UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

PERSONNEL AND READINESS

APR 26 2023

The Honorable Jack Reed
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

The Department's response to the Joint Explanatory Statement, page 148, accompanying H.R. 2471, the Consolidated Appropriations Act for Fiscal Year 2022 (Public Law 117–103), "Department of Defense Controlled Access to Health Information," is enclosed.

The report describes the measures taken by the Defense Health Agency (DHA) in response to the recommendations from the final report of the Department of Defense Office of the Inspector General, "Audit of the Department of Defense's Controls on Health Information of Well-Known Department of Defense Personnel," including the implementation of enhanced information system controls to help deter and improve early detection of potential unauthorized access of protected health information.

DHA performed an extensive review of the unauthorized and undetermined access of protected health information identified in the audit. The report describes in detail the findings of this review, including any disciplinary action against individuals found to have accessed protected health information without authorization.

Thank you for your continued strong support for the health and well-being of our Service members, veterans, and their families. I am sending similar letters to the other congressional defense committees.

Sincerely,

Gilbert R. Cisneros, Jr.

Enclosure:
As stated

cc:
The Honorable Roger F. Wicker
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

PERSONNEL AND READINESS

APR 26 2023

The Honorable Mike D. Rogers
Chairman
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

The Department's response to the Joint Explanatory Statement, page 148, accompanying H.R. 2471, the Consolidated Appropriations Act for Fiscal Year 2022 (Public Law 117–103), "Department of Defense Controlled Access to Health Information," is enclosed.

The report describes the measures taken by the Defense Health Agency (DHA) in response to the recommendations from the final report of the Department of Defense Office of the Inspector General, "Audit of the Department of Defense's Controls on Health Information of Well-Known Department of Defense Personnel," including the implementation of enhanced information system controls to help deter and improve early detection of potential unauthorized access of protected health information.

DHA performed an extensive review of the unauthorized and undetermined access of protected health information identified in the audit. The report describes in detail the findings of this review, including any disciplinary action against individuals found to have accessed protected health information without authorization.

Thank you for your continued strong support for the health and well-being of our Service members, veterans, and their families. I am sending similar letters to the other congressional defense committees.

Sincerely,

Gilbert R. Cisneros, Jr.

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

PERSONNEL AND
READINESS

APR 2 6 2023

The Honorable Jon Tester
Chairman
Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

The Department's response to the Joint Explanatory Statement, page 148, accompanying H.R. 2471, the Consolidated Appropriations Act for Fiscal Year 2022 (Public Law 117–103), "Department of Defense Controlled Access to Health Information," is enclosed.

The report describes the measures taken by the Defense Health Agency (DHA) in response to the recommendations from the final report of the Department of Defense Office of the Inspector General, "Audit of the Department of Defense's Controls on Health Information of Well-Known Department of Defense Personnel," including the implementation of enhanced information system controls to help deter and improve early detection of potential unauthorized access of protected health information.

DHA performed an extensive review of the unauthorized and undetermined access of protected health information identified in the audit. The report describes in detail the findings of this review, including any disciplinary action against individuals found to have accessed protected health information without authorization.

Thank you for your continued strong support for the health and well-being of our Service members, veterans, and their families. I am sending similar letters to the other congressional defense committees.

Sincerely,

Gilbert R. Cisneros, Jr.

Enclosure:
As stated

cc:
The Honorable Susan Collins
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

PERSONNEL AND
READINESS

APR 26 2023

The Honorable Ken Calvert
Chairman
Subcommittee on Defense
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

The Department's response to the Joint Explanatory Statement, page 148, accompanying H.R. 2471, the Consolidated Appropriations Act for Fiscal Year 2022 (Public Law 117–103), "Department of Defense Controlled Access to Health Information," is enclosed.

The report describes the measures taken by the Defense Health Agency (DHA) in response to the recommendations from the final report of the Department of Defense Office of the Inspector General, "Audit of the Department of Defense's Controls on Health Information of Well-Known Department of Defense Personnel," including the implementation of enhanced information system controls to help deter and improve early detection of potential unauthorized access of protected health information.

DHA performed an extensive review of the unauthorized and undetermined access of protected health information identified in the audit. The report describes in detail the findings of this review, including any disciplinary action against individuals found to have accessed protected health information without authorization.

Thank you for your continued strong support for the health and well-being of our Service members, veterans, and their families. I am sending similar letters to the other congressional defense committees.

Sincerely,

Gilbert R. Cisneros, Jr.

Enclosure:
As stated

cc:
The Honorable Betty McCollum
Ranking Member

Report to the Congressional Defense Committees

Department of Defense Controlled Access to Health Information

April 2023

The estimated cost of this report or study for the Department of Defense (DoD) is approximately $4,300 for the 2022 Fiscal Year. This includes $2,000 in expenses and $2,300 in DoD labor.

Generated on 2022 June 2

Report/Study Cost Estimate
(4-972947F)

EXECUTIVE SUMMARY

This report is in response to Joint Explanatory Statement, page 148, accompanying H.R. 2471, the Consolidated Appropriations Act for Fiscal Year 2022 (Public Law 117–103), requesting the status of the implementation of recommendations from the Department of Defense (DoD) Office of the Inspector General (OIG) report, "Audit of the DoD's Controls on Health Information of Well-Known DoD Personnel," and any additional cybersecurity measures taken by the Department. In its report, OIG recommended that DoD develop and implement the necessary information system controls to detect potential unauthorized access of protected health information (PHI) of all DoD personnel and perform a review of the unauthorized and undetermined access of PHI identified in the audit. OIG specified that, based on the results of the review, DoD should take disciplinary action against any individuals found to have accessed PHI without authorization and report those incidents as required by the applicable laws and existing DoD guidance. This report summarizes information system controls in use within the Military Health System (MHS) to prevent and detect potential unauthorized access of PHI of DoD personnel; provides an overview of the results of the Defense Health Agency (DHA) analysis of incidents cited by OIG; and cites any subsequent disciplinary action and formal reporting.

INFORMATION SYSTEM CONTROLS TO DETECT POTENTIAL UNAUTHORIZED ACCESS

Protecting the medical records of all personnel from any unauthorized access, including employee snooping, is something DHA strives for each day through training, certification, internal controls, and systems hardening. While it is not possible to prevent unauthorized employee access of medical records in all cases, it is possible to reduce risk. The interdepartmental nature of medicine requires teams of people to treat a single patient. For example, a primary care physician requires the support of other people in labs, pharmacy, radiology, and multiple departments in a hospital. By design, the medical records of DoD personnel can be viewed by many providers and support staff across the MHS, and it is possible for authorized personnel to abuse their privileges. DHA mitigates risk of unauthorized access or release of beneficiaries' PHI by implementing enterprise-level strategies to standardize and enforce security policies and procedures. Current DHA guidance incorporates DoD Security Directives and Instructions, as well as best practices tailored to the needs of the medical community. Risk of unauthorized access or release of PHI is managed through:

- Mandatory completion of Health Insurance Portability and Accountability Act (HIPAA) training prior to a user receiving access to MHS electronic health record (EHR) systems.

- Use of strong passwords and multi-factor authentication on MHS clinical work stations and approved systems.

- Identification and mitigation of network vulnerabilities (e.g., scanning, monitoring, and patching).

- Encryption of patient health data transmitted between systems using Federal Information Processing Standards 140-2 compliant cryptography.

- Automated configuring systems to lock automatically in areas where casual access by non-privileged users could be a problem. (An exception is granted for treatment and operating rooms where display of relevant patient data is required throughout a procedure.)

- Limiting access to PHI by means of the MHS user account management process, which requires annual verification that user access and privileges are appropriately aligned with a user's role.

- Use of system audit log monitoring procedures to review documented user activity.

The targeted actions taken by DHA while implementing the OIG recommendations build upon the steps listed above. Through each of the efforts described below, DHA has significantly enhanced its capability to detect and prevent potential unauthorized access; these enhanced capabilities facilitate identification of, and support disciplinary action and reporting for, unauthorized access of PHI.

EHR Enhanced Protection Program for Senior DoD Personnel: In Fourth Quarter, Fiscal Year (FY) 2020, in response to guidance from the Secretary of Defense and initial findings from the OIG audit, the DHA implemented its 4-Star Protocol EHR Protection program. The objective of these enhanced protections is to limit access to medical records of high-profile DoD personnel to only those medical professionals with a need to know (e.g., the clinician assigned as the individual's Primary Care Manager). At the inception of the program, enhanced protections were automatically implemented for the Secretary of Defense, Deputy Secretary of Defense, and Chairman of the Joint Chiefs of Staff. Others who qualify for this program include those in the rank of General or Admiral, and civilian personnel in positions of responsibility specified in Code 2 and part of Code 3 of the DoD Revised Order of Precedence. As incoming high-profile personnel are confirmed by the U.S. Senate and assume their new role, they are presented with the option to opt into this program via an unclassified email announcing their eligibility for the program and requesting a secure internet protocol router phone call. During this call, the DHA Chief Information Officer (CIO) provides detailed information regarding the enhanced protection options and their associated risks so an informed decision can be made. These enhanced protections may also be selected for spouses and immediate family members. Regardless of whether a qualified individual opts in or not, access to their medical records is routinely monitored. Access monitoring is performed for the records of qualified individuals in each of the legacy EHR systems: Armed Forces Health Longitudinal Technology Application (AHLTA), Composite Health Care System (CHCS), Essentris, Health Artifact and Image Management Solution (HAIMS), and the Joint Longitudinal Viewer (JLV)[1].

[1] AHLTA is the DoD outpatient EHR. CHCS serves as the foundation for AHLTA and enables DoD providers to document patient health information and history, electronically order laboratory and radiology tests/services, retrieve test results and order/prescribe medications. Essentris is the DoD inpatient EHR. HAIMS provides DoD and Department of Veterans Affairs (VA) health care providers global visibility and access to artifacts and images. JLV is a clinical application that provides an integrated, read-only display of health data from the DoD, VA, and private sector partners in a common data viewer.

Restriction of access to medical records of those who opted into the program and monitoring for all qualified individuals requires coordination between the DHA CIO and the Program Executive Office, Defense Healthcare Management Systems. A combination of record blocking, marking records as sensitive, and monitoring of weekly system audit logs is employed. Audit logs capture user actions spanning from user login and patient search and selection data, to user requests to view record/document details, as well as AHLTA break-the-glass transactions on sensitive patients or sensitive clinical information. Break-the-glass is a measure that ensures a provider who does not have access to certain medical information can obtain it when warranted, like when treating a patient experiencing a medical emergency, but must consent to be audited for accessing sensitive data. This ensures the event is documented and auditable.

Enhanced Legacy System Records Protections for All Beneficiaries: In the Fourth Quarter FY 2021, DHA implemented enhanced records protection functionality for all MHS beneficiary records within CHCS and AHLTA. Within CHCS this functionality consists of a system prompt requiring the user to select a Reason for Unlock when no clinical event or other qualifying healthcare activity exists. Conditions where a user is prompted to enter a reason when accessing a beneficiary record include: no active inpatient admission exists for the beneficiary record; no upcoming appointment is scheduled within the next 7 days; and no active order is associated with the end-user accessing the record. Whenever a user attempts to access a patient's record meeting the above conditions, they are prompted by the system to select a Reason for Access. These include Ancillary Processing, Chart Review, and Coder. (Users can view the full list of reasons for access by typing a pair of question marks into the Reason for Unlock prompt.) If none of the available options adequately describes the need for access, the user can enter a free text comment by selecting Other from the list of options. After a user selects an option, the beneficiary's record will be unlocked and available to that user for 24 hours.

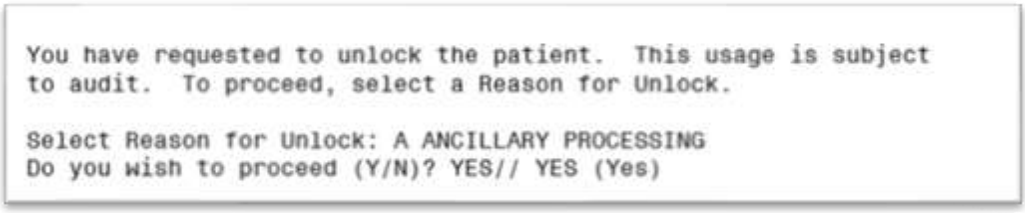

Figure 1: CHCS Reason for Unlock Dialog Box

Similar functionality was implemented within AHLTA; a dialog box (see Figure 2) incorporating radio buttons and a text box prompts the user to provide a Reason for Unlock when no clinical event or other qualifying healthcare activity exists.

Figure 2: AHLTA Reason for Unlock Dialog Box

DHA has taken targeted steps to promote and ensure compliance with the use of the Reason for Unlock capability and to prevent attempts to bypass the capability (e.g., by entering random characters or weak justifications.) Following implementation of this capability, the office of the DHA CIO initiated routine reviews of system audit log reports to identify any users failing to provide an adequate justification. Any non-compliant users are contacted directly by the office of the DHA CIO to demonstrate the high level of oversight being applied to the use of this capability, and to promote enhanced awareness and understanding of the consequences for non-compliance and access of patient information without authorization. Further, a policy memorandum was issued by the DHA Assistant Director for Health Care Administration in First Quarter, FY 2022, making compliance with the Reason for Unlock mandatory for all system users.

In concert with the implementation of the CHCS and AHLTA dialog boxes, break-the-glass transaction requirements were augmented to require that a system user acknowledge that proceeding with viewing any data marked sensitive will result in the action being captured in a system audit report. Users are now required to enter a comment explaining why they need to break-the-glass on sensitive information. This comment must be between 5 and 60 characters long and be descriptive of why the user needs to access the information. Any comments entered are displayed in audit reports. These system audit reports are scrutinized by DHA to determine whether the action was authorized or not. Previous break-the-glass policy required consent to audit sensitive data once per patient session for all sensitive data viewed, instead of prompting the user each time they open a document, as instituted under the new policy. Additional controls include the forced close of any open JLV tabs and Windows when exiting a patient view.

EHR Modernization: As of April 2023, MHS GENESIS is deployed to nearly 80 percent of military treatment facilities, increasing the number of DoD beneficiaries benefiting from the centralized control, monitoring, and auditing capabilities this modern, commercial EHR system provides to protect against unauthorized access to records. The enterprise-wide

deployment of MHS GENESIS is complete at approximately 110 of 138 commands. Throughout 2023, MHS GENESIS will complete deployment at stateside facilities and then move to installations in the European and Indo-Pacific regions. MHS GENESIS is a role-based system and information access is based on the role assigned to individuals required to perform their duties. When accessing a record for the first time, a user is required to Assign a Relationship (i.e., state their role and duties in relationship to this patient) before being allowed to proceed. Like the legacy EHR systems, this action is documented and auditable. Figure 3 depicts the Assign Relationship window presented to a hospitalist attempting to enter a patient's record for the first time. Figure 4 depicts the Patient/Provider Relationships (PPR) summary view of each user who has entered the patient's chart and the relationship established. The PRR summary is readily available within the patient chart.

In second quarter FY 2022, an advanced capability to support tracking, auditing, and real time alerts of user access to confidential patient data was fully implemented within MHS GENESIS. Access to this capability will be expanded to the DHA privacy and security offices by the end of FY 2022 to augment their ability to spot check, query, ensure compliance, and assist in any investigations of HIPAA breach allegations.

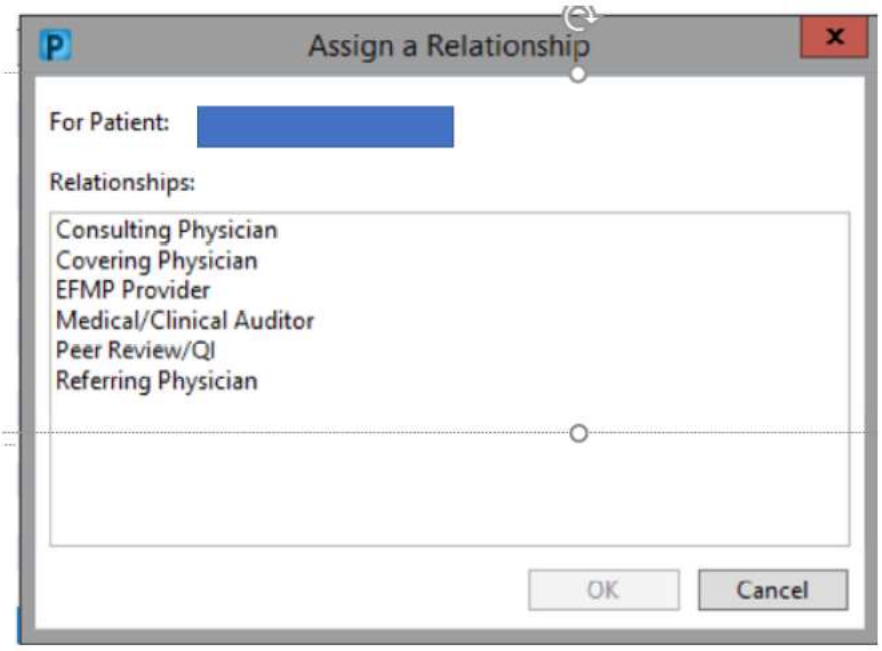

Figure 3: MHS GENESIS Assign a Relationship Dialog Box

While commercial EHRs like MHS GENESIS, which is based on the Cerner Millennium product, are not specifically designed with insider threat security risks in mind, DHA will continue to investigate opportunities to implement additional means of protection against unauthorized access to patient medical records as the MHS GENESIS system matures. Beyond the clinical operations focus, DHA has taken steps to ensure other reporting and analytics capabilities are reviewed to mitigate HIPAA concerns and national security risks. For example, the output from HealtheIntent, the Cerner data and insights platform that aggregates and

normalizes data extracted from EHRs and other clinical and non-clinical sources, is de-identified before it is authorized for release.

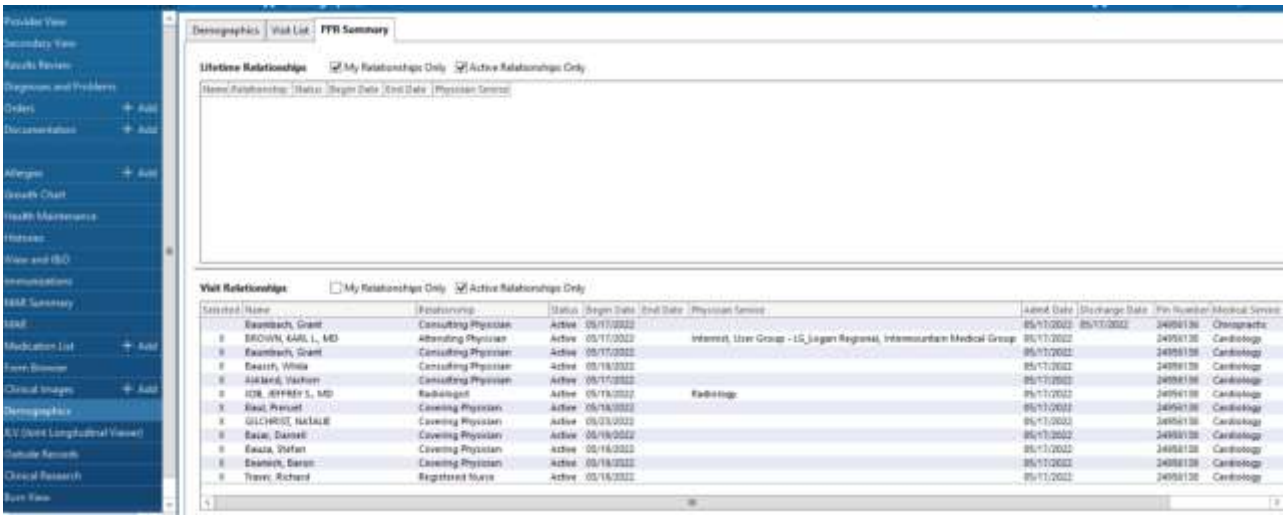

Figure 4: MHS GENESIS Assign a Relationship Dialog Box

REVIEW OF UNAUTHORIZED AND UNDETERMINED ACCESS OF PHI

DHA conducted a review of the unauthorized and undetermined access to PHI identified in the OIG audit and imposed and documented the appropriate disciplinary action against individuals found to have accessed PHI without authorization. In cases where the violators did not have authorization to access an individual's PHI but did not retain or further disclose any information, counseling and remedial HIPAA training were imposed. For low-risk violations where undetermined access to an individual's PHI occurred, remedial training was typically limited to a short 1.5-hour course, while more egregious low risk violations involving access to PHI without authorization resulted in more intensive remedial training. This included a 20-hour extra military instruction (EMI) program on HIPAA and the importance of safeguarding personally identifiable information, impact to the command's mission, and the legal and punitive consequences for violations. EMI training sessions are typically required to be completed in addition to the regular duty day. For substantiated violations cited in the OIG report that were determined to be of higher risk, more severe penalties were levied, including two suspensions and three terminations. As required, any substantiated violations have been reported in accordance with applicable laws and DoD guidance. Breaches related to the National Capital Region, prior to transition to DHA, were reported to the Defense Privacy, Civil Liberties and Transparency Division via the Compliance and Report Tool (CART). Additionally, breaches involving the Services received after transition to DHA, were also reported to CART as required.

The DHA review and any subsequent sanctions were executed in accordance with current privacy and breach prevention policy and best practices. Regularly communicating the implications of compliance violations for individuals and the organization, and ensuring consequences are imposed plays a significant role in ensuring staff members take compliance seriously. DHA actively promotes awareness of its policy and best practices to help prevent violations and breaches from occurring and uses standard disciplinary processes to determine

specific sanctions according to the severity and circumstances of violations. It is standard practice to include consequences and penalties for staff member noncompliance in employee manuals; to require retraining and completion of remedial training on the appropriate privacy and security policies; and to impose stiffer penalties such as suspension, revocation of access, or termination for substantiated violations. Enforcement of sanctions for compliance violations is vital to breach prevention, including employee snooping activities.

Going forward, the enhancements made to both the legacy EHR systems and MHS GENESIS will play a critical role in deterring unauthorized access and in aiding and informing any required review or audit of record access. The availability of data on the Reason for Unlock/Assign Relationship supplied by the individual user is expected to significantly reduce the likelihood that a reason for record access is labeled as undetermined by supporting the determination of whether an official reason for access exists and assisting in substantiating allegations. In turn, these enhancements and the real time, documented context they capture will provide DHA with the data required to better assess suspected violations and to impose stiffer penalties for compliance when violations occur.

CONCLUSION

DHA remains steadfast in its commitment to fulfilling its responsibility for safeguarding the privacy and security of PHI while balancing the need to maintain and share information about individuals to perform MHS' mission and business functions. The enhanced protections and improved auditing capabilities implemented within its legacy EHR systems facilitate the monitoring and detection of potential unauthorized access to PHI and support timely disciplinary action and required reporting of any identified unauthorized access. Through its ongoing EHR modernization, the Department will realize a centrally managed, standardized set of enterprise-wide information system controls and processes to further enhance protections against the unauthorized access of PHI of its personnel. DHA will continue to demonstrate due diligence in prevention of unauthorized access to PHI of DoD beneficiaries and will ensure that sanction policies are applied appropriately against workforce members who fail to comply with the privacy/security policies and procedures of the organization.