

**VA EASTERN COLORADO HEALTH CARE SYSTEM
VETERANS HEALTH ADMINISTRATION
DEPARTMENT OF VETERANS AFFAIRS**

00Q-78

(00Q)

PATIENT ABUSE AND NEGLECT

1. PURPOSE: To establish health care system policy and procedures to be followed in cases of alleged or suspected patient or resident abuse and/or neglect.

2. POLICY: It is the policy of the Eastern Colorado Health Care System (ECHCS) that no patient or resident will be mistreated, abused, or neglected in any way by an employee. ECHCS has zero tolerance for patient abuse or neglect.

3. DEFINITIONS:

a. Patient Abuse is defined as an act that involves physical, emotional, psychological, sexual, and/or verbal abuse, including but not limited to:

- (1) Intentional omission of care;
- (2) Willful violations of a patient's privacy;
- (3) Intimidation, harassment, or ridicule of a patient;
- (4) Willful physical injury;
- (5) Unintended injury as stated above, through employee's course of actions;
- (6) Physical striking of a patient;
- (7) Inappropriate verbal or insulting behavior, or remarks toward/about a patient;
- (8) Abandoning, neglecting or isolating a patient;
- (9) Threatening a patient;
- (10) Exploiting a patient;
- (11) Stealing from, or taking advantage of, a patient with respect to financial gain or other personal matters; and/or
- (12) Any action or behavior that conflicts with patient's rights, identified in ECHCS policy 00-14, Patient Rights and Responsibilities.

b. A patient refers to any individual receiving VA care in any setting, venue, or program.

c. A resident refers to any veteran receiving care in a residential program, such as the Community Living Center, Residential Rehabilitation Program, or Domiciliary.

4. RESPONSIBILITIES:

a. The ECHCS Executive Leadership Team (ELT) is responsible for ensuring compliance with this policy by all employees. The ELT is responsible for establishing a **culture of safety** and creating a blame-free environment that promotes reporting of unsafe conditions or practices, near misses, and adverse events; ensures that all suspected cases of patient abuse are investigated; reviews all comments regarding the incident and ensures that appropriate actions are taken in cases of substantiated abuse. The ELT is responsible for ensuring a preliminary review of each allegation of abuse is conducted and a timely report of findings is submitted; informing the Director of findings and makes recommendations for further action, as appropriate.

b. Clinical Service Chiefs, Associate Chief Nurses and Supervisors are responsible for ensuring the supervisor immediately initiates a fact-finding, collecting all appropriate information related to the incident, and referring the matter immediately to their associated ELT member, Human Resources, and Quality Management.

c. Supervisors are responsible for:

(1) Annually reviewing this policy with their employees. (Attachment A).

(2) 4.b. above.

(3) When informed of a possible incident of patient abuse or neglect, the Supervisor will notify their chain of supervisory command and a member of the Executive Leadership Team (ELT). If criminal acts or suspected criminal acts occur, the informed Supervisor is to report those events to the VA Police immediately. Failure to report an incident of patient abuse may result in administrative action.

NOTE: *The Police will call the VA Office of the Inspector General (OIG) if needed. Of course, all employees have the right to contact OIG.*

(4) The Supervisor/Manager will notify the physician in charge of the patient to ensure the patient receives appropriate treatment, if necessary.

(5) Submit the completed fact-finding to Human Resources and in adherence to Policy 05-12 Disciplinary and Adverse Actions. Administrative Investigation (AI) may need to be delayed while a criminal investigation is active.

d. The VA Police are responsible for investigating and referring criminal acts for prosecution.

e. The Employee is responsible for:

(1) Reporting any suspected or actual incidents of patient abuse and/or neglect to his/her immediate supervisor within one (1) hour of awareness of the event, or immediately to prevent further endangerment of the Veteran.

(2) Becoming familiar with the contents of this policy. Every employee should avoid any act which could be construed as abuse, neglect, or mistreatment of patients.

(3) An employee that witnesses any patient abuse, neglect or mistreatment and does not report it to the proper authority is also subject to disciplinary action based on the seriousness of the offense.

f. Quality Management is responsible for reviewing all fact-finding in collaboration with Human Resources Management Service and the affected Service Chief to determine if the case will be forwarded to the Director for consideration of an AI. Additionally, ensuring that all formally-appointed AIs are coordinated, all board members receive the training required to fulfill their assigned responsibility, and that all substantiated cases of abuse are reported to appropriate officials within the specified time frame.

g. Human Resources is responsible for advising management regarding appropriate administrative action to be pursued.

5. PROCEDURES:

a. Policy understanding and expectations to report:

(1) Human Resources will provide every new employee a copy of this policy at new employee orientation.

(2) The Patient Abuse Statement of Understanding (Attachment A) will be signed by the new employee and filed in the employee's Official Personnel Folder and Competency Assessment file.

(3) Supervisors will re-distribute and/or discuss this policy in a staff meeting and assure that every employee in his/her department signs the Patient Abuse and Neglect Statement of Understanding on an annual basis. The Patient Abuse and Neglect Statement of Understanding will be maintained in the employee's unit six-part Official Personnel Folder and Competency Assessment file.

b. Reporting and investigation of abuse or neglect:

(1) The employee will notify his/her immediate supervisor on duty within one (1) hour of awareness of the event, or immediately to prevent further endangerment of the Veteran.

(2) Employees who become aware of possible abuse or neglect of a patient (After notification to the supervisory chain of command and ELT) will initiate one of the three following procedures within 24 hours: 1) the electronic Joint Patient Safety Reporting (JPRS) electronic tool, 2) call the patient safety Hotline 1-SAFE (7233), or 3) complete a Patient Safety Report form (see Attachment B). The JPRS is the preferred method.

(3) The supervisor will subsequently notify a member of the ELT within one (1) hour of being informed of the alleged abuse or neglect.

(4) Actual or possible criminal acts must be reported to the VA Police without delay. VA Police will initiate a preliminary investigation, and if the act is believed to be felonious, the VA OIG will be notified. If criminal behavior is substantiated, the VA Police and/or the VA OIG will refer the case for prosecutorial review.

(5) If necessary, an Administrative Board of Investigation (AIB) will be conducted in accordance with VHA Handbook 1050.01 VHA National Patient Safety Improvement Handbook; VA Handbook 0700, Administrative Investigations.

(6) Allegations of patient abuse must be investigated by an AIB. Exceptions to the requirement are when the patient is known by the treatment team to use allegations of this nature or the threat of such allegations to manipulate staff and when patient judgement is impaired. If the employee admits to patient abuse, the AIB is discretionary. If, during an AIB, it appears a criminal act occurred or may have occurred, the AIB must be suspended immediately and the matter be referred to VA law enforcement.

(7) The patient's perception of how s/he was treated is seriously considered when determining whether abuse occurred. Even without direct patient input, such as patients with limited cognition, abuse can be substantiated.

6. CONCURRENCES: Deputy Director, Chief of Staff, Associate Director of Patient Care Services, Regional Manager Southern Colorado CBOCs, Associate Directors, Assistant Director, Police Service, Deputy Chiefs of Staff, Chief Nurses, Nurse Managers, Clinical Service Chiefs, Clinical Section Chiefs, Ethics Committee, Health Information Management Section, Human Resources, Quality Management, Patient Safety, Risk Management, Privacy, Human Resources, NNU-Denver, and AFGE.

If there is a conflict between the provisions of this policy and the applicable bargaining unit agreement, the terms of the bargaining unit agreement will prevail. Union Participation should be in accordance with the current contract.

7. REFERENCES:

VHA Directive 1199, Reporting Cases of Abuse and Neglect, November 28, 2017.

VHA Directive 1050.01, National Patient Safety Improvement Handbook, March 4, 2011.

The Joint Commission Edition 2018, Provision of Care, Treatment, and Services (PC.01.02.09) and Right and Responsibilities of the Individual (RI.01.06.03) and Care Treatment and Services (CTS.02.02.05).

ECHCS 00-14 Patient Rights and Responsibilities dated October 3, 2017.

VA Handbook 0700, Administrative Investigations, May 25, 2002.

8. RESCISSION: 00-78 Patient Abuse, 2015**9. REVIEW DATE:** April 2021


Sallie A. Houser-Hanfelder, FACHE
Director

Attachments: A - Patient Abuse Statement of Understanding
B - Patient Safety Reporting

PATIENT ABUSE AND NEGLECT STATEMENT OF UNDERSTANDING

*Do Not Remove from Official Personnel Folder While Employed at Department
of Veterans Affairs, Eastern Colorado Health Care System*

This is to certify that I have read and understand the VA policy on Patient Abuse. I understand that abuse, verbal and/or physical, involving VA patients will not be tolerated. I understand that if an allegation of patient abuse is substantiated, I will be subject to appropriate administrative actions, up to and including removal from my position within the health care system.

I also understand that criminal behavior must be reported to the VA Police or the VA Office of Inspector General (OIG) immediately and that substantiated criminal behavior will be referred to the United States Attorney or local Prosecutor as appropriate.

Receipt of a copy of ECHCS Policy 00Q-78, Patient Abuse, is hereby acknowledged and will be reviewed/signed annually.

Initial Signatures

Employee's printed
name/signature

date

Supervisor's printed
name/ signature

date

Annual Signatures

Employee's signature

date

Supervisor's signature

date

Employee's signature

date

Supervisor's signature

date

Employee's signature

date

Supervisor's signature

date

Employee's signature

date

Supervisor's signature

date

Employee's signature

date

Supervisor's signature

date

Employee's signature

date

Supervisor's signature

date

Patient Safety Reporting Options

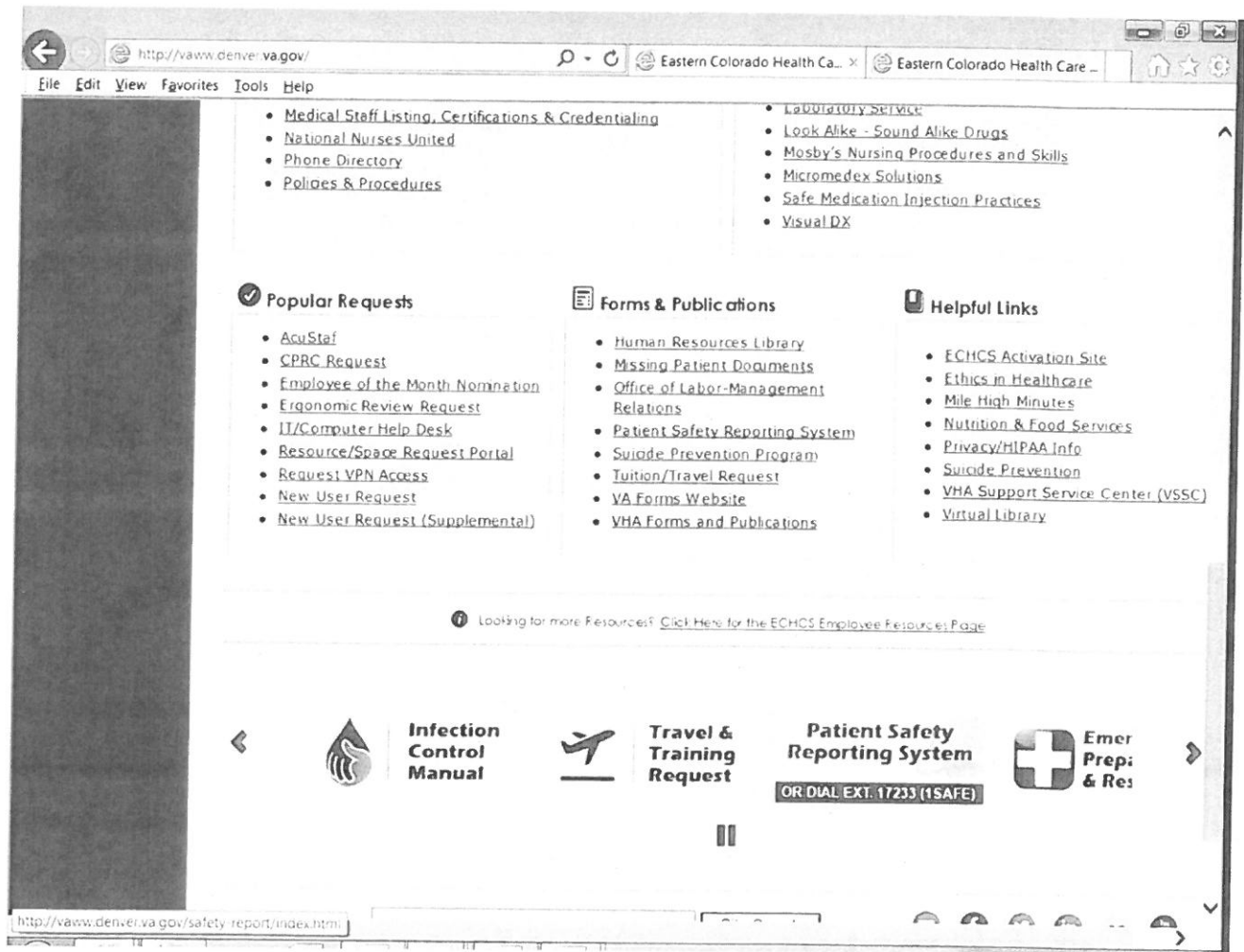
A Patient Safety report is communicated from staff (clinical and non-clinical) to the Patient Safety office regarding observed events or close calls that could harm our patients at any level.

1. JPRS Electronic Reporting System available on the ECHCS homepage
2. Patient Safety Hotline – “1-SAFE” or 17233
3. Paper Patient Safety Report

Available on the ECHCS Homepage

Place in Confidential envelope

Address to “00Q-PS” – delivered to Patient Safety office



QMI USE ONLY	
SAC: A _____ p _____ Close Call _____	
CODE: M F S R E Tx A D U W O	Category/contributing factor: _____

PATIENT SAFETY REPORT

PATIENT NAME: _____ SSN: _____ VS: _____	DATE: _____ TIME: _____ PATIENT STATUS: In _____ Out _____ UNIT: _____ LOCATION: _____ DIAGNOSIS: _____ MENTAL STATUS: _____ ACTIVITY LEVEL: _____	CATEGORY MEDICATION: _____ FALL: _____ PARASUICIDE: _____ MISSING: _____ OTHER: _____
DESCRIBE EVENT: _____ ACTUAL EVENT or CLOSE CALL (CIRCLE)		
FALLS Prior fall (documented) YES _____ NO _____ Is patient confused? YES _____ NO _____ Was patient's medical condition the primary contributing factor? (e.g., diabetes, seizure, medication, arthritis, etc.) YES _____ NO _____ Were any of the following environmental issues the primary contributing factor? (Check only one) Lightning _____ Toilet height _____ Side-rails _____ Sink height _____ Bed height _____ Flooring _____ Footwear _____ Wet floor _____ Grabbing for an item _____ Other obstacles (describe) _____ Prior to fall patient was _____ in bed _____ in chair _____ ambulating Does the patient have an IV Heparin lock? YES _____ NO _____ Did the patient fall while in restraints? YES _____ NO _____	MEDICATIONS [Check <u>one</u> in each below] <u>Type of error</u> Wrong Dose _____ Wrong Route _____ Wrong Rate _____ Wrong Dosage Form _____ Wrong Drug _____ Wrong Time _____ Wrong Preparation _____ Wrong Patient _____ Extra Dose _____ Omission _____ Known Allergy _____ <u>Category</u> Prescribing _____ Dispensing _____ Administration _____ Monitoring effects _____ Monitoring systems _____ <u>Other related issues</u> Lack of communication _____ Distraction _____ Labeling _____ Equipment (e.g., BCMA) _____ Packaging Design _____ Storage _____ Look-alike name or table: _____ Limited staffing _____	
PARA-SUICIDE [Attempt/Gesture] To report a suicide or para-suicidal event, please use the PROGRESS NOTE title: SUICIDAL / PARA-SUICIDAL EVENT (This form is no longer used for this section of the Patient Safety Report)	MISSING PATIENT <i>Attach Missing Patient Check List</i> ETOH/ Substance Abuse listed on as active diagnosis on current admission YES _____ NO _____ Safety Risk Assessment Tool Complete YES _____ NO _____ (For patients of psychiatric patients only) Date _____ Low Risk = voluntarily admitted patient with intact decision-making ability High Risk (check one) ☐ Court appointed legal guardian ☐ Considered a danger to self or others ☐ 72-hour Mental Health Hold ☐ Lacks cognitive ability to make decisions ☐ Physical or mental impairment that increases risk of harm _____ ☐ Mental Health Certification _____ short-term _____ long-term	

Patient Safety Report
Page 2

DISRUPTIVE BEHAVIOR Patient to patient Patient to staff or others Police Notified CODE 3 or 4 called Other _____ Type of incident: Loud demanding Verbal threat Possession of weapon Violence against property Violence against people: Touched in threatening way Inflicted serious harm requiring medical care Interventions: Resolved verbally Police intervened Restraints applied Is person medicated Person placed in secure room Other: _____ Reason for outbreak of behavior: _____ Does patient have previous history of assaults: yes no Was the employee injured during the disruptive behavior incident? YES NO Name of injury: _____ Referred to Employee Health / ER / Private Provider? (Circle) YES NO N/A	
OTHER PATIENT SAFETY ISSUES (circle). Check related issues as indicated. Death Surgical Suicide Within 24 hours of admission Delay in Diagnosis/Treatment due to: Equipment Lab Radiology Specialty Availability Patient Abuse Patient Injury in Restraints or Seclusion Care planning Communication Equipment Lack of Observation Orientation training Staffing Levels Surgical Issue: Consent Contamination Needle count Sponge count Other Transfusion Error: Communication Consent Equipment Multiple samples Orientation training Reaction not assessed Staffing Verification Wrong Site Surgery: Communication w/ patient Communication w/ surgical team Competency Credentialing Distraction Patient assessment Policy for Verification not followed Utility of Equipment Failure Equipment Number: _____ Type of Equipment: _____ Other Patient Injury: _____	
MD NOTIFICATION Name: _____ Date: _____ Time: _____	REPORTER Name: _____ Date: _____ Time: _____
PHYSICIAN REPORT [only necessary for actual events, not close calls]	
PRINT NAME: _____ SIGNATURE: _____ Date: _____ Time: _____	
QUALITY MANAGEMENT COMMENTS: No further action required RCA Initiated	
PATIENT SAFETY MANAGER: _____ DATE: _____	
This form must be initiated within 24 hours of the incident and forwarded to the QM office ASAP. Patient-Focused Care staff forward through appropriate channels. The event should be documented in the progress notes. No mention of this form should be made in the medical record nor should this form be placed in the medical or administrative sections of the patient's record. This information is protected in 35 U.S.C. 5705. DO NOT MAKE COPIES DVAMC 10-2633	

**VA EASTERN COLORADO HEALTH CARE SYSTEM
VETERANS HEALTH ADMINISTRATION
DEPARTMENT OF VETERANS AFFAIRS**

00-23

APR 28 2016

(05)

EMPLOYEE/PATIENT RELATIONSHIPS

1. PURPOSE: To emphasize the employee behavior expectations with regard to the therapeutic relationship between VA Eastern Colorado Health Care System (ECHCS) employees and current or former patients of this facility, and broadens the coverage to all employees.

2. POLICY:

a. Patients who seek treatment from this health care system are considered to be in a vulnerable and disadvantaged position. Patients will be treated with the utmost respect and dignity by all employees. Employees will ensure their interactions with patients, both on and off duty, reflect the highest level of professionalism and therapeutic benefit.

b. All employees, regardless of service or assignment, are expected to limit their contact and interchange with patients to those actions and attitudes that will be beneficial to the patient, or administratively necessary to support the therapeutic environment.

c. Inappropriate social, business and sexual relationships between patients and employees may be considered justification for the formal charge of patient abuse, which may subject an employee to various levels of disciplinary action including dismissal. Other criminal charges and civil actions are also possible under State law.

d. Relationships that predate contact within ECHCS are not ordinarily covered by this policy. However, an attempt to use one's ECHCS position to initiate, resume, intensify, or compromise the pre-existing relationship is covered.

e. Definitions:

(1) Therapeutic Relationships: All relationships between employees and patients for the purpose of or in support of evaluation, treatment, referral, and follow up, along with all services or departments that support their function.

(2) Social/Sexual Relationships: All relationships between an employee and patient for the purpose of pleasure, entertainment, and personal fulfillment not directly associated with the patient's therapeutic regimen. Sexual relationships include but are not limited to kissing, touching, and sexual intercourse.

(3) Business Relationships: Any interactions/transactions between patients and employees which may be licit or illicit for monetary or personal gain including but not limited to gambling, betting, dealing drugs, contraband, financial employment, joint business ventures, bartering or contractual agreements.

(4) Patients: Any patient who receives treatment from the VA whether in an inpatient or outpatient status.

3. RESPONSIBILITY:

a. It is the responsibility of each employee to become familiar with and abide by the contents of this policy. Each employee should avoid any act which could be construed as a violation of this policy, give the appearance of improper action, or could discredit the Department of Veterans Affairs.

b. Human Resources Management Service will ensure that new employees review this policy in New Employee Orientation.

c. Managers who become aware of possible inappropriate social/sexual/business relationships between employees and patients will be responsible for documenting the alleged occurrence and informing their respective Executive Leadership Team (ELT) Member within eight business hours.

4. PROCEDURES:

a. All employees must report their knowledge or suspicion of any incident of inappropriate social/sexual/business relationship between employees and patients to the respective Service Chief within eight business hours of identification of information.

b. Police Service will investigate the alleged occurrence for criminal implications.

c. Alleged violations of this policy will be reported to the Service Chief and fact-finding will be conducted*. Pending the outcome of the fact finding, an employee suspected of violating this policy may be 1) detailed to another area of responsibility within his/her respective service, 2) detailed to another area of the Health Care System, or 3) placed in a non-duty status with pay.

*The fact finding will be concluded within 72 business hours unless extended by appropriate ELT member.

d. Once the fact finding is complete, the ELT will determine the need for either an Administrative Board of Investigation or appropriate administrative action. The Service Chief and a consultant within Human Resources, will recommend the appropriate administrative action to the Director.

5. CONCURRENCES: Human Resources, AFGE Local #2241 and #2430, Organizational Improvement, Fiscal, Regional Manager Southern Colorado CBOCs, Chief of Staff, Associate Chief of Staff CBOCs, Assistant Director, Associate Director, Associate Director Patient Care Services, Privacy, Patient Safety.

If there is a conflict between the provisions of this policy and the applicable bargaining unit agreement, the terms of the bargaining unit agreement prevail. Union participation should be IAW the current contract.

6. REFERENCES:

00-78, Patient Abuse and Neglect

00-14, Patient Rights and Responsibilities

VHA Handbook 1050.01 National Patient Safety Improvement Handbook

7. RESCISSION: 00-23 Employee/Patient Relationships, dated November 10, 2012

8. REVIEW DATE: April 2019


Sallie A. Houser-Hanfelder, FACHE
Director

Department of Veterans Affairs (VA) National Rules of Behavior**1. Background**

a. Section 5723(b)(12) of title 38, United States Code, requires the Assistant Secretary for Information and Technology to establish "VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department's missions and functions." The Office of Management and Budget (OMB) Circular A-130, Appendix III, paragraph 3(a)(2)(a) requires that all Federal agencies promulgate rules of behavior that "clearly delineate responsibilities and expected behavior of all individuals with access" to the agencies' information and information systems, as well as state clearly the "consequences of behavior not consistent" with the rules of behavior. **The National Rules of Behavior that begin on page G-3, are required to be used throughout the VA.**

b. Congress and OMB require the promulgation of national rules of behavior for two reasons. First, Congress and OMB recognize that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g. digital, paper), are essential aspects of their job. Second, individuals must be held accountable for their use of VA information and information systems.

c. VA must achieve the Gold Standard in data security which requires that VA information and information system users protect VA information and information systems, especially the personal data of veterans, their family members, and employees. Users must maintain a heightened and constant awareness of their responsibilities regarding the protection of VA information. The Golden Rule with respect to this aspect of an employee's job is to treat the personal information of others the same as they would their own.

d. Since written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using "due diligence" and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and VA Directives.

2. Coverage

a. The attached VA National Rules of Behavior must be signed annually by all VA employees who are provided access to VA information or VA information systems. The term VA employees includes all individuals who are employees under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees. Directions for signing the rules of behavior by other individuals who have access to VA information or information systems, such as contractor employees, will be addressed in subsequent policy. VA employees must initial and date each page of the copy of the VA National Rules of Behavior; they must also provide the information requested on the last page, sign and date it.

b. The VA National Rules of Behavior address notice and consent issues identified by the Department of Justice and other sources. It also serves to clarify the roles of management

and system administrators, and serves to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

c. The VA National Rules of Behavior use the phrase “VA sensitive information”. This phrase is defined in VA Directive 6500, paragraph 5q. This definition covers all information as defined in 38 USC 5727(19), and in 38 USC 5727(23). The phrase “VA sensitive information” as used in the attached VA National Rules of Behavior means:

All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information, financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information, information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege, and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

d. The phrase “VA sensitive information” includes information entrusted to the Department.

3. Rules of Behavior

a. Immediately following this section is the VA approved National Rules of Behavior that all employees (as discussed in paragraph 2a of Appendix G) who are provided access to VA information and VA information systems are required to sign in order to obtain access to VA information and information systems.

Department of Veterans Affairs (VA) National Rules of Behavior

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

1. GENERAL RULES OF BEHAVIOR

a. I understand that when I use any Government information system, I have NO expectation of Privacy in VA records that I create or in my activities while accessing or using such information system.

b. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), VA, and law enforcement personnel.

c. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

d. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal, civil, and/or administrative penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

e. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my Operating Unit's Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.

f. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my supervisor, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

g. I understand that the VA National Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

h. I understand that the VA National Rules of Behavior do not supersede any local policies that provide higher levels of protection to VA's information or information systems. The VA National Rules of Behavior provide the minimal rules with which individual users must comply.

i. I understand that if I refuse to sign this VA National Rules of Behavior as required by VA policy, I will be denied access to VA information and information systems. Any refusal to sign the VA National Rules of Behavior may have an adverse impact on my employment with the Department.

2. SPECIFIC RULES OF BEHAVIOR.

a. I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor and the ISO when the access is no longer needed.

b. I will follow established VA information security and privacy policies and procedures.

c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001.

e. I will secure VA sensitive information **in all areas** (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local Chief Information Officer (CIO).

f. I will properly dispose of VA sensitive information, either in hardcopy, softcopy or electronic format, in accordance with VA policy and procedures.

g. I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff.

h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.

- i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500.
- j. I will not store any passwords/verify codes in any type of script file or cache on VA systems.
- k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.
- l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any VA electronic communication system.
- m. I will not auto-forward e-mail messages to addresses outside the VA network.
- n. I will comply with any directions from my supervisors, VA system administrators and information security officers concerning my access to, and use of, VA information and information systems or matters covered by these Rules.
- o. I will ensure that any devices that I use to transmit, access, and store VA sensitive information outside of a VA protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).
- p. I will obtain the approval of appropriate management officials before releasing VA information for public dissemination.
- q. I will not host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized **in writing** by my local CIO and I will ensure that all such activity is in compliance with Federal and VA policies.
- r. I will not attempt to probe computer systems to exploit system controls or access VA sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the VA CIO.
- s. I will protect Government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.
- t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software **authorized by the VA** on VA equipment or on computer systems that are connected to any VA network.
- u. If authorized, by waiver, to use my own personal equipment, I must use VA approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure

the software is configured to meet VA configuration requirements. My local CIO will confirm that the system meets VA configuration requirements prior to connection to VA's network.

v. I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w. I will not disable or degrade software programs used by the VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or to create, store or use VA information.

x. I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access VA information or information systems or to create, store or use VA information.

y. I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-VA entity's Rules of Behavior to obtain access to information or information systems controlled by that non-VA entity, I still must comply with my responsibilities under the VA National Rules of Behavior when accessing or using VA information or information systems. However, those Rules of Behavior apply to my access to or use of the non-VA entity's information and information systems as a VA user.

bb. I understand that remote access is allowed from other Federal government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

cc. I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I must use VA-provided IT equipment for remote access when possible. I may be permitted to use non-VA IT equipment [Other Equipment (OE)] only if a VA-CIO-approved waiver has been issued and the equipment is configured to follow all VA security policies and requirements. I agree that VA OI&T officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of VA sensitive information.

dd. I agree that I will not have both a VA network connection and any kind of non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my local CIO.

ee. I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO. I agree that I will not access, transmit or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

ff. I will obtain my VA supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using VA sensitive information outside of VA's protected environment..

gg. I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations, e.g., at home and during travel, and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location pursuant to an approved telework agreement with VA sensitive information that authorized OI&T personnel may periodically inspect the remote location for compliance with required security requirements.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data.

ii. I will not store or transport any VA sensitive information on any portable storage media or device unless it is encrypted using VA approved encryption.

jj. I will use VA-provided encryption to encrypt any e-mail, including attachments to the e-mail, that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. VA sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific VA systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

3. Acknowledgement and Acceptance

a. I acknowledge that I have received a copy of these Rules of Behavior.

b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

[Print or type your full name]

Signature

Date

Office Phone

Position Title