PUBLICATION

U.S. Department of Veterans Affairs Overhauls Cybersecurity Rules for Government Contractors

Authors: Alisa L. Chestler
February 16, 2023

On January 25, the Department of Veterans Affairs (VA) published a new final rule amending contractual provisions in the VA Acquisition Regulation (VAAR) to address data privacy, protection, and cybersecurity. The aim of the new provisions is to regulate the acquisition of information technology (IT), provide guidelines for handling health information and other VA-sensitive information, and establish a contractual obligation for adherence to the VA Cybersecurity Program.

The new provisions will be mandatory for inclusion in all VA contracts and subcontracts awarded or renewed after February 24, 2023. For contractors and subcontractors with active contracts with the VA, the current contractual requirements will remain in force until the existing contract is either renewed or terminated. VA contractors must begin to put a plan together to comply with the new regulations and understand how the changes will affect operations.

The new VAAR provisions implement requirements adopted from the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and create new categories of VA data requiring protection due to the risk of harm that would result from an exposure. The new categories include personnel information, confidential commercial information, attorney work product, and protected health information (PHI). The adoption and implementation of these provisions expands the scope of who falls under the VA's contractual ambit.

Basic Safeguarding of Covered Contractor Information Systems

The VA is adding a new subpart 804.19 to the VAAR: "Basic Safeguarding of Covered Contractor Systems." This is applicable to any contractor, subcontractor, or business associate system that may contain VA information or VA-sensitive information. Due to the broad definition of "VA-sensitive information," and with "VA information" remaining undefined– the policies outlined in this section are likely to affect any contractor, subcontractor, or business associate that transmits or otherwise handles information in performance of a VA contract or subcontract.

Requirements include:

1. Compliance with VA privacy and confidentiality laws, VA and Veterans Health Administration (VHA) regulations, HIPAA, and the Privacy Act of 1974
2. Annual VA security awareness training
3. Annual VHA Privacy and HIPAA training if accessing PHI
4. Report actual or suspected security and privacy incidents to contracting officer or contracting officer's representative (COR) within **one hour** of discovery or suspicion
5. Compliance with VA personnel security and suitability program requirements for background screening
6. Compliance with contracting officer or COR direction in the event of an incident
7. All employees with access to VA information or VA sensitive information to sign an acknowledgment they have read, understand, and agree to abide by the VA National Rules of Behavior
8. Maintenance of records and compliance reports regarding HIPAA Security and Privacy Rules

9. Contractors and subcontractors flowing down all requirements in subcontracts and business associate agreements (BAAs)

Liquidated Damages

The VA is also adding Subpart 811.5 to prescribe policies for incorporating a liquidated damages clause in contracts involving VA-sensitive personal information—whether with the VA or issued by another agency. In the event of a data breach involving sensitive personal information maintained, processed, or used by contractors or any subcontractors, the contractor is required to pay liquidated damages to the VA. The funds from liquidated damages will be used by the VA to provide credit protection services to affected individuals. These damages apply regardless of whether the contractor or subcontractor was negligent in handling information or in the security of its network.

Importantly, the liquidation clause does not apply to *all* VA information; rather, only to "VA-sensitive personal information." This term, as used in this sub-part, is undefined. However, because liquidated damages will be used to provide credit protection services to those affected, these probably will only apply where there is a breach of VA data whose exposure could risk causing harm to individuals. Importantly, this is a distinct category of data that is narrower in scope than the new category of VA-sensitive information, which includes contractual information, legal documents, and other information that does not directly pertain to individuals.

Contractors are also required to flow down the liquidated damages clause described above when the subcontractor is required to enter into a BAA with VHA.

Gray Market and Counterfeit Items

Gray market items are "original equipment manufacturer goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory." Counterfeit items are those that are not manufactured by the original manufacturer but intended to be fraudulently substituted for the same purpose. Gray market and counterfeit items are prohibited under VA contracts. In solicitations for commercial products or services, the VA may deem "refurbished" items as either acceptable or unacceptable in the contract.

Protection of Privacy

A VA contractor with access to PHI is currently required to enter a BAA. For all downstream BAAs with subcontractors, contractors will be required to flow down the liquidated damages clause described above when the contractor is required to enter a BAA with VHA.

Acquisition of Information Technology

In contracts for IT hardware, software, and services, contractors are required to protect VA information, information systems, and IT by complying with the VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series. This requirement applies to contractors and subcontractors for IT products and services in which VA-sensitive information or sensitive personal information is handled.

To satisfy the cybersecurity requirements of the VAAR, in addition to compliance with VA Directives, contractors, subcontractors, and third-party servicers or associates providing support are required to "employ adequate security controls" and use common security configurations available from the National Institute of Standards and Technology's (NIST) website.

Finally, for IT or IT-related supplies and services, a contractor is required to submit a VA Section 508 Checklist in its response to the solicitation.

Part 852—Solicitation Provisions and Contract Clauses

Effective February 24, 2023, the VA will include the following clauses in contracts and renewed contracts to implement the policies and provisions detailed above. Importantly, the following are material terms of the contract. If the VA determines that a contactor violates any of the VA's confidentiality, privacy, or security provisions, the VA may withhold payments or terminate the contract at the government's discretion.

Information and Information Systems Security

VA contractors will see this clause where FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems" is required to be included in the contract. Contractors are required to flow down this clause to subcontractors that are covered by the following requirements.

Incident Reporting Requirement

Although objections were raised when the proposed rule was issued in late 2021, contractors, subcontractors, third-party affiliates, and business associates are required to notify the contracting officer or COR within **one hour** of an identified or suspected security or privacy incident. Each contract will stipulate the timeline for remediating the vulnerability, but the VA requires that timeline to be within 60 days of discovery or disclosure. For breaches involving suspected criminal activity, affected entities are required to simultaneously notify both the VA and law enforcement, including the VA Office of Inspector General and VA Office of Security and Law Enforcement.

Security Controls

This clause applies to "contractors, subcontractors, their employees, third parties, and business associates with access to VA information, information systems, or IT or providing and accessing IT-related goods and services[.]" Under this clause, those entities are required to adhere to the comprehensive security controls detailed in VA Directive 6500, the VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series.

Encryption, Firewalls, and Security

Contractors and subcontractors are required to store or transmit VA sensitive information using encryption tools validated under FIPS 140-3. All firewall and web service security controls must meet the VA's minimum requirements as outlined in the VA Configuration Guidelines.

Personnel

Applicable entities and their employees who work with VA information are subject to the same background investigations as VA appointees or employees with access to the same types of information, as determined by VA Directive and Handbook 0710.

Personnel Training

All personnel with access to VA information or information systems must complete annual privacy, information security, and rules of behavior training and sign an acknowledgment of understanding the responsibilities of compliance with the VA Information Security Rules of Behavior for Organizational Users.

Employee Reassignment or Termination

Contractors and subcontractors are required to notify the VA within **four hours** of when an employee working on a VA information system or with access to VA information is reassigned or leaves the contractor or subcontractor. When such an employee is terminated, the contracting officer or COR must be notified **immediately**.

Domestic Development and Operations

To the maximum extent practicable, software development and outsourced operations must be located in the United States. If the contractor intends to conduct development or operations outside the U.S., the contractor is required to state in its proposal the location(s) of the development or operations and include a detailed IT Security Plan that addresses mitigations for communication, control, and data protection issues.

Permissible Use of Data

Any information the VA makes available to a contractor or subcontractor under a contract is only authorized to be used for the stated contract purpose. Any other use requires prior written approval by the VA.

On-site Inspections

The VA reserves the right to conduct both scheduled and unscheduled on-side inspections, assessments, or audits of contractor and subcontractor IT resources, information systems, and assets to ensure compliance with federal and VA requirements. Contractors and subcontractors are required to provide all necessary access during such inspections.

Co-mingling of Data

Contractors and subcontractors are prohibited from co-mingling VA information with any other data in the contractor's information systems or media storage devices.

Data Retention, Destruction, and Contractor Self-certification

Contractors and subcontractors are responsible to collecting and destroying VA data or materials to the point that it is no longer readable or able to be reconstructed in any way. Unless explicitly authorized, making copies of VA information is prohibited. Prior to termination or completion of the contract, contractors and subcontractors must provide the contracting officer or COR a plan for destruction of all VA data in accordance with VA Handbook 6500, the VA Cybersecurity Program, and NIST Special Publication 800-88 for the purposes of wiping all IT devices. **Within 30 days** after termination or completion of the contract, contractors and subcontractors must certify to the contracting officer or COR in writing that all data has been properly destroyed.

Return of VA Data and Information

When no longer needed either during performance or upon completion or termination of the contract, VA Information must be returned to the VA or maintained by the contractor or subcontractor until otherwise directed. If the contractor is required to store or electronically transmit VA-sensitive information, it must do so using encryption tools provided by the VA.

Use of VA Data and Information

Contractors and subcontractors may only use VA data and information in ways stipulated in the contract. If relevant privacy laws or security standards change during the period of performance, the VA and contractors agree to negotiate in good faith to implement updates as required.

Disclosure of VA Data and Information

Contractors and subcontractors may only disclose VA data and information either in response to a court order or with VA's prior written approval. Upon receipt of any court order, contractors must immediately refer the court order to the contracting officer or COR for response. All disclosures must be documented and maintained. Upon request of the contracting officer or COR, contractors must provide a full accounting of disclosures **within 15 calendar days**.

Compliance with Privacy Statutes and Regulations

Notwithstanding the disclosure requirements above, contractors and subcontractors are prohibited from disclosing VA information protected by VA privacy statutes, applicable regulations, or HIPAA. If disclosure of such information is pursuant to a court order, the contractor is required to immediately refer the request to the contracting officer or COR for response.

Liquidated Damages

Contractors and subcontractors that require access to sensitive personal information are required to **immediately** notify the contracting officer or COR of any security incident involving sensitive personal information. After such an incident, the contractor or subcontractor is required to pay liquidated damages per affected individual in an amount specified by the contracting officer and included in the contract. The contractor may elect to pay actual damages in an amount approved by the contracting officer for identity protection services in lieu of the stipulated liquidated damages. Should the VA elect to terminate the contract as a result of such a breach, the contractor may also be liable for costs for the repurchase of goods or services.

Gray Market and Counterfeit Items

Contractors and subcontractors are prohibited from supplying gray market and counterfeit equipment or parts to the VA. All vendors are required to be either an original equipment manufacturer (OEM) or an authorized dealer, distributor, or reseller that is verified by an authorization letter from the OEM. In addition, all associated software and services must be in accordance with the OEM terms and conditions. However, contractors may provide the VA with used, refurbished, or remanufactured parts where the vendor is an OEM or authorized dealer, distributor, or reseller for the purpose of the equipment or service in question.

Security Requirements for IT Resources

Regardless of location, contractors are responsible for securing all of their systems that connect to a VA network or operated for the VA.

Within **90 days** of a VA contract being awarded, the contractor is required to submit to the contracting officer an Information System Security Plan that provides an overview of the security controls in place and the procedures the contractor will follow to ensure security of VA information and systems. Contractors must also submit to the contracting officer written proof of system security accreditation for all non-VA owned systems, as well as a risk assessment, security test and evaluation, disaster recovery plan, and continuity of operations plan.

Contractors are required to annually verify to the contracting officer, in writing, that their Information System Security Plans remain valid.

Information System Design and Development

Where a contractor designs or develops and information system for or on behalf of the VA at a non-VA facility, the contractor must comply with Federal Information Security Modernization Act (FISMA), HIPAA regulations, NIST, and other VA security and privacy control requirements for federal information systems. For procured systems and technologies, the contractor is responsible for ensuring that no upgrades and security fixes negatively affect VA systems.

Information System Hosting, Operation, Maintenance, or Use

Contractors that host, operate, maintain, or use IT systems on behalf of the VA are responsible for ensuring those systems comply with HIPAA Privacy and Security Rules, the Privacy Act, VA regulations, FISMA, NIST, FIPS, the Federal Risk and Authorization Management Program (FedRAMP), and VA security and privacy directives and handbooks. This includes "risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system." Contractors are also required to provide and gain approval of a privacy impact assessment prior to approval to operate.

A contractors also must conduct an annual FISMA security controls assessment and an annual self-assessment on all systems and outsourced services required under the contract.

Security Controls Compliance Testing

With 10 working days' notice, contractors are required to fully cooperate with and assist the VA in evaluating the security controls at any location and on any information system where VA information is processed or stored. In the event of a security incident or at any other time as determined by the VA, the government may conduct unannounced security control assessments.

Information and Communication Technology Accessibility Notice

Contractors providing information and communication technology systems or supplies to the VA must self-evaluate and submit the appropriate VA Section 508 checklists for technology accessibility in accordance with the Rehabilitation Act of 1973.

Summary

The new VA contractual clauses levy significant requirements on contractors and subcontractors for data privacy, protection, and cybersecurity. Notably, the VA has expanded the scope of the types of data that contractors are required to safeguard, including VA-sensitive information, sensitive personal information, and protected health information, and imposed stringent reporting timelines for cybersecurity incidents.

In some cases, contractors may have to significantly overhaul their current practices. VA contractors and subcontractors should not wait until a current contract expires to come into compliance. To avoid being in breach of contract with the VA, contractors and subcontractors should carefully review their contractual obligations to implement new policies and procedures under these new clauses. The VA will begin enforcing these contractual provisions for contracts entered or renewed after February 24, 2023.

For assistance in bringing your business into compliance or any questions about the new VA cybersecurity policies, please contact Alisa L. Chestler, CIPP/US, or any member of the Baker Donelson Data Protection, Privacy and Cybersecurity Team.