CLEAN DESK

1. PURPOSE. To establish policy and procedure for clean desks.

2. POLICY. Employees will adhere to reasonable privacy steps in their assigned work area (clean desk) to protect sensitive information from misuse, loss, unauthorized access, unintended modification and/or disclosure.

3. DEFINITIONS.
   a. Secure Work Area. Work area that can be locked to prohibit entry.
   b. Security. Protecting information from unauthorized disclosure or intelligible interception.
   c. Sensitive Information. Sensitive information is 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. Unsecured Work Area. An open workstation or area that cannot be locked to prohibit entry.

4. PROCEDURE.
   a. The organization will provide secure methods of conducting business while maintaining the ability to work effectively. This policy will present a positive image to our customers, present the opportunity to reduce the use of paper, and aid in accounting for and fortification of sensitive information.
   b. The clean desk policy applies to all employees, volunteers, students, residents, interns, contractors and others performing work for NF/SGVHS, referred to elsewhere as employees.
c. The level at which the policy will be applied is determined by the physical security of worksite and the level of sensitivity of information used.

(1) Unsecured Areas.

(a) Employees must be conscientious of sensitive information on desktops and other work areas in the course of their daily work. Only sensitive information currently being used should be visible on the desktop and should be protected when dealing with customers. When not being used by staff, sensitive information is protected by covering or securing in a manner to prevent incidental disclosure.

(b) Desks in open areas are to be cleared of sensitive information when unattended. During unattended periods, all sensitive information will be properly secured.

(c) Lock all desks and filing cabinets that contain sensitive information at the end of each working day.

(d) Ensure discarded materials are appropriately disposed of to avoid unwanted disclosure.

(2) Secure Areas.

(a) Shared offices with lockable doors.

(b) Lock door(s) when the office is unattended.

(c) Employees must be conscientious of sensitive information on desktops and other work areas in the course of their daily work. Only sensitive information currently being used should be visible on the desktop and should be protected when dealing with customers. When not being used by staff, sensitive information is protected by covering or securing in a manner to prevent incidental disclosure.

(d) Lock all room doors at the end of each working day. As appropriate, consider securing desks and filing cabinets containing sensitive information as well.

(e) Ensure discarded materials are appropriately disposed of to avoid unwanted disclosure.

(3) Private offices with lockable doors.

(a) Lock door(s) when the office is unattended.

(b) Employees must be conscientious of sensitive information on desktops and other work areas in the course of their daily work. Only sensitive information currently being used should be visible on the desktop and should be protected when dealing with customers. When not being used by staff, sensitive information is protected by covering or securing in a manner to prevent incidental disclosure.

(c) Lock all room doors at the end of each working day. As appropriate, consider securing desks and filing cabinets containing sensitive information as well.
(d) Ensure discarded materials are appropriately disposed of to avoid unwanted disclosure.

d. Health Record File Areas.

(1) Access to health records and health record file areas is limited to authorized personnel.

(2) Health records in file areas and other areas where health records are temporarily stored (clinic or treatment areas, record review areas, quality assurance areas, release of information, etc.) must be locked when responsible personnel are not present to ensure the security of the area and to ensure records are not accessible to unauthorized individuals.

e. Transporting Sensitive Information.

(1) Health records and/or other sensitive information being transported within the facility are protected by securing in a manner to prevent incidental disclosure. Sensitive information should never be left unattended during transport.

(2) Sensitive information must not be taken to alternative work locations without written authorization by the employee’s supervisor. Authorization should be carried with the employee at all times during travel to and while at the alternative work location, with a copy provided to and maintained by the local Information Security Officer (ISO). Sensitive information must be safeguarded at all times and should not be left unattended in a vehicle while away from the home facility.

f. General Procedures for Maintaining a Clean Desk.

(1) Tidy one’s desk at the end of the day and store sensitive information appropriately, according to the physical security of the worksite, as above.

(2) Don’t leave hard copy materials containing sensitive information lying out where anyone may view.

(3) Sensitive materials including patient information, employee information, and/or other personal data shall be disposed of appropriately, by shredding, by burning, or utilizing appropriate locked containers.

(4) Secure day planners, Rolodex, notebooks, and other materials that contain sensitive information.

(5) Lock cell phones, personal digital assistants (PDAs), and other electronic devices with a pass code.

(6) Appropriately erase or secure white boards that contain sensitive information.

(7) In unsecured areas, do not use bookshelves to store binders with sensitive information.

(8) Keep file cabinets with sensitive information closed and locked as practical. Do not leave keys in their locks.
(9) Never leave access codes/cards or keys exposed; always keep them secure and report any breach immediately.

(10) Keep all personal effects secured.

(11) Close applications and lock workstations when leaving your work area. Do not leave portable media such as CDs or floppy disks in drives.

(12) Immediately remove printed materials from fax machines and/or printers. Only authorized personnel are allowed to print extractions from the electronic record or to make copies from the paper chart.

(13) Strive to handle paper only one time. Act on it, file it, or appropriately dispose.

(14) Do not post sensitive documents, including but not limited to, user IDs and passwords, IP addresses, contracts, social security numbers, patient lists, employee records, and/or anything you wouldn’t want disclosed.

(15) If possible, desks and furniture should be positioned so that sensitive material is not visible from either the windows or the hallway. Otherwise, use a screen filter to minimize the viewing angle on a computer monitor, and/or close blinds on windows. Precautions must be taken by staff to ensure the sensitive information on computer screens cannot be seen by individuals who do not have a legitimate need-to-know.

(16) Challenge unauthorized persons who enter your work area.

g. It is intended that employees will abide by this policy without compromising their ability to efficiently complete their duties. The policy is to be applied in the most effective means for the employee’s work area. Individual barriers in compliance with the policy, and/or any suspected violations of this policy should be reported to the supervisor and/or the Privacy Officer, and/or Information Security Officer (ISO).

5. RESPONSIBILITY.

a. The Director is responsible for ensuring a clean desk policy, is in place and administered.

b. The Privacy Officer is responsible for the administration of the provisions of the Privacy Act, in regards to this clean desk policy.

   (1) Issuance of local policies and procedures consistent with national privacy policies and appropriate to implement this clean desk policy, and monitoring compliance with such policies and procedures.

   (2) Providing guidance to staff on privacy-related matters including the clean desk policy.

   (3) Assistance to supervisory staff and/or employees with barriers to compliance with the clean desk policy.
(4) Investigating possible violations of the clean desk policy, and initiating corrective action and/or referring to appropriate official/supervisor for corrective action.

(5) Timely reporting of all actual and/or suspected breaches of privacy to the tracking system as designated by the VA Privacy Service.

c. The ISO is responsible for implementing security controls to ensure the confidentiality, availability, and integrity of our three major information systems (VISTA, LAN, and PBX).

(1) Application and monitoring of the clean desk policy as it relates to information security.

(2) Assistance to supervisory staff and/or employees with barriers to compliance with the clean desk policy.

(3) Investigating possible information security related violations of the clean desk policy, and initiating corrective action and/or referring to appropriate official/supervisor for corrective action.

(4) Timely reporting of all actual and/or suspected breaches of information security to the tracking system as designated by the VA Security Operations Center (SOC).

d. Service Chiefs and supervisors are responsible for:

(1) Assuring employee education regarding the clean desk policy;

(2) Assisting employees with barriers in implementing the clean desk policy;

(3) Monitoring areas under their supervision for compliance with the clean desk policy; and,

(4) Reporting actual and/or suspected breaches of privacy to the Privacy Act Officer and/or ISO, as appropriate.

e. All employees are responsible for:

(1) Protecting the confidentiality of sensitive information utilized in their daily activities, by complying with all Federal laws and regulations, VA regulations and policies, and VHA policies relating to privacy;

(2) Compliance with the clean desk policy and/or identifying specific barriers to compliance;

(3) Informing the supervisor, Privacy Officer, and/or ISO; as appropriate; of barriers to compliance with the clean desk policy; and,

(4) Reporting all possible breaches of privacy to the employee’s supervisor or appropriate privacy official in a timely manner.

(5) The security of not only the data utilized in their daily activities, but also all data to which employee has access.
6. REFERENCES.

   a. VHA Handbook 1605.1, Privacy and Release of Information.
   b. VHA Handbook 1907.01, Health Information Management and Health Records.
   c. VHA Directive 1605, VHA Privacy Program.
   d. VA Directive 6502, Privacy Program.
   e. VA Handbook 6500, Information Security Program.
   f. VA IT Directive 06-2, Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations.
   g. 00-12, Disposal of Sensitive Printed Material.
   h. HIPAA, 45 CFR, Part 160 and 164.
   i. 5 U.S.C. 552a, 38 CFR, Sections 1.575-1.584
   j. 38 U.S.C. 5705, 38 CFR 17.500-17.511

7. RESCISSIONS. None.


9. FOLLOW-UP RESPONSIBILITY. Privacy Officer.