Defense Health Agency
PROCEDURAL INSTRUCTION

NUMBER 8140.01
August 14, 2018

HIT (J-6)/CSD

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

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 (c) through (m), establishes the Defense Health Agency's (DHA) procedures for acceptable use of DHA IT by authorized and privileged users.

2. APPLICABILITY. This DHA-PI applies to:

a. All users of DHA IT.

b. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this DHA-PI as the "DoD Components").

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

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

b. Completion of a signed user agreement is required by each user before access to DHA IT is granted. DHA IT user agreements will include, at a minimum, the language required in Reference (m). In addition, a separate user agreement is required for privileged users' access using the language contained in the Appendix of Enclosure 3.

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

d. Information created, copied, stored, or disseminated from DHA IT assets by DHA IT Users, as defined in this instruction, may constitute Controlled Unclassified Information (CUI) (e.g., personal and medical information). All CUI will require safeguarding and marking with the appropriate control markings, in accordance with Reference (j), and will not be disseminated to anyone without a specific need-to-know.

e. DHA IT will only be accessed by DHA IT Users via a Common Access Card (CAC) or Alternate Token.

f. Initial and annual completion of DoD-approved Cyber Awareness training is required as a condition of access for DHA IT Users to be granted and retain access to DHA IT. Failure to comply will result in suspension of access to DHA IT.

g. Administrative and/or judicial sanctions will apply to DHA IT Users who knowingly, willfully, or negligently compromise, damage, or place DHA information at risk by not ensuring implementation of DoD's IT security requirements.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release**. This DHA-PI is available on the Internet from the Health.mil site at: www.health.mil/DHAPublications.

7. 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 DHA-PI 5025.01 (Reference (c)).

R. C. BONO
VADM, MC, USN
Director

Enclosures
1. References
2. Responsibilities
3. Procedures

Appendix
Defense Health Agency Information Technology Privileged User Access Agreement and Acknowledgement of Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
(c) DHA-Procedural Instruction 5025.01, "Publication System," August 21, 2015
(d) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(e) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(f) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015
(g) DoD Manual 8570.01, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended
(h) DoD Regulation 5500.07-R, "Joint Ethics Regulation (JER)," August 1993
(i) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended
(j) DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
(k) DoD 5200.2-R, "Personnel Security Program," January 1, 1987, as amended
(l) DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Healthcare Programs," August 12, 2015
(m) DoD Chief Information Officer Memorandum, "Policy on use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," May 9, 2008

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, will ensure that all personnel with access to DHA IT are appropriately cleared and qualified under the provisions of Reference (k), and that access to all DHA IT processing specified types of information (e.g., CUI) under the purview is authorized in accordance with References (d) through (m).

2. CHIEF INFORMATION OFFICER, MILITARY HEALTH SYSTEM. The Chief Information Officer, Military Health System, 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-PI, and control access to DHA IT.

c. Terminate authorized and privileged user access for violations of References (d) through (m) and this DHA-PI.

3. DHA DEPUTY ASSISTANT DIRECTORS, SPECIAL STAFF, AND SURGEONS GENERAL OF THE SERVICE MEDICAL DEPARTMENTS. The DHA Deputy Assistant Directors, Special Staff, and Surgeons General of the Service Medical Departments will:

a. Ensure that DHA IT Users, assigned to or sponsored by their organization, complete initial and annual DoD Cyber Awareness training.

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

4. DHA IT USERS. DHA IT Users will comply with References (d) through (m) and the procedures of Enclosure 3. Those who function as privileged users will additionally complete the DHA IT Privileged User Access Agreement and Acknowledgement of Responsibilities, language for which is contained in the Appendix of Enclosure 3.

ENCLOSURE 3

PROCEDURES

There are two distinct types of users of any DoD network: authorized users who are appropriately cleared individuals with a requirement to access a DoD IS for performing or assisting in a lawful and authorized governmental function and; privileged users who are authorized users that also perform security-relevant functions (e.g., have access to system control, monitoring, administration, criminal investigation, or compliance functions). As a result of that distinction, separate procedures for these two groups are outlined below. In addition, because the DHA network provides access to the Internet, it is necessary to clearly spell out authorized and prohibited uses of DHA IT.

1. AUTHORIZED USERS. DHA IT Users will adhere to the following requirements for official use of DHA IT:

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. Complete DD Form 2875, "System Authorization Access Request (SAAR)."

c. Immediately report all Cybersecurity-related events, potential threats, and vulnerabilities to the Global Service Center at 1-800-600-9332 and, wherever possible the local Information System Security Officer (ISSO) or, in the absence of an ISSO, the local Information System Security Manager (ISSM).

d. Immediately notify their 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).

e. Digitally sign all emails that contain embedded hyperlinks and/or attachments by utilizing a DoD-approved Public Key Infrastructure.

f. Digitally sign and encrypt all emails containing CUI, which includes, but is not limited to, PII or PHI. Do not use personal or commercial email accounts for transmission of CUI, including PII or PHI data.

g. Protect DHA IT and resident data from unauthorized access.

h. Use only government-procured and DHA-approved removable storage devices/flash media.

i. Obtain authorization (written approval or digitally signed emails) from their O-6/GS-15 supervisor and approval of the Authorizing Official or Authorizing Official's Designated

Representative to use flash media in support of operational mission essential requirements.

j. Coordinate with the ISSM or ISSO on procedures to obtain a removable storage device/flash media and on the proper use and disposal of removal storage devices.

k. Encrypt all removable storage devices containing CUI.

l. Use DHA IT only for official or authorized purposes.

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

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

o. Use non-mission-related contact information, such as personal telephone numbers or postal/email addresses, to establish personal accounts, when such information is required for Internet-based Capabilities (IbC) personal accounts.

p. Disclaim opinions in IbC personal accounts with the following statement: "The views presented are those of the individual and do not necessarily represent the views of the DoD or the DHA" (Reference (h)).

q. Avoid dissemination and discussion of non-public information in IbC personal accounts.

r. Protect DHA IT from theft, loss, or damage.

s. Use CACs or Alternate Tokens to access DHA IT, except where there has been approval by the AO for an alternative access method.

t. Maintain physical possession of DoD/DHA authentication mechanisms, e.g., CAC, at all times.

u. Users will 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) will be through the DoD VPN connection only.

2. PRIVILEGED USERS. In addition to the requirements of Enclosure 3, Section 1, privileged users will:

a. Configure and operate IT within the authorities vested in them per DoD Cybersecurity policies and procedures, and notify the responsible ISSO or, in the absence of an ISSO, the responsible ISSM, of any changes that might impact security postures.

b. Complete the Defense Information System Agency "Privileged User Cybersecurity

Responsibilities" training course and provide certificate of completion to the ISSM.

c. Complete a DHA IT Privileged User Access Agreement and Acknowledgement of Responsibilities, language for which is contained in the Appendix of Enclosure 3 and provide to the ISSM.

d. Be fully qualified per References (f) and (g), as well as trained and certified to DoD baseline requirements to perform their Cybersecurity duties.

e. Complete specified computing environment training.

f. Ensure that PHI and PII are removed from DHA IT in such a way that the data may not be recovered or reconstructed (e.g., degauss, smelt, incinerate, disintegrate, pulverize) prior to use of the DHA IT by any individual without authorization and need-to-know.

3. AUTHORIZED USE. DHA IT may be used for the 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:

a. Emailing short messages to a relative or colleague.

b. Accessing personal email accounts.

c. Announcing organizational-related activities (e.g., office luncheons, retirement or departure events, and holiday office parties).

d. Making a medical, dental, auto repair, or similar appointment.

e. Authorizing a financial transaction (not related to gambling, personal financial gain, or operating a private business).

f. Reading news or professional journals.

g. Accessing personal IbC accounts, such as Facebook, Twitter, etc.

4. PROHIBITED USE. Do not use DHA IT for prohibited activities that include:

a. Soliciting business, advertising, or engaging in other selling activities in support of private business enterprises or outside employment or for personal financial gain.

b. Non-official fundraising activities.

c. Endorsing any product or service, participating in any lobbying activity, or engaging in

any political activity, including campaign fundraising.

d. Use of DHA network as a staging ground or platform to gain unauthorized access to other systems.

e. Accessing, creating, downloading, viewing, storing and copying, or transmitting materials related to illegal gambling, illegal weapons, and/or any other prohibited or illegal activities.

f. Accessing, creating, downloading, viewing, storing, copying, or transmitting materials that are sexually explicit/oriented or involve gambling, racist, or terrorist activities.

g. 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.

h. Creating, copying, or transmitting chain letters or other unauthorized mailings regardless of the subject matter.

i. Participating in "letter-bombing;" that is, sending the same email repeatedly to one or more recipients to interfere with the recipient's use of email.

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

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

l. Sending, whether initiating or replying to, inappropriate messages or messages containing inappropriate language.

m. Transmitting CUI, including PII and PHI in emails and via the Internet without ensuring appropriate security controls (e.g., use of Federal Information Processing Standards' compliant encryption algorithms) are in place.

n. Attempting to circumvent, disable, or compromise DHA security features and authentication measures.

o. Downloading shareware/freeware software, malicious code, or executable programs (e.g., .EXE, .COM, .BAT, or script .INI files). (Note: Usage of Network File System open-source software is permitted with a risk assessment and Authorizing Official/Authorizing Official's Designated Representative approval).

p. Accessing sites known for hacker attacks or hacker activity.

q. Opening email attachments from unknown or questionable sources.

r. Attempting to connect unapproved personal wireless devices to DHA IT.

s. Sending CUI to personal email addresses.

t. Unilaterally bypassing, straining, or testing IT Cybersecurity mechanisms.

u. Introducing or using unauthorized software, firmware, or hardware on DHA IT.

v. Attempting to circumvent or change the DHA deployed tools and standardized configurations without approval.

w. Relocating or changing DHA IT equipment or the network connectivity of equipment without proper authorization.

x. Auto-forwarding email(s) from a DoD Enterprise Email account to personal or commercial email accounts.

y. Using commercial or personal email accounts to conduct official business.

z. Conducting official DoD communication in IbC personal accounts.

aa. Disclosing CUI or any other nonpublic information that aggregates to reveal sensitive or classified information in IbC personal accounts.

ab. Introducing material that is inconsistent with the information classification (e.g., classified, CUI, PHI, PII) for which the system is authorized.

ac. Accessing internet sites that post or collect classified or controlled government information (e.g., Wikileaks).

ad. Accessing a system owned and/or managed by DHA for reasons not related to an official job function(s) to include but not limited to accessing one's own electronic medical record for personal purposes to the extent that such record is maintained within a DHA system.

APPENDIX

DEFENSE HEALTH AGENCY INFORMATION TECHNOLOGY PRIVILEGED USER ACCESS AGREEMENT AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

Date: _____

1. I understand there are two DoD Information Systems (ISs), classified Secret Internet Protocol Router Network (SIPRNet) and Non-Classified Internet Protocol Router Network (NIPRNet), and that I have the necessary clearance for privileged access to DHA [specify which IS the privileges are for]. I will not introduce or process data or software for the IS that I have not been specifically authorized to handle.

2. 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.

3. 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.

4. 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 flash drive/memory sticks and cards.

5. 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 [IS NAME] Information System Security Manager (ISSM) or Information System Security Officer (ISSO). 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 [IS NAME] ISSM or ISSO.

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

7. 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 [IS NAME] ISSM or ISSO.

8. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the [IS NAME] local area networks.

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

a. Introducing classified information into a NIPRNET environment.

b. Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, or racist; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, federal, national, or international law.

c. Storing, accessing, processing, or distributing Classified, Proprietary, Controlled Unclassified Information, For Official Use Only, or Privacy Act protected information in violation of established security and information release policies.

d. Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

e. Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

f. Engaging in political activity.

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

h. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by organization (e.g., organization social event fund raisers and charitable fund raisers, without approval).

i. Gambling, wagering, or placing of any bets.

j. Writing, forwarding, or participating in chain letters.

k. Posting personal home pages.

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

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

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

13. 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 [IS NAME] ISSM.

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

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

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

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

a. Revocation of IS privileged access;
b. Counseling;
c. Adverse actions pursuant to the Uniform Code of Military Justice and/or criminal prosecution;
d. Disciplinary action, discharge, or loss of employment; and
e. Revocation of security clearance.

18. I will obtain and maintain required certification(s), according to DoD Manual 8570.01, "Information Assurance Workforce Improvement Program," dated December 19, 2005 (as amended), and the certification provider, to retain privileged system access.

INFORMATION SYSTEM NAME _____

NAME _____

SIGNATURE _____

Date _____

GLOSSARY

PART 1. ABBREVIATIONS AND ACRONYMS

CAC	Common Access Card
CUI	Controlled Unclassified Information
DHA	Defense Health Agency
DHA-PI	Defense Health Agency-Procedural Instruction
IbC	Internet-based Capabilities
IS	Information System
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
PHI	protected health information
PII	personally identifiable information

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 IS for performing or assisting in a lawful and authorized governmental function.

CUI. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. Includes: For Official Use Only, Law Enforcement Sensitive, DoD Unclassified Controlled Nuclear Information, PII, PHI, and Limited Distribution.

DHA 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 DHA. For purposes of the preceding sentence, equipment is used by DHA if the equipment is used by DHA directly or is used by a contractor under a contract with DHA, which, (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related

resources. For the purposes of this Instruction, DHA IT does not include IT 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 IT User. All authorized users of DHA IT resources to include: assigned or attached Service members, federal civilians, contractors (when required by the terms of applicable contract), and other personnel officially assigned temporary or permanent duties at DHA to include regional and field activities (remote locations).

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).

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

PHI. Individually identifiable health information created, received, or maintained by a covered entity, including DHA, that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by DHA in its role as an employer.

PII. Information which can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, and any other demographic, personnel, medical, and financial information. PII includes any information that is linked to a specified individual, alone, or when combined with other personal or identifying information.

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)