

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE
FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE
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.

ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

A contractor/subcontractor 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.

All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

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

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).

VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and

policies in this contract.

The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

If VA determines that the contractor has violated any of the information confidentiality, privacy, and security 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.

If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

I. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

The contractor/subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COTR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

VA prohibits the installation and use of personally-owned or contractor/subcontractor-owned equipment or software on VA's network. If non-VA

owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches.

Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the Contractor at the end of lease, for trade-in, or other purposes. The options are: Contractor must accept the system without the drive;

VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

The equipment Contractor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the purchase order or contract.

(c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

6. SECURITY INCIDENT INVESTIGATION

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.

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.

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.

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.

7. LIQUIDATED DAMAGES FOR DATA BREACH

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.

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:
 - date of occurrence;
 - 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 affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

Notification;

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

Data breach analysis;

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

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

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

SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

Contractor Rules of Behavior

Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall sign on an annual basis an acknowledgement that they have read, understand, and agree to abide by VA's Contractor Rules of Behavior which is included in the training outlined in paragraph (Training). If the

contractor anticipates that the services under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the Contractor's designated representative. By signing the Rules of Behavior on behalf of the Contractor, the designated representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing VA's information and information systems. [A copy of the signed rules of behavior must be submitted before work begins \(within 5 business days of contract award\).](#)

TRAINING

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:

Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;

Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;

Successfully complete *VHA Privacy Policy Training* if Contractor will have access to PHI;

Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

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

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

Failure to complete the mandatory annual training and sign the Rules of Behavior annually, 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.

VA training site is located at www.tms.va.gov

There is only one course the contractor needs to complete and print the certificate at the end. A copy of the completed certificate must be submitted before work begins (within 5 business days of contract award).

+++++

[Instructions to get to the Courses in TMS](#)

www.tms.va.gov

Log onto the site and create a new user account; if you already don't have one. Search for your course entitled [VA Privacy and Information Security Awareness and Rules of Behavior. Complete course, print certificate \(s\), and sign/print contractor rules of behavior.](#)

VA Learning University (VALU)

Help Desk: 1-866-496-0463

valmshelp@va.gov

+++++

[Examples](#)



VA Privacy and Information Security Awareness and Rules of Behavior



CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

The following security requirement must be addressed regarding Contractor supplied equipment: Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COTR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

All contractor employees who require access to the Department of Veterans Affairs' computer systems shall be the subject of a background investigation and must receive a favorable adjudication from the VA Security and Investigations Center (07C). The level of background security investigation will be in accordance with VA Directive 0710 dated September 10, 2004 and is available at: <http://www.va.gov/pubs/asp/edsdirec.asp> (VA Handbook 0710, Appendix A, Tables 1 - 3). Appropriate Background Investigation (BI) forms will be provided upon contract (or task order) award, and are to be completed and returned to the VA Security and Investigations Center (07C) within 30 days for processing. Contractors will be notified by 07C when the BI has been completed and adjudicated. These requirements are applicable to all subcontractor personnel requiring the same access. If the security clearance investigation is not completed prior to the start date of the contract, the employee may work on the contract while the security clearance is being processed, but the contractor will be responsible for the actions of those individuals they provide to perform work for the VA. In the event that damage arises from work performed by contractor personnel, under the auspices of the contract, the contractor will be responsible for resources necessary to remedy the incident.

The investigative history for contractor personnel working under this contract must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO).

Should the contractor use a Contractor other than OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

Background Investigation

Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is:

- X ☐ Low/NACI
☐ Moderate/MBI
☐ High/BI

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, ""Personnel Security Suitability Program,"" Appendix A)
Low	National Agency Check with Written Inquiries (NACI) A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.

The position sensitivity impact for this effort has been designated as [Low] Risk and the level of background investigation is [NACI].

The contractor does not require a full background investigation security clearance.

2. Contractor Responsibilities

a. The contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by the Office of Personnel Management (OPM) through the VA, the contractor shall reimburse the VA within 30 days.

b. Background investigations from investigating agencies other than OPM are permitted if the agencies possess an OPM and Defense Security Service certification. The Contractor Cage Code number must be provided to the Security and Investigations Center (07C), which will verify the information and advise the contracting officer whether access to the computer systems can be authorized.

c. The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain a U.S. citizenship and are able to read, write, speak and understand the English language.

d. After contract award and prior to contract performance, the contractor shall provide the following information, using Attachment TBD_, to the CO:

(1) List of names of contractor personnel.

(2) Social Security Number of contractor personnel. (Do Not Send Electronically, Contact Contracting Officer for instructions)

(3) Home address of contractor personnel or the contractor's address.

e. The contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.

Failure to comply with the contractor personnel security requirements may result in termination of the contract for default.

g. Further, the contractor will be responsible for the actions of all individuals provided to work for the VA under this contract. In the event that damages arise from work performed by contractor provided personnel, under the auspices of this contract, the contractor will be responsible for all resources necessary to remedy the incident.

3. Government Responsibilities

a. The VA Security and Investigations Center (07C) will provide the necessary forms to the contractor or to the contractor's employees after receiving a list of names and addresses.

b. Upon receipt, the VA Security and Investigations Center (07C) will review the completed forms for accuracy and forward the forms to OPM to conduct the background investigation.

c. The VA facility will pay for investigations conducted by the OPM in advance. In these instances, the contractor will reimburse the VA facility within 30 days.

d. The VA Security and Investigations Center (07C) will notify the contracting officer and contractor after adjudicating the results of the background investigations received from OPM.

e. The contracting officer will ensure that the contractor provides evidence that investigations have been completed or are in the process of being requested.

CONFIDENTIALITY AND NONDISCLOSURE

It is agreed that:

1. The preliminary and final deliverables and all associated working papers, application source code, and other material deemed relevant by the VA which have been generated by the contractor in the performance of this task order are the exclusive property of the U.S. Government and shall be submitted to the CO at the conclusion of the task order.

The CO will be the sole authorized official to release verbally or in writing, any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this task order. No information shall be released by the contractor. Any request for information relating to this task order presented to the contractor shall be submitted to the CO for response.

Press releases, marketing material or any other printed or electronic documentation related to this project, shall not be publicized without the written approval of the CO.

Business Associate Agreement

a. The contractor is subject to the provisions of a Business Associate Agreement for use or disclosure of protected health information. The contractor must review, sign, and return Attachment A to the Contracting Officer within 5 business days of contract award.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH
ADMINISTRATION AND
<COMPANY/ORGANIZATION>

Whereas, <COMPANY/ORGANIZATION> (Business Associate) provides <BRIEFLY DEFINE SERVICES (i.e., medical device, transcription, publishing, etc.)> services to the Department of Veterans Affairs Veterans Health Administration (Covered Entity); and

Whereas, in order for Business Associate to provide <BRIEFLY DEFINE SERVICES (i.e., medical device, transcription, publishing, etc.)> services to Covered Entity, Covered Entity discloses to Business Associate Protected Health Information (PHI) and Electronic Protected Health Information (EPI) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996), and its implementing regulations, 45 C.F.R. Parts 160, 162, and 164 (“the HIPAA Privacy and Security Rules”); and

Whereas, the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009), pursuant to Title XIII of Division A and Title IV of Division B, called the Health Information Technology for Economic and Clinical Health (HITECH) Act, provides modifications to the HIPAA Privacy and Security Rules; and

Whereas, Department of Veterans Affairs Veterans Health Administration is a “Covered Entity” as that term is defined in the HIPAA implementing regulations, 45 C.F.R. § 160.103; and

Whereas, <COMPANY/ORGANIZATION>, including its employees, officers, contractors, subcontractors, or any other agents, as a recipient of PHI from Covered Entity in order to provide <BRIEFLY DEFINE SERVICES (i.e., medical device, transcription, publishing, etc.)> services to Covered Entity, is a “Business Associate” of Covered Entity as that term is defined in the HIPAA implementing regulations, 45 C.F.R. § 160.103; and

Whereas, pursuant to the Privacy and Security Rules, all Business Associates of Covered Entities must agree in writing to certain mandatory provisions regarding the Use and Disclosure of PHI; and

Whereas, the purpose of this Agreement is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the Business Associate Agreement requirements at 45 C.F.R. §§ 164.308(b), 164.314(a), 164.410, 164.502(e), and 164.504(e), as may be amended.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

Definitions. Unless otherwise provided in this Agreement, capitalized terms and phrases that are defined in the Privacy and Security Rules have the same meanings as set forth in the Privacy and Security Rules. When the phrase “Protected Health Information” and the abbreviation “PHI” are used in this Agreement, they include the phrase “Electronic Protected Health Information” and the abbreviation “EPI.”

2. Ownership of PHI. PHI provided by Covered Entity to Business Associate and its contractors, subcontractors, or other agents, or gathered by them on behalf of Covered Entity under this Agreement is the property of Covered Entity.
3. Scope of Use and Disclosure by Business Associate of Protected Health Information. Unless otherwise limited herein, Business Associate may:

- A. Make Uses and Disclosures of PHI that is disclosed to it by Covered Entity or received by Business Associate on behalf of Covered Entity as necessary to perform its obligations under this Agreement and all applicable agreements, provided that such Use or Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity and complies with Covered Entity's minimum necessary policies and procedures;
- B. Use the PHI received in its capacity as a Business Associate of Covered Entity for its proper management and administration and to fulfill any legal responsibilities of Business Associate;
- C. Make a Disclosure of the PHI in its possession to a third party for the proper management and administration of Business Associate or to fulfill any legal responsibilities of Business Associate; provided, however, that the Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity, or is Required by Law; and Business Associate has received from the third party written assurances that (a) the information will be held confidentially and used or further disclosed only for the purposes for which it was disclosed to the third party or as Required By Law, (b) the third party will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the information may have been breached, and (c) the third party has agreed to implement reasonable and appropriate steps to safeguard the information;
- D. Engage in Data Aggregation activities, consistent with the HIPAA Privacy Rule; and
- E. De-identify any and all PHI created or received by Business Associate under this Agreement, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule.

Obligations of Business Associate. In connection with its Use or Disclosure of PHI, Business Associate agrees that it will:

Consult with Covered Entity before making the Use or Disclosure whenever Business Associate is uncertain whether it may make a particular Use or Disclosure of PHI in performance of this Agreement;

Ensure any employee, officer, contractor, subcontractor, or other agent of Business Associate who has access to PHI receives at a minimum annual privacy and security awareness training that conforms to the requirements of Covered Entity;

Develop and document policies and procedures and use reasonable and appropriate safeguards to prevent use or disclosure of PHI other than as provided by this Agreement;

D. To the extent practicable, mitigate any harmful effect of a Use or Disclosure of PHI by Business Associate in violation of this Agreement that is known or, by exercising reasonable diligence, should have been known to Business Associate;

E. Maintain a system or process to account for any Security Incident, Privacy Incident, or Use or Disclosure of PHI not authorized by this Agreement of which Business Associate becomes aware;

Notify Covered Entity within 24 hours of Business Associate's discovery of any incident which may potentially be a data breach, including a HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI, whether secured (PHI which has been destroyed or in the alternative has been rendered unreadable, unusable, or undecipherable through methodology specified by the Department of Health and Human Services in guidance issued under § 13402(h)(2) of the HITECH Act) or unsecured (PHI not secured through the use of a technology which renders it unusable, unreadable, or indecipherable through such methodology), not provided for by this Agreement and promptly provide a report to Covered Entity within ten (10) business days of the notification;

(1) An incident is any physical, technical, or personal activity or event that, a reasonable person believes, increases risk of inappropriate or unauthorized use or disclosure of PHI or causes Covered Entity to be considered non-compliant with the HIPAA Privacy and Security Rules;

(2) A breach, as defined in 45 C.F.R. § 164.402, is an unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the individual;

(3) A breach, consistent with 45 C.F.R. § 164.410(a)(2), will be treated as discovered as of the first day on which such breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate, or any employee, officer, contractor, subcontractor, or other agent of Business Associate;

(4) Notification will be made by Business Associate to the Director, Health Information Governance, by email at VHABAAIssues@va.gov of any HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this Agreement; and

(5) A written report of the incident, submitted to the Director, Health Information Governance, within ten (10) business days after initial notification, will document the following:

(a). The identification of each individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the breach;

(b). A brief description of what occurred, including the date of the breach and the date of the discovery of the breach (if known);

(c). A description of the types of secured and/or unsecured PHI that was involved;

(d). A description of what is being done to investigate the breach, to mitigate further harm to individuals, and the reasonable and appropriate safeguards being taken to protect against future breaches; and

(e). Any other information described in 45 C.F.R. § 164.404(c);

(6) This report should be documented as a letter and sent to:

Director, Health Information Governance
Department of Veterans Affairs – Veterans Health Administration
Office of Informatics and Analytics (10P)
810 Vermont Avenue NW
Washington, DC 20420

Implement administrative, physical, and technical safeguards and controls for the PHI that Business Associate receives, maintains, or transmits on behalf of Covered Entity, including policies, procedures, training, and sanctions, in compliance with Federal Information Security Management Act (FISMA), Pub. L. No. 107-347, 116 Stat. 2946 (2002); the HIPAA Privacy and Security Rules, 45 C.F.R. Parts 160, 162, and 164; standards and guidance from the Office of Management and Budget and the National Institute of Standards and Technology; Federal Records Act requirements, National Archives and Records Administration regulations, to include applicable records retention schedules, and other laws, regulations, and policies pertaining to safeguarding VA Sensitive Data;

Require contractors, subcontractors, or other agents to whom Business Associate provides PHI received from Covered Entity to agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement, including implementation of administrative, physical, and technical safeguards and controls, including policies, procedures, training, and sanctions, in compliance with the above-referenced legal authorities;

Obtain satisfactory written assurances from contractors, subcontractors, or other agents to whom Business Associate provides PHI received from Covered Entity that the contractors, subcontractors, or other agents agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement;

J. If Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within ten (10) business days of receiving a written request from Covered Entity:

(1) Make available PHI in the Designated Record Set or System of Records necessary for Covered Entity to respond to individuals' requests for access to PHI about them that is not in the possession of Covered Entity;

(2) Incorporate any amendments or corrections to the PHI in the Designated Record Set or System of Records in accordance with the Privacy Act and the HIPAA Privacy Rule; and

(3) Maintain the information necessary to document the disclosures of PHI sufficient to make an accounting of those disclosures as required under the Privacy Act, 5 U.S.C. § 552a, and the HIPAA Privacy Rule, and within ten (10) business days of receiving a request from Covered Entity, make available the information necessary for Covered Entity to make an accounting of Disclosures of PHI about an individual in the Designated Record Set or System of Records;

Utilize only contractors, subcontractors, or other agents who are physically located within a jurisdiction subject to the laws of the United States and ensure that no contractor, subcontractor, or agent maintains, processes, uses, or discloses PHI received from Covered Entity in any way that will remove the PHI from such jurisdiction. Any modification to this provision must be approved by Covered Entity in advance and in writing;

L. Provide satisfactory assurances that the confidentiality, integrity, and availability of the PHI provided by Covered Entity under this Agreement are reasonably and appropriately protected;

M. Upon completion or termination of the applicable contract(s) or agreement(s), return and/or destroy, at Covered Entity's option, the PHI gathered, created, received, or processed during the performance of the contract(s) or agreement(s). No data will be retained by Business Associate, or contractor, subcontractor, or other agent of Business Associate, unless retention is required by law and specifically permitted by Covered Entity. As deemed appropriate by and under the direction of Covered Entity, Business Associate shall provide written assurance that all PHI has been returned to Covered Entity or destroyed by Business Associate. If immediate return or destruction of all data is not possible, Business Associate shall notify Covered Entity and assure that all PHI retained will be safeguarded to prevent unauthorized Uses or Disclosures;

N. Be liable to Covered Entity for any civil or criminal penalties imposed on Covered Entity under the HIPAA Privacy and Security Rules in the event of a violation of the Rules as a result of any practice, behavior, or conduct by Business Associate;

O. Make available to Covered Entity its practices, policies and procedures, for the purpose of determining compliance with this Agreement and underlying agreements; and

P. Make available to the Secretary of Health and Human Services Business Associate's internal practices, books, and records, including policies and procedures, relating to the Use or Disclosure of PHI for purposes of determining Covered Entity's compliance with the Privacy and Security Rules, subject to any applicable legal privileges.

5. Obligations of Covered Entity. Covered Entity agrees that it:

Has obtained or will obtain from Individuals any consents, authorizations, and other permissions necessary or required by laws applicable to Covered Entity for Business Associate and Covered Entity to fulfill their obligations under this Agreement;

Will promptly notify Business Associate in writing of any restrictions on the Use and Disclosure of PHI about Individuals that Covered Entity has agreed to that may affect Business Associate's ability to perform its obligations under this Agreement; and

Will promptly notify Business Associate in writing of any change in, or revocation of, permission by an Individual to use or disclose PHI, if such change or revocation may affect Business Associate's ability to perform its obligations under this Agreement;

6. Material Breach and Termination.

A. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

Provide an opportunity for Business Associate to cure the breach or end the violation;

Terminate this Agreement and underlying contract(s) if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or

(3) Immediately terminate this Agreement and underlying contract(s) if cure is not possible; or

(4) If Business Associate has breached a material term of this Agreement and neither termination nor cure is feasible, report the violation to the Secretary of Health and Human Services.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity, if appropriate, upon review as defined in Section 12 of this Agreement.

C. Automatic Termination. This Agreement will automatically terminate upon completion of the Business Associate's duties under all underlying agreements or by mutual written agreement to terminate underlying agreements.

D. Effect of Termination. Termination of this Agreement will result in cessation of activities by Business Associate involving PHI under this Agreement.

7. Amendment. Business Associate and Covered Entity agree to take such action as is necessary to amend this Agreement for Covered Entity to comply with the requirements of the Privacy and Security Rules or other applicable law.

8. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

9. Other Applicable Law. This Agreement does not and is not intended to abrogate any responsibilities of the parties under any other applicable law.

10. Effect of Agreement. With respect solely to the subject matter herein, the terms and conditions in a National Business Associate Agreement, executed by the Director, Health Information Governance, or a designated representative, will supersede any local business associate agreement between Business Associate and a component of VHA. The parties also agree that a National Business Associate Agreement, unless itself modified by the parties, will control and cannot be superseded, modified, or nullified by any local business associate agreement.

11. Effective Date. This Agreement shall be effective on the last signature date below.

12. Review Date. The provisions of this Agreement will be reviewed by Covered Entity every two years from Effective Date to determine the applicability of the agreement based on the relationship of the parties at the time of review.

By:	By:	
Name:	Name:	
Title:	Title:	
Date:	Date:	