 of 4

ENCLOSURE (4-3)

Navy Bureau of Medicine and Surgery (cont'd)

FOR OFFICIAL USE ONLY WHEN FILLED

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing or modifying their USER IDENTIFICATION (ID).

(1) Name. The last name, first name, and middle initial of the user.
(2) Organization. The user's current organization (i.e., USS xx, DoD, and government agency or commercial firm).
(3) Office Symbol/Department. The office symbol within the current organization (i.e., SDI).
(4) Telephone Number/DSN. The Defense Switching Network (DSN) and commercial phone number of the user.
(5) Official E-mail Address. The user's official e-mail address.
(6) Job Title/Grade/Rank. The civilian job title (i.e., Systems Analyst YA-02, military rank (CAPT, United States Navy) or "CONT" if user is a contractor.
(7) Official Mailing Address. The user's official mailing address.
(8) Citizenship (United States (US), Foreign National (FN), Local National (LN), or Other). Identify appropriate citizenship in accordance with (IAW) SECNAV M-5510.30.
(9) Designation of Person (Military, Civilian, Contractor).
(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date of completion.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(11) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
(12) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters or settings.)
(12a) If Block 12 is Privileged, user must sign a Privilege Access Agreement form. Enter date of when Privilege Access Agreement (PAA) form was signed. Users can obtain a PAA form from the Information Assurance Manager (IAM) or Appointee.
(13) User Requires Access To. Place an "X" in the appropriate box. Specify category.
(14) Verification of Need to Know. To verify that the user requires access as requested.
(14a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
(15) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
(15a) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
(15b) Date. Date supervisor signs the form.
(16) Supervisor's Organization/Department. Supervisor's organization and department.
(16a) Official E-mail Address. Supervisor's e-mail address.
(16b) Phone Number. Supervisor's telephone number.
(17) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.
(17a) Phone Number. Functional appointee telephone number.
(17b) Date. The date the functional appointee signs the OPNAV 5239/14.
(18) Signature of Information Assurance Manager (IAM) or Appointee. Signature of the IAM or Appointee of the office responsible for approving access to the system being requested.
(19) Organization/Department. IAM's organization and department.
(20) Phone Number. IAM's telephone number.
(21) Date. The date the IAM signs the OPNAV 5239/14 form.
(22) Standard Mandatory Notice and Consent Provision and User Responsibilities. These items are in accordance with DoD Memo dtd May 9, 2008 (Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement) and DON CIO message Responsible and Effective Use of Dept of Navy Information Technology Resources" DTG 161108Z JUL 05.
(23) Name. The last name, first name, and middle initial of the user.
(24) User Signature. User must sign the OPNAV 5239/14 with the understanding that they are responsible and accountable for their password and access to the system(s). User shall digitally sign form. Pen and ink signature is acceptable for users that do not have a Common Access Card (CAC) or the ability to digitally sign the form.
(25) Date. Date signed.

C. PART III: Certification of Background Investigation or Clearance.

(26) Type of Investigation. The user's last type of background investigation (i.e., National Agency Check (NAC), National Agency Check with Inquiries (NACI), or Single Scope Background Investigation (SSBI)).
(26a) Date of Investigation. Date of last investigation.
(26b) Clearance Level. The user's current security clearance level (Secret or Top Secret).
(26c) Identify the user's IT designation level. If Block 12 is designated as "Authorized" then IT Level Designation is "Level III". If Block 12 is designated as "Privileged" then IT Level Designation is "Level I or II" based on SECNAV M-5510.30 dtd June 2006.
(27) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
(28) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.
(29) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.
(30) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the functional activity or the customer with approval from OPNAV. This information will specifically identify the access required by the user.

(31 - 33b). Fill in appropriate information.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed or mailed. If the completed form is transmitted electronically, the e-mail must be digitally signed and encrypted.

FILING: Form is purposed to use digital signatures. Digitally signed forms must be stored electronically to retain non-repudiation of electronic signature. If pen and ink signature must be applied, original signed form must be retained. Retention of this form shall be IAW SECNAV Manual M-5210.1, Records Management Manual. Form may be maintained by the Navy, the user's IAM, and/or Security Manager. Completed forms contain Personal Identifiable Information (PII) and must be protected as such.

OPNAV 5239/14 (Rev 9/2011)
REPLACES (Rev 7/2008), WHICH IS OBSOLETE FOR OFFICIAL USE ONLY WHEN FILLED

Page 4 of 4

ENCLOSURE (4-4)

Navy Bureau of Medicine and Surgery (cont'd)

From: Privacy Program Office, U.S. Navy Bureau of Medicine and Surgery
To: Chief Information Officer, U.S. Navy Bureau of Medicine and Surgery (BUMED)

Subj: RESPONSE: DOD OFFICE OF INSPECTOR GENERAL DRAFT REPORT, "PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES"

1. M311 Privacy Office has reviewed the DOD IG Audit D2017-D000RC-0113 and concurs with the recommendations outlined in recommendation (2) for Surgeon General and BUMED CIO; however, our response should include current actions and policies to manage items (b), (c) and (d).

2. Recommendation 2
(b) Recommend POA&M and incorporation into Management Internal Control Program.
(c) - BUMED M6 routinely validates the accuracy of inventory systems through annual data calls, BUMED/DHA Governance process and DITPR reviews.
(d) - Existing and new IT systems collecting, storing, or transmitting PII/PHI are evaluated for privacy impact assessment (PIA) requirements through governance, accreditation, and RMF/ATO process. Once a discrepancy between any of those processes or the inventory systems (eMASS and DITPR) are discovered, System Managers for those systems are directed to initiate a PIA.

3. The BUMED Privacy Office defers to the Regions and M6 concerning recommendations 1,3,4,5, and 6. These items should be considered for incorporation in the BUMED Management Internal Control Program as an Addressable Unit.

4. Point of Contact: [redacted], [redacted] or [redacted]

Enclosure (3)

Military Sealift Command

DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
471 EAST C STREET
NORFOLK VA 23511-2419

5000
Ser N02
8 Mar 18

From: Commander, Military Sealift Command
To: Inspector General, Department of Defense

Subj: RESPONSE TO DEPARTMENT OF DEFENSE INSPECTOR GENERAL DRAFT AUDIT REPORT – PROTECTION OF PATIENT HEALTH INFORMATION AT NAVY AND AIR FORCE MILITARY TREATMENT FACILITIES PROJECT NO. D2017-D000RC-0113.000

Ref: (a) DoD Draft Audit Report, Project No. D2017-D000RC-0113.000 of 30 Jan 18

Encl: (1) Military Sealift Command (MSC) Responses to the Findings and Recommendations contained in the subject report.

1. In response to reference (a), enclosure (1) provides MSC's responses to the recommendations included in the subject report.

2. Reference (a) requested a review of the report's markings. A Freedom Of Information Act (FOIA) review was completed and no exemptions were identified; however, the FOUO classification review is in progress and will be forwarded via separate correspondence.

3. We appreciate the opportunity to review and comment on the findings and recommendations. My point of contact for this document is [redacted], MSC Audit Liaison, who can be contacted at: [redacted].

J. A. CARTER
Chief of Staff

Military Sealift Command (cont'd)

DoDIG Report Project #D2017-D000RC-0113.000
PROTECTION OF PATIENT HEALTH INFORMATION
AT NAVY AND AIR FORCE
MILITARY TREATMENT FACILITIES

Recommendation #1 (a-i) Chief Information Officer, USNS Mercy:

a. Implement appropriate configuration changes to enforce the use of a Common Access Card to access all systems that process, store, and transmit patient health information, or obtain a waiver that exempts the system from using Common Access Cards.

Partially Concur. MERCY CIO does not have the administrative privileges to modify or develop new access methods. The USNS MERCY is unique in that it reports both through standard shipboard and Navy Medicine for Medical Treatment Facility (MTF) for Information Management/Information Technology (IM/IT) requirements. Space and Naval Warfare (SPAWAR) System Center Atlantic (SPAWAR) completed a requirements document in 2015 which delineates all program requirements, medical/non-medical applications, and the full range of all capabilities and requirements of the USNS MERCY (T-AH 19) to include the Memorandum of Understanding (MOU) between Naval Medical Center San Diego (NMCSD) and MTF MERCY. This MOU addresses IM/IT support for all medical applications to ensure compliance with governing policy and requirements.

Alternative Corrective Actions:
(1) In concert with BUMED, USNS MERCY CIO shall implement appropriate configuration changes as directed down by NMCSD to enforce CAC enabled configuration changes to include CHCS and CARESTREAM. Estimated Completion Date: **15 APRIL 2018**

(2) For medical application program in which SPAWAR is the program manager for Fleet medical applications to include AHLTA-T, Maritime Medical Modules, TC2 programs, MERCY CIO shall submit a request for CAC enabled configuration changes to these programs of record. Estimated Completion Date: **15 APRIL 2018**

b. Configure passwords for all systems that process, store, and transmit patient health information to meet DoD length and complexity requirements.

Concur. USNS MERCY will implement the requirement for a 15 character login requirement for [redacted], [redacted], [redacted] and [redacted] until PKI technology is available for these programs or DHA obtains a waiver. The 15 character passwords will include the requirement for one lower case, one upper case, one symbol and one number. Estimated Completion Date: **15 APRIL 2018**

c. Develop a Plan of Action and Milestones and take appropriate steps to mitigate known network vulnerabilities in a timely manner.

Concur. USNS MERCY and MSC N6 have developed plan of action and milestones in support of the NIPR authority to operate (ATO) process. Estimated Completion Date: **15 APRIL 2018**

1

Enclosure (1)

Military Sealift Command (cont'd)

DoDIG Report Project #D2017-D000RC-0113.000
PROTECTION OF PATIENT HEALTH INFORMATION
AT NAVY AND AIR FORCE
MILITARY TREATMENT FACILITIES

d. Require written justification for obtaining access to all systems that process, store, and transmit patient health information and implement procedures to grant access to the systems based on roles that align with user responsibilities.

Concur. All personnel assigned to MERCY are required to complete a SAAR-N access request form IAW SECNAVINST 5239.3C. The following corrective actions will be taken to implement this corrective recommendation:

(1) The USNS MERCY CIO shall revise their current standard operating procedure (SOP) to modify the SAAR-N form comments with different levels of access based on clinical and patient care needs. Estimated Completion Date: **15 APRIL 2018**

(2) The submitted SAAR-N form will be countersigned by the immediate supervisor to validate the access requirement. The documents shall be maintained on file until the service member is detached from the ship. Estimated Completion Date: **15 APRIL 2018**

(3) The USNS MERCY CIO will review and update the Individual Identification Authentication SOP defining the Individual identification authentication policy to ensure that DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user logon ID) and password. Estimated Completion Date: **15 APRIL 2018**

e. Configure all systems that process, store, and transmit patient health information to lock automatically after 15 minutes of inactivity.

Concur. USNS MERCY CIO shall validate that AHLTA-T, Carestream, Maritime Medical Modules and TC2 settings are in compliance with the locally to meet the 15 minute automatic log off requirement. Once the programs are validated and within compliance, a letter shall be submitted to the MERCY MTF Commanding Officer. Estimated Completion Date: **15 APRIL 2018**

f. Appropriately configure and regularly review system audit reports and logs to identify user and system activity anomalies.

Concur. USNS Mercy CIO shall revise SOPs and implement practices to meet recommendations found in the audit report for mitigating activity anomalies. This shall be achieved by implementing a monthly audit and submission of a report from the MERCY CIO to the Commanding Officer. Estimated Completion Date: **15 APRIL 2018**

g. Develop and maintain standard operating procedures for granting access, assigning and elevating privileges, and deactivating user access.

2

Enclosure (1)

Military Sealift Command (cont'd)

DoDIG Report Project #D2017-D000RC-0113.000
PROTECTION OF PATIENT HEALTH INFORMATION
AT NAVY AND AIR FORCE
MILITARY TREATMENT FACILITIES

Concur. USNS MERCY CIO shall review and modify existing SOP for granting access, assigning/elevating privileges, and revoking access. Estimated Completion Date: **15 APRIL 2018**

h. Review and identify all systems used to process, store, and transmit patient health information, develop a baseline of systems used at the military treatment facility, and regularly, at least annually, validate the accuracy of the inventory of systems.

Concur. MERCY has a list of systems that contain patient health information (PHI). MTF CO will submit an annual validation letter to COMSC. Estimated Completion Date: **15 APRIL 2018**

i. Develop and maintain access request forms for all users of systems that process, store, and transmit patient health information, and verify, at least annually, the continued need for system access.

Partially Concur. USNS MERCY maintains SAAR-N access forms on file. USNS Mercy CIO will modify their existing SOP to remove access to the system upon a service member's transfer from the command. In addition, USNS MERCY CIO will audit authorized users within system against the ship's manning roster within 30 days of return from deployment and monthly by the MERCY CIO to ensure accurate accountability for user access.

Recommendation #3: The Commander, USNS Mercy, review the performance of the Chief Information Officer and consider administrative action, as appropriate, for not following Federal and DoD guidance for protecting patient health information to include: not mitigating known vulnerabilities in a timely manner; not developing plans of action and milestones for unmitigated vulnerabilities; and not formally accepting risks for unmitigated vulnerabilities.

Non-Concur. The CIO performing the function during the audit is no longer employed as a contractor for USNS MERCY.

Alternative Action We Will Take to Correct the Finding: The implementation of corrective recommendations places a more defined process in place with more inherent checks and balances. These revised processes ensure oversight and accountability of the IM/IT program. Estimated Completion Date: **15 APRIL 2018**

Recommendation #4: Chief Information Officer, USNS Mercy, [redacted] and [redacted] for systems that process, store, and transmit patient health information.

Concur. The only program applicable is [redacted]. MERCY CIO shall submit to NMCSD a request to [redacted] for [redacted] which supports the teleradiology operating system. MST MTF Program

3

Enclosure (1)

Military Sealift Command (cont'd)

DoDIG Report Project #D2017-D000RC-0113.000
PROTECTION OF PATIENT HEALTH INFORMATION
AT NAVY AND AIR FORCE
MILITARY TREATMENT FACILITIES

Manager is actively seeking Navy Medical Logistics Command (NMLC) assistance to either correct [redacted] or replace this system. Estimated Completion Date: **15 APRIL 2018**

Recommendation #6: The Commander, USNS Mercy, implement physical access controls to identify and record the names of personnel and the times when personnel accessed a patient's paper medical records, and regularly, at least monthly, reconcile the logs against the list of authorized personnel with access to area.

Concur. USNS MERCY CIO shall develop an internal SOP that addresses the security and access to the health records. Specific areas to address are the physical security to comply with a two lock system (space access door and health records file cabinets). Sickcall will ensure a NAVMED 6150/7 health record custody card shall be utilized to document health record accountability and auditing compliance. In addition, Sickcall will implement a sign out / in log for every health record requested. NAVMED 6150/7 health record custody cards will be reconciled against the check-out log on a monthly basis to ensure 100% accountability.

4

Enclosure (1)

Acronyms and Abbreviations

AFMS	Air Force Medical Service
AHLTA	Armed Forces Health Longitudinal Technology Application
AHLTA-T	Armed Forces Health Longitudinal Technology Application-Theater
BMBB/TS	Blood Management Blood Bank/Transfusion Service
BUMED	Navy Bureau of Medicine and Surgery
CAC	Common Access Card
CHCS	Composite Health Care System
CIO	Chief Information Officer
DHA	Defense Health Agency
EHR	Electronic Health Record
Essentris	Clinical Information System/Essentris Inpatient System
HAIMS	Health Artifact and Imaging Management Solution
HIPAA	Health Insurance Portability and Accountability Act
Innovian	Draeger Innovian Anesthesia
MHS	Military Health System
MTF	Military Treatment Facility
PACS	Picture Archiving and Communication System
PIA	Privacy Impact Assessment
PHI	Patient Health Information
POA&M	Plan of Action and Milestones
SOP	Standard Operating Procedure
TC2	Theater Medical Information Program CHCS Cache System

Glossary

Audit Logs. A system-generated record of system activities performed in a given period.

Authentication. A process that verifies the identity of a user and is a prerequisite to allowing access to an information system.

Category I Vulnerability. Any vulnerability, if exploited, that would directly and immediately result in the loss of confidentiality, availability, or integrity of data.

Category II Vulnerability. Any vulnerability, if exploited, that could result in the loss of confidentiality, availability, or integrity of data.

Common Access Card (CAC). Identification card with a microchip that provides access to DoD computer networks and systems for Government employees and eligible contractor personnel.

Covered Entities. As defined by HIPAA, are (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit health-related information for transactions covered by Department of Health and Human Services standards.

Critical Vulnerabilities. If exploited, would likely result in privileged access to servers and information systems and, therefore, would require immediate patches.

Data at Rest. Information that resides or is stored on systems or electronic media such as compact discs.

Data in Transit. Information transferred from one system or network to another.

Deactivated Access. Prevents users from accessing a system but does not remove the user or information entered by the user from the system.

Healthcare Business Associate. An organization that assists covered entities in performing healthcare activities and functions.

High Vulnerabilities. If exploited, could result in obtaining elevated privileges, significant data loss, and network downtime.

Information Assurance. Processes and controls that protect and defend the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems.

Information Assurance Vulnerability Alerts. Notifications that are generated when vulnerabilities may result in an immediate and potentially severe threat to DoD systems and information, requiring corrective actions based on the severity of the risk.

Least privilege. A security objective requiring access needed only to perform official duties.

Nonprivileged User. A user not authorized to perform security-related functions.

Patch. An update to an operating system, application, or other software issued to correct specific problems.

Patient Health Information (PHI). Information created or obtained by a covered entity for an individual related to the past, present, or future physical or mental health or condition of an individual; the information can be used to identify the individual.

Privacy Impact Assessment (PIA). A written analysis of potential privacy risks and mitigating actions.

Public Key Infrastructure. Typically used to verify signatures or encrypt data.

Standard Operating Procedure (SOP). Written and detailed instructions that document a repetitive activity to perform specific functions uniformly and serve as a vital tool to transfer knowledge.

Token. Used to authenticate a user's identity.

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/.

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098