Defense Health Agency

PROCEDURAL INSTRUCTION

NUMBER 8100.01
January 12, 2021

DAD-IO

SUBJECT: Information Security Compliance for Defense Health Agency Financially Auditable Information Systems

References: See Enclosure 1

1. PURPOSE. This Defense Health Agency-Procedural Instruction (DHA-PI), based on the authority of References (a) and (b), and in accordance with the guidance of References (e), (j) through (l), and (p) through (r), establishes responsibilities for financially auditable systems. It provides direction to implement DHA procedures that contribute to a clean financial audit for the DoD.

2. APPLICABILITY. This DHA-PI applies to all organizations or facilities which manage or operate DHA Information Systems (ISs) that are material to financial auditability. As of February 2020, the list of DHA ISs which have been identified as material to DHA financial auditability includes:

a. Armed Forces Billing and Collection Utilization Solution (ABACUS)

b. Coding and Compliance Editor (CCE)

c. Composite Healthcare System (CHCS)

d. Defense Medical Logistics Standard Support (DMLSS)

e. Military Health System (MHS) GENESIS

3. POLICY IMPLEMENTATION.

a. Site Commanders/Directors and staff at facilities where DHA ISs are used have a significant role in implementing, enforcing, and maintaining applicable DHA IS information security controls. Proper implementation requires Site Commanders/Directors and staff to manage across their supporting human resources (HR), information technology, and financial sections. For example, Site Commanders/Directors are responsible for account management controls for their users' accounts because personnel security, in-/out-processing, and granting of system permissions are all established locally.

b. This DHA-PI directs Site Commanders/Directors, or their formally appointed delegates, to regularly assess the status of their sites' compliance with the applicable DHA IS information security controls.

c. The information security control compliance monitoring and reporting procedures established in this DHA-PI align with Government Accountability Office (GAO), Office of Management and Budget (OMB), and DoD financial auditing requirements established in References (f) through (i) and are separate and distinct from the Cybersecurity and Risk Management Framework (RMF) procedures described in the DHA Cybersecurity Program Management Administrative Instruction (Reference (l)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3, and References (m) through (o).

6. PROPONENT. The proponent of this DHA-PI is the Deputy Assistant Director (DAD), Information Operations (IO). When an Activity is unable to comply with this publication the activity may request a waiver by providing justification that includes a full analysis of the expected benefits and must include a formal review by the activities senior legal officer. The activity director or senior leader will endorse the waiver request and forward it through their chain of command to the Director, DHA, to determine if the waiver may be granted.

7. RELEASABILITY. **Cleared for public release**. This DHA-PI is available on the Internet from the Health.mil site at: https://health.mil/Reference-Center/Policies and is also available to authorized users from the DHA SharePoint site at: https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx.

8. EFFECTIVE DATE. This DHA-PI:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with Reference (c).

/S/
RONALD J. PLACE
LTG, MC, USA
Director

Enclosures
1. References
2. Responsibilities
3. Site Level Compliance Reporting Procedure
4. Compliance Reporting Requirements

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs," September 30, 2013, as amended

(b) DoD Directive 5136.13, "DHA," September 30, 2013

(c) DHA-PI 5025.01, "Publication System," August 24, 2018

(d) The Federal Information Security Modernization Act (FISMA) of 2014

(e) National Institute of Standards and Technology (NIST) SP 800-53, revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," January 22, 2015

(f) GAO-09-232G, "Federal Information System Controls Audit Manual (FISCAM)," February 2, 2009

(g) GAO-18-568, "Generally Accepted Government Auditing Standards 2018 Revision ('Yellow Book')," July 17, 2018

(h) OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control"

(i) DoD Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer "Financial Integrity and Audit Readiness Guidance," April 2017

(j) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

(k) DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," March 12, 2014, as amended

(l) DHA-Interim Procedures Memorandum 18-015, "Cybersecurity Program Management," September 28, 2020

(m) DHA DAD IO Memorandum, "Access Controls for DHA System User Account Management," August 28, 2018[1]

(n) System Management Plans (SMPs) for Auditable DHA Deputy Assistant Director, Information Operations Systems[2]

(o) Information Security Compliance Reporting Instructions (CRIs) for Auditable DHA Deputy Assistant Director, Information Operations Systems[3]

(p) DoD 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019

[1] https://info.health.mil/dadio/CM/wg/hitwg/Documents/Forms/AllItems.aspx?RootFolder=%2Fdadio%2FCM%2Fwg%2Fhitwg%2FDocuments%2FMHS%20CIO%20Directives%2FFiscal%20Year%202018%20Directives&FolderCTID=0x0120001380F919218F84488DCED55DF43386CA&View=%7B4066D62C%2D77CC%2D48D1%2DB0E5%2D1164F6E0CDC1%7D

[2] https://info.health.mil/dadio/CM/wg/hitwg/Documents/Forms/AllItems.aspx?RootFolder=%2Fdadio%2FCM%2Fwg%2Fhitwg%2FDocuments%2FMHS%20CIO%20Directives&FolderCTID=0x0120001380F919218F84488DCED55DF43386CA&View=%7B4066D62C%2D77CC%2D48D1%2DB0E5%2D1164F6E0CDC1%7D

[3] https://info.health.mil/dadio/CM/wg/hitwg/Documents/Forms/AllItems.aspx?RootFolder=%2Fdadio%2FCM%2Fwg%2Fhitwg%2FDocuments%2FMHS%20CIO%20Directives&FolderCTID=0x0120001380F919218F84488DCED55DF43386CA&View=%7B4066D62C%2D77CC%2D48D1%2DB0E5%2D1164F6E0CDC1%7D

(q) DoDM 6028.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019
(r) DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. Director, DHA, will: Enforce DHA compliance with the DHA-PI.

2. SECRETARIES OF MILITARY MEDICAL DEPARTMENTS. The Secretaries of the Military Medical Departments will ensure that applicable facilities under their control comply with this DHA-PI.

3. DAD-IO. DAD-IO will monitor compliance with this DHA-PI and work with applicable DHA IS Owners and Site Commanders/Directors to resolve non-compliance issues.

4. DHA IS OWNERS. DHA IS Owners, defined as DHA Program Managers who own and manages applicable DHA ISs, will:

a. Provide information security control guidance by publishing policies and procedures governing how Site Commanders/Directors will implement, enforce, maintain, assess, report, and mitigate identified weaknesses in their sites' compliance with applicable information security controls.

(1) The full list of Federal Information Security Modernization Act information security requirements (Reference (d)).

(2) The full list of National Institute of Standards and Technology SP 800-53 (Reference (e)) information security controls.

(3) Processes and standards for assessing financially auditable systems' compliance with applicable information security controls as prescribed in Reference (f).

(4) Enterprise level DHA guidance on the specific information security controls applicable to each financially auditable DHA system and the unique processes by which those controls should be implemented and operated at the site level are detailed in the individual system-specific System Management Plans (Reference (n)).

(5) Enterprise level DHA guidance on the applicable procedures by which sites using financially auditable DHA systems should assess and report the status of their compliance with the information security controls described in Reference (n) are detailed in the individual system-specific CRI documents (Reference (o)).

b. Monitor user information security control compliance and require Site Commanders/ Directors to implement corrective action to mitigate any identified deficiencies.

(1) In accordance with Reference (o), DHA IS Owners will review each user entity site's monthly compliance report along with any applicable supporting evidentiary artifacts. Reports will be maintained for a period of no less than 3 years.

(2) If a site reports non-compliance with applicable information security controls, the DHA IS Owner will require the site to undertake specific corrective actions to mitigate the identified risks and bring the site into compliance.

(3) DHA IS Owners will monitor the status of all required corrective actions to confirm successful mitigation of the identified risk.

5. MILITARY HEALTH SYSTEM (MHS) FUNCTIONAL LEADS. MHS Functional Leads, defined as the leaders of the MHS functional communities which comprise the primary user base for applicable DHA ISs (e.g., DHA Medical Logistics for DMLSS, DHA Uniform Business Office (UBO) for ABACUS), will:

a. Support DHA Market and/or Military Medical Department leadership in their efforts to ensure their facilities' compliance with this DHA-PI.

b. Serve as liaison between DHA IS Owners and System Users to ensure that guidance produced by DHA IS Owners is disseminated to and implemented by each system's applicable DHA functional community.

6. DIRECTORS, DHA LARGE MARKETS, SMALL MARKETS AND STAND-ALONE ORGANIZATIONS (SSO), DEFENSE HEALTH REGIONS. Directors, DHA Large Markets, Small Markets and Stand-Alone Organization, Defense Health Region will: Ensure that applicable facilities under their control comply with this DHA-PI.

7. SITE COMMANDERS/DIRECTORS. Site Commanders/Directors, defined as Commanders/Directors of Military Treatment Facilities (MTFs) or other facilities at which site personnel operate applicable DHA ISs, will:

a. Implement site-level information security controls to ensure that their sites effectively implement, enforce, and maintain compliance with DHA IS information security controls, in accordance with the instructions and procedures described in References (n) and (o). At the discretion of the Site Commander/Director, this responsibility can be formally delegated to the site's Chief Information Officer (CIO) through a signed memorandum for record.

b. Assess, report, and mitigate weaknesses in site-level information security control compliance.

(1) In accordance with Reference (o), Site Commanders/Directors will ensure that their sites assess and report the status of their sites' compliance with applicable DHA IS information security controls through submission of DHA's "CIO Monthly Reporting and Certification" available at https://learn.insights.health.mil/resources/#!/cio-report. Enclosure (4) summarizes reporting requirements.

(2) For the information security controls not included in the CIO Monthly Reporting and Certification, Site Commanders/Directors will ensure that their sites assess and report the status of their sites' compliance with DHA ISs as directed in Reference (o).

(3) For sites found to be non-compliant with DHA IS information security controls, Site Commanders/Directors will ensure that their sites implement applicable corrective actions to remediate identified compliance deficiencies as needed.

8. SITE CIOs. Site CIOs, defined as the CIOs of MTFs or other facilities at which site personnel operate applicable DHA ISs, will:

a. Assist Site Commanders/Directors to effectively implement, enforce, and maintain compliance with DHA IS site-level information security controls at their sites, by executing the procedures described in References (n) and (o).

b. Assist Site Commanders/Directors to continuously assess, report, and mitigate identified weaknesses in their sites' information security control compliance status to DHA, supported by required evidentiary artifacts, by executing the procedures described in Reference (o) as discussed above in Enclosure 2, "Site Commanders/Directors." In particular, Site CIOs are responsible for completing and submitting the Site CIO Monthly Reporting Template, on behalf of their Site Commanders/Directors.

9. SITE HR ORGANIZATIONS. Site HR organizations, defined as the HR organizations within MTFs or other facilities at which site personnel operate applicable DHA ISs, will:

a. Assist Site Commanders/Directors to effectively implement, enforce, and maintain compliance with DHA IS site-level information security controls at their sites, by executing procedures related to personnel security, in-/out-processing, and duty assignments described in References (n) and (o) as discussed above in Enclosure 2, "Site Commanders/Directors." In particular, Site HR organizations are responsible for monitoring site personnel arrivals, departures, and changes in duty assignments to ensure that applicable DHA IS accounts used by site personnel are accordingly modified and/or revalidated.

b. Assist Site Commanders/Directors to continuously assess, report, and mitigate identified weaknesses in their sites' information security control compliance status to DHA, supported by required evidentiary artifacts, by executing the procedures related to personnel security, in-/out-processing, and duty assignment described in Reference (o) as discussed above in Enclosure 2, "Site Commanders/Directors." In particular, Site CIOs are responsible for completing and submitting the CIO Monthly Reporting and Certification on behalf of their Site Commanders/Directors.

10. SYSTEM USERS. System users, defined as MTF or other facility personnel who use or operate applicable DHA ISs, will:

a. Assist Site Commanders/Directors to effectively implement, enforce, and maintain compliance with DHA IS information security controls at their sites, by executing the procedures described in References (n) and (o).

b. Assist Site Commanders/Directors to continuously assess, report, and mitigate identified weaknesses in their sites' information security control compliance status to DHA, by executing the procedures described in Reference (o).

ENCLOSURE 3

SITE LEVEL COMPLIANCE REPORTING PROCEDURES

1. ASSESS AND REPORT SITE LEVEL IS CONTROL COMPLIANCE

a. Each Site (defined as MTF or other facility at which site personnel operate applicable DHA ISs, as defined in Enclosure 2 of this DHA-PI) will continuously assess and report their site's information security control compliance status to the system's DHA IS Owner, supported by required evidentiary artifacts, in compliance with the procedures described in Reference (o).

b. Each Site will provide regular reports to the DHA IS Owner and appropriate functional community on the status of their site's compliance with the applicable site-level information security controls identified in Reference (n).

c. Each Site will complete and submit the CIO Monthly Reporting and Certification to report on specific site-level information security controls, in compliance with the procedures described in Reference (o). The CIO Monthly Reporting and Certification is available at https://learn.insights.health.mil/resources/#!/cio-report.

2. The currently approved version of the Template is accessible within the "CIO Monthly Certification Folder" of the DAD-IO "MTF Toolkit" on the DHA SharePoint LaunchPad available at https://learn.insights.health.mil/resources/#!/cio-report.

ENCLOSURE 4

COMPLIANCE REPORTING REQUIREMENTS

Information Security Control Compliance: Reporting Requirements			
Control Domain	Identified Control	Reporting Frequency	Actions Required
System Security	Local Network RMF Compliance	Annually	● Confirm site's local network has a current RMF Authority to Operate ● Confirm applicable DHA systems are authorized to operate on the site network*
	System Vulnerability Scan Review	Monthly	● Confirm site has executed/reviewed security scans to identify vulnerabilities in its local network and/or its servers for applicable DHA systems ● Confirm site has fully mitigated or has Plan of Actions and Milestones in place for identified vulnerabilities**
	Audit Log Monitoring	Monthly	● Confirm site has correctly generated the required server audit logs for applicable DHA systems at the Application, Operating System, and Database levels (e.g., account creation/modification/termination logs, user activity logs, transaction history logs, interface history logs, server backup logs), ● Confirm site log data is consistently independently reviewed for completeness and accuracy ● Confirm logs are retained according to the mandated retention schedule*
Access Control	User Account Management	Annually	● Confirm site has followed required system procedures for applicable DHA systems and maintained adequate records for: ○ New user account creation/provisioning, ○ Annual review of system audit log data to recertify existing user accounts/permissions, ○ Prompt deactivation of terminated user accounts according to the mandated schedule***
	Privileged User Transaction Monitoring	Monthly	● Confirm site has reviewed applicable system logs to monitor privileged user account activity within applicable DHA systems ● Independently verify privileged users are not performing unauthorized transactions within the systems' production environments****
Segregation of Duties (SoD)	Incompatible User Role/Job Duty Analysis	Annually	● Confirm site has analyzed the risk of SoD conflicts between site personnel job duties and site user account permissions for applicable DHA systems ● Confirm site has implemented appropriate mitigations for any identified conflicts***
Configuration Management	System Configuration Scan Review	Quarterly	● Confirm site has reviewed and revalidated its as-built server configuration settings for applicable DHA systems against the expected/mandated configuration settings to identify any anomalies and implemented ● Confirm site has implemented any required corrective actions****
Contingency Planning	System Backup and Restoration Monitoring	Monthly	● Confirm the existence and completeness of the site's daily server backup data for applicable DHA systems ● Confirm server backup media are properly stored at an offsite storage facility ● Confirm server restoration process from the stored backups has been annually tested and confirmed to be operational****

*Only applicable to sites which use financially auditable DHA systems and manage their own local networks

**Only applicable to sites which use financially auditable DHA systems and manage their own local networks and/or manage their own server data for financially auditable DHA systems

***Applicable to all sites using financially auditable DHA systems

****Only applicable to sites which use and manage their own server data for financially auditable DHA systems

Information Security Control Compliance: Reporting Methods and Responsible Personnel									
Control Domain		System Security			Access Control		SoD	Configuration Management	Contingency Planning
Identified Control		Local Network RMF Compliance	System Vulnerability Scan Review	Audit Log Monitoring	User Account Management	Privileged User Transaction Monitoring	Incompatible User Role/Job Duty Analysis	System Configuration Scan Review	System Backup and Restoration Monitoring
Person Responsible For Reporting	**ABACUS**	DHA DAD-IO	DHA DAD-IO	VENDOR	Site UBO Site HR	VENDOR	Site UBO Site HR	VENDOR	VENDOR
	CCE	DHA DAD-IO	DHA DAD-IO	DHA DAD-IO	Site Patient Administration/Coders Site HR	DHA DAD IO	Site Patient Administration /Coders Site HR	DHA DAD-IO	DHA DAD-IO
	CHCS	Site CIO	DHA DAD-IO	DHA DAD IO	Site CIO Site Clinicians Site HR	DHA DAD-IO	Site CIO Site Clinicians Site HR	Site CIO	Site CIO
	DMLSS	DHA DAD-IO	DHA DAD-IO	DHA DAD-IO	Site MEDLOG Site HR	DHA DAD-IO	Site MEDLOG Site HR	DHA DAD-IO	DHA DAD-IO
	DHA eCommerce System	DHA DAD, Financial Operations (FO)	DHA DAD-FO	DHA DAD-FO	DHA DAD-FO	DHA DAD-FO	DHA DAD-FO	DHA DAD-FO	DHA DAD-FO
	MHS GENESIS	Program Executive Office Defense Healthcare Management Systems (PEO DHMS)	PEO DHMS	PEO DHMS	Site Clinicians Site HR	PEO DHMS	Site Clinicians Site HR	PEO DHMS	PEO DHMS
	Purchased Care Operation System	DHA DAD-IO	DHA DAD-IO	DHA DAD-IO	DHA DAD FO	DHA DAD-IO	DHA DAD-FO	DHA DAD-IO	DHA DAD-IO
Reporting Method	**ABACUS**	Enterprise Mission Assurance Support Service (eMASS)	eMASS	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log reports	Audit Log Reports
	CCE	eMASS	eMASS	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	Audit Log Reports

	CHCS	eMASS	eMASS	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	Audit Log Reports
	DMLSS	eMASS	eMASS	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	Audit Log Reports
	DHA eCommerce System	eMASS	eMASS	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	Audit Log Reports
	MHS GENESIS	eMASS	eMASS	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	Audit Log Reports
	Purchased Care Operation System	eMASS	eMASS	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	CIO Monthly Reporting Tool	Audit Log Reports	Audit Log Reports

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ABACUS	Armed Forces Billing and Collection Utilization Solution
CCE	Coding and Compliance Editor
CHCS	Composite Healthcare System
CIO	Chief Information Officer
CRI	Compliance Reporting Instruction
DAD	Deputy Assistant Director
DHA	Defense Health Agency
DMLSS	Defense Medical Logistics Standard Support
eMASS	Enterprise Mission Assurance Support Service
FO	Financial Operations
GAO	Government Accountability Office
HR	Human Resources
IO	Information Operations
IS	Information System
MEDLOG	Medical Logistics
MHS	Military Health System
MTF	Military Treatment Facility
PEO DHMS	Program Executive Office Defense Healthcare Management Systems
PI	Procedural Instruction
RMF	Risk Management Framework
SoD	Segregation of Duties
UBO	Uniform Business Office