Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 8400.01
March 7, 2024

DHA, J-6 DAD-IO

SUBJECT: Acceptable Use of Defense Health Agency Information Technology (IT)

References: See Enclosure 1.

1. PURPOSE. This Defense Health Agency Administrative Instruction (DHA-AI), based on the authority of references (a) and (b), and in accordance with the guidance of references (c) through (y), establishes the Defense Health Agency (DHA) policy for acceptable use of DHA Information Technology (IT) by Authorized Users and Privileged Users, as well as the procedures for establishing, maintaining, and disseminating said policy. This DHA-AI also establishes the standard process through which DHA IT access requests are made for both Authorized Users and Privileged Users.

2. APPLICABILITY. This DHA-AI applies to: the DHA Enterprise (components and activities under the authority, direction, and control of the DHA) to include: all DHA IT Users; Military Medical Treatment Facilities (MTFs) under the authority, direction, and control of the DHA; all personnel to include: assigned or attached Active Duty and Reserve members, federal civilians, members of the Commissioned Corps of the Public Health Service, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary or permanent duties at DHA, the Defense Health Networks and field activities (remote locations), and subordinate organizations administered and managed by DHA.

3. POLICY IMPLEMENTATION. It is DHA's instruction, pursuant to References (d) through (y), that:

a. DHA IT, as defined in this instruction, are to be used for official and authorized purposes only.

b. Completion of a signed DHA Authorized User Agreement is required for each user before any manner of access to DHA IT is granted. This User Agreement is to be composed of the standard Department of Defense (DoD) Notice and Consent, DHA Acceptable Use, and User Responsibilities language as required by reference (d) and outlined in Appendix (A) of Enclosure 3 at a minimum. In addition, a separate user agreement is required for Privileged User access

using the language contained in Appendix (B) of Enclosure 3 at a minimum. Privileged Users must complete the Authorized User Account process before their Privileged User accounts can be created.

c. DHA IT require compliance with the DoD Notice and Consent Banner upon access.

d. DHA IT Users may be required to sign separate and/or acknowledge separate acceptable use requirements and separate user agreements for IT that are not under DHA control or oversight. The content of those documents is out-of-scope of this DHA-AI. This DHA-AI does not negate the use of those documents for such IT. Individual DHA IT (e.g., organizations, Systems, Programs of Record, Platform ITs) may have more restrictive acceptable use requirements and separate user agreements with requirements beyond those stated in this DHA-AI. At no time are these additional requirements or agreements for these DHA IT to be considered valid where they impose less restrictive guidance. Federal Information and information-related activities (such as accessing, creating, collecting, downloading, viewing, processing, maintaining, disseminating, disclosing or disposing of information/data) involving assets and Users, as defined in this AI, including Covered Defense Information (CDI) and all subsets thereof (such as Controlled Unclassified Information [CUI], Personally Identifiable Information [PII], and Protected Health Information [PHI]) require safeguarding and marking with the appropriate control markings in accordance with Reference (k) not to be disseminated to anyone that does not possess a specific need-to-know. DHA J-1, Administration & Management, is charged with the roles and responsibilities for CUI Oversight. DoD and DHA instructions for CUI are available at https://www.dodcui.mil and https://info.health.mil/cos/admin/ma/IS/CUI.

e. DHA personnel will access DHA IT by their assigned Common Access Card (CAC) or by an approved Alternate (Alt) Token for Authorized User access or an Alt Token for Privileged Users.

f. DHA personnel must complete and provide a DoD-approved Cyber Awareness training certification to access DHA IT. After which, annual completion of said training is required as a condition to maintain access to DHA IT. Failure to comply with this training requirement will result in the complete suspension of their access regardless of authorized or privileged user status. NOTE: Additional training requirements may vary depending on system specific training might be needed. Refer to local departmental policies, guidelines, and procedures to determine the appropriate training requirements for each role.

g. DHA IT User behavior is monitored to detect potentially unauthorized activity. Punitive measures and procedures will be applied in cases where uniformed, civilian, or contractor personnel are found in violation of applicable cybersecurity laws, policies and/or standards. Failure to observe the prohibitions and mandatory provisions of this DHA-AI by military personnel is a violation of the Uniform Code of Military Justice, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contractor personnel will be handled according to local laws and the terms of the contract. Additionally, violations by National Guard military personnel may determine prosecution for a subject member under their respective State Military Code or result in

administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Appropriate restrictions will be applied against workforce members who fail to comply with this instruction and applicable security policies and procedures. Appropriate restrictions are determined based on the severity and circumstances of the violation and may be applied using the standard disciplinary processes already in place, where appropriate. In some cases, the type and severity of restrictions imposed, and the categories of violation are at the discretion of the DoD MTF or other entity.

4. CANCELED DOCUMENTS. This DHA-AI cancels DHA-PI 8140.01, Acceptable Use of Defense Health Agency Information Technology (IT), October 16, 2018.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. Cleared for public release. This DHA-AI is available on the Internet from the Health.mil site at: www.health.mil/DHAPublications and https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Forms/AllItems.aspx.

8. EFFECTIVE DATE. This DHA-AI:

a. Is effective upon signature.

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

CROSLAND.TELITA.1017383040
Digitally signed by CROSLAND.TELITA.1017383040
Date: 2024.03.07 10:09:39 -05'00'

TELITA CROSLAND
LTG, USA
Director

Enclosures
1. References
2. Responsibilities
3. Procedures

Appendices:
1. DHA Authorized User Agreement
2. DHA Privileged User Agreement

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended.
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013, as amended.
(c) DHA Procedural Instruction 5025.01, "Publication System," April 1, 2022
(d) DoD Instruction 8500.01, "Cybersecurity," October 7, 2019
(e) DoD Instruction 8170.01 "Online Information Management and Electronic Messaging," August 24, 2021
(f) DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020
(g) DoD Instruction 8140.02, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements," December 21, 2021
(h) DoD Manual 8140.03. "Cyberspace Workforce Qualification and Management Program," February 15, 2023
(i) DoD 5500.07-R, "Joint Ethics Regulation (JER)," August 1993, as amended
(j) Chairman of the Joint Chiefs of Staff Instruction 6510.01, "Information Assurance (IA) and Support to Computer Network Defense (CND)," current edition.
(k) DoD Instruction 5200.48, Controlled Unclassified Information (CUI), March 6, 2020
(l) DoD Manual 5200.2, "Procedures for the DoD Personnel Security Program (PSP)," October 29, 2020
(m) DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Healthcare Programs," August 12, 2015
(n) DoD Manual 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DOD Health Care Programs" March 13, 2019
(o) DHA Administrative Instruction 074, "Workforce Training Pursuant to the Requirements of the Privacy Act and Health Insurance Portability and Accountability Act," December 2, 2014
(p) DHA Administrative Instruction 5200.02, "Information Security Program," October 6, 2020
(q) CNSS Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022
(r) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022
(s) DoD Manual 1000.13, Volume 1, "DoD Identification (ID) Cards: ID Card Life-Cycle," January 23, 2014, as amended.
(t) United States Code, Title 10, Chapter 47 (also known as the "Uniform Code of Military Justice (UCMJ)")
(u) DoD Instruction 5400.17, "Official Use of Social Media for Public Affairs," August 12, 2022, as amended
(v) NIST SP 1800-21, "Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)", September 2020
(w) United States Code, Title 18, Crimes and Criminal Procedure, U.S. Government Publishing Office, https://www.govinfo.gov/USCODE-2009-title18
(x) NIST SP 800-88 Rev 1, "Guidelines for Media Sanitization", December, 2014

(y) DHA-AI 081, “Employee Use of Information Technology (IT)”, September 15, 2015

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA will ensure that personnel with access to DHA IT are appropriately cleared and qualified under the provisions of reference (k), and Federal Information will only be accessed by authorized users for authorized purposes in accordance with References (d) through (y).

2. CHIEF INFORMATION OFFICER, DHA. The Chief Information Officer, DHA, will:

a. Develop, implement, maintain, and enforce a Cybersecurity Program that is consistent with the strategy and direction of the DoD Senior Information Security Officer and the Defense Cybersecurity Program, and is compliant with Reference (d).

b. Monitor DHA IT Users' compliance with this DHA-AI and control access to DHA IT.

c. Apply appropriate sanctions based on the severity and circumstances of the violation up to and including the termination of authorized and privileged user access for violations of this AI and References (d) through (y).

3. DHA ASSISTANT DIRECTORS, DEPUTY ASSISTANT DIRECTORS, J-DIRS, AND SPECIAL STAFF. The DHA Assistant Directors, Deputy Assistant Directors and Special Staff will:

a. Ensure that DHA IT Users, assigned to or sponsored by their organization, complete DoD Cyber Awareness training before access is granted (Reference (y)).

b. Verify DHA workforce members, including civilians, military personnel, and contractor support staff, complete the initial Privacy Act/HIPAA training within 30 days upon hire and complete refresher training on an annual basis thereafter (see Reference (o)).

c. Approve the denial of access for any DHA personnel who fail to complete Privacy Act/HIPAA training within the allotted timeframes.

d. Ensure that DHA IT Users, assigned to or sponsored by their organization, use DHA IT in accordance with References (d) through (y) and the procedures of this DHA-AI.

e. Approve the denial of access for any DHA personnel who fail to adhere to security guidelines.

4. SYSTEM OWNERS. DHA System Owners are responsible for creating and maintaining Authorized User and Privileged User accounts. System Owners may delegate the appropriate authorized and/or privileged permissions to System Administrators deemed necessary for the maintenance (e.g., provision, adjust, de-provision) of accounts as well as removal of inactive accounts. The responsibilities of the System Owners include:

a. An annual review of every user account to ensure appropriate levels of access.

b. Revising System Access forms when a user changes user roles within the system.

c. De-provisioning user accounts within 24 hours when access is no longer required.

d. Retaining documentation on active users as long as the users still have active accounts.

e. Retaining documentation on inactive accounts for a period in accordance with relevant OSD Records and Information Management regulations at https://www.esd.whs.mil/RIM/.

5. DHA IT USERS. DHA IT Users will comply with References (d) through (y) and the procedures of Enclosure 3. Those who function as privileged users will additionally complete the DHA Privileged User Agreement language for what is contained in Enclosure 3 and Appendix 2.

ENCLOSURE 3

PROCEDURES

1. BACKGROUND. The two distinct types of personnel using the DHA network are the: Authorized and Privileged Users with different access and restriction levels for accessible use. Both types of users are collectively referred to as "Users." The DHA considers that these two types of users require different levels of access and different needs for restriction of acceptable use. Separate procedures for these two groups are outlined within Appendix 1 and 2. Because DHA networks may provide access to the Internet, it is necessary to clearly spell out the authorized and the prohibited uses of DHA IT.

2. AUTHORIZED USERS. Authorized Users are appropriately cleared individuals with a requirement to access an IS for performing or assisting in a lawful and authorized governmental function. Authorized User account(s) are those with limited privileges that are sufficient to execute general work-related tasks. Authorized Users must use their CACs or approved Authorized User Alt Tokens to access their Authorized User accounts. Appendix 1 provides the standard procedures for DHA Authorized User.

3. PRIVILEGED USERS. Privileged Users are those that are trusted to perform security-relevant functions that Authorized Users do not have sufficient permissions to perform. Privileged Users have greater permissions than Authorized Users. Privileged Users must first obtain a CAC or otherwise approved Authorized User Alt Token to get a Privileged User Alt token. Privileged Users must use/utilize their Privileged User Alt Tokens to access their privileged accounts. Privileged Users implement approved secure baseline configurations, incorporate secure configuration settings, and conduct configuration monitoring activities as needed. Privileged Users must complete the Authorized User Account process prior to the creation of their Privileged User account. Privileged Users are not to use privileged credentials to operate as Authorized Users. Appendix 2 provides standard procedures for Privileged Users.

APPENDIX 1

DHA AUTHORIZED USER AGREEMENT

1. STANDARD USER AGREEMENT TEXT. This appendix applies to access requests for Authorized User status. Users may copy and paste the DoD Notice and Consent, Acceptable Use, and DHA Authorized User Responsibilities, in their entirety into DD Form 2875 Block 21 as part of the user's Authorized User System Authorization Access Request (SAAR). Alternatively, users may copy this content into a separate form that must be signed by the requestor and accompany the requestor's SAAR for processing. All access requests must be submitted via the DISA approved DD Form 2875 SAAR form including the appropriate Consent Notice and Acceptable Use Policy for the specific type of access being requested (e.g., Authorized User or Privileged User). Waivers will not be accepted.

2. STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER. The following text within Table 1 is standard text available for users to copy and paste into a SAAR Request.

Table 1. Standard Mandatory DoD Notice And Consent Banner Text

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER
a. You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. b. By using this IS (which includes any device attached to this IS), you consent to the following conditions: (1) The U.S. Government (USG) routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. (2) At any time, the USG may inspect and seize data stored on this IS. (3) Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. (4) This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. (5) Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

3. STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS. The following text within Table 2 is standard text available for users to copy and paste into SAAR Requests.

Table 2. Standard Mandatory Notice And Consent Provision For All DoD Information System User Agreements Text

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS
By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems: a. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only. b. You consent to the following conditions: (1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. (2) At any time, the U.S. Government may inspect and seize data stored on this information system. (3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose. (4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy. (5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below: (a) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality. (b) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies. (c) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

Table 2. Standard Mandatory Notice And Consent Provision For All DoD Information System User Agreements Text, Continued

(d) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(e) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(f) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

(7) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

4. ACCEPTABLE USE OF DHA IT. The following text in Table 3 is standard text available for users to copy and paste into SAAR Requests.

Table 3. DHA Acceptable Use

ACCEPTABLE USE OF DHA IT
a) AUTHORIZED PERSONAL USE. Personnel may use DHA IT in accordance with authorized purposes of reasonable duration and frequency so as not to adversely affect the performance of official duties. Whenever possible, such use should be made during the employee's personal time, such as after duty hours or during lunch periods. Examples of authorized use are as follows: (1) Emailing short messages to a relative or colleague. (2) Announcing organizational-related activities (e.g., office luncheons, retirement or departure events, and holiday office parties). (3) Making a medical, dental, auto repair, or similar appointment. (4) Authorizing a financial transaction (not related to gambling, personal financial gain, or operating a private business). (5) Reading news or professional journals. (6) Accessing personal Internet-based Capabilities (IbC) accounts, (e.g., social media sites) according to reference (e).
b) PROHIBITED USE. Personnel may not use DHA IT for any illegal activities as defined in Reference (w), Title 18 of the United States Code USC Part I – Crimes, as well as the following prohibited activities: (1) Soliciting private business, advertising, or engaging in other selling activities in support of private business enterprises, outside employment, or for personal financial gain.

Table 3. Acceptable Use of DHA IT Text, Continued

(2) Promoting and using unofficial fundraising activities (e.g., GoFundMe, GiftsandGo).

(3) Engaging in political activity, to include endorsing candidates, products, services, participating in campaign fundraising, and any type of lobbying activities.

(4) Using the DHA network as a staging ground or platform to gain unauthorized access to other systems.

(5) Accessing public cloud platforms for creating or storing data or using web-based applications in the performance of official duties (e.g., file storage, online faxing, online printing).

(6) Accessing online gambling sites or gambling-related material while using DHA IT.

(7) Willingly accessing, creating, downloading, viewing, storing, copying, or transmitting material s that are sexually explicit or oriented

(8) Willingly engaging in gambling, promoting racist, or inciting terrorist activities via online resources.

(9) Purposely participating in "spamming" that is, exploiting bulk e-mail services or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited email, or other activities identified in Cyber Awareness Training such as phishing, spearfishing, whaling, or denial of service.

(10) Using the system for personal financial gain, such as advertising, solicitation of services, sale of personal property (e.g., online sale and auction sites), or stock trading (e.g.., issuing buy, hold, and/or sell directions to an online broker).

(11) Posting organizational information to external news groups, bulletin boards, or other public forums without authority.

(12) Sending, initiating or replying to messages containing language counter intuitive to a professional environment (e.g., excessive expletives, derogatory comments) or otherwise prohibited by reference (t), Uniform Code of Military Justice (UCMJ),
Article 134 – Indecent Language .

(13) Deliberately transmitting DoD controlled information (e.g., CUI, PII and PHI) to external parties in emails, social media sites, public cloud platforms, or other public Internet venues without official approval and failing to secure information using official transport encryption tools or mechanisms (e.g., FIPS-140-2/3 or DoD SAFE file transfer site).

(14) Attempting to circumvent, disable, or compromise cybersecurity security controls that could impact the confidentiality, availability, and integrity of the system's security posture (e.g., authentication safeguards).

(15) Willingly downloading open-source software or applications without an approved software assessment completed.

(16) Deliberately accessing sites of dubious origin known for hacker attacks or hacker activity.

(17) Knowingly opening email attachments from unknown or questionable sources.

Table 3. Acceptable Use of DHA IT Text, Continued

(18) Intentionally attempting to connect unapproved personal mobile devices (both wired and wireless) s to DHA IT (e.g., government furnished laptop or desktop).

(19) Deliberately bypassing, straining, or testing system cybersecurity security control mechanisms.

(20) Willingly attempting to circumvent or change the DHA deployed tools (e.g., host-based protection, anti-malware software) and standardized configurations (e.g., DHA desktop configuration) without approval from the cognizant authority.

(21) Knowingly relocating or changing DHA IT equipment or the network connectivity of equipment without proper authorization.

(22) Purposely auto-forwarding email(s) from an official email account (e.g., health.mil) to personal or commercial email accounts. In accordance with reference (e).

(23) Voluntarily introducing material that is inconsistent with the information type (e.g., classified, CUI, PHI, PII) for which the system is authorized.

(24) Consciously accessing internet sites that post collected 'leaked' classified or CDI.

5. DHA AUTHORIZED USER RESPONSIBILITES. The following text in Table 4 is standard text available for users to copy and paste into SAAR Requests.

Table 4. DHA Authorized User Responsibilities

DHA AUTHORIZED USER RESPONSIBILITES

Authorized Users of DHA IT will adhere to the following responsibilities:

a. Provide evidence of completion for DoD Cyber Awareness training as a condition of access to DHA IT, and complete annually thereafter to maintain access.

b. If a DHA IT user identifies potential violations (such as unauthorized use of external storage devices) along with suspicious behavior affecting computer systems under the NIWC CSSP scope of responsibility (e.g., MedCOI, DHA network), the DHA IT user shall follow these procedures to document and report the observed behavior:

(1) The IT user shall not take any remediation action without first consulting the NIWC Watch Officer

(2) Follow the instructions on either the MedCOI Incident Self-Report form or SIPRNet Self-Report Form: NIWC Cybersecurity Service. The forms are accessible at https://kbs.nsoc.med.osd.mil/CNDSubscriber

Table 4. DHA Authorized User Responsibilities, Continued

(3) MedCOI and SIPRNet NIWC CSSP OPS watch contact information:
Office: 843.218.3011
ECVoIP: 302.514.0000
24/7/365 Watchdesk: 1-866-786-4432
Group MedCOI Distro: usn.jbcharleston.niwcatlanticsc.mbx.cssp-watch@health.mil
Group SIPRNet Distro: usn.jbcharleston.niwcatlanticsc.list.cssp-watch@mail.smil.mil

c. Immediately notify the supervisor and the local organizational Privacy Official if there is a suspected or actual breach involving personally identifiable information (PII) or protected health information (PHI).

d. Digitally sign emails that contain embedded hyperlinks and/or attachments by utilizing a DoD-approved Public Key Infrastructure according to reference (e).

e. Digitally sign and encrypt emails containing CUI according to reference (e). Categories of Information available at the DoD Registry: https://www.dodcui.mil/, which includes, but is not limited to, PII or PHI. Do not use personal or commercial email accounts for transmitting CUI.

f. Protect DHA IT and Federal Information from unauthorized access.

g. Use only government-procured removable media devices as defined by NIST and the Committee on National Security Systems Instruction (CNSSI) 4009. (See 'Removable media' in GLOSSARY, PART II. DEFINITIONS).

h. Coordinate with the ISSM/ISSO to obtain a Data Loss Prevention Removable Media Request prior to using the removable media device. The removable media device must be approved locally and at the enterprise level. Retain all approval documentation as part of the appropriate IS Authorization Package. The Data Loss Prevention Removable Media Request Standard Operating Procedure can be accessed at https://info.health.mil/dadio/infosec/nso/EPS.

Table 4. DHA Authorized User Responsibilities, Continued

i. Use DHA IS only for official and authorized purposes.

j. Observe DHA's instructions and procedures governing the secure operation and authorized use of DHA IT.

k. Properly mark and classify information (e.g., emails, briefings, documents, or reports).

l. Protect DHA IS from theft, loss, or damage.

m. Use Common Access Card (CACs) or alternative (Alt) Tokens to access DHA IT, except where there has been approval by the Authorizing Official (AO) for an alternative access method.

n. Maintain continuous physical possession of physical token authentication mechanisms (e.g., CACs or Alt Tokens) according to Reference (r).

o. Immediately establish a connection to the DHA network via the VPN client when connected via the public Internet. All connections for Government official business to the Internet (e.g., hotel/home wired/wireless networks) must be through the DoD VPN connection only.

p. Use only DHA approved electronic messaging accounts to conduct official business. These accounts must be utilized according to reference (e). Additionally, DoD personnel must not use personal, nonofficial accounts, to conduct official DoD communications [except] when the combined three conditions exist:

(1) Emergencies and other critical mission needs.

(2) When official communication capabilities are unavailable, impractical, or unreliable.

(3) It is in the interests of DoD or other USG missions.

q. Maintain control of non-disclosed or potential aggregated nonpublic electronic information to DHA authorized IT systems that meet the minimum security controls that protect CUI or other types of sensitive information.

APPENDIX 2

DHA PRIVILEGED USER AGREEMENT

1. STANDARD PRIVILEGED USER TEXT. The content of this appendix applies to access requests for Privileged User status. Users may copy and paste the DoD Notice and Consent, Acceptable Use, and DHA Privileged User Responsibilities, in their entirety into DD Form 2875 Block 21 as part of the user's Privileged User SAAR. Alternatively, they may copy this content into a separate form that must be signed by the requestor and accompany the requestor's SAAR for processing. Privileged Users must first obtain a CAC to get an Alt token. Privileged Users shall use their Alt Tokens to access their privileged accounts, and their CACs to access their authorized accounts.

2. STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER. The following text within Table 5 is standard text available for users to copy and paste into SAAR Requests.

Table 5. Standard Mandatory DoD Notice And Consent Banner Text

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: a. The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. b. At any time, the USG may inspect and seize data stored on this IS. c. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. d. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. e. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

3. STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS. The following text within Table 6 is standard text available for users to copy and paste into SAAR Requests.

Table 6. Standard Mandatory Notice And Consent Provision For all DoD Information System User Agreements Text

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

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

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

b. You consent to the following conditions:

c. The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

d. At any time, the U.S. Government may inspect and seize data stored on this information system.

e. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

f. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

g. Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(1) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(2) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(3) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

Table 6. Standard Mandatory Notice And Consent Provision For all DoD Information System User Agreements Text, Continued

(4) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(5) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(6) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

h. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

i. All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

4. DHA ACCEPTABLE USE. The following text in Table 7 is standard text available for users to copy and paste into SAAR Requests.

Table 7. DHA Acceptable Use

DHA ACCEPTABLE USE

a. I understand that I am prohibited from the following while using DHA IT:

(1) Introducing classified information into the MedCOI environment.

(2) Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is not mission- or business-oriented. This information shall not contain information that has been determined by U.S. law, applicable State law, or DoD policy that contains unprotected speech considered not to be protected under the 1st Amendment of the U.S. Constitution (e.g., subversive activity, fighting words, true threats, some types of obscenities, and child pornography)

Table 7. DHA Acceptable Use, Continued

(3) Storing, accessing, processing, or distributing Classified, Proprietary, or CUI Categories of Information available at the DoD Registry: https://www.dodcui.mil/ in violation of established security and information release policies.

(4) Accessing public cloud platforms for creating or storing of data or using web-based applications in the performance of official duties (e.g., file storage, online faxing, online printing).

(5) Storing, accessing, processing, or distributing information outside of protected systems of the appropriate classification (e.g., classified on unclassified, DoD-controlled information on systems that are not certified to contain that level of information).

(6) Obtaining, installing, and using software and applications in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

(7) Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code (e.g., malware), engaging in online political activity, to include endorsing candidates, products, services, participating in campaign fundraising, and any type of lobbying activities.

(8) Using the system for personal financial gain, such as advertising or solicitation of services or sale of personal property (e.g., online sale and auction sites), or stock trading (e.g., issuing buy, hold, and/or sell directions to an online broker).

(9) Promoting and/or participating in unofficial fundraising activities either for profit or non-profit (e.g., GoFundMe, Gift & Go) unless the activity is specifically approved by DHA.

(10) Accessing gambling sites, gambling, wagering, or placing bets.

(11) Posting home pages, personal or otherwise, unless specifically permitted by DOD Social Media Policy or MHS Social Media Policy.

b. I understand that personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

c. I understand that if I am in doubt as to any of my roles or responsibilities, I will contact the [IT NAME] ISSM or ISSO for clarification.

d. I understand that all information processed on the [IS NAME] is subject to monitoring. This includes email(s) and browsing the Web.

e. I will not allow any user who is not cleared access to the network or any other connected system without prior approval or specific guidance from the [IT NAME] ISSM.

f. I will use the special access or privileges granted to me ONLY to perform authorized tasks or mission-related functions.

g. I will not use any DoD/Components' owned IT to violate software copyright by making illegal copies of software.

Table 7. DHA Acceptable Use, Continued

h. I will ONLY use my PRIVILEGED USER account for official administrative actions. This account will NOT be used for day-to-day network communications.

i. I understand that failure to comply with the above requirements will be reported and may result in the following actions:

(1) Revocation of IT privileged access

(2) Counseling

(3) Adverse actions pursuant to the Uniform Code of Military Justice and/or criminal prosecution

(4) Disciplinary action, discharge, or loss of employment

(5) Revocation of security clearance according to Reference (p).

j. I will obtain and maintain required certification(s), according to References (f) through (h) in order to maintain compliance with applicable DoD Cyber workforce position requirements and to retain privileged system access.

5. DHA PRIVILEGED USER RESPONSIBILITIES. The following text in Table 8 is standard text available for users to copy and paste into SAAR Requests.

Table 8. DHA Privileged User Responsibilities

DHA PRIVILEGED USER RESPONSIBILITIES

a. I understand there are two DoD Information Systems the classified Secret Internet Protocol Router Network (SIPRNet) and Non-Classified Medical Community of Interest Network (MedCOI), and that I have the necessary clearance for privileged access to the DHA IT requested. I will not introduce or process data or software for the IS that I have not been specifically authorized to handle.

b. I understand the need to protect all passwords and other authenticators at the highest level of data they secure. I will not share any password(s), accounts(s), or other authenticators with other coworkers or other personnel. As a privileged user, I understand the need to protect the root password and/or authenticators at the highest level of data it secures. I will NOT share the root password and/or authenticators with coworkers or other personnel.

c. I understand that I am responsible for all actions taken under my account(s), root, or otherwise. I will not attempt to "hack" the network or any connected IS or gain access to data to which I do not have authorized access.

d. I understand my responsibility to appropriately protect and label all output generated under my account, including printed materials, magnetic tapes, floppy disks, downloadable hard disk files, and removeable media.

Table 8. DHA Privileged User Responsibilities, Continued

e. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual possible compromise of data or file access controls to the appropriate Information System Security Manager (ISSM) or Information System Security Officer (ISSO) for the requested DHA IT. I will NOT install, modify, or remove any hardware or software (e.g., freeware/shareware and security tools) without written permission and approval from the ISSM or ISSO.

f. I will not install any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).

g. I will not add/remove any users' names to the Domain Administrators, Local Administrator, or Power Users group without the prior approval and direction of the ISSM or ISSO.

h. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the local area networks.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

Alt	Alternate
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
CAC	Common Access Card
CDI	Covered Defense Information
CI	Counter Intelligence
CNNS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COMSEC	Communications Security
CSSP	Cyber Security Service Provider
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
DHA IS	Defense Health Agency Information System
DHA IS User	Defense Health Agency Information System User
DHA IT	Defense Health Agency Information Technology
DHA IT User	Defense Health Agency Information Technology User
eSATA	External Serial ATA
FIPS	Federal Information Processing Standard
IbC	Internet-based Capabilities
IS	Information System
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
LE	Law Enforcement
MedCOI	Medical Community Of Interest
MMC	Multi Media Card
NIST	National Institute of Standards and Technology
NIWC	Naval Information Warfare Center
PHI	Protected Health Information

PII	Personally Identifiable Information
PIT	Platform Information Technology
PM	Program Manager
SAAR	System Authorization Access Request
SP	Special Publication
UMD	Universal Media Disc
USB	Universal Serial Bus
USG	United States Government
VPN	Virtual Private Network
xD	Extreme Digital

PART II. DEFINITIONS

authorized purposes. Personal use within specified limits as permitted by an appropriate level supervisor.

authorized user. Any appropriately cleared individual with a requirement to access a DoD Information System (IS) for performing or assisting in a lawful and authorized governmental function.

Covered Defense Information (CDI). Is used to describe information that requires protection under DFARS Clause 252.204-7012. It is defined as unclassified Controlled Technical Information (CTI) or other information as described in the CUI Registry that requires safeguarding/dissemination controls and is either marked or otherwise identified in the contract and provided to the contractor by DoD in support of the performance of the contract; or collected/developed/received/transmitted/used/stored by the contractor in the performance of the contract.

Controlled Unclassified Information (CUI). Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls (Section 2002.4 of Title 32 CFR). It includes only the CUI Categories of Information available at the DoD Registry:

Cyber Incident. Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.

DHA Information System (IS). Any IS connected to a network that is: a) operated by DHA, or b) under the authority of the DHA Cyber Security Service Provider (CSSP). For the purposes of this Instruction, DHA IS does not include DHA IS that is designed and authorized to be publicly

available, as well as the interconnected non-DoD ISs that are operated by DHA's purchased care contractors.

DHA IS User. All authorized users of DHA IS.

DHA Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by DoD. The term IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Per DoDI 8500.01 "Cybersecurity", Inc Change 1 Effective Oct 7 2019: DHA IT includes Information Systems (Major Applications, Enclaves), PITs, PIT Systems, IT Services (Internal, External), and IT Products (Software, Hardware, Applications).

DHA IT User. All authorized users of DHA IT.

DHA System Owners are responsible for creating and maintaining Authorized User and Privileged User accounts. System Owners may delegate the appropriate authorized and/or privileged permissions to System Administrators deemed necessary for the maintenance (e.g., provision, adjust, de-provision) of accounts as well as removal of inactive accounts.

Internet-based Capabilities (IbC). All public information capabilities or applications available across the Internet from locations not directly or indirectly controlled by DoD or the Federal Government (i.e., locations not owned or operated by DoD, another federal agency, or by contractors or others on behalf of DoD or another federal agency).

Incident. An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

IT. IT includes any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

malware. Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, and availability of an information system. A virus, worm, Trojan horse, ransomware, spyware, adware, keylogger, botnet, or other code-based entity that infects a host. (NIST SP 1800-21).

official use. Use(s) that directly furthers the interests of the DoD and the duties prescribed for the individual position.

Protected Health Information (PHI). Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a DoD covered entity in its role as employer. Information which has been de-identified in accordance with Paragraph 4.5.a is not PHI. PHI is a subset of PII, with respect to living persons. (DoDM 6025.18)

Personally Identifiable Information (PII). Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (OMB A-130)

Privileged User. A user that is authorized to perform security-relevant functions (e.g., have access to system control, monitoring, administration, criminal investigation, or compliance functions)

Removable media. Per CNSSI 4009, "CNSS Glossary," March 2, 2022: Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD). See also portable storage device.