VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR INCLUSION INTO CONTRACTS

1. GENERAL

Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A contractor/subcontrator shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

3. VA INFORMATION CUSTODIAL LANGUAGE

a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. If VA determines that the contractor has violated any of the information confidentiality, privacy, security, and other provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

4. SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any

unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

5. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. The contractor/subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

(1) Nature of the event (loss, theft, unauthorized access);

(2) Description of the event, including:

(a) date of occurrence;

(b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

(3) Number of individuals affected or potentially affected;

(4) Names of individuals or groups affected or potentially affected;

(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

(6) Amount of time the data has been out of VA control;

(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

(8) Known misuses of data containing sensitive personal information, if any;

(9) Assessment of the potential harm to the affected individuals;

(10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

(11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of $__37.50__ per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

(1) Notification;

(2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

(3) Data breach analysis;

(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

(5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

6. TRAINING

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

(1) Successfully complete the appropriate VA privacy training and annually complete required privacy training (See below training); and

(2) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

b. The contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

7. ADDITIONAL REQUIREMENTS

a. The COR is responsible for coordinating with the Police prior to contractor arrival to identify the names of contractor personnel so that Police can ensure sufficient number of contractor badges are available for issuance prior to beginning work. COR is also responsible for signing out and signing in temporary contractor badges.

b. The COR is also responsible for maintaining copies of signed Privacy training for all contractors according to RCS 10-1.

c. Any work performed outside of official VA business hours after hours will require escorts.

d. Escort duties for un-cleared contractors are strictly limited to government officials, specifically VA employees. At no time are contractors allowed to escort other contractors.

VA Privacy Training for Personnel without Access to VA Computer Systems or Direct Access or Use to VA Sensitive Information

The Department of Veterans Affairs, VA must comply with all applicable privacy and confidentiality statutes and regulations. One of the requirements in VA is to have all personnel trained annually on privacy requirements. "Privacy" represents what must be protected by VA in the collection, use, and disclosure of personal information whether the medium is electronic, paper or verbal.

This document satisfies the "basic" privacy training requirement for a contractor, volunteer, or other personnel **only if** the individual does not use or have access to any VA computer system such as Time and Attendance, PAID, CPRS, VistA Web, VA sensitive information or protected health information (PHI), whether paper or electronic. You will find this training outlines your roles and responsibility for protecting VA sensitive information (medical, financial, or educational) that you may incidentally or accidentally see or overhear.

If you have direct access to protected health information or access to a VA computer system where there is protected health information such as CPRS, VistA Web, you must take "Privacy and HIPAA Focused Training" (TMS 10203). "VA Privacy and Information Security Awareness and Rules of Behavior" (TMS 10176) is always required in order to use or gain access to a VA computer systems or VA sensitive information, whether or not protected health information is included. Both trainings are located within the VA Talent Management System (TMS): https://www.tms.va.gov

What is VA Sensitive Information/Data?
All Department information and/or 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 not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

What is Protected Health Information?
The HIPAA Privacy Rule defines protected health information as Individually Identifiable Health Information transmitted or maintained in any form or medium by a covered entity, such as VHA.

What is an "Incidental" Disclosure?
An incidental disclosure is one where an individual's information may be disclosed incidentally even though appropriate safeguards are in place. Due to the nature of VA communications and practices, as well as the various environments in which Veterans receive healthcare or other services from VA, the potential exists for a Veteran's protected health information or VA sensitive information to be disclosed incidentally.

For example:

- You overhear a healthcare provider's conversation with another provider or patient even when the conversation is taken place appropriately.
- You may see limited Veteran information on sign-in sheets or white boards within a treating area of the facility.
- Hearing a Veteran's name being called out for an appointment or when the Veteran is being transported/escorted to and from an appointment.

Safeguards You Must Follow To Secure VA Sensitive Information:

- Secure any VA sensitive information found in unsecured public areas (parking lot, trash can, or vacated area) until information can be given to your supervisor or Privacy Officer. You must report such incidents to your Privacy Officer timely.
- Don't take VA sensitive information off facilities grounds without VA permission unless the VA information is general public information, i.e., brochures/pamphlets.
- Don't take pictures using a personal camera without the permission from the Medical Center Director.
- Any protected health information overheard or seen in VA should not be discussed or shared with anyone who does not have a need to know the information in the performance of their official job duties, this includes spouses, employers or colleagues.
- Do not share VA access cards, keys, or codes to enter the facility.
- Immediately report lost or stolen Personal Identity Verification (PIV) or Veteran Health Identification Cards (VHIC), any VA keys or keypad lock codes to your supervisor or VA police.
- Do not use a VA computer using another VA employee's access and password.
- Do not ask another VA employee to access your own protected health information. You must request this information in writing from the Release of Information section at your facility.

What are the Six Privacy Laws and Statutes Governing VA?

1. Freedom of Information Act (FOIA) compels disclosure of reasonably described VA records or a reasonably segregated portion of the records to any person upon written request unless one or more of the nine exemptions apply.
2. Privacy Act of 1974 provides for the confidentiality of personal information about a living individual who is a United States citizen or an alien lawfully admitted to U.S. and whose information is retrieved by the individual's name or other unique identifier, e.g. Social Security Number.
3. Health Insurance Portability and Accountability Act (HIPAA) provides for the improvement of the efficiency and effectiveness of health care systems by encouraging the development of health information systems through the establishment of standards and requirements for the electronic transmission, privacy, and security of certain health information.
4. 38 U.S.C. 5701 provides for the confidentiality of all VA patient and claimant information, with special protection for their names and home addresses.
5. 38 U.S.C. 7332 provides for the confidentiality of drug abuse, alcoholism and alcohol abuse, infection with the human immunodeficiency virus (HIV) and sickle cell anemia medical records and health information.

6. 38 U.S.C. 5705 provides for the confidentiality of designated medical-quality assurance documents.

What are the Privacy Rules Concerning Use and Disclosure?
You are not authorized to use or disclose protected health information. In general, VHA personnel may only use information for purposes of treatment, payment or healthcare operations when they have a need-to-know in the course of their official job duties. VHA may only disclose protected health information upon written request by the individual who is the subject of the information or as authorized by law.

How is Privacy Enforced?
There are both civil and criminal penalties, including monetary penalties that may be imposed if a privacy violation has taken place. Any willful negligent or intentional violation of an individual's privacy by VA personnel, contract staff, volunteers, or others may result in such corrective action as deemed appropriate by VA including the potential loss of employment, contract, or volunteer status.

Know your VA/VHA Privacy Officer and Information Security Officer. These are the individuals to whom you can report any potential violation of protected health information or VA sensitive information, or any other concerns regarding privacy of VA sensitive information.

YOU ARE RESPONSIBLE FOR PROTECTING THE CONFIDENTIAL INFORMATION OF OUR VETERANS

_____ _____
Employee (Print Name) Date

_____
Employee Signature

_____
Print Name of Contract Agency, if contractor

_____
Print Name of VHA Department/Supervisor/Local COR

PROVIDE A COPY OF THIS FORM TO YOUR SUPERVISOR/LOCAL COR
FOR DATA ENTRY INTO TALENT MANAGEMENT SYSTEM