Report No. DODIG-2017-085

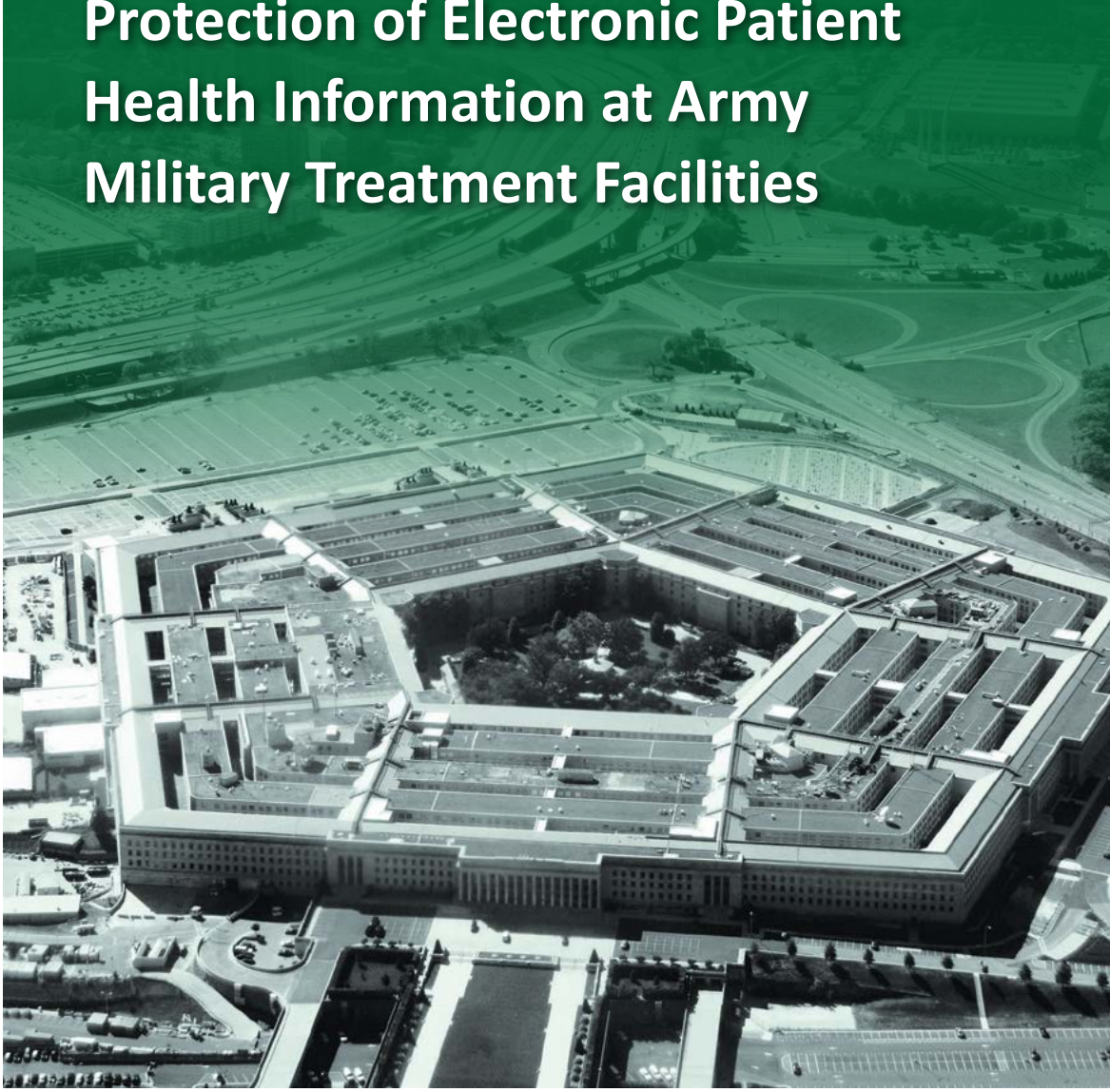
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

JULY 6, 2017

Protection of Electronic Patient Health Information at Army Military Treatment Facilities



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~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.

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

Results in Brief

Protection of Electronic Patient Health Information at Army Military Treatment Facilities

July 6, 2017

Objective

We determined whether the Army designed and implemented effective security protocols to protect electronic health records (EHRs)[1] and individually identifiable health information (patient health information) from unauthorized access and disclosure.

Background

We selected a nonstatistical sample of 3 of the 71 Army military treatment facilities (MTFs) within the scope of this audit to visit. Specifically, we visited two facilities in the Army's Regional Health Command-Central–Brooke Army Medical Center, Fort Sam Houston, Texas, and Evans Army Community Hospital, Fort Carson, Colorado, and one in the Regional Health Command–Atlantic–Kimbrough Ambulatory Care Center, Fort Meade, Maryland. We reviewed three DoD EHR systems, and seven Army-specific systems at the three locations.

Findings

Defense Health Agency (DHA) and Army officials did not consistently implement effective security protocols to protect systems that stored, processed, and transmitted EHRs and electronic patient health information. Specifically, they did not:

- enforce the use of Common Access Cards (identification cards with microchips) because of compatibility issues or ease of access by multiple users; and

[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.

Findings (cont'd)

- comply with DoD password complexity requirements because system administrators considered existing authentication requirements sufficient (authentication is a process to verify a user's identity).

In addition, the Brooke Army Medical Center, Evans Army Community Hospital, and Kimbrough Ambulatory Care Center did not:

- mitigate known vulnerabilities affecting Army networks because MTF Chief Information Officers (CIOs) stated that implementing patches could limit system availability;
- [redacted] for systems that contained patient health information because the [redacted] could slow system availability;
- grant user access to three DoD EHR and four Army-specific systems based on the user's assigned duties because they did not align user responsibilities to specific system roles;
- configure two DoD EHR and five Army-specific systems to automatically lock after 15 minutes of inactivity because the MTF CIOs did not want to limit system availability during interactions with patients;
- consistently review system activity logs to identify unusual or suspicious activities and access because the MTF CIOs did not dedicate resources to perform the task or properly configure the systems to generate audit logs; and
- develop standard operating procedures to manage system access because they did not consider documented procedures necessary.

Officials from the U.S. Army Medical Command and the MTFs also were not aware of all Army-specific systems operating on their networks that stored, processed, and transmitted patient health information because U.S. Army Medical Command officials did not require MTFs to identify systems that contained patient health information. Furthermore, the DHA CIO did not develop a privacy impact assessment

Results in Brief

Protection of Electronic Patient Health Information at Army Military Treatment Facilities

Findings (cont'd)

for the Comed Anatomic Pathology System (laboratory system) because he thought the assessment was conducted as part of the privacy impact assessment for another system.

Without well-defined and effectively implemented security protocols, the DHA and Army unnecessarily introduced risks that could compromise the integrity, confidentiality, and availability of patient health information. Security protocols, when not applied or ineffective, increase the risk of cyber attacks, system and data breaches, data loss or manipulation, and unauthorized disclosures of patient health information. In addition, ineffective security protocols that result in a Health Insurance Portability and Accountability Act[2] violation could cost MTFs up to $1.5 million per year in penalties for each category of violation.

Recommendations

We recommend, among other recommendations, that the CIOs for DHA, U.S. Army Medical Command, and MTFs:

- implement configuration changes to enforce the use of Common Access Cards when accessing DoD EHR systems and Army-specific systems;
- configure passwords for the DoD EHR systems and Army-specific systems to meet DoD complexity requirements; and
- [redacted] on all systems that contain patient health information.

In addition, we recommend that the CIOs for the U.S. Army Medical Command and MTFs review all systems used to process, store, and transmit patient health information, develop a baseline of systems used at each MTF, and regularly validate the accuracy of the inventory of Army-specific systems. We also recommend that the MTF CIOs:

- develop a plan of action and milestones and take appropriate and timely steps to mitigate known network vulnerabilities;
- implement procedures to grant access to DoD EHR systems and Army-specific systems based on roles that align with user responsibilities;
- configure all Army-specific systems to automatically lock after 15 minutes of inactivity;
- appropriately configure and regularly review system audit logs to identify user and system activity anomalies; and
- develop standard operating procedures for granting access, assigning and elevating privileges, and deactivating user access.

Furthermore, we recommend that the MTF Commanders review the performance of their CIOs, and consider administrative action, as appropriate, for not following Federal and DoD guidance for protecting patient health information.

Management Comments and Our Response

The Director, DHA, agreed to coordinate with the Service Surgeons General to enforce Common Access Card usage. Therefore, the recommendation to implement configuration changes to enforce the use of Common Access Cards when accessing DoD EHR systems is resolved. We will close the recommendation once we obtain documentation that shows DHA implemented a

[2] The Health Insurance Portability and Accountability Act of 1996 requires covered entities to implement administrative, technical, and physical safeguards to protect the integrity and confidentiality of patient health information from unauthorized use or disclosure.

Results in Brief

Protection of Electronic Patient Health Information at Army Military Treatment Facilities

Comments (cont'd)

Common Access Card solution for one DoD EHR system and global security policies or system configuration settings that show the Service Surgeons General enforced Common Access Card usage for the other two DoD EHR systems.

The Chief of Staff, U.S. Army Medical Command, agreed to coordinate with DHA to enforce Common Access Card usage and password complexity requirements, mitigate network vulnerabilities, [redacted] control system access and privileges, implement automatic system lockout procedures, and configure and review audit logs. In addition, the Chief of Staff agreed to complete a baseline of Army-specific systems that process, store, and transmit Patient Health Information, and that the U.S. Army Medical Command would validate its inventory at least annually. Therefore, the recommendations are resolved. We will close the recommendations once we obtain:

- U.S. Army Medical Command's plan describing how it will ensure the MTFs use Common Access Cards to access systems with patient health information and comply with DoD password complexity requirements;
- global security policies or system configuration settings that show MTFs used Common Access Cards to access DoD EHR systems and Brooke Army Medical Center used Common Access Cards to access the Mammography Reporting System, complied with DoD password complexity requirements, [redacted] automatically locked systems after defined periods of inactivity or documented risk acceptance, and configured audits logs to identify anomalous activity;
- vulnerability scans that show the MTFs mitigated known vulnerabilities;
- written procedures that show how MTFs will manage system access, to include requiring written justification to support the need for system access and specific privileges; and
- a documented baseline of systems used by MTFs to process, store, and transmit patient health information.

However, the Director, DHA, and the Chief of Staff, U.S. Army Medical Command, partially addressed the specifics of the recommendations to:

- ensure MTFs configured the three EHR systems to meet DoD password complexity requirements;
- [redacted] or obtain a current waiver exempting [redacted] for one EHR system;
- implement procedures to ensure DHA develops privacy impact assessments for all systems that store, process, and transmit patient health information; and
- review the performance of CIOs and consider administrative action for not following Federal and DoD guidance for protecting patient health information.

Because the Director and the Chief of Staff did not fully address the specifics of those recommendations, the recommendations are unresolved. The Director, DHA, and the Chief of Staff, U.S. Army Medical Command, should provide comments to the final report by August 4, 2017. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, Health Information Technology, Defense Health Agency	1.b, 1.c, 1.d	1.a	
Commander, Brooke Army Medical Center	4		
Commander, Evans Army Community Hospital	4		
Commander, Kimbrough Ambulatory Care Center	4		
Chief Information Officer, U.S. Army Medical Command, Department of the Army		2.a, 2.b, 2.c	
Chief Information Officer, Kimbrough Ambulatory Care Center		3.a, 3.b, 3.c, 3.d, 3.e, 3.f, 3.g, 3.h, 3.i, 5	
Chief Information Officer, Brooke Army Medical Center		3.a, 3.b, 3.c, 3.d, 3.e, 3.f, 3.g, 3.h, 3.i, 6	
Chief Information Officer, Evans Army Community Hospital		3.a, 3.b, 3.c, 3.d, 3.e, 3.f, 3.g, 3.h, 3.i	

Please provide Management Comments by August 4, 2017.

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

July 6, 2017

MEMORANDUM FOR DIRECTOR, DEFENSE HEALTH AGENCY
COMMANDING GENERAL, U.S. ARMY MEDICAL COMMAND
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Protection of Electronic Patient Health Information at Army Military Treatment Facilities (Report No. DODIG-2017-085)

We are providing this report for review and comment. The Defense Health Agency, the U.S. Army Medical Command, and the Army military treatment facilities did not consistently implement effective security protocols to protect systems that stored, processed, and transmitted electronic health records and electronic patient health information. Ineffective security protocols introduced unnecessary risk that could compromise the integrity, confidentiality, and availability of patient health information and result in up to $1.5 million per year in penalties for each category of Health Insurance Portability and Accountability Act of 1996 violations. We conducted this audit in accordance with generally accepted government auditing standards.

We considered comments from the Director, Defense Health Agency, and the Chief of Staff, U.S. Army Medical Command, when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Director, Defense Health Agency, to Recommendation 1.a and comments from the Chief of Staff, U.S. Army Medical Command, to Recommendations 2.a, 2.b, 2.c, 3.a, 3.b, 3.c, 3.d, 3.e, 3.f, 3.g, 3.h, 3.i, 5, and 6 addressed all specifics of the recommendations and conformed to the requirements of DoD Instruction 7650.03.

Comments from the Director, Defense Health Agency, to Recommendations 1.b, 1.c, and 1.d and comments from the Chief of Staff, U.S. Army Medical Command, to Recommendation 4 only partially addressed the specifics of the recommendations. Therefore, those recommendations are unresolved. The Director, Defense Health Agency, and the Chief of Staff, U.S. Army Medical Command, should provide additional comments on Recommendations 1.b, 1.c, 1.d, and 4, respectively, by August 4, 2017.

Please send a PDF file containing your comments to audrco@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
Readiness and Cyber Operations

Contents

Introduction

Objective

Our audit objective was to determine whether the Army designed and implemented effective security protocols to protect electronic health records (EHRs) and individually identifiable health information (patient health information [PHI])[3] from unauthorized access and disclosure. For this audit, we focused on Army medical centers, hospitals, and clinics. See the Appendix for a discussion on the scope and methodology, and prior audit coverage.

We selected a nonstatistical sample of 3 of the 71 Army military treatment facilities (MTFs) to visit within the scope of this audit. We reviewed three DoD EHR systems, and seven Army-specific systems at the three locations.

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.

On August 21, 1996, Congress passed Public Law 104-191, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA)," requiring covered entities[4] to implement administrative, technical, and physical safeguards to protect the integrity and confidentiality of PHI from unauthorized use or disclosure. HIPAA includes provisions for securing electronic PHI to provide patients assurance on the integrity, confidentiality, and availability of their personal information. If the provisions are violated, covered entities could be fined up to $1.5 million a year per violation category.[5] 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.

[3] PHI is medical information that is obtained by medical personnel related to the physical or mental health or condition of a patient.

[4] 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.

[5] 42 U.S. Code § 1320d-5 describes four categories related to HIPAA violations that covered entities (1) were unaware of, (2) should have been aware of, (3) willfully neglected but addressed timely, and (4) willfully neglected and not addressed timely.

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, which includes transferring and securing medical records and ensuring privacy of medical, health, and other sensitive information. The DoD Military Health System provides medical and dental services to about 9.4 million beneficiaries at more than 673 MTFs,[6] including 55 military hospitals and 373 military medical clinics worldwide. The Defense Health Agency (DHA) supports the delivery of health services to Military Health System beneficiaries and manages the systems that process, store, or transmit EHRs and other PHI. Specifically, DHA manages the following DoD legacy[7] EHR systems used by healthcare 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 Composite Health Care System (CHCS). An outpatient care system used to track appointments, order laboratory tests, authorize radiology procedures, and prescribe medications.
- 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.

U.S. Army Medical Command's Role in Protecting Health Information

The U.S. Army Medical Command (MEDCOM) provides sustained health services for about 4 million active duty members across the Military Services, including retirees and their family members, through 71 MTFs located worldwide. MEDCOM provides oversight of the MTFs and their networks and systems to ensure that they comply with Army and DoD information assurance[8] requirements. MEDCOM operations are managed through four major subordinate Regional Health Commands: the Regional Health Command–Atlantic in Fort Belvoir, Virginia; Regional Health Command-Central in San Antonio, Texas; the Regional Health Command-Europe in Sembach, Germany; and the Regional Health Command–Pacific in Honolulu, Hawaii.

[6] A facility established to provide medical and dental care to eligible individuals. Under HIPAA, MTFs are included in the health plans and health care provider categories.

[7] Medical Health System GENESIS will eventually replace the three legacy EHR systems. After several delays, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics expects to begin fielding Medical Health System GENESIS in FY 2017. Medical Health System GENESIS is not expected to be fully operational until FY 2022. Sites will continue to use CHCS, AHLTA, and Essentris for at least a year after Medical Health System GENESIS is operational.

[8] Information assurance is processes and controls that protect and defend the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems.

Army Medical Treatment Facilities and Systems Reviewed

The Army MTFs use DoD EHR systems and other systems managed by the Army to process, store, and transmit electronic PHI.[9] For this audit, we visited two facilities in the Army's Regional Health Command-Central–Brooke Army Medical Center (Brooke), Fort Sam Houston, Texas, and Evans Army Community Hospital (Evans), Fort Carson, Colorado, and one in the Regional Health Command-Atlantic–Kimbrough Ambulatory Care Center (Kimbrough), Fort Meade, Maryland. In addition to the three DoD EHR systems, Brooke, Evans, and Kimbrough used other Army-specific systems to process, store, and transmit electronic PHI. Table 1 describes the Army-specific systems used at each MTF that were included in the audit scope.

Table 1. Army-Specific Systems Used at Each MTF Visited

System Name	System Description
Coagulation Clinic Web Application	The application provides critical long-term tracking of patients receiving anti-coagulation therapy.
Comed Anatomic Pathology System (CoPath)	The system allows users to enter patient data, pathology orders, and results, and generates procedure worklists and result reports.
Exit Writer	The program provides tools for writing and reconciling electronically issued prescriptions.
High Interest Patient Database (HIP)	The database documents the care and risk management procedures of complex patients, which includes patients with suicidal and homicidal tendencies as well as patients with mental health issues.
Mammography Reporting System (MRS)	The system documents and communicates mammography results to patients.
Picture and Archiving Communications System (PACS)	The system provides radiologists access to radiology exam images regardless of their physical location.
Surgery Scheduling System	The system is used for scheduling and managing operating room assignments.

Guidance on Protecting Patient Health Information

Federal, DoD, and Army guidance prescribes requirements to protect systems that store, process, 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). Requires covered entities to implement administrative, technical, and physical safeguards to protect the integrity and confidentiality of PHI from unauthorized use or disclosure.

[9] Electronic PHI is a subset of health information used to identify an individual and is transmitted by or maintained in electronic media.

- *DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Healthcare Programs," August 12, 2015.* Implements information security policy requirements by establishing policy and assigning responsibilities for covered entities to protect PHI that is created, received, maintained, or transmitted electronically.
- *DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003.* Requires covered entities to protect personally identifiable health information.
- *National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.* 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[10] requirements. The guidelines apply to all components of an information system that process, store, or transmit Federal information.
- *Army Regulation 25-2, "Information Assurance," March 23, 2009.* Provides procedures for achieving acceptable levels of security for information systems connecting to or interfacing with an Army-managed network.

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.[11] We identified an internal control weakness related to protecting systems that store, process, and transmit PHI. Specifically, DHA and Army officials did not consistently implement technical, physical, and administrative protocols to protect DoD EHR systems and Army-specific systems from unauthorized access and disclosure. We will provide a copy of the final report to the senior officials responsible for internal controls at DHA, MEDCOM, and the MTFs.

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

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

Finding

DHA and Army Security Protocols for Systems Containing Patient Health Information Were Not Effective

DHA and Army officials[12] did not consistently implement effective security protocols to protect systems that stored, processed, and transmitted EHRs and PHI. Specifically, DHA and Army officials did not:

- enforce the use of Common Access Cards (CACs)[13] to access the three DoD EHR systems and two Army-specific systems because system administrators stated that the CAC software was incompatible with older system software or did not allow multiple users to log in and out of the systems without rebooting local terminals.
- comply with DoD password complexity requirements for Essentris and two Army-specific systems because system administrators considered existing network authentication requirements sufficient to control access.

In addition, system and network administrators at Brooke, Evans, and Kimbrough did not:

- consistently mitigate known vulnerabilities affecting Army networks because MTF Chief Information Officers (CIOs) did not want to implement certain network security patches[14] that they thought could negatively affect system availability.
- [redacted] for [redacted] four Army-specific systems, and external media that contained PHI because DHA and Army officials stated the [redacted] could negatively affect system availability or considered the HIPAA warning label sufficient to protect data stored on external media.[16]
- grant user access to the three DoD EHR systems and four Army-specific systems based on the user's assigned duties because they did not require user justifications for access and align user responsibilities to specific system roles.

[12] Army officials include MEDCOM, MTF chief information officers, and MTF information assurance managers and officers.

[13] CACs are identification cards with a microchip that provide access to DoD computer networks and systems for Government employees and eligible contractor personnel.

[14] A patch is an update to an operating system, application, or other software issued to correct specific problems.

[15] [redacted]

[16] External media is portable electronic storage media such as magnetic, optical, and solid-state devices that can be inserted into and removed from a computing device. Examples include hard discs, floppy discs, zip drives, compact discs, thumb drives, and similar universal serial bus storage devices.

- configure two DoD EHR systems and five Army-specific systems to automatically lock after 15 minutes of inactivity because the MTF CIOs did not want to negatively affect system availability.
- consistently review system activity reports to identify unusual or suspicious activities and access because the MTF CIOs did not dedicate resources to perform the task or properly configure the systems to generate system activity reports.
- develop standard operating procedures to manage system access because they did not consider documented procedures necessary.

Officials from MEDCOM and the MTFs also were not aware of all Army-specific systems operating on their networks that stored, processed, and transmitted PHI because MEDCOM officials did not require MTFs to provide them a report identifying systems that contained PHI. Furthermore, the DHA CIO did not develop a privacy impact assessment[17] for CoPath because he thought the assessment was conducted as part of the CHCS privacy impact assessment.

Without well-defined, effectively implemented system security protocols, the DHA and Army introduced unnecessary risks that could compromise the integrity, confidentiality, and availability of PHI. Security protocols, when not applied or ineffective, increase the risk of cyber attacks, system and data breaches, data loss or manipulation, and unauthorized disclosures of PHI. In addition, ineffective administrative, technical, and physical security protocols that result in a HIPAA violation could cost MTFs up to $1.5 million per year in penalties for each category of violation.[18]

System Security Protocols Were Ineffective or Not Implemented

DHA and Army security protocols over its systems that stored, processed, and transmitted EHRs were ineffective to protect against unauthorized access to or disclosure of PHI. Specifically, DHA and Army system and network administrators did not:

- require the use of CACs to access the three DoD EHR systems and two Army-specific systems;
- configure passwords to meet DoD password complexity requirements for [redacted] and two Army-specific systems;
- consistently mitigate known network vulnerabilities at Brooke, Evans, and Kimbrough;

[17] Privacy impact assessments are a written analysis of potential privacy risks and mitigating actions.
[18] Section 1320, title 42 United States Code (2015).

- [redacted] for [redacted] four Army-specific systems, and external media;
- grant user access to the three DoD EHR systems and four Army-specific systems based on the user's assigned responsibilities;
- configure two EHR systems and five Army-specific systems to automatically lock after specified periods of inactivity in accordance with DoD requirements;
- consistently review system activity reports to identify unusual or suspicious activities and access at Brooke, Evans, and Kimbrough; and
- develop standard operating procedures for granting, elevating, and deactivating[19] system access, and assigning system privileges.

Common Access Cards Were Not Consistently Used

DHA and Army officials did not enforce CAC usage to access the three DoD EHR systems and two Army-specific systems, and they partially enforced CAC usage for one Army-specific system. DHA configured the three DoD EHR systems to use CACs to access health records and other PHI in AHLTA, CHCS, and Essentris, but DHA and Army officials did not require its use. DoD Instruction 8520.03 requires DoD Components to use CACs to access all DoD networks and systems to comply with two-factor authentication requirements.[20] Two-factor authentication is based on using something in a user's possession such as a token[21] and entering something known only to the user such as a personal identification number. DHA and Army officials considered using single-factor authentication, such as a user name and password, more efficient to access PHI while providing bedside care; however, single-factor authentication is the least stringent and presents a greater risk of compromise. DHA and MTF CIOs did not enforce the use of CACs for AHLTA and Essentris because the systems did not allow multiple users to log into and out of the systems without rebooting local terminals, which interfered with timely patient care.

In addition, MEDCOM and MTF CIOs did not configure CoPath and Exit Writer at Evans to authenticate using CACs. Instead, CoPath and Exit Writer users at Evans accessed the systems using single-factor authentication. MEDCOM and the Evans CIO did not configure the systems to authenticate using CACs because system administrators stated the CAC software was incompatible with the older systems.

[19] Deactivated access prevents users from accessing a system, but does not remove the user or information entered by the user from the system.

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

[21] A token is used to authenticate a user's identity.

The CIOs for DHA, MEDCOM, and the MTFs should either configure the DoD EHR systems and Army-specific systems to use CACs to access systems that process, store, and transmit PHI, or obtain a waiver that exempts the systems from using CACs.

Furthermore, the MEDCOM and Brooke CIOs did not require all MRS users to use a CAC to access the system. Although technologists and receptionists used CACs to access MRS, the Brooke CIO allowed radiologists to use only a user name and password to access the system. The MRS system administrator stated he did not require radiologists to use CACs because its use prevented them from accessing multiple systems and applications concurrently. At Brooke, radiologists used MRS, PACS, and other applications simultaneously to interpret mammography results. The MRS system administrator stated Brooke planned to test other capabilities that would allow radiologists to access multiple systems using CACs, but did not have a timeframe for conducting those tests or upgrading the system. The Brooke CIO should develop, test, and implement applicable changes to MRS to allow system users to authenticate using a CAC when accessing multiple systems simultaneously.

DoD Instruction 8520.03 allows the use of single-factor authentication if DHA obtains a waiver. However, DHA did not obtain waivers exempting the use of CACs for AHLTA, CHCS, and Essentris users. On October 8, 2013, the CHCS program manager requested an extension until September 2014, to comply with the Military Health System's public key infrastructure[22] requirements for using CACs. DHA officials stated that developers continued to work on a solution to use CACs for CHCS, but the system still did not support CAC usage and DHA officials did not request and obtain a waiver exempting its use as of March 2017.

Passwords for Systems Containing Patient Health Information Did Not Meet Complexity Requirements

DHA and Army system administrators did not configure system passwords for [redacted] to meet DoD complexity requirements. Specifically, system administrators configured [redacted] to require only an [redacted] password at Brooke and Evans, and a [redacted] password at Kimbrough. Additionally, Army system administrators at Evans configured [redacted] to require only a [redacted] password and an [redacted] password for [redacted] In each instance, the system administrators stated that they did not properly configure passwords because they considered existing network authentication controls sufficient to control access to individual systems.

[22] Public key infrastructure uses certificates, instead of user name and passwords, to authenticate a user's identify.

However, allowing users to access individual systems, once on the networks, without using strong passwords that met DoD requirements increased the MTFs risk of compromising PHI.

Army Regulation 25-2 and the Defense Information Systems Agency Security Technical Implementation Guide on Application Security[23] require system passwords to be at least 15 characters in length. 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.

- Lowercase letter
- Uppercase letter
- Number
- Symbol

Countless programs are available today and used for the purpose of exploiting weak passwords to gain unauthorized access to systems by guessing common words and phrases, using personal information associated with specific users, randomly generating potential words based on the dictionary, or using a combination of various methods and programs to repeatedly attempt to access sensitive information protected by passwords. A longer, more complex password decreases the ability of hackers and others performing a cyber attack to obtain a system password using resources available to the attacker. The CIOs for DHA, MEDCOM, and the MTFs should properly configure passwords to meet DoD complexity requirements for systems that process, store, and transmit PHI.

Network Vulnerabilities Were Not Consistently Mitigated

~~(FOUO)~~ Network administrators at Brooke, Evans, and Kimbrough did not consistently mitigate known network vulnerabilities. In addition, the CIOs at Brooke, Evans, and Kimbrough did not develop plans of action and milestones (POA&Ms) to address how and when network vulnerabilities affecting their networks would be mitigated. DoD Instruction 8500.01 requires DoD Components to mitigate vulnerabilities to protect their networks.[24] Chairman of the Joint Chiefs of Staff Manual 6510.02 requires a [redacted],[25] [redacted].[26]

[23] Application Security and Development Security Technical Implementation Guide, Release 4, July 25, 2016.

[24] DoD Instruction 8500.01, "Cybersecurity," March 14, 2014.

[25] 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.

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

Comparative network scans from September 2016 and January 2017 from Brooke, Evans, and Kimbrough showed older and recently issued vulnerabilities were not mitigated. Table 2 shows the number, by year, of unmitigated network vulnerabilities at Brooke, Evans, and Kimbrough.

Table 2. Unmitigated Network Vulnerabilities at Brooke, Evans, and Kimbrough

Year Identified	Number of Unmitigated Vulnerabilities		
	Brooke	Evans	Kimbrough
2008	0	1	1
2009	1	1	0
2010	0	2	1
2011	3	4	1
2012	3	5	3
2013	1	6	7
2014	5	9	10
2015	31	61	47
2016	48	52	47
Total	**92**	**141**	**117**

Note: Data current as of January 2017.

~~(FOUO)~~ At Brooke, 92 of the 171 vulnerabilities identified on a September 4, 2016, network scan remained unmitigated based on the results from a January 5, 2017, network scan. The 92 vulnerabilities included 6 critical and 60 high vulnerabilities.[27] For example, one of the unmitigated [redacted] vulnerabilities, identified in June 2016, could allow attackers to [redacted] to a system. Although the associated information assurance vulnerability alert required DoD Components to mitigate the vulnerability or develop a POA&M by July 6, 2016, Brooke had not mitigated the vulnerability or developed a POA&M. Brooke officials stated that they mitigated vulnerabilities using two processes; an automated configuration management tool to push security patches and a manual process to mitigate vulnerabilities affecting laptops, desktops, and servers that could not be corrected using the automated tool.[28] The 92 unmitigated vulnerabilities, which required system administrators to manually address, indicates that the manual process was not effective to timely mitigate those vulnerabilities.

[27] 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, and network downtime.

[28] The Brooke CIO stated the command's vulnerability scan results included vulnerabilities affecting medical devices, but did not identify those vulnerabilities separately.

~~(FOUO)~~ At Evans, 141 of the 170 vulnerabilities identified on a September 21, 2016, network scan remained unmitigated based on the results from a January 11, 2017, scan. The 141 vulnerabilities included 2 critical and 103 high vulnerabilities. For example, one of the unmitigated [redacted] vulnerabilities, identified in February 2016, could allow an attacker to [redacted] Although the information assurance vulnerability alert required DoD Components to mitigate the vulnerability or include it in a POA&M by March 3, 2016, Evans had not mitigated the vulnerability or developed a POA&M. At Evans, the information systems security manager stated that although he briefed the Evans CIO on the unmitigated vulnerabilities, he did not develop a POA&M for the vulnerabilities that were not mitigated as required.

~~(FOUO)~~ At Kimbrough, 117 of the 129 vulnerabilities identified on a September 27, 2016, network scan remained unmitigated based on the results from a January 25, 2017, scan. The 117 vulnerabilities included 5 critical and 112 high vulnerabilities. For example, an unmitigated vulnerability from 2008 could allow an attacker to [redacted] Although the information assurance vulnerability alert required DoD Components to mitigate the vulnerability or include it in a POA&M by December 4, 2008, Kimbrough had not mitigated the vulnerability or developed a POA&M.

Network administrators at Brooke, Evans, and Kimbrough did not timely mitigate vulnerabilities because the MTF CIOs directed them not to implement required network security patches that could negatively affect system availability. At Evans, for example, administrators stated that after implementing a patch in October 2016, patients were unable to contact the call center one morning. The MTF CIOs were concerned that implementing other patches could result in similar availability or other problems.

Brooke, Evans, and Kimbrough had a vulnerability management program that identified and mitigated some vulnerabilities; and they used automated tools to push certain security patches; and tested mitigation solutions. However, the MTF CIOs did not meet the program's expectations to effectively manage risk when they decided not to mitigate vulnerabilities that may reduce network availability. Without a rigorous and systematic process to ensure security patches are implemented in a timely manner, the MTF CIOs increased their risk that cyber attacks or other malicious actions could exploit the vulnerabilities and therefore, compromise sensitive PHI 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 Brooke, Evans, and Kimbrough should review the performance

of their CIOs 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 believed to negatively impact patient care.

[redacted] *Was Not Consistently Protected*

DHA and Army officials did not consistently [redacted] for [redacted] and four Army-specific systems that contained PHI. DoD Instruction 8580.02 requires the use of [redacted] to protect PHI.[29] System administrators at Brooke, Evans, and Kimbrough did not [redacted]. System administrators did not [redacted] data because they stated that the [redacted] would limit system availability. Although DHA and Army officials obtained waivers exempting the MTFs from [redacted] on all five systems in 2013 and 2014,[30] they did not obtain similar exemptions from [redacted] in 2015 and 2016. Without [redacted] DHA and the MTFs increased their risk that sensitive PHI could be compromised if existing security controls that they relied on to protect the information were breached. The CIOs for DHA and the MTFs should [redacted] sensitive PHI [redacted]

In addition, PACS users at Kimbrough did not adequately protect PACS-related PHI downloaded to external media. Specifically, PACS users placed only a HIPAA warning label on the external media instead of using a password because they considered the HIPAA warning label to be sufficient. However, the warning label did not prevent unauthorized access to the information and could possibly attract more attention to the information if the external media was lost or stolen. NIST SP 800-53 requires Components to restrict access to data stored on removable media. Within the last 2 years, Kimbrough reported an incident that involved providing a compact disc to a patient that contained sensitive PHI of another patient. While this incident did not compromise the patient's health

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

[30] The 2013 and 2014 waivers from DHA and the Army identified mitigating security protocols they implemented to reduce the risk of unauthorized access to the data on the servers.

information, unauthorized access to or disclosure of PHI increases risk to the patient's finances, reputation, and medical care. The Kimbrough CIO should require PACS users, at a minimum, to require a password to protect PHI stored on or downloaded to external media.

User Roles and Privileges Did Not Always Align With User Responsibilities

Army system administrators did not consistently grant users' access to the three DoD EHR systems and four Army-specific systems based on defined roles that aligned with user responsibilities. MTFs 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. NIST SP 800-53 and DoD Instruction 8530.01 require access to systems to be granted based on the principle of least privileges.[31] We selected a statistical sample of users from the three DoD EHR systems and seven Army-specific systems to validate whether user roles and privileges aligned with their responsibilities. If we identified an issue, we are 90-percent confident the error rate related to user roles and responsibilities was greater than 5 percent (see Appendix for sampling methodology).

At Brooke, we tested user access to CHCS, AHLTA, Essentris, the Surgery Scheduling System, MRS, and the HIP database. We did not identify problems in how the developer granted access to HIP; however, we identified 43 instances where improvements to managing user access to CHCS, AHLTA, Essentris, MRS, and the Surgery Scheduling System were needed. For example, system administrators for AHLTA did not provide system access request forms for five users and, therefore, we could not determine whether access was granted based on assigned duties. In addition, system administrators granted user access to Essentris without completed access request forms and instead relied on their understanding of user responsibilities. Furthermore, system administrators for CHCS did not update user roles and deactivate users from the system in a timely manner. We identified one CHCS user account that was created in 2015 and never used, but the account remained active until we notified the system administrator in September 2016. Table 3 identifies the number of users and sample size, by system, and the types of access-related problems we identified at Brooke.

[31] Least privilege is a security objective requiring access needed only to perform official duties.

Table 3. Access Control Problems to Patient Health Information at Brooke

Issue Identified	CHCS	AHLTA	Essentris	MRS	Surgery Scheduling System
	Sample Size/Number of Users				
	45/4,017	45/5,074	45/5,154	21/39	45/2,345
Missing Access Request Forms	4	5			
Written Justification for Obtaining Access Did Not Exist	1	17	3		
Elevated Privileges Provided Without Written Justification	4				2
System Roles Did Not Align With User Duties	2		1	1	
Inactive Users Retained System Access	3				

Note: Data current as of November 2016.

At Evans, we tested user access to CHCS, AHLTA, Essentris, the Surgery Scheduling System, Exit Writer, CoPath, and PACS. We did not identify problems in how administrators granted access to Essentris and CoPath. However, we identified 58 instances where improvements were needed to manage access to CHCS, AHLTA, the Surgery Scheduling System, Exit Writer, and PACS. For example, we identified that staff physicians had, among other levels of access, administrative access that allowed them system administrator privileges. With administrative access, staff physicians could bypass system controls to add system users, elevate user access privileges, or reconfigure system security protocols. If staff physicians bypass system controls, system and data integrity could be compromised. Table 4 identifies the number of users and sample size, by system, and the types of access-related problems we identified at Evans.

Table 4. Access Control Problems to Patient Health Information at Evans

Issue Identified	CHCS	AHLTA	Surgery Scheduling System	Exit Writer	PACS
	Sample Size/Number of Users				
	45/3,106	45/2,488	43/368	32/81	44/574
Missing Access Request Forms	4			19	
Elevated Privileges Provided Without Written Justification	7	13	4	3	1
System Roles Did Not Align With User Duties	2				
Required Training to Obtain System Access Was Not Completed		4			
Inactive Users Retained System Access					1

Note: Data current as of October 2016.

At Kimbrough, we tested user access to CHCS, AHLTA, Essentris, PACS, and the Coagulation Clinic Web Application. We did not identify problems in how administrators granted access to the Coagulation Clinic Web Application; however, we identified 123 instances where improvements to managing access to CHCS, AHLTA, Essentris, and PACS were needed. Specifically, system administrators for AHLTA, CHCS, and Essentris did not provide system access request forms for 118 users and, therefore, we could not determine whether access was granted based on assigned duties. For the users with shared accounts, Kimbrough officials did not ensure Kimbrough acquired an appropriate number of PACS software licenses to ensure each user had a separate account. DoD Instruction 8580.02 requires system access based on individual and unique accounts to identify and monitor user activity. Table 5 identifies the number of users and sample size, by system, and the types of access-related problems we identified at Kimbrough.

Table 5. Access Control Problems to Patient Health Information at Kimbrough

Issue Identified	CHCS	AHLTA	Essentris	PACS
	Sample Size/Number of Users			
	45/650	43/480	30/70	49/117
Missing Access Request Forms	45	43	30	
Users Shared System Accounts				5

Note: Data current as of September 2016.

An effective account management process, which includes establishing conditions for user roles; authorizing specific levels of access; and creating, modifying, monitoring, and disabling user access in a timely manner increases the likelihood that only authorized users obtained access to systems and Army networks. Limiting access to PHI based on a user's role in the system that aligns with assigned duties reduces the risk of intentional and unintentional disclosure of sensitive information. The MTF CIOs should require written justification as a condition for obtaining access to DoD EHR systems and all Army-specific systems used to store, process, and transmit PHI and implement procedures to grant access to the systems based on roles that align to user responsibilities.

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

System administrators at Brooke, Evans, and Kimbrough did not appropriately configure two DoD EHR systems and five Army-specific systems that contained PHI to automatically lock after 15 minutes of inactivity. Army Regulation 25-2 and the Defense Information Systems Agency Security Technical Implementation Guide for Application Security requires systems to automatically lock for nonprivileged users[32] after no more than 15 minutes of inactivity. Table 6 identifies the systems that took longer than 15 minutes to automatically lock and those that were not configured to automatically lock.

[32] A nonprivileged user is not authorized to perform security-related functions.

Table 6. Automatic Lockout Settings for Inactivity

System Name	Minutes Before System Automatically Locked		
	Brooke	Evans	Kimbrough
AHLTA			30
CHCS			150
Coagulation Clinic Web Application			120
Surgery Scheduling System	NC	60	
PACS		24	
HIP Database	NC		
Exit Writer		NC	

NC (not configured) indicates the system was not configured to automatically lock.
Note: Blank cells indicate the system was appropriately configured to meet DoD standards.

The developer for HIP and the system administrators for the Surgery Scheduling System at Brooke and the system administrators for Exit Writer and PACS at Evans did not configure the systems to automatically lock after any period of inactivity because they relied on the network configuration settings at each MTF to meet the requirement. At those MTFs, the system administrators stated the network automatically locked after 15 minutes of inactivity. At Evans, however, we determined that the network and PACS automatically locked after 24 minutes of inactivity, 9 minutes after system administrators stated the network and system would lock. At Kimbrough, administrators configured the systems to automatically lock after more than 15 minutes of inactivity because they wanted to allow additional time for users to perform assigned duties. The Kimbrough CIO was not concerned with the extended automatic lockout times because he stated the screensaver function for each workstation automatically locked after 10 minutes of inactivity. Although a screensaver locked the workstations after 10 minutes of inactivity, the systems themselves did not lock. If users logged back into the workstation to perform any number of duties and walked away from their workstation, the systems and PHI contained in them were vulnerable to compromise until the screensaver again locked the workstation. Automatically locking systems and user accounts within DoD required timeframes limits the potential for unauthorized access and prevents malicious actions that could jeopardize patient care. The MTF CIOs should configure all systems used to process, store, and transmit PHI to automatically lock after 15-minutes of inactivity.

System Activity Was Not Consistently Reviewed

Brooke and Evans system administrators did not consistently review system activity reports to assess user activity, failed login attempts, and possible data exfiltration attempts for Essentris and four Army-specific systems. Although Brooke and Evans administrators configured Essentris, CoPath, and the Surgery Scheduling System to generate system activity reports, the MTF CIOs did not dedicate resources or prioritize system activity review tasks. DoD Instruction 8580.02 requires DoD Components to perform regular system activity reviews to protect PHI.

Although the database developers at Brooke reviewed the HIP activity report to monitor successful log-in attempts and user activity, their reviews did not include failed log-in attempts because the database developers did not configure the system to record that information. In addition, the system administrators for Exit Writer at Evans did not review system activity because they did not configure the system to generate system activity reports. Evans officials did not consider system activity reviews necessary based on the low number of system users at the site.[33] NIST SP 800-53 requires audit logs[34] to include descriptions of user activity, and all log-in and data exfiltration attempts. Audit logs that record required information and are regularly reviewed to identify unauthorized access attempts and activity could be used to prevent a breach and provide forensic evidence that aids in investigating and identifying sources of malicious behavior. The MTF CIOs should appropriately configure and regularly review system audit logs to identify user and system activity anomalies.

Procedures for Managing Access to EHRs and Army-Specific Systems Were Not Consistently Developed

Systems administrators at Brooke, Evans, and Kimbrough did not consistently develop standard operating procedures for two DoD EHR systems and six Army-specific systems to grant, elevate, and deactivate system access. In addition, system administrators at Brooke and Kimbrough developed written procedures for elevating system access and assigning system privileges for only 3 of the 10 systems.[35] DoD Instruction 8580.02 requires policies and procedures for granting and modifying access to PHI. System administrators did not develop standard operating procedures because they considered documented procedures

[33] As of October 2016, Exit Writer had 81 users at Evans.

[34] Audit logs, if properly configured, provide automated and chronological records of system activity.

[35] Brooke system administrators developed procedures for Essentris, CHCS, and MRS. Kimbrough system administrators developed procedures for Essentris.

unnecessary and instead, relied on verbal discussions to manage system access. Although the Kimbrough CIO provided unsigned standard operating procedures, he also acknowledged that they were unofficial until signed. Table 7 identifies, by location, the systems without standard operating procedures for managing access.

Table 7. 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)		
	Brooke	Evans	Kimbrough	Brooke	Evans	Kimbrough
AHLTA		X	X			X
CHCS		X	X			X
Essentris		X				
PACS		X	X		X	X
Exit Writer		X			X	
CoPath		X			X	
HIP Database	X					
Surgery Scheduling System	X	X			X	
Coagulation Clinic Web Application						X

Standard operating procedures are written and detailed instructions that document a repetitive activity to perform specific functions uniformly and serve as a vital tool to transfer knowledge. Without standard operating procedures, system users could misinterpret procedures and miscommunicate information that could impact the integrity of PHI. The MTF CIOs should develop and maintain standard operating procedures that address processes for granting access, assigning and elevating privileges, and deactivating user access.

MEDCOM and MTFs Could Not Account for Systems Containing Patient Health Information

The CIOs for MEDCOM, Brooke, Evans, and Kimbrough were not aware of all Army-specific systems used at Army MTFs that stored, processed, or transmitted PHI. NIST SP 800-53 requires organizations to identify and account for all information systems that contain PHI. Although MEDCOM officials stated that they used the Army's Investment Management and Portfolio Analysis Coordination Tool to account for Army-specific systems, the information they provided for

Brooke, Evans, and Kimbrough was unreliable. For example, Brooke provided a list from the Investment Management and Portfolio Analysis Coordination Tool that included Army-specific systems and medical devices; however, neither Brooke nor MEDCOM could differentiate the systems containing PHI from the medical devices. Additionally, the Kimbrough CIO did not maintain a complete list of systems used at the site that stored, processed, and transmitted PHI and could not provide assurance that the site protected all systems against unauthorized disclosure of or access to sensitive PHI.

DHA plans to replace AHLTA, CHCS, and Essentris with the Military Health System GENESIS.[36] The lack of awareness by the Army for specific systems used at the MTFs could present challenges for Military Health System GENESIS developers when implementing interface controls between Army-specific systems and the new EHR system. To avoid unnecessarily delaying DoD's transition to the Military Health System GENESIS, incurring additional costs to develop system interfaces, and not implementing adequate security protocols needed to protect the sensitive information, a complete inventory of systems containing PHI is needed. The CIOs for MEDCOM and the MTFs should identify all systems used to process, store, and transmit PHI, develop a baseline of systems used at each MTF, and regularly, at least annually, validate the accuracy of the inventory of Army-specific systems.

Privacy Impact Assessment for CoPath Did Not Exist

The DHA CIO did not develop a privacy impact assessment for CoPath.[37] DoD Instruction 5400.16[38] requires a privacy impact assessment for all systems that collect, maintain, and disseminate personally identifiable information. DHA did not develop the assessment because the DHA CIO thought the system was included in the privacy impact assessment for CHCS. However, the CHCS privacy impact assessment did not include CoPath. Additionally, the DHA CIO stated he was unsure whether CoPath required a separate privacy impact assessment because the system only interfaced with CHCS. Privacy impact assessments document privacy risks affecting an information system that collects, maintains, uses, and disseminates personally identifiable information electronically. Completing a privacy impact assessment improves a system owner's ability to protect sensitive information in accordance with applicable laws and regulations and documents needed protocols and processes to mitigate potential privacy risks. The DHA CIO should implement procedures to develop privacy impact assessments for all systems, including CoPath, which store, process, and transmit PHI.

[36] Although the DoD initially planned to transition to the Military Health System GENESIS at four MTFs in the Pacific Northwest in December 2016, system interface problems delayed the transition until at least February 2017.

[37] DHA developed and maintains CoPath, but the Army uses the system to support specific health-related mission needs.

[38] DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015.

Increased Risk of Unauthorized Disclosures of Patient Health Information

DHA, MEDCOM, and the Army MTFs use DoD and Army-specific systems and databases to process, store, and transmit sensitive PHI. Under HIPAA, DHA, MEDCOM, and the Army 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 the risk of unauthorized access to and disclosure of sensitive PHI. In addition, mitigating known vulnerabilities timely and regularly monitoring system activity decreases the risk that cyber attackers could exploit known system and network weaknesses. Furthermore, limiting access to PHI to users with a mission need reduces the risk of intentional or unintentional disclosures of sensitive information. However, DHA, MEDCOM, and the Army MTFs did not consistently implement security protocols or, when implemented, they were ineffective to consistently protect PHI from being compromised. As such, the DoD EHR systems used to store PHI for about 4 million service members, retirees, and family members are exposed to greater risks of the information being compromised unless actions are taken to improve security.

Since August 1, 2016, healthcare providers, health plans, and healthcare business associates[39] reported 178 data breaches to the Secretary of the Department of Health and Human Services. The breaches affected more than 11 million individuals as a result of hacking incidents, data loss, theft, improper disposal of data, and unauthorized access.[40] Ten of the 178 breaches were the result of compromised EHRs at healthcare provider facilities.[41] 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 that could impact 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 MTFs up to $1.5 million per year in penalties for each category of violation.

[39] A healthcare business associate is an organization that helps covered entities carry out its healthcare activities and functions.

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

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

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

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Chief Information Officer, Health Information Technology, Defense Health Agency:

a. Implement appropriate configuration changes to enforce the use of Common Access Cards to access the Armed Forces Health Longitudinal Technology Application, Composite Health Care System, and Clinical Information System/Essentris Inpatient System or obtain a waiver that exempts the systems from using Common Access Cards.

Defense Health Agency Comments

The Director, DHA, responding for the DHA CIO, agreed stating that DHA would coordinate with the Service Surgeons General to enforce CAC usage. The Director stated that AHLTA and Essentris were CAC-enabled and that the Services and MTFs were responsible for enforcing CAC usage. She also stated that DHA was testing a proposed CAC solution for CHCS.

Our Response

Comments from the Director, DHA, addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain a memorandum or policy that verifies DHA implemented a CAC solution for CHCS and documentation such as global security policies or system configuration settings that show the Service Surgeons General have enforced the use of CACs to access AHLTA and Essentris.

b. Configure passwords for the [redacted] to meet DoD complexity requirements.

Defense Health Agency Comments

The Director, DHA, responding for the DHA CIO, agreed, stating that [redacted] had the ability to meet DoD password complexity requirements. The Director also stated that DHA would coordinate with the Services and MTFs to ensure accountability and enforce password complexity policies.

Our Response

Comments from the Director, DHA, partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. We agree [redacted] is capable of being configured to meet DoD password complexity requirements; however, MTF officials did not consistently comply with configuration requirements. The Director's response was unclear whether DHA would ensure accountability and enforce password complexity compliance for only [redacted] or the [redacted] Although we did not identify instances where MTFs did not meet password complexity requirements for [redacted] at the sites visited, our intent was to ensure DHA enforced the requirements across MTFs using [redacted] Therefore, the Director should provide comments to the final report describing DHA's plan to enforce the use of CACs on [redacted] We will close the recommendation once we obtain documentation such as system configuration settings that show the MTFs configured the systems to meet DoD password complexity requirements.

c. [redacted] for the [redacted]

Defense Health Agency Comments

The Director, DHA, responding for the DHA CIO, agreed, stating that although [redacted] the system hardware and Oracle database [redacted] However, the Director stated that DHA maintained a waiver to [redacted] for the [redacted].[42]

[42] The [redacted] Privacy Impact Assessment, October 10, 2013, states that the [redacted] is a component of [redacted] that centrally stores all PHI data.

Our Response

Comments from the Director, DHA, partially addressed the recommendation; therefore, the recommendation is unresolved. We agree DHA had waivers that exempted it and the MTFs [redacted] and the [redacted] from June 2014 through June 2015. The June 2014 waivers required DHA to evaluate the ability of newer technology to meet [redacted] was not possible, resubmit an annual waiver request. However, DHA has not resubmitted a waiver request and, therefore, has not had an approved exemption from [redacted] since June 2015. The Director should provide comments to the final report addressing actions taken to [redacted] We will close the recommendation once we verify DHA obtained a waiver accepting the risk of [redacted] or developed solutions to overcome the hardware and software challenges to [redacted]

d. Implement procedures to verify that privacy impact assessments are developed for all systems, including the Comed Anatomic Pathology System, that store, process, and transmit patient health information.

Defense Health Agency Comments

The Director, DHA, responding for the DHA CIO, agreed, stating that CoPath was an Army-specific system. The Director also stated that DHA provided the audit team an interface control document describing the interface requirements between CHCS and CoPath.

Our Response

Comments from the Director, DHA, partially addressed the recommendation; therefore, the recommendation is unresolved. The Director's response did not address actions DHA would take to ensure privacy impact assessments for all systems were developed. As previously reported, the DHA did not develop a privacy impact assessment for CoPath. DoD Instruction 5400.16 requires a privacy impact assessment for all systems that collect, maintain, and disseminate personally identifiable information.

In addition, the Director stated that CoPath was an Army-specific system. Based on the Director's comments, to the extent that the comments indicate ownership of the system, Army and other DHA officials repeatedly stated that CoPath was DHA-owned and maintained. As the Director stated, we received and reviewed the interface control document during the audit, but it did not establish system ownership for CoPath or meet the requirements of a privacy impact assessment. Therefore, the Director should provide comments to the final report

to address actions DHA will take to develop privacy impact assessments for all DHA systems. We will close the recommendation once we obtain written procedures describing how DHA will ensure it completes privacy impact assessments for all systems containing PHI, including CoPath.

Recommendation 2

We recommend that the Chief Information Officer, U.S. Army Medical Command, Department of the Army:

a. **Develop and implement a plan to ensure the military treatment facilities appropriately configure changes to enforce the use of Common Access Cards to access the Armed Forces Health Longitudinal Technology Application, Composite Health Care System, and Clinical Information System/Essentris Inpatient System.**

b. **Develop and implement a plan to ensure the military treatment facilities configure passwords for the [redacted] to meet DoD complexity requirements.**

c. **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 Army-specific systems.**

U.S. Army Medical Command Comments

The Chief of Staff, MEDCOM, responding for the MEDCOM CIO, agreed, stating that MEDCOM would coordinate with DHA to standardize the use of CACs and complex passwords across the Military Health System. He stated that, in FY 2014, health information technology transitioned to DHA as a shared service. As such, the Chief of Staff stated that the DHA CIO was the authorizing official for accreditation and cybersecurity issues.

The Chief of Staff also stated that MEDCOM would review and identify Army-specific systems that process, store, and transmit PHI, and validate its inventory of systems annually during the Organizational Inspection Program. The Chief of Staff stated that MEDCOM planned to complete the initial baseline by August 1, 2017. Furthermore, the Chief of Staff stated that MEDCOM would collaborate with clinical personnel to reduce risks to patient safety while taking actions to implement the recommendations.

Our Response

Comments from the Chief of Staff, MEDCOM, addressed all specifics of the recommendations; therefore, the recommendations are resolved. We will close Recommendations 2.a and 2.b once we obtain MEDCOM's plan describing how it will ensure MTFs use CACs to access systems with PHI and comply with DoD password complexity requirements. We will close Recommendation 2.c once we verify MEDCOM completed a baseline of Army-specific systems that process, store, and transmit PHI.

Recommendation 3

We recommend that the Chief Information Officers for Army Military Treatment Facilities:

a. Implement appropriate configuration changes to enforce the use of Common Access Cards to access all Army-specific systems containing patient health information or obtain a waiver that exempts the systems from using Common Access Cards.

b. Configure passwords for all Army-specific systems to meet DoD complexity requirements.

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

d. [redacted] for all Army-specific systems that store patient health information.

e. Require written justification as a condition for obtaining access to the Armed Forces Health Longitudinal Technology Application, Composite Health Care System, Clinical Information System/Essentris Inpatient System, and all Army-specific systems and implement procedures to grant access to the systems based on roles that align with user responsibilities.

f. Configure all Army-specific systems to automatically lock after 15 minutes of inactivity.

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

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

i. 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 Army-specific systems.

U.S. Army Medical Command Comments

The Chief of Staff, MEDCOM, responding for the MTF CIOs, agreed, stating that MEDCOM would coordinate with DHA to enforce CAC usage and password complexity, mitigate network vulnerabilities, [redacted] control system access and privileges, implement automatic system lockout procedures, and configure and review audit logs based on standard Military Health System solutions. The Chief of Staff also stated that MEDCOM would collaborate with clinical personnel to minimize risks to patient safety and ensure access to care while implementing the recommendations.

Furthermore, the Chief of Staff stated that MEDCOM would review and identify Army-specific systems that process, store, and transmit PHI, and validate its inventory at least annually during the Organizational Inspection Program. The Chief of Staff stated that MEDCOM planned to complete the initial baseline by August 1, 2017.

Our Response

Comments from the Chief of Staff, MEDCOM, addressed all specifics of the recommendations; therefore, the recommendations are resolved. We will close Recommendations 3.a and 3.b once we obtain documentation such as global security policies or system configuration settings that show MTFs used CACs to access systems and complied with DoD password complexity requirements; Recommendations 3.c and 3.d once we obtain vulnerability scans that show the MTFs mitigated known vulnerabilities and other documentation such as global security settings that show [redacted] Recommendation 3.e and 3.h once we obtain written procedures that show how MTFs will manage system access, to include requiring written justification to support the need for system access and specific privileges; Recommendations 3.f and 3.g once we obtain documentation such as security configuration settings that show MTFs automatically locked systems after defined periods of inactivity or documented risk acceptance, and configured audits logs to identify anomalous activity; and Recommendation 3.i once we obtain a documented baseline of systems used by MTFs to process, store, and transmit PHI.

Recommendation 4

We recommend that the Commanders, Brooke Army Medical Center, Evans Army Community Hospital, and Kimbrough Ambulatory Care 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 believed to negatively impact patient care.**

U.S. Army Medical Command Comments

The Chief of Staff, MEDCOM, responding for the Commanders, Brooke, Evans, and Kimbrough, partially agreed, stating that the CIOs needed to follow Federal and DoD guidance to protect PHI. He also agreed with the unmitigated vulnerabilities we identified at the Army MTFs. The Chief of Staff stated MEDCOM planned to coordinate with DHA and vendors to mitigate the known vulnerabilities.

However, the Chief of Staff disagreed with the recommendation for the Commanders to review the CIO's performance and consider administrative action. The Chief of Staff stated that Commanders would continue to review the CIOs performance based on established standards and take administrative action, if needed, based on that process.

Our Response

Comments from the Chief of Staff, MEDCOM, partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. The Chief of Staff agreed to coordinate with DHA and vendors to mitigate known vulnerabilities. However, the Chief of Staff considered existing processes sufficient to review personnel performance and take administrative action, if warranted. Without additional information on the processes and procedures the Chief of Staff described, we are unable to determine whether existing performance review processes meet the intent of our recommendation. Therefore, the Chief of Staff should provide comments to the final report that describe existing processes for holding staff accountable for their performance. We will close the recommendation once we obtain vulnerability scans or other documentation to verify the known

vulnerabilities at Brooke, Evans, and Kimbrough were mitigated. The Chief of Staff will also need to provide documentation that shows an accountability performance standard within the CIO's existing performance management plan that focuses on protecting PHI.

Recommendation 5

We recommend that the Chief Information Officer, Kimbrough Ambulatory Care Center, require Picture Archiving and Communications System users, at a minimum, to require a password to protect patient health information stored on or downloaded to external media.

U.S. Army Medical Command Comments

The Chief of Staff, MEDCOM, responding for the Kimbrough CIO, agreed, stating that MEDCOM would coordinate with DHA to ensure the MTF implemented controls that aligned with standard Military Health System policy.

Our Response

Comments from the Chief of Staff, MEDCOM, addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain written procedures that require Kimbrough to protect PHI stored on or downloaded to external media.

Recommendation 6

We recommend that the Chief Information Officer, Brooke Army Medical Center, develop, test, and implement applicable changes to the Mammography Reporting System to allow users to authenticate using a Common Access Card when accessing multiple systems simultaneously.

U.S. Army Medical Command Comments

The Chief of Staff, MEDCOM, responding for the Brooke CIO, agreed, stating that MRS, in addition to the Peer Review system, did not require all users to authenticate on the applications using CACs. The Chief of Staff stated that MRS required CAC authentication for all users except radiologists. He also stated that all users, including radiologists, were required to first log into PACS workstations using their CACs before they could access radiology information using a username and password from any of the four systems[43] that interfaced with PACS. The Chief of Staff stated that Army Regulation 25-2 authorizes the use of usernames and passwords for systems that do not support CAC authentication.

[43] In addition to MRS, PACS, and the Peer Review system, the Powerscribe Voice Recognition and Vitrea 3D rendering software stored PHI and were used by radiologists to support medical diagnoses and procedures.

In addition, the Chief of Staff stated that a firewall separated systems with radiology information from other hospital network communications and controlled access to the systems using specific access control lists. He also stated that PACS workstations were physically located in restricted areas and deployed with group policies to further restrict access to sensitive information. Furthermore, the Chief of Staff stated that MRS had an approved accreditation through September 26, 2017. However, the Chief of Staff stated that Brooke was upgrading MRS to support CAC-based authentication and expected to complete testing and implement the solution by the end of May 2017.

Our Response

Comments from the Chief of Staff, MEDCOM, addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation such as global security policies or system configuration settings that show Brooke used CACs to access MRS.

Management Comments on Internal Controls and Our Response

U.S. Army Medical Command Comments

The Chief of Staff, MEDCOM, disagreed that the Army did not consistently protect EHRs and Army-specific systems from unauthorized access and disclosure. He stated that the MTFs have not reported instances of system breaches, data loss, or manipulation related to the control weaknesses described in this report.

The Chief of Staff also stated that health information technology was a shared service and the DHA had responsibility for the systems under its control. He stated that internal control weaknesses related to DHA-owned systems that store, process, and transmit should be directed to DHA to ensure standard solutions are developed and implemented across the DoD.

Our Response

We acknowledge that the MTFs did not report security breaches, data loss, and data manipulation; however, we did identify instances where unintended or unauthorized PHI disclosures occurred. For example, Kimbrough reported that it provided a compact disc with PHI data to the wrong patient and did not use solutions to encrypt or restrict access to the information.

Security incidents and breaches occur and go undetected even with robust security programs that include continuously monitoring system and data risks, and mitigating vulnerabilities and security control weaknesses in a timely manner. We agree protecting systems that process, store, and transmit PHI is a shared responsibility between DHA and the MTFs; however, the MTFs are responsible for protecting Army-specific systems and PHI at individual locations. We also agree that DHA is responsible for protecting or overseeing the implementation of DoD-wide solutions to protect DoD EHR systems. The security protocol weaknesses we identified in the report, if corrected, increase DHA and the Army's ability to limit the risk of security breaches and unauthorized disclosures of PHI. If not corrected, internal or external cyber attacks designed to exploit weak or lax internal controls and security protocols unnecessarily expose PHI and about 4 million service members, retirees, and family members to greater risks of the information being compromised.

Appendix

Scope and Methodology

We conducted this performance audit from August 2016 to March 2017 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 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 DHA, MEDCOM, and select Army MTFs from the Central and Atlantic Regional Health Commands. We also interviewed system owners, CIOs, system administrators, developers, and users to identify specific protocols implemented to protect systems that store, process, and transmit PHI.

We reviewed Federal laws and DoD policy, including guidance from DHA and the Army, related to complying with HIPAA security rules and implementing system security protocols. We selected a nonstatistical sample of 3 of the 71 Army MTFs to visit within the scope of this audit to review whether the DHA and the Army assessed security risks and tested the appropriateness and effectiveness of implemented system security protocols to protect the three DoD EHR systems and seven Army-specific systems used at Brooke in Fort Sam Houston, Texas; Evans in Fort Carson, Colorado; and Kimbrough in Fort Meade, Maryland from unauthorized access to and disclosure of PHI.

We selected one clinic, one hospital, and one medical center to incorporate different types of medical facilities in the Central and Atlantic Regional Commands. Table 8 describes the Army-specific systems used at each MTF that were included in the audit scope.

Table 8. Army-Specific Systems Used at Each MTF Visited

System Name	Systems Used at MTFs Visited		
	Brooke	Evans	Kimbrough
Coagulation Clinic Web Application			X
CoPath		X	
Exit Writer		X	
HIP	X		
MRS	X		
PACS		X	X
Surgery Scheduling System	X	X	

We statistically selected 674 of 26,541 users from the three DoD EHR systems and seven Army-specific systems to validate whether the users were authorized to access PHI. 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. If we identified issues, we are 90-percent confident the error rate related to user roles and responsibilities was greater than 5-percent. We tested security protocols for the three EHR systems and seven Army-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;
- system maintenance; and
- workforce security.

Use of Computer-Processed Data

We used computer-processed data from the DoD EHR systems and Army-specific systems to generate user lists at each site visited. System administrators provided extracts of active and inactive users from the systems as Microsoft Excel spreadsheets and Adobe Acrobat documents. We used the documentation

to compile a universe of users at Brooke, Evans, and Kimbrough. To assess the reliability of the data, we selected a sample and compared the data to information obtained from testing users' access to the DoD EHR systems and Army-specific systems.

The 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 and Army-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.

Use of Technical Assistance

The DoD OIG Quantitative Methods Division provided assistance in developing the statistical sampling methodology that we used to select DoD EHR system and Army-specific system users.

Prior Coverage

During the last 5 years, the DoD Office of Inspector General (DoD OIG) and the Government Accountability Office (GAO) issued four reports discussing DoD electronic health records. Unrestricted DoD OIG can be accessed at http://www.dodig.mil/pubs/index.cfm.

GAO

GAO-15-530, "Electronic Health Records: Outcome-Oriented Metrics and Goals Needed to Gauge DoD's and VA's 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: VA 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

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 and 46 percent of the 3,217 records transferred by the Navy were not timely.

Management Comments

Defense Health Agency

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

APR 2 4 2017

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Draft Report for Audit of Securing Army Electronic Health Records (D2016-D000RC-0187.000)

Thank you for the opportunity to review and comment on the Department of Defense Inspector General Draft Report, "Improved Security Protocols Are Needed to Protect Army Electronic Health Records."

We found no factual errors in the draft report. We concur with the report's findings and conclusions. My specific comments to your recommendations 1.a, 1.b, 1.c, and 1.d are attached.

Please feel free to direct any comments on this topic to [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 Army Electronic Health Records (D2016-D000RC-0187.000)*
"IMPROVED SECURITY PROTOCOLS ARE NEEDED TO PROTECT ARMY ELECTRONIC HEALTH RECORDS"
DEFENSE HEALTH AGENCY COMMENTS TO THE RECOMMENDATIONS

Recommendation 1.a. (page 22)
We recommend that the Chief Information Officer, Health Information Technology, Defense Health Agency (DHA):

a. Implement appropriate configuration changes to enforce the use of Common Access Cards (CACs) to access the Armed Forces Health Longitudinal Technology Application, Composite Health Care System, and Clinical Information System/Essentris Inpatient System or obtain a waiver that exempts the systems from using CACs.

DHA Response: DHA concurs with this recommendation regarding CAC use enforcement and will coordinate with Service Surgeons General to work toward enforcement of CAC usage. AHLTA and Essentris are CAC enabled with compliance enforced at the Service and Military Treatment Facility (MTF) level. A proposed CAC solution for CHCS is currently in testing.

Recommendation 1.b. (page 22)
We recommend that the Chief Information Officer, Health Information Technology, DHA:

b. Configure passwords for the [redacted] and [redacted] to meet Department of Defense (DoD) complexity requirements.

DHA Response: DHA concurs with this recommendation. [redacted] (a Commercial Off The Shelf (COTS) product) provides password capability that meets DoD complexity requirements; DHA will work with Service/MTF leadership to enforce these policies and ensure appropriate accountability.

Recommendation 1.b on page 23

Recommendation 1.c. (page 22)
We recommend that the Chief Information Officer, Health Information Technology, DHA:

c. [redacted] for the [redacted]

DHA Response: DHA concurs with this recommendation. The underlying [redacted] system hardware and Oracle database do not currently allow [redacted] The required waiver for [redacted] continues to be maintained. Data continues to be [redacted]

2

Recommendation 1.c on page 23

Defense Health Agency (cont'd)

Recommendation 1.d. (page 22)
We recommend that the Chief Information Officer, Health Information Technology, DHA:

d. Implement procedures to verify that privacy impact assessments are developed for all systems, including the Comed Anatomic Pathology System, that store, process, and transmit patient health information.

DHA Response: DHA concurs with this recommendation. Comed Anatomic Pathology System (CoPath) is an Army-specific COTS system. An Interface Control Document specifying the interface requirements between CHCS and the CoPath System was provided during the course of the audit.

3

Final Report Reference

Recommendation 1.d on page 24

U.S. Army Medical Command

DEPARTMENT OF THE ARMY
OFFICE OF THE SURGEON GENERAL
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042-5140

REPLY TO ATTENTION OF

MCIR

01 MAY 2017

MEMORANDUM FOR Department of Defense Inspector General, Contract Management and Payments, ATTN: [redacted], 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Reply to DoDIG Draft Report, Improved Security Protocols Are Needed to Protect Army Electronic Health Records (Project No. D2016-D000RC-0187.000)

1. Thank you for you the opportunity to review this report.

2. The Defense Health Agency (DHA) was established to assume responsibility for shared services, functions and activities of the Military Health System and other common clinical and business processes. Health Information Technology transitioned to the DHA as a shared service in FY14. The transition consolidates health information technology management, infrastructure, and applications under DHA, creating a single point of accountability for the delivery of information technology services. Therefore, findings and recommendations involving systems that store, process and transmit patient health information should be coordinated and jointly addressed by the Army and DHA to ensure standardized solutions are developed and implemented across the Department of Defense.

3. Our comments on the recommendations are enclosed for your consideration.

4. Our point of contact is [redacted], Internal Review and Audit Compliance Office, [redacted], or email [redacted].

FOR THE SURGEON GENERAL:

ROBERT L. GOODMAN
Chief of Staff

Encl

U.S. Army Medical Command (cont'd)

US Army Medical Command (MEDCOM) and
Office of The Surgeon General (OTSG)

Comments on DoDIG Draft Report
Improved Security Protocols
Are Needed to Protect Army Electronic Health Records
(Project No. D2016-D000RC-0187.000)

RECOMMENDATION 2: DoDIG recommends the Chief Information Officer, US Army Medical Command:

a. Develop and implement a plan to ensure the Military Treatment Facilities (MTFs) appropriately configure changes to enforce the use of Common Access Cards (CAC) to access the Armed Forces Health Longitudinal Technology Application (AHLTA), Composite Health Care System (CHCS), and Clinical Information System/Essentris Inpatient System.

b. Develop and implement a plan to ensure the MTFs configure passwords for the [redacted] to meet DoD complexity requirements.

c. Review and identify all systems used to process, store, and transmit patient health information, develop a baseline of systems used at each MTF, and regularly, at least annually, validate the accuracy of the inventory of Army-specific systems.

RESPONSE: Concur. Health Information Technology transitioned to the Defense Health Agency (DHA) as a shared service in FY14, and the DHA Chief Information Officer is the Authorizing Official for accreditation and cyber security issues. Accordingly, MEDCOM will coordinate with DHA to ensure standardized implementation of CAC use and password complexity across the Military Health System (MHS). Collaboration with clinical personnel will minimize risks to patient safety and ensure access to care during implementation.

In addition, MEDCOM will review and identify Army-specific systems used to process, store, and transmit patient health information and validate inventory accuracy at least annually during the Organizational Inspection Program. The review and baseline inventory is expected to be complete by 1 August 2017.

RECOMMENDATION 3: DoDIG recommends the Chief Information Officers for Army MTFs:

a. Implement appropriate configuration changes to enforce the use of CACs to access all Army-specific systems containing patient health information or obtain a waiver that exempts the systems from using CACs.

Encl

U.S. Army Medical Command (cont'd)

b. Configure passwords for all Army-specific systems to meet DoD complexity requirements.

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

d. [redacted] for all Army-specific systems that store patient health information.

e. Require written justification as a condition for obtaining access to the AHLTA, CHCS, Clinical Information System/Essentris Inpatient System, and all Army-specific systems and implement procedures to grant access to the systems based on roles that align with user responsibilities.

f. Configure all Army-specific systems to automatically lock after 15 minutes of inactivity.

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

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

i. Review and identify all systems used to process, store, and transmit patient health information, develop a baseline of systems used at each MTF, and regularly, at least annually, validate the accuracy of the inventory of Army-specific systems.

RESPONSE: Concur. MEDCOM will coordinate with DHA and work toward enforcement of CAC usage; password complexity; mitigation of network vulnerabilities; [redacted] system access and privileges; automatic lockout procedures; audit log configuration and review within the parameters of standard MHS solutions. Collaboration with clinical personnel will ensure implementation minimizes risks to patient safety and ensuring access to care.

In addition, MEDCOM will review and identify Army-specific systems used to process, store, and transmit patient health information and validate inventory accuracy at least annually during the Organizational Inspection Program. The review and baseline inventory is expected to be complete by 1 August 2017.

RECOMMENDATION 4: DoDIG recommends the Commanders, Brooke Army Medical Center, Evans Army Community Hospital, and Kimbrough Ambulatory Care 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.

2

U.S. Army Medical Command (cont'd)

- Not formally accepting risks for unmitigated vulnerabilities believed to negatively impact patient care.

RESPONSE: OTSG/MEDCOM assumes responsibility for the recommended actions and partially concurs with the recommendation. We agree on the necessity for Chief Information Officers to follow Federal and DoD guidance for protecting patient health information and concur DoDIG found un-remediated vulnerabilities at some Army MTFs. MEDCOM will coordinate with DHA and third party vendors to remediate and/or mitigate all known vulnerabilities.

OTSG/MEDCOM does not concur with the recommendation to review the performance of the Chief Information Officers and consider administrative action. MTF Commanders will continue to objectively review performance of personnel based on established standards in accordance with applicable regulations. If administrative action is deemed appropriate, it will be addressed through that process.

RECOMMENDATION 5: DoDIG recommends the Chief Information Officer, Kimbrough Ambulatory Care Center, require Picture Archiving and Communications System users, at a minimum, to require a password to protect patient health information stored on or downloaded to external media.

RESPONSE: Concur. MEDCOM will coordinate with DHA to ensure implementation aligns with standardized policy across the MHS.

RECOMMENDATION 6: DoDIG recommends the Chief Information Officer, Brooke Army Medical Center, develop, test, and implement applicable changes to the Mammography Reporting System to allow users to authenticate using a CAC when accessing multiple systems simultaneously.

RESPONSE: Concur. The Mammography Reporting System (MRS) is CAC-enabled for all roles except radiologist. All users, including radiologists, first have to log onto the Picture Archiving and Communications System (PACS) workstations using CAC based network authentication before gaining access all radiology information systems. MRS is one of four applications (MRS, Powerscribe Voice Recognition, Peer Review, and Vitrea 3D rendering software) integrated into the PACS application using application interfaces. This integration provides the interface between the five applications to allow a radiologist to use the PACS to manage a comprehensive and reliable patient dataset to provide diagnosis of disease.

During the DoDIG visit, not all applications supported CAC authentication (specifically MRS and Peer Review). Once a radiologist authenticates into the workstation using their CAC, the radiologist uses their user name and password to access the other applications including MRS and Peer Review. The other MRS roles, including technologist, use CAC authentication into MRS to manage patient workflow within the

3

U.S. Army Medical Command (cont'd)

Mammography Section (other roles do not use the PACS/MRS integration to perform their duties like radiologists). The MRS user name and password configuration is set on only four PACS workstations used by the 63 radiologists for mammography diagnosis after successful network authentication utilizing CAC onto the PACS workstation itself.

AR 25-2 section 4-5 c(7) authorizes the use of username and password for systems which are incapable of CAC authentication until these systems are replaced. To further mitigate the potential for a security breach, all radiology medical systems, to include MRS, Powerscribe Voice Recognition, Peer Review, and Vitrea 3D and PACS, reside on a network which is separated from all other hospital network traffic through the use of firewall access control lists. All PACS workstations are physically located within areas that are restricted from patient access and all PACS workstations are deployed with security controls and group policies which mandate lock out times and do not allow radiologists to access hard drives, emails, or other non-medical applications that could impact the medical device classification of the applications. MRS has an approved DoD Information Assurance Certification and Accreditation Process with an authorization termination date of 26 September 2017.

Two of the integrated information systems (MRS and Peer Review) that did not support CAC authentication are scheduled for upgrades in order to meet CAC compliance. During the week of 13 March, Peer Review was upgraded and formal testing of the CAC-based authentication integration is scheduled for the week of 3 April 2017 with the vendor. The MRS application is scheduled for upgrade the week of 10 April 2017, with subsequent testing of CAC-based authentication and integration with all of the applications connected to the PACS. We anticipate a total CAC-based solution for all of the integrations will be complete by the end of May 2017.

REVIEW OF INTERNAL CONTROLS: DoDIG reported internal control weakness related to protecting systems that store, process, and transmit PHI. Specifically, DHA and Army officials did not consistently implement technical, physical, and administrative protocols to protect DoD Electronic Health Record (EHR) systems and Army-specific systems from unauthorized access and disclosure.

RESPONSE: MEDCOM does not concur with the conclusion that the Army did not consistently protect EHR and Army-specific systems from unauthorized access and disclosure. There have been no reported instances of system breaches, data loss, or manipulation at MTFS associated with the conditions discussed in the report.

Further, health information technology is a Shared Service and responsibility for these systems resides with DHA. Internal control weaknesses involving systems that store, process and transmit PHI should be addressed by DHA to ensure standardized solutions are developed and implemented across DoD.

Glossary

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

Common Access Cards (CACs). Identification cards 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, require immediate patches.

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

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

External Media. Portable electronic storage media such as magnetic, optical, and solid-state devices that can be inserted into and removed from a computer. Examples include hard discs, floppy discs, zip drives, compact discs, thumb drives, and similar universal serial bus storage devices.

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. Is 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 from an individual that is created or obtained by a covered entity 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 Assessments. A written analysis of potential privacy risks and mitigating actions.

Standard Operating Procedures. 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.

Acronyms and Abbreviations

AHLTA	Armed Forces Health Longitudinal Technology Application
CAC	Common Access Card
CHCS	Composite Health Care System
CIO	Chief Information Officer
CoPath	Comed Anatomic Pathology System
DHA	Defense Health Agency
EHR	Electronic Health Record
Essentris	Clinical Information System/Essentris Inpatient System
HIP	High Interest Patient Database
HIPAA	Health Insurance Portability and Accountability Act
MEDCOM	United States Army Medical Command
MRS	Mammography Reporting System
MTF	Military Treatment Facility
NIST SP	National Institute of Standards and Technology Special Publication
PACS	Picture Archiving and Communications System
PHI	Patient Health Information
POA&M	Plan of Action and Milestones

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/programs/whistleblower.

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

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
www.dodig.mil/pubs/email_update.cfm

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

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