PEPR Account Activation Request Form

See Pages 28-30 for Form Instructions and Guidance.
Upon Completion Email to SDD Access: DHA.SDDAccess@mail.mil
DCS Users - Upon Completion Email to PAT&IS: dcs@dha.mil

1. System Access (Please check the system for which you have mission/contract related access requirement)	
	PCDIS & PRDM - Purchased Care Detail Information System & Provider Reporting Data Mart
	DCS – Duplicate Claims System
	PEPR Satellite Systems – Specify Below
	CBM - Consolidated Bad Master
	CK - Claims Check
	MH - Mental Health
	QRDF - Quick Response Data File
	RF - Reference File
	TA - TED Auditing
2. Employment Category (Please check the category that applies)	
	Government Employee, Uniformed Service Member, Military, or Civil Service working within/for DoD MHS
	Contractor working within the DoD Military Health System
	Government Employee, Uniformed Service Member, Military, or Civil Service working for other agency or directorate not a part of the DoD Military Health System
	Contractor working for Government Agency, not a part of the DoD Military Health System
	Other (Please describe) ____

3. Applicant/Requestor Information	
Rank/GS Level/Title:	
Name (Last, First, MI):	
Complete Office Mailing Address:	
Sponsoring Organization Name: ***(Not Project Name)***	
If Contractor, Employer Name	
Commercial Telephone Number:	
DSN:	
Email:	

Account Validation PIN: Enter a 4 digit numeric PIN that you will use to validate your identity for account administration purposes.				

Applicant/Requestor Digital Signature:____

4. Action

Check action requested: □ NEW □ CHANGE □ DELETE □ OTHER ____________________

If you have a User ID, please enter it here: ______________ (If your account has expired, enter your last user ID)

Requested Access (Required for DCS users only): **□ READ ONLY** **□ READ/WRITE (supervisor must complete 4.A., below)**

Requesting Access to following contractor region number(s)*:____

*If access to multiple contractor regions is required, all region contractor numbers must be specified.

4. A. Special Permissions Data for READ/WRITE Users (To be completed by requestor's supervisor)

Permission to create User Defined Codes? (Requires Prime Contractor approval): □ YES □ NO

Permission to unarchive sets? (Requires Prime Contractor approval): □ YES □ NO

Supervisor Signature: ____ **Phone#:**_______________________

Prime Contractor Signature: ____ **Phone#:**_______________________

5. SDD Rules of Behavior

1. Have you READ the SDD Rules of Behavior appended at the end of this document? □ YES □ NO
2. Do you ACCEPT the terms set forth in the SDD Rules of Behavior? □ YES □ NO

6. DOD Cyber Awareness Challenge Training

1. Have you successfully completed DoD Cyber Awareness Challenge Training? □ YES □ NO
2. Have you signed and emailed the DoD Cyber Awareness Challenge Certificate to SDD? □ YES □ NO

6. A. PCDIS Training **(Required for all users requesting access to PCDIS) Enter date (mm/dd/yyyy).**

Date: _________________ □ LIVE □ NO

7. Data Sharing Agreement (DSA) for Contractor

If you are an MHS Contractor and/or non-MHS Employee, please provide the following information:

Employer Name:	
Project description requiring this access:	
What is the DSA # that exists for this project?	
Project period of performance:	

8. User Security Clearance Level **(mark appropriate level):**

	ADP II/NACLC	Notes: 1. A minimum of ADP Level II is required. 2. The use of SECRET is authorized if the requestor's clearance has been active within 2 years of application date.
	ADP I	
	Other (specify) Type ___________________ Date __________________	
	If SECRET, provide: Date of Birth: ___________________ Place of Birth: ______________________________	

9. DHA PEPR Account Applicant Signature **(All Applicants/Users must read and sign)**

By signing below, I am acknowledging that (1) all statements made on this form are true and correct; and (2) I am only authorized to use DHA PEPR Systems as designated above for my current position/duty and agree to relinquish my PEPR accounts to the SDD Program Executive Office upon departure from my current position/duty. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I further acknowledge that substantial civil and criminal penalties and/or administrative sanctions may be levied against those who violate the provisions of the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Signature ____ **Date** _________________________

10. Use of Mobile Computing Equipment

□ Mobile computing equipment (Laptop computer, external hard drive, CDs/DVDs, floppy disks, PDA, cell phone, or other movable media) **WILL BE USED** to connect to this SDD product.
Certification on Attachment B **MUST BE COMPLETED.**

□ Mobile computing equipment will not be used to connect to this SDD product.

11. Commander, Supervisor, or Security Officer Certification of Citizenship

By signing below, I am certifying that ________________________ (applicant) is a U.S. Citizen and has a mission essential or contract-driven requirement to access PEPR, and that the DSA referenced, if any, is applicable. I further acknowledge that substantial criminal penalties including fines and imprisonment, and/or administrative sanctions may be levied against those who violate the provisions of the Privacy Act of 1974 and/or HIPAA. I shall notify the SDD Program Executive Office upon departure of this applicant from their current position/duty or when access is no longer required.

Commander/Supervisor/Security Officer Name	
Title or Position	
Organization, Office, Company	
Office Mailing Address	
Email Address	
Commercial Telephone	
DSN	
Verification of Need to Know: I certify that this user requires access as requested.	□ YES □ NO

Signature ____ **Date** __________________________

12. Government Sponsor

Sponsoring Organization Name	
Commander / Supervisor / Sponsor Name (Last, First, MI)	
Title	
Office Mailing Address	
Email Address	
Commercial Telephone	
DSN	
Required for DCS and TA users only	
Access Level Approved	□ READ ONLY □ READ/WRITE □ R/W/ADMIN
Required for DCS users only	
Unarchive Sets?	□ YES □ NO
Create User Defined Codes?	□ YES □ NO
Contractor Region Numbers Granted	

Government Sponsor Signature: ______________________________________ **Date** ______________________

13. BOXI/BCS Application and Level of Access – To be completed by Government Sponsor POC or Supervisor	
The official duties of this individual require the following BOXI/BCS application and level of access (select one of the following):	
Application Access: User requires access to BOXI/BCS Application ***(Not applicable for DCS or TA Applications)***	□ YES □ NO
Level of Access	
Viewer: User can access only predefined reports published to a public folder. User will not be able to create ad hoc reports.	□
Reporter: User can access predefined reports, create ad hoc reports, and save to personal folders.	□
Publisher: User can access predefined reports, create ad hoc reports, save to personal and public folders. ***This access will require approval from PEPR Functional* Sponsor *and SDD PO Approving Authority.***	□

Government Sponsor POC or Supervisor Signature: ____________________________________**Date** _________

SDD PO Approving Authority Signature: ____ **Date** ________

(Required for Publisher access only)

14. Protected Health Information Access – To be completed by Government Sponsor POC or Supervisor

The official duties of this individual require access to patient identifying data? □ YES □ NO

If YES, please complete Attachment A.

Government Sponsor POC or Supervisor Signature: _________________________________ **Date** _________

DO NOT WRITE BELOW THIS BOX

15. SDD Certification (For SDD use only)

□Form □EDIPI □PIN □RoB □DoD IA Trng □AppSigned □CertSigned □SponSigned □PHI/PII SDDAccess______

I certify that SDD requirements have been validated. Specified access is recommended.

SDD PO Approving Authority Name: ____________________________________

Signature ____ **Date** _______________________

Attachment A

Justification for Access to Protected Health Information (PHI)

Generally speaking, only healthcare providers involved in the treatment of patients are allowed access to patient-identifying data regarding patients under their care. Such access could also extend to healthcare managers and administrative support personnel with specific, defined roles regarding paying or receiving reimbursement on medical claims and essential activities in support of health care operations. The use or disclosure of protected health information outside these parameters and without the patient's consent may violate the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A more detailed description regarding the required protection of individually identifiable data is available at http://www.tricare.mil/tma/privacy/hipaa.aspx.

Please identify your requirements for access to patient identifiable data.

Privacy Act

Some data are protected under the provisions of the Privacy Act of 1974. The data contains patient and provider identity information and thus requires safeguards from unauthorized access and use. I agree to comply with the Privacy Act of 1974 and to be responsible for the use of this data to properly safeguard patient and provider identifying data in accordance with the 30 Oct 2001 OASD (HA) memorandum signed by Major General Randolph, Deputy Executive Director TMA, subject "*Supplemental Guidance for the Management and Control of Patient Sensitive/Medical Record Information in the Military Health System*." In addition, I acknowledge that I may be subject to civil suit under the Privacy Act or 1974 for damages which occur as a result of willful or intentional actions which violate an individual's rights under the Privacy Act of 1974.

PHI

I accept responsibility for the PHI data in PEPR that is in my possession and will ensure that all reasonable efforts are made in order to protect the data from unauthorized access and misuse.

HIPAA

I acknowledge that under HIPAA (P.L. 104-191), Congress has established criminal penalties for knowingly violating patient privacy. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to ten years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

User Signature ____Date ____________________

Printed Name ____

Attachment B
Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media

DoD Policy Memorandum, “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media”, July 3, 2007

References (a) DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6. 2003, (b) DoDD 8100.2, “Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),” April 14, 2004, as supplemented by ASD Nil/DoD CIO memorandum, same subject, June 2, 2006, (c) DoD Policy Memorandum, “Department of Defense Guidance on Protecting Personally Identifiable Information (P11),” August 18, 2006, and (d) DoD Policy Memorandum, “Protection of Sensitive DoD Data at Rest on Portable Computing Devices,” April 18, 2006 require that:

(1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as thumb drives and compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.
(2) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c).

Handling and Storage

- During travel, laptops and PDAs must be hand carried and never checked as baggage. If possible, carry diskettes or removable hard drives separate from the laptop.
- If a laptop or PDA is stored in a hotel locker room, it must be kept out of plain view. A laptop or PDA may not be left unattended in a vehicle.

Incident Handling

- In the event of any suspicious activity, breach in security of the remote device, or upon the detection of a virus, Trojan Horse, or malware disconnect from the VPN connection, cease all operation on the device, and report the incident to the SDD IAM, Mr. Joseph Ibanez, joseph.g.ibanez.civ@mail.mil.

Please identify which mobile computing devices/removable storage media you will be using to access or obtain PHI (protected health information) from this SDD product: (check all that apply)

□ Laptop	□ External Hard Drive	□ CDs/DVDs	□ Floppy Disks
□ PDA	□ Cell Phone	□ Other	

If other, please describe: ____

User Certification: I understand the requirement for encryption of sensitive unclassified data at rest (in particular, PHI) on mobile computing devices and removable storage media. I certify that a data at rest encryption product, meeting the DOD specifications has been installed and is operating on any such mobile computing devices that I will use to access data from this SDD product. Further, I certify that I will ensure that this data at rest encryption product shall be maintained at the most recent version and shall be kept updated according to manufacturers' latest available patches, service packs or other product updates. Further, I will keep this product installed and operational as long as my SDD product account is active.

User Signature ____**Date** ________________________

User Printed Name____

Information Assurance/Information Security Officer Certification: I certify that I have personal knowledge of the installation and proper operation of data at rest encryption product on the above named user's computer. I will ensure that required updates are applied as available.

Make and model of mobile computing device(s):

Make	**Model**	**Serial Number**
__________________	____________________	_________________________
__________________	____________________	_________________________

IA/ISO Signature ____**Date** ________________________

IA/ISO Printed Name____

IA/ISO Email Address____**Phone ( ) __________________**

Attachment C
Solutions Delivery Division (SDD)
Rules of Behavior

DEFENSE HEALTH SERVICES SYSTEMS (DHSS)

RULES OF BEHAVIOR

(ROB)

February 2015

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

DISCLAIMER III

1 INTRODUCTION 4

1.1 What are Rules of Behavior? 4

1.2 Why are Rules of Behavior Needed? 4

2 GENERAL PRINCIPLES 5

2.1 Computer Programs and Data Ownership 5

2.1.1 Proper Use of Government Computer Systems 5

2.1.2 Misuse of Government Computer Systems 5

3 SECURITY AWARENESS 6

3.1 General Procedures 6

4 ADMINISTRATIVE POLICIES 6

4.1 Official Work and Use of Government Equipment 7

4.2 Position Devices to Prevent Unauthorized Personnel from Reading the Information . 7

4.3 Identification and Authentication 7

4.3.1 CAC Enforcement 7

4.3.2 Password Guidelines 7

4.4 Properly Mark Materials and Media 8

4.5 Remote Access Protections 9

4.6 Removal of Equipment 9

4.7 Software Policy 9

4.8 User Agreement 9

5 PRIVACY RESPONSIBILITIES 9

5.1 User Responsibilities 11

5.2 Review Unclear Information 12

6 REFERENCES 13

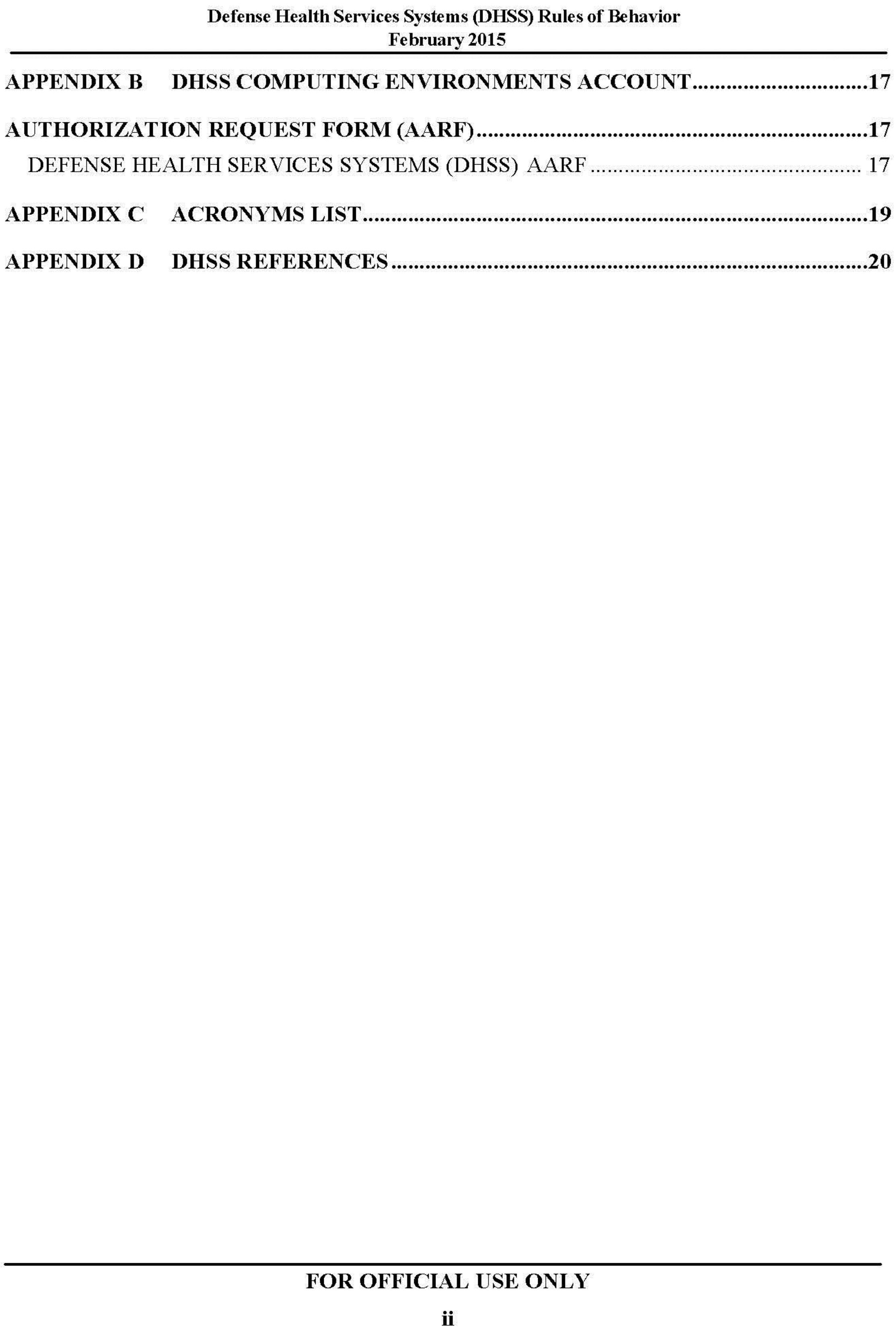
6.1 Other Policies and Procedures 13

7 RULES OF BEHAVIOR RECEIPT ACKNOWLEDGEMENT FORM 14

8 SIGNATURE APPROVAL 15

APPENDIX A SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR) 16

DEFENSE HEALTH SERVICES SYSTEMS (DHSS) DD Form 2875 Access Form 16



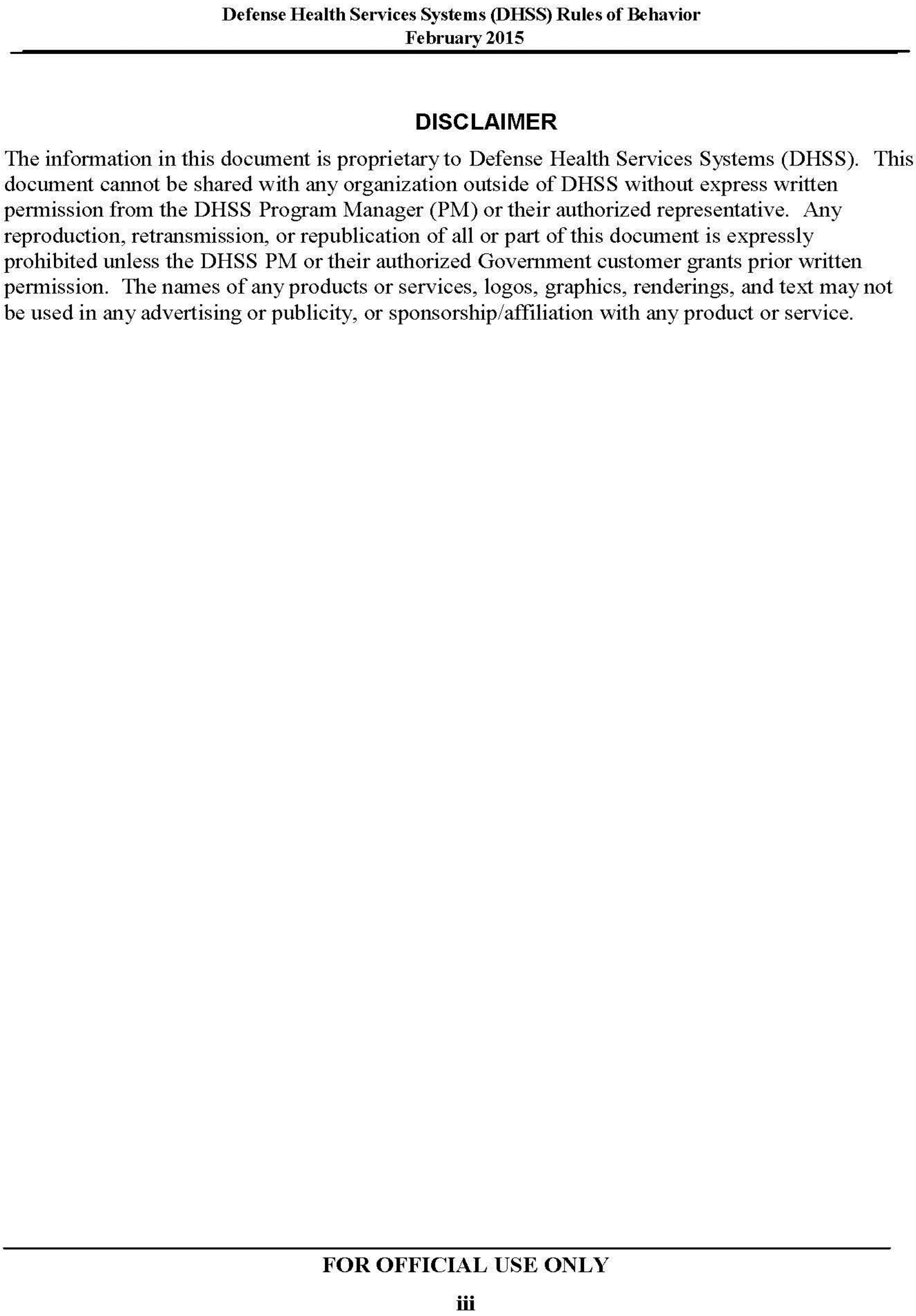
APPENDIX B DHSS COMPUTING ENVIRONMENTS ACCOUNT 17

AUTHORIZATION REQUEST FORM (AARF) 17

DEFENSE HEALTH SERVICES SYSTEMS (DHSS) AARF 17

APPENDIX C ACRONYMS LIST 19

APPENDIX D DHSS REFERENCES 20



DISCLAIMER

The information in this document is proprietary to Defense Health Services Systems (DHSS). This document cannot be shared with any organization outside of DHSS without express written permission from the DHSS Program Manager (PM) or their authorized representative. Any reproduction, retransmission, or republication of all or part of this document is expressly prohibited unless the DHSS PM or their authorized Government customer grants prior written permission. The names of any products or services, logos, graphics, renderings, and text may not be used in any advertising or publicity, or sponsorship/affiliation with any product or service.

1 INTRODUCTION

All DHSS users and employees must be informed of their responsibility for the use, protection, and release of DHSS information. Some basic concerns include the loss of data, threats, computer crimes, computer viruses, the abuse or unauthorized use of software and equipment, the release of sensitive data, and so forth. DHSS users and employees need to comply with the Federal, Department of Defense (DoD), and DHSS computer security policies and procedures described in this document.

The DHSS Rules of Behavior (RoB) document describes acceptable guidelines from various federal and DoD regulatory documents. Users who do not comply with the prescribed Rules of Behavior are subject to penalties that are imposed under existing policies and regulations, including written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment and possible criminal prosecution.

All users of DHSS applications, both internal and external, that access, store, or transmit information contained within or exported from any DHSS application are required to follow the rules outlines in this Rules of Behavior document.

The DHSS Program Executive Office (PEO) is responsible for supporting and enforcing the policies outlined. The DHSS PEO requires that all users with an active account on any DHSS application have a valid RoB acknowledgement form on file with the DHSS Access Office. The DHSS PEO is not accepting any substitutions for this requirement.

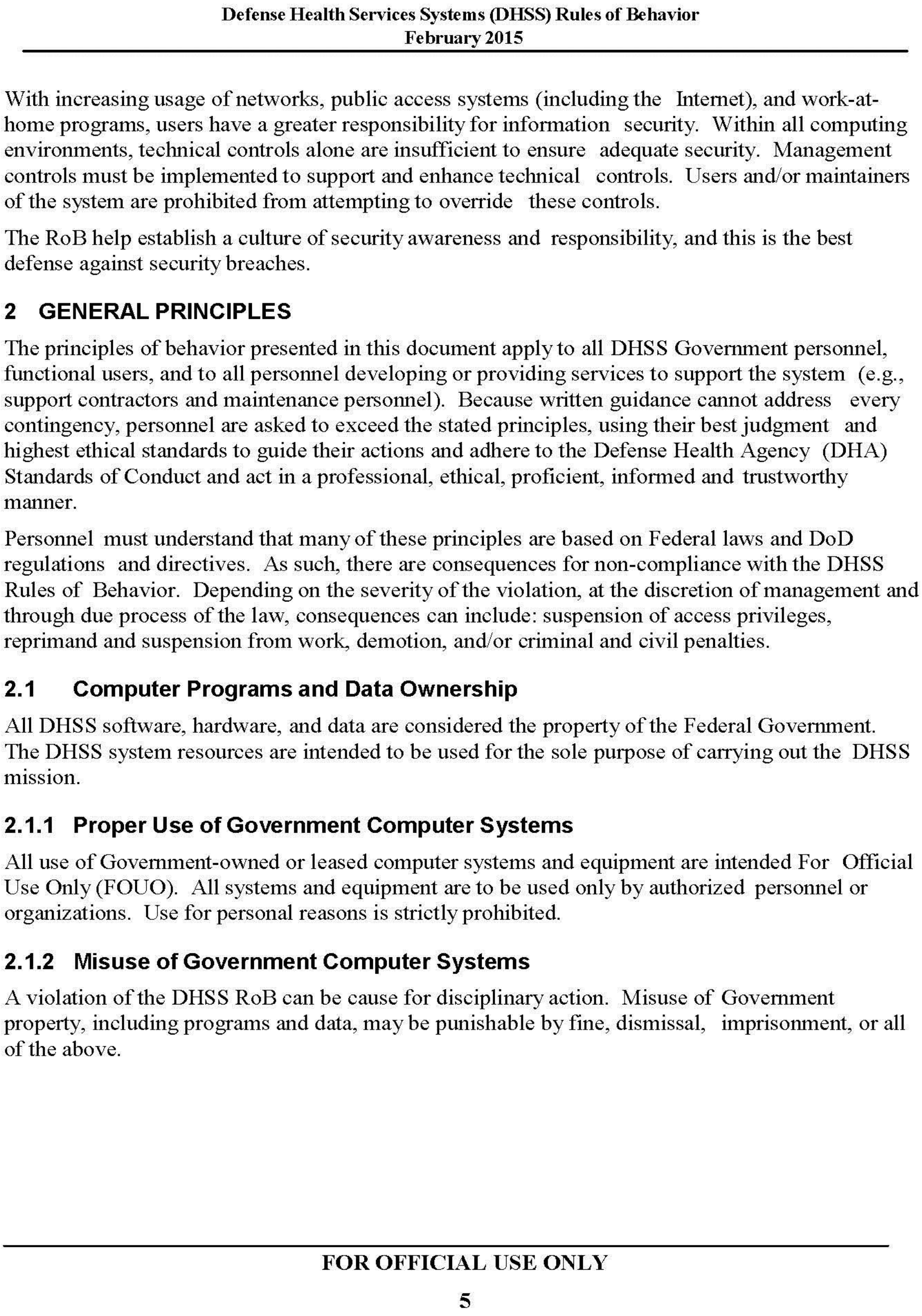
1.1 What are Rules of Behavior?

IA control, PRRB-1 (Security Rules of Behavior or Acceptable Use Policy) - RoB is part of a comprehensive program to provide appropriate protection to DoD AISs. The RoB represents a new approach to information security to provide awareness of a system user and/or maintainer's responsibility, and to hold users accountable for their actions with respect to information assurance (IA). RoB establishes ethical and practical standards because knowledgeable users are the foundation of a successful security program.

RoB informs system users and maintainers of what is expected of them and how to actively protect the system and the data that it processes. RoB call on users to be proactive by being alert to threats and vulnerabilities, staying abreast of security policies and issues, and reporting incidents. Users are expected to act ethically, take initiative, and accept responsibility for safeguarding information resources. The DHSS RoB applies to all users of DHSS Information System s (ISs).

1.2 Why are Rules of Behavior Needed?

It is common knowledge among private industry and Government organizations that the primary threats to AISs are inadvertent mistakes made by functional and administrative users. The most serious threat to information and AIS resources has frequently been internal misuse through miscommunication.



With increasing usage of networks, public access systems (including the Internet), and work-at-home programs, users have a greater responsibility for information security. Within all computing environments, technical controls alone are insufficient to ensure adequate security. Management controls must be implemented to support and enhance technical controls. Users and/or maintainers of the system are prohibited from attempting to override these controls.

The RoB help establish a culture of security awareness and responsibility, and this is the best defense against security breaches.

2 GENERAL PRINCIPLES

The principles of behavior presented in this document apply to all DHSS Government personnel, functional users, and to all personnel developing or providing services to support the system (e.g., support contractors and maintenance personnel). Because written guidance cannot address every contingency, personnel are asked to exceed the stated principles, using their best judgment and highest ethical standards to guide their actions and adhere to the Defense Health Agency (DHA) Standards of Conduct and act in a professional, ethical, proficient, informed and trustworthy manner.

Personnel must understand that many of these principles are based on Federal laws and DoD regulations and directives. As such, there are consequences for non-compliance with the DHSS Rules of Behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand and suspension from work, demotion, and/or criminal and civil penalties.

2.1 Computer Programs and Data Ownership

All DHSS software, hardware, and data are considered the property of the Federal Government. The DHSS system resources are intended to be used for the sole purpose of carrying out the DHSS mission.

2.1.1 Proper Use of Government Computer Systems

All use of Government-owned or leased computer systems and equipment are intended For Official Use Only (FOUO). All systems and equipment are to be used only by authorized personnel or organizations. Use for personal reasons is strictly prohibited.

2.1.2 Misuse of Government Computer Systems

A violation of the DHSS RoB can be cause for disciplinary action. Misuse of Government property, including programs and data, may be punishable by fine, dismissal, imprisonment, or all of the above.

3 SECURITY AWARENESS

IA control PRTN-1 (Training – IA Awareness) - The security policy of DHSS is that all users are to receive a basic level of security awareness training. All authorized IS users, including contract personnel, will receive initial and annual security awareness training. The DHSS Security Access Office will document and maintain the status of initial and annual security awareness compliance for each user. Internal DHSS users are notified annually of the requirement to execute their information security training by the DHSS Security Access Office. External DHSS users are required to submit IA certificates to the DHSS Security Access Office annually. To support IA professionals, the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) IA Portal provides DoD IA policy, training requirements, and DoD-sponsored training. The DISA IASE IA Portal is located at http://iase.disa.mil/.

3.1 General Procedures

DHSS general procedures are as follows:

- Do not reconfigure equipment, software, consoles, or workstations without approval.
- DHSS practices the principle of "least privilege". That is, each user is granted only those privileges needed to perform authorized tasks. Each user only has access to options allowed for his or her particular application user security level. Contact your supervisor or security manager if your user privileges exceed what you require to perform your role.
- Protect passwords, information, equipment, systems, networks, and communications pathways to which you have access. In addition:
- Minimize the threat of viruses by write-protecting diskettes, checking "foreign" data for viruses, and never circumventing the anti-virus safeguards of the system.
- Never leave your workstation unattended without removing your Common Access Card (CAC) from the card reader and locking the workstation.
- Report anything unusual or suspicious (especially viruses) to your supervisor, the local security manager or the Information Assurance Manager (IAM).
- Do not share your CAC or your CAC Personal Identification Number (PIN).

4 ADMINISTRATIVE POLICIES

Administrative security management refers to the proactive approach of system managers and administrators to maintain up to date security policy and procedures for AIS and technologies under their purview. This constant vigilance includes an annual self-assessment of these IS. The goal is to provide a risk management approach that crosses all the security disciplines.

Administrative security includes activities associated with configuration management of the components and application development lifecycle. DHSS administrative policies are as follows:

4.1 Official Work and Use of Government Equipment

Use of Government equipment for personal business or non-work related activities is strictly prohibited. DHSS personnel should understand the following:

- Keeping family or personal records, playing computer games, or loading unauthorized software onto Government computers is not authorized.
- There is no distinction between stand-alone and on-line computer systems.
- Administrative users shall grant access to systems and data only to those who have an official need to know.
- Use of Government computers for any type of non-official activity is not authorized.

4.2 Position Devices to Prevent Unauthorized Personnel from Reading the Information

IA control, PEDI-1 (Data Interception) - Devices that display or output classified or sensitive information in human-readable form needs to be positioned to deter unauthorized individuals from reading the information. Devices include, but are not limited to, printed output, monitors and mobile devices. Do not permit printouts with DoD sensitive information to remain unattended. Position monitors to avoid people without a need to know from reading what is displayed.

4.3 Identification and Authentication

IA control IAIA-1 (Individual Identification and Authentication) - DHSS applications are required to comply with DoD Instruction 8520.2, which states that all user authentications must be via Public Key Infrastructure (PKI). PKI for the DoD is mainly accomplished through the use of the Common Access Card (CAC). For all DHSS application (s) that are not fully compliant with DoDI 8520.2, the DHA requires an Authentication Security Plan (ASP) to detailing why the application is not compliant, how compliance will be achieved, the milestones for compliance, and any mitigation strategies in use to reduce the likelihood of compromise due to the lack of PKI enforcement.

4.3.1 CAC Enforcement

CAC enforced authentication is accomplished via a DoD CAC. User access requires a valid CAC and PIN. No user can gain access to neither the DHSS application nor the environment unless they have a CAC card.

Three (3) failed attempts will render the CAC disabled. Users must follow the CAC PIN reset process by visiting a Real-time Automated Personnel Identification System (RAPIDS) site (http://www.dmdc.osd.mil/rsl/appj/site;jsessionid=d-3B6Dc3L1BibXNLX4ViHMBKPautIz93qycQMP4VMK5I7a_HN2jQ!-1031112072?execution=e1s1).

4.3.2 Password Guidelines

IA control IAIA-1 (Individual Identification and Authentication) - If a DHSS application employs the uses of passwords, the following password guidelines must be followed:

- Passwords must be a minimum of fifteen alphanumeric characters.
- Passwords must consist of 2 uppercase alphabetic characters, 2 lowercase alphabetic characters, 2 numeric characters, and 2 special characters.
- Change passwords at least every 60 days.
- Avoid obvious readable passwords. Avoid passwords that incorporate personal data elements (e.g., your name, child's name, date of birth, address, telephone number, social security number, dictionary words, or other personal attributes).
- Do not reuse passwords. Vary new passwords from old passwords by at least four characters.
- Do not change your password more than once per 24 hours unless you believe it has been compromised.
- Avoid common words found in a dictionary.
- Change your password immediately if it has been exposed, guessed or compromised.
- Do not accept another user's password, even if offered.
- Do not post passwords on terminals, blackboards, bulletin boards, or in any other location where they may be disclosed.
- Do not share user identification (ID) and passwords.
- Users are prohibited from using another individual's password.
- Safeguard your password. Commit it to memory; do not post it or write it down.
- Protect passwords by using permitted passwords, changing them frequently, using meaningless character strings, safeguarding and not sharing your password with anyone

For DHSS applications that utilize username and passwords, system administrators are required to comply with the following:

- Configure the application so that passwords are shadowed (i.e., not visible as plaintext characters when entered.)
- Ensure that users are provided unique user identifier in the form of a unique token or user ID and password before accessing the system.
- Ensure that vendor-provided user accounts and passwords are removed or changed.

Users are required to notify the system administrator, the IAM if violations of the above are noted.

4.4 Properly Mark Materials and Media

IA control ECML-1 (Marking and Labeling) requires that information and DoD information systems that store, process, transmit, or display data in any form or format, that is not approved for public release, comply with all requirements for marking and labeling contained in policy and guidance documents.

4.5 Remote Access Protections

IA control EBRU-1 (Remote Access Information Protection) requires that all users protect information regarding specific remote access points unless a validated need to know exists. Remote access point uniform resource locator (URL) or Internet Protocol (IP) addresses will not be posted to publically accessible web sites or other non-protected medium.

The DHSS user is responsible for handling sensitive data as FOUO whether or not it is marked as such. Printed products and other forms of transmission media (that is, tapes, removable drives, external hard drives, and disks) containing DHSS data must also be treated and safeguarded in accordance with the sensitive nature of the data. Users should ensure that the material is protected from unauthorized disclosure. DHSS documents, media and/or containers should bear external markings of DHSS ownership and sensitivity markings reading FOUO in accordance with DoD regulations and directives. If any printed DHSS report that contains sensitive information is not marked FOUO, then the user will hand print “FOR OFFICIAL USE ONLY” on the bottom of every page.

4.6 Removal of Equipment

Property passes are to be obtained from your Property Custodial Officer before the removal of any DHSS equipment from the facility. Additionally, the DHSS Program Management Office (PMO) must be notified when DHSS equipment is removed from a site.

4.7 Software Policy

DHSS licenses the use of computer software from a variety of external vendors. DHSS does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.

With regards to software use on local area networks or on multiple machines, DHSS users shall use the software only in accordance with the license agreement.

DHSS users that become aware of any misuse of software or related documentation shall notify their supervisor or the security manager.

According to the U.S. copyright law, illegal reproduction of software can result in civil damages of as much as $100,000 and criminal penalties, including fines and imprisonment. DHSS users who create, acquire, or use unauthorized/unlicensed copies of DHSS computer software, or possess software that is not for official Government business shall be subject to discipline. Such discipline may include termination.

4.8 User Agreement

The user agreement is contained in Attachment A, Rules of Behavior Receipt Acknowledgement Form. Users are required to digitally sign and return the form to the DHSS Security Access Office at dhssaccess@dha.mil.

5 PRIVACY RESPONSIBILITIES

It is the responsibility of the DHSS PEO to ensure the following privacy responsibilities are followed:

- Personal data, records, historical data, logistical data, and system documentation is maintained in accordance with the applicable laws and regulations.

  NOTE: Never leave sensitive information out in the open (for example on top of desks). Sensitive unclassified information must always be contained in a properly secured area (for example, closed or locked files or drawers).

- Users shall take such actions, as considered appropriate, to ensure that any personal information contained in a system of records, of which they have access to and are using to conduct official business, shall be protected so that the security and confidentiality of the information shall be preserved.
- Users shall not disclose any personal information contained in the DHSS IS, systems of records except as authorized by DoD 5400.11-R, "Department of Defense Privacy Program", or other applicable laws or regulations. Personnel willfully making such disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.
- Per DoD 5400.11-R, Personal Information is information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc.
- Such information is also known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specified individual).
- Users shall report any unauthorized disclosures of personal information from the DHSS system or records or the maintenance of any system of records that are not authorized by

  DoD Directive to the applicable Security Manager.

- IA Control PECS-1 (Clearing and Sanitizing) - All documents, equipment, and machine-readable media containing sensitive data should be properly cleared and sanitized in accordance with DoD 5200.1-R and if applicable, Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD [C3I]) Memorandum, dated June 4, 2001, subject: "Disposition of Unclassified DoD Computer Hard Drives." DHSS users have a responsibility to:
  - Delete sensitive information from hard drives and removable media permanently by formatting or overwriting. If assistance is needed in performing these tasks, ask the hosting facility or security manager.
  - Dispose of unneeded software media by completely destroying them, or re- formatting the media prior to re-use.
  - Shred, tear into small pieces, or burn sensitive documents so that it cannot be reconstructed. Do not throw sensitive documents into a wastebasket.

5.1 User Responsibilities

DHSS users have a responsibility to assess the sensitivity of the data they have access to, and to ensure it is safeguarded appropriately. Ultimately, computer security is each user's responsibility. The user must be alert to possible breaches in security and adhere to the security regulations that have been established within the DoD. The security practices listed above are not inclusive, but rather designed to remind the user and to raise the user's awareness toward securing automated information system resources.

DHSS user responsibilities and expected behavior includes, but are not limited to:

- All users will ensure that all output containing sensitive information is marked with "FOR OFFICIAL USE ONLY." If any printed report that contains sensitive information is not marked FOUO, then the user should hand print "FOR OFFICIAL USE ONLY" on the document appropriately. An UNCLASSIFIED document containing FOUO information is required to be marked "FOR OFFICIAL USE ONLY" on the bottom of every page.
- Attend and take mandatory security awareness and education training annually as required by the DHSS Security Office.
- Adhere to the letter and spirit of all applicable Government laws, regulations, contracts, policies, standards, guidelines, and procedures relevant to accessing DHSS.
- Position monitors to avoid people without a need to know DHSS information from reading what is displayed. Do not allow printouts with DoD sensitive information to remain unattended.
- Do not process, store, or transmit DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access controls.
- Comply with copyright and site licenses of proprietary software. No personal unauthorized software is allowed on DHSS provided Government Furnished Equipment (GFE) or contractor equipment used to remotely support DHSS assets. Personal unauthorized software is any software package installed that is not GFE and not approved by the DHSS PM for installation on the computing device.
- Notify the local site security manager, the IAM if access to resources or data is beyond what you need.
- Users shall not use their trusted position and access rights to exploit system controls or to access data for any reason other than their official duties.
- Protect against disaster by backing up your data and files at frequent intervals.
- Protect against viruses by never bringing unauthorized or personal software to work. Beware of borrowed or unsolicited software; these may contain a computer virus designed to capture, alter, or destroy data.
- Scan all media inserted into or software downloaded onto workstations used to support DHSS. Beware of borrowed or unsolicited software; these may contain a malware such as computer viruses, Trojans etc. designed to capture, alter, or destroy data.

- Protect sensitive unclassified or classified information from disclosure, alteration, and loss.
- Do not share data with any individual that does not have a valid need to know and applicable security clearance. If there is doubt, then the data should not be shared.
- Do not share your CAC or your CAC PIN.
- Never leave your workstation unattended without removing your CAC from the card reader or locking the keyboard with the password-protected feature.
- Protect your area by recognizing, politely inquiring, and assisting people who you do not recognize in your work area. Report any suspected non-credentialed individual on the premises.
- Protect your equipment by practicing good housekeeping at all times, including no smoking, drinking, or eating around your personal computer, terminal, or workstation. Keep electrical appliances away from your computer and media.
- Protect DHSS information and equipment from theft, destruction or misuse.
- Protect your media by labeling all storage media and locking up software, removable media, and equipment that contains fixed media.
- The user must use an approved encryption method to protect sensitive information stored on recordable media; including laptops, universal serial bus (USB) drives, and external disks or transmitted downloaded via e-mail or remote connections.
- Realize that the RoB applies even if you do not read them. Violations may result in loss of computer access, written reprimands, monetary fines, dismissal, or imprisonment.
- Recognize that users shall abide by any additional local rules established by their system managers or IAM.
- Report all suspected fraud, waste or misuse of DHSS system resources, security violations and all suspected security violations to your supervisor, the security manager, or the IAM

- Upon final checkout or departure from your current position, do not have in your possession any sensitive DHSS unclassified or classified information in any form, nor any Government-owned equipment, software, storage media, user manuals, or system documentation, unless authorized.
- If security has been compromised or may be compromised, notify the appropriate site security personnel immediately.

5.2 Review Unclear Information

DHSS users should review the information that was unclear in this document and ask the DHSS Security Access Office questions covering those areas.

6 REFERENCES

6.1 Other Policies and Procedures

The Rules of Behavior are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing DHSS applications.

This Rules of Behavior is part of the overarching DHSS Account Management Policy. If you require access to a specific system(s) based on your responsibilities, please contact the DHSS Program Office point of contact (POC) for instructions and requirements.

These rules are consistent with the policy and procedures described in the following directives:

System Account Authorization Request (SAAR) DD Form 2875 is the required document for authorizing access for supporting DHSS. This document authorizes properly cleared individuals with the need-to-know access to DHSS information systems.

The DD Form 2875 is the standard Department of Defense form used to request an account to provide access to computing asset and systems housed in an off-site facility controlled by an external organization.

This form applies to all military, DoD Civilians, Contractors and other assigned personnel requiring access to DHSS Information Systems. In Appendix B you will find a sample DD Form 2875 and completion instructions.

Account Authorization Request Form (AARF) PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to DHSS systems and information. In Appendix C you will find a sample AARF and completion instructions.

7 RULES OF BEHAVIOR RECEIPT ACKNOWLEDGEMENT FORM

I have received a copy of the DHSS Rules of Behavior for information systems technology and security that provides information on Federal regulations, user responsibilities, and computer security policies and procedures. In compliance with DHSS security program, I have read the rules in their entirety. I recognize that it is my responsibility to ensure that I comply with the computer security policies and procedures described in the DHSS Rules of Behavior document.

Employee Name: ____

Title: ____

Organization Name and Address: ______________________________

Telephone Number: ____

Email: ____

Employee Signature: ____

DHSS Security Access Office Acknowledgement Signature: ________________

NOTE: **Sign and return this form to the DHSS Security Access Office.**

8 SIGNATURE APPROVAL:

Process Owner Approval

Date

Narinder Saund

Chief Technology Officer (CTO)

Authorizing Official Designated Representative (AODR)

Program Support Division

Defense Health Services Systems

Program Executive Office (DHSS PEO)

DHSS Sub-Process Area Owner Approval

Information Assurance (IA)

27 Feb 2015

Date

IBANEZ.JOSEPH.G D.1181220631

Digitally signed by IBANEZ.JOSEPH.G D.1181220631
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=TMA, cn=IBANEZ.JOSEPH.G D.1181220631
Date: 2015.02.27 10:00:09 -05'00'

Joseph Ibanez

Director, Cyber Security /Chief Information Security Officer (CISO)/Information Systems Security Manager (ISSM)

Program Support Division

Defense Health Services Systems

Program Executive Office (DHSS PEO)

DHSS PEO Quality Assurance Approval

ERIKSON.MARY.M.1010690150

Digitally signed by ERIKSON.MARY.M.1010690150
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=ERIKSON.MARY.M.1010690150
Date: 2015.03.03 09:52:10 -05'00'

Date

Mary Erikson

Quality Assurance Section Lead

Program Support Division

Defense Health Services Systems

Program Executive Office (DHSS PEO)

Deputy Program Executive Officer Approval

HARRINGTON.CHRISTOPHER.JOHN.1012595324

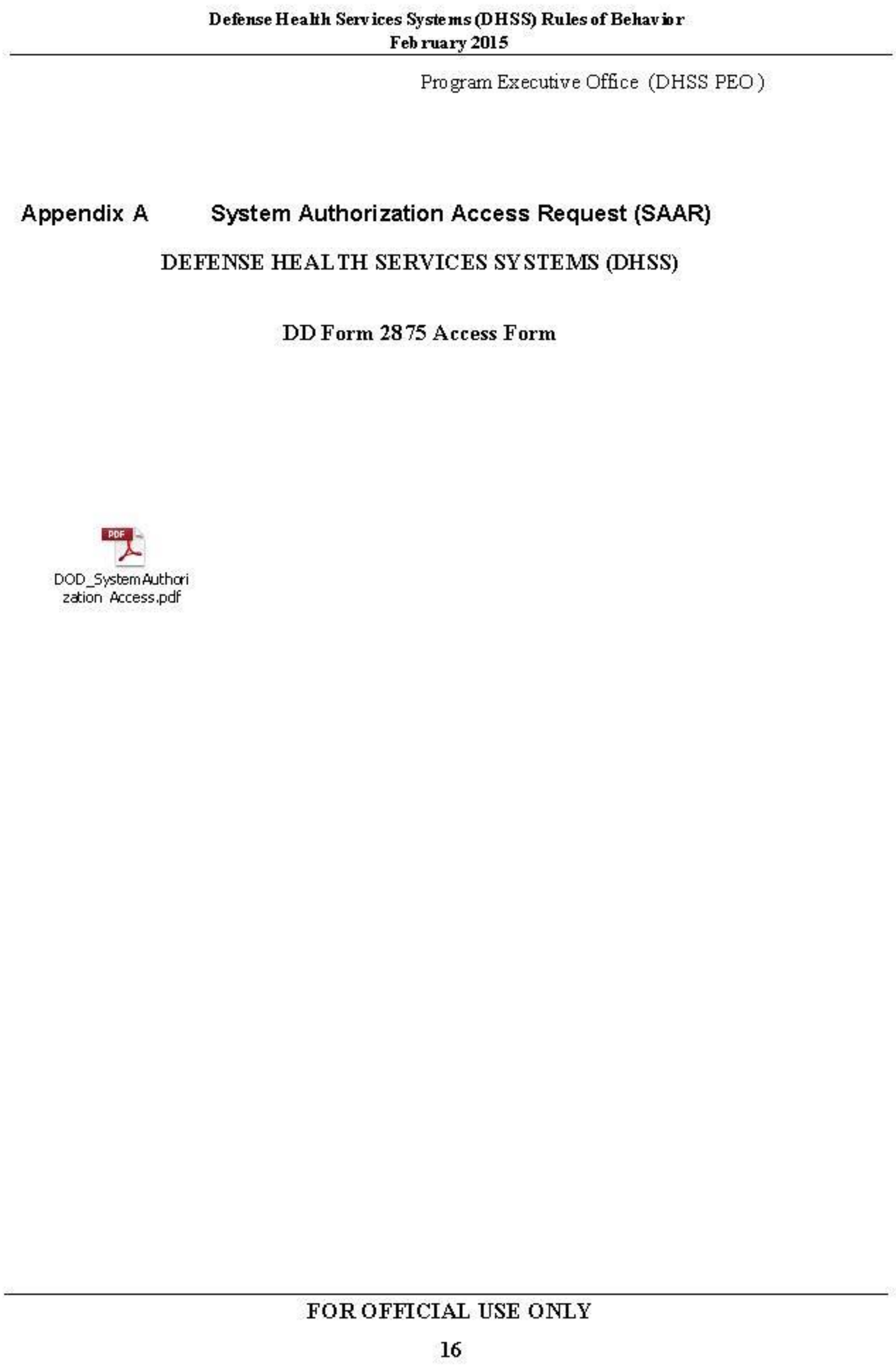
Digitally signed by HARRINGTON.CHRISTOPHER.JOHN.1012595324
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=HARRINGTON.CHRISTOPHER.JOHN.1012595324
Date: 2015.03.03 12:53:31 -05'00'

Date

Christopher J. Harrington

Deputy Program Executive Officer

Defense Health Services Systems



Defense Health Services Systems (DHSS) Rules of Behavior
February 2015

Program Executive Office (DHSS PEO)

Appendix A System Authorization Access Request (SAAR)

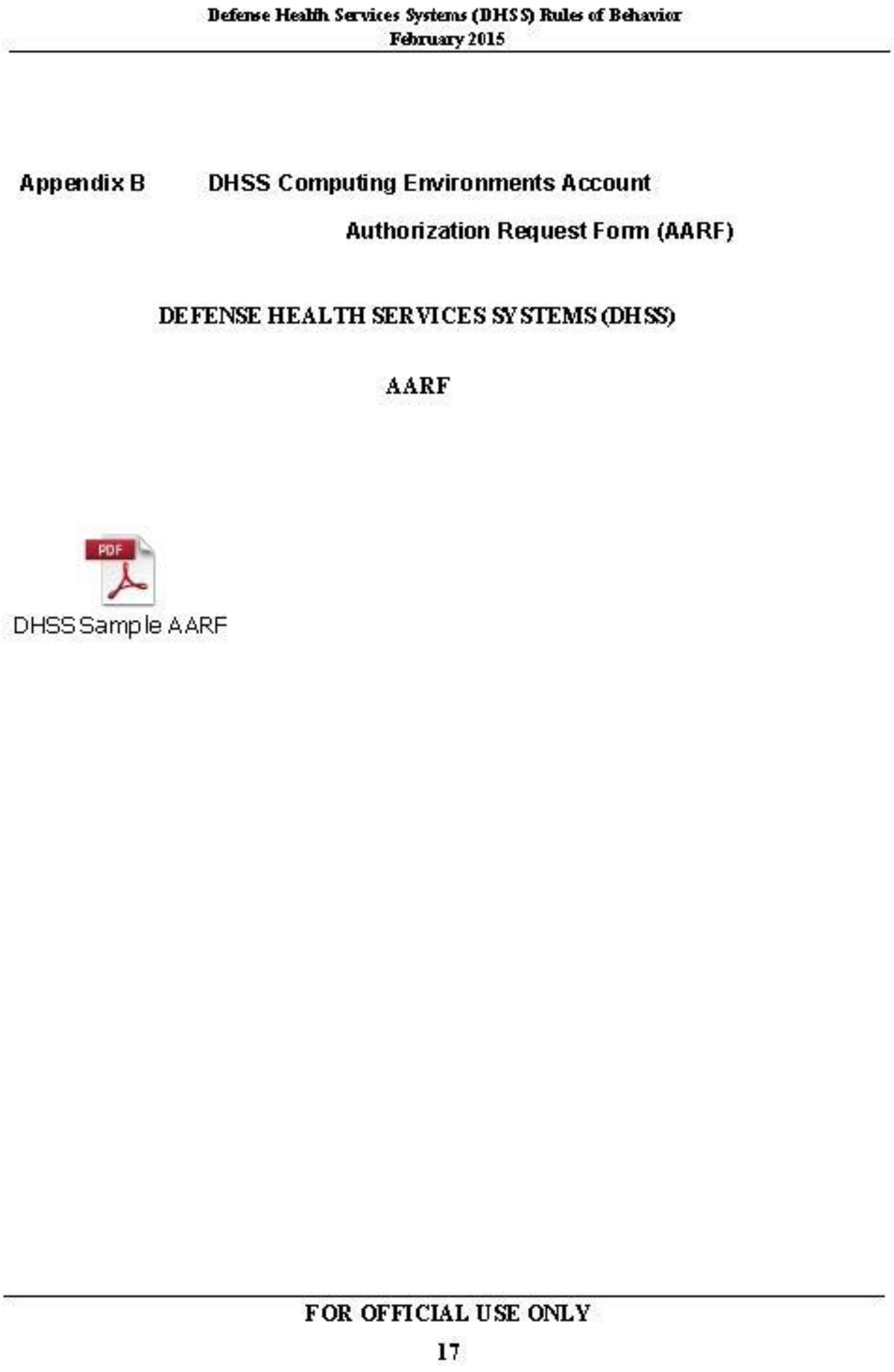
DEFENSE HEALTH SERVICES SYSTEMS (DHSS)

DD Form 2875 Access Form

DOD_SystemAuthorization Access.pdf

FOR OFFICIAL USE ONLY

16



Appendix B DHSS Computing Environments Account Authorization Request Form (AARF)

DEFENSE HEALTH SERVICES SYSTEMS (DHSS)

AARF

DHSS Sample AARF

Appendix C ACRONYMS List

AARF:	Account Authorization Request Form
AIS:	Automated Information System
ASD (C3I):	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
CAC:	Common Access Card
DHA:	Defensive Health Agency
DHSS:	Defensive Health Services Systems
DISA:	Defense Information Systems Agency
DoD:	Department of Defense
FOUO:	For Official Use Only
GFE:	Government Furnished Equipment
IA:	Information Assurance
IAM:	Information Assurance Manager
iAS:	identity Authentication Services
IASE:	Information Assurance Support Environment
ID:	Identification
IP:	Internet Protocol
IS:	Information System
PIN:	Personal Identification Number
PKI:	Public Key Infrastructure
PM:	Program Manager
PMO:	Program Management Office
POC:	Point of Contact
RAPIDS:	Real-Time Automated Personnel Identification System
RoB:	Rules of Behavior
SAAR:	System Authorization Access Request
URL:	Uniform Resource Locator
USB:	Universal Serial Bus

Appendix D DHSS REFERENCES

1. DHSS 2875 Account Access Procedure
2. DHSS Deactivation Procedure
3. DHSS Access Review Procedure
4. DHSS Access Management Procedure

Instructions and Guidance for
PEPR Account Activation Request Form

1. **System Access**. Select one or more PEPR tools you wish to access. If you request access for PCDIS and later need access to HA/TA or PEPR Satellite Reports a separate PEPR Account Activation Request Form is required at that time.

Overview of the PEPR Systems

CBM	CBM (Consolidated Bad Master) allows the Government to monitor and report on TED records that have validity or relational edit errors and have not been fully corrected by the contractor. CBMprovides the most current information on outstanding TED record by maintaining and reporting the outstanding claims with missing or invalid information [System contains Personal Health Information (PHI)]
CK	CK (Claim Check) produces monthly reports from the netted TED Master de-duped files identifying add-back and denial records by state and region in order to determine the total amounts saved as a result of reconciling duplicate claims.
CRDM	CRDM (Common Reporting Data Mart) uses the Purchased Care Data Warehouse (PCDW) to extracts the necessary subset of data, performing derivations where needed to provide the various downstream applications with a complete set of data.
DCS	The DHA Duplicate Claims System (DCS) was developed by the DHA to automate the resolution of duplicate claim payments. The system facilitates the identification of actually duplicate claim payments, the initiation and tracking of recoupments, and the removal of duplicate records from the Health Care Record (HCSRs) or TRICARE Encounter Data (TED) database. The system also generates operational and management reports.
MH	MH (Mental Health) calculates average charge per day for inpatient mental health diagnoses for specified high volume providers, and compares it to similar data for a base period to determine amount of change.
PCDIS & PRDM	PCDIS (Purchased Care Detail Information System) functions as a “search window” into the DHA Purchased Care Data Warehouse (PCDW). This data includes all HCSR and TED claims for care received outside MTFs by DHA beneficiaries, as well as active duty Supplemental Care, DHA Europe, and DHA Prime Remote. With PCDIS, you can: • Use the online retrieval paths to view summary and detail data contained in Health Care Service Records (HCSR) and TED claims for both institutional (i.e., hospital) and non-institutional (i.e., professional service, provider, medical group care) • Run pre-formatted and ad-hoc reports from within the PCDIS web-enabled application
QRDF	QRDF (Quick Response Data File) produces “as-requested” health record information products by beneficiary or provider from TED data sources. The information can be acquired for a time period from FY 1985 to the present date. (System contains PHI)
RF	RF (Reference Files) used for coding or classification purposes in analysis and event reporting. Reference Files maintained by PEPR include Defense Information Medical System (DMIS), Domestic and Foreign Zip Codes (CAD), Zip Code Exceptions, Contract Region File (CRF), Procedure Codes (CPT-4 and HCPCS), Diagnosis and Operation/Non-Surgical Procedure Codes (ICD-9-CM), Hospital Departments, Do Not Load/ Do Not Pay (Procedure Code), and General Reference Data.
TA	TA (TED Auditing) provides a mechanism for the Claims Audit Review Services (CARS) contractor and Defense Health Agency Activity (DHA) to track and monitor the claim-processing performance of Managed Care Support Contractor (MCSC), Managed Care Support Services (MCSS) and TRICARE Dual Eligibility Fiscal Intermediary (TDEFIC) contractors. Provides an audit trail with the appropriate error code, facilitates the input of detailed explanations for assessing errors and error amounts, and determines the contractor payment error and occurrence error performance standard.

2. **Employment Category**. Check category that applies.

3. **Applicant/Requestor Information**. Please fill in all applicable fields. You must select a 4-digit Account Validation PIN. It may be any 4-digit number that you will remember if needed to verify your identity for account administration purposes (i.e. password reset). For instance, you may use the last 4-digits of your social security number or month and day of birth, etc.

4. **Password Action/Access Authorization Requested**. Check to indicate whether this is a request for a new PEPR user account or an account or password change, account deletion or reactivation. If you have a user ID, please provide it. If your account has expired, please provide your last user ID if known.

4.A. **Special Permissions Data for Read/Write Users (Required for only DCS users).** Select the various special permissions required for your mission or contract related work. These special permissions must be approved by your supervisor and prime contractor.

5. **SDD Rules of Behavior.** The SDD Rules of Behavior is appended to the end of this document for your review and acceptance to the terms and conditions set forth by SDD Program Executive Office.

6.A. **DoD Cyber Awareness Challenge Training**. DoDD 8570.1 “Information Assurance Training, Certification, and Workforce Management”, August 15, 2004 requires that information system users complete Cyber Awareness Challenge Training on an annual basis. In accordance with this directive, the SDD Program Executive Office must have a copy of your DoD Cyber Awareness Challenge Certificate on file.

If you have not completed online Cyber Awareness Challenge Training in the past year, you will need to take the training, complete the test, download the form, sign it and send it via fax to SDD Access at 866-551-1249 or email at DHA.SDDAccess@mail.mil. The DoD Information Assurance training can be accessed on the Defense Information Systems Agency’s (DISA) website: http://iase.disa.mil/eta/online-catalog.html. Select Cyber Awareness Challenge.

6.B. **Product Training.** The SDD Program Executive Office (PEO) requires that users of PCDIS complete either classroom or web-based training (WBT). The WBT training and tests are located at the MHS Learn website: https://mhslearn.csd.disa.mil. Select “MHS Staff Training” to log in. Once logged in, enter “PCDIS” under Search Catalog. Select “SDD- (PCDIS) Purchase Care Detail Information System” to begin training. Once complete, enter the date of course completion or scheduled date (in the case of live training) in mm/dd/yyyy format and the type of training (live or web-based training (WBT), as appropriate, on Page 1 of this form.

7. **Data Sharing Agreement (DSA) Number.** Non-MHS personnel (generally other DoD employees) and/or contractors working for the MHS/DoD requiring access to PEPR data are required to have a current Data Sharing Agreement on file with the DHA Privacy and Civil Liberties Office. Please include PEPR and BCS/BOXI in the Project Title field of your Data Sharing Agreement Application (DSAA). BCS/BOXI is a SDD application that provides reporting and analytical services to the user communities of the Patient Encounter Processing and Reporting (PEPR) systems. For information pertaining to Data Sharing Agreements, please refer to the DHA Privacy and Civil Liberties Office website at http://www.tricare.mil/tma/privacy.

8. **Security Clearance Level**. All users of PEPR must have a minimum security clearance of ADP Level II. Users should contact their organization’s Security Officer or Personnel Office for assistance.

9. **PEPR Account Applicant Signature and Electronic Data Interchange Personal Identifier (EDIPI)**. All applicants must digitally sign this form to verify the truth and accuracy of the information presented herein. In order to access PEPR, each applicant must have a valid CAC or PIV card. To verify your CAC/PIV is valid please digitally sign the form.

To receive current e-mail notifications on PEPR or BCS/BOXI updates, news, and/or system outages, please register at https://public.govdelivery.com/accounts/USMHSSDD/subscriber/new

10. **Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media**

Government and commercial vendors are required to provide data at rest encryption products for all mobile computing devices used to connect to SDD products. If a PEPR applicant will be connecting to PEPR using a mobile computing device, the PEPR applicant is required to complete and submit Attachment B.

Encryption Standards/Approved Software

- A FIPS 140-2 approved file encryption algorithm (i.e., AES) must be used for full disk encryption to encrypt data on the remote device. Products that may be utilized include but are not limited to:
  PGP – https://www.pgp.com/products/wholediskencryption/index.html
- Mobile computing equipment users encrypt all temporary folders (e.g., C:\temp, C:\windows\temp, Temporary Internet Files, etc.) so that any temporary files created by programs are automatically encrypted.

DoD Components shall purchase data at rest encryption products through the DoD Enterprise Software Initiative (ESI), that substantially reduce the cost of common-use, commercial off-the-shelf software. For additional details, please log on to http://www.esi.mil and at http://iase.disa.mil.

11. **Commander, Supervisor or Security Officer Certification of Citizenship.** The requestor’s commander, supervisor, or security officer (the requestor’s employer) must certify that the requestor is a U.S. Citizen and has a mission or contract related requirement to access PEPR. All fields must be completed. Signature is required.

12. **Government Sponsor.** Please fill in all applicable fields.

13. **Level of Access**. The official duties of this individual require the following level of access (select one of the roles). Publisher role should only be chosen if absolutely needed to perform work functions. This access will require approval from PEPR Functional Sponsor and SDD PO Approving Authority.

14. **Protected Health Information Access**. If the official duties of this individual require access to patient identifying data, please complete Attachment A: Justification for Access to Protected Health Information (PHI).

Upon completion of Block 14, fax this form to SDD Access at 866-551-1249 or email to DHA.SDDAccess@mail.mil.

(Include Attachment A, if required.) If you are OCONUS and having trouble with the fax, please contact the Defense Health Agency (DHA) Global Service Center at servicecenter@dha.mil or 1-800-600-9332 for an alternate number.

15. **SDD Certification**. For SDD use only.

Attachment A. Justification for Access to Patient Identifiable Data.

All users require justification for access to the protected health information contained in PEPR.

User justification and signature is required.

Attachment B. Encryption of Sensitive Unclassified Data at Rest on Mobile Computing and Removable Storage Media

All users require justification for access to the protected health information contained in PEPR.

The form must be filled out by both the user and the user's Information Assurance or Information Security Officer.

Attachment C. SDD Rules of Behavior

All users must read and ACCEPT the terms set forth in the SDD Rules of Behavior.

IMPORTANT: KEEP A COPY OF THIS FORM IN A SAFE PLACE FOR YOUR RECORDS AND FUTURE REFERENCE.