United States Government Accountability Office

Report to the Ranking Member, Committee on Veterans' Affairs, House of Representatives

May 2026

# PRIVACY AND CYBERSECURITY

# VA Has Made Progress Enhancing Security Controls for Protected Health Information


GAO-26-108651

GAO Highlights

PRIVACY AND CYBERSECURITY

# VA Has Made Progress Enhancing Security Controls for Protected Health Information

GAO-26-108651 May 2026

A report to the Ranking Member of the Committee on Veterans' Affairs, House of Representatives

For more information, contact Jennifer R. Franks at FranksJ@gao.gov.

## What GAO Found

The Veterans Health Administration (VHA) uses the services of external entities, known as business associates, to act on behalf of health care providers or other business associates to create, receive, maintain, or transmit protected health information (PHI). Veterans Affairs (VA) has implemented PHI sharing agreements with these entities to ensure they address requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. GAO reviewed 73 randomly selected sharing agreements and found that 100 percent of them included all 12 HIPAA Privacy Rule requirements for use and disclosure of PHI. Further, VHA documented responsibilities for conducting performance audits to confirm that external entities are protecting veterans' PHI.

VA took steps to secure the health information in a key system used by its Million Veteran Program (MVP), which is focused on examining how genetics, lifestyle, military experiences, and exposures affect health and wellness in veterans. However, deficiencies existed in certain cybersecurity controls related to asset and risk management; configuration management; identity and access management; and continuous monitoring and logging. As a result of these deficiencies, VA had reduced assurance of the confidentiality and integrity of sensitive health information in the MVP. In September 2025, GAO made 13 recommendations to VA to address these deficiencies.

Since September 2025, VA implemented nine of the 13 recommendations and partially implemented three others (see figure). GAO will continue to monitor VA's progress in implementing the remaining recommendations.

**Figure: VA Progress, as of March 2026, in Addressing 13 GAO Recommendations Made in September 2025**

| | Status of related recommendations | | |
|---|---|---|---|
| Security control area | Implemented | Partially implemented | Not implemented |
| Asset and risk management | 4 | 1 | – |
| Configuration management | 1 | 1 | – |
| Identity and access management | 3 | – | 1 |
| Continuous monitoring and logging | 1 | 1 | – |

Implemented - VA successfully completed actions to implement the recommendation.

Partially implemented - VA had made progress but had not completed implementation.

Not implemented - VA had not provided sufficient evidence that it had implemented the recommendation.

Source: Based on GAO analysis of Veterans Affairs (VA) data. | GAO-26-108651

## Why GAO Did This Study

Within VA, VHA oversees the delivery of health care services to millions of veterans. The amount of PHI used by VHA and shared with external entities highlights the importance of protecting the privacy of PHI.

Further, VA is responsible for the cybersecurity of veterans' sensitive health data, such as information in systems used to support its MVP. Since launching in 2011, about 1 million veterans have joined MVP, making it the nation's largest biorepository of veteran data.

GAO was asked to review VA's privacy and cybersecurity efforts. In September 2025, GAO issued a sensitive report with limited distribution on the extent to which VHA oversaw the privacy of veterans' health information shared with external entities, and the extent to which VA protected the confidentiality and integrity of veterans' health information in its MVP, among other things. In that report, GAO identified security control deficiencies in a system supporting MVP and made 13 recommendations to address them.

This report is a public version of the September 2025 report, with sensitive information removed. For this public report, GAO also determined the extent to which VA had taken corrective actions to address the previously identified security control deficiencies and the 13 related recommendations for improvement. GAO reviewed supporting documents and interviewed agency officials regarding VA's actions to address these recommendations.

# Contents



Figures

## Abbreviations

| | |
|---|---|
| BA | business associate |
| BAA | business associate agreement |
| DOD | Department of Defense |
| EHR | electronic health record |
| EHRM | Electronic Health Record Modernization |
| EHRM-IO | Electronic Health Record Modernization Integration Office |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act of 2014 |
| HHS | Department of Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| IAP | Office of Information Access and Privacy |
| IT | information technology |
| MVP | Million Veteran Program |
| NIST | National Institute of Standards and Technology |
| OCR | Office for Civil Rights |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PCA | Privacy Compliance and Accountability Office |
| PHI | protected health information |
| PII | personally identifiable information |
| POAM | plan of action and milestones |
| VA | Department of Veterans Affairs |
| VHA | Veterans Health Administration |

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 21, 2026

The Honorable Mark Takano
Ranking Member
Committee on Veterans' Affairs
House of Representatives

Dear Ranking Member Takano:

Federal agencies, including the Department of Veterans Affairs (VA), collect and process large amounts of personally identifiable information (PII) that are used for various government programs.[1] The PII collected by federal agencies, along with the increasing sophistication of IT, highlights the importance of strong programs for ensuring privacy protections. Such programs are especially critical when considering recent breaches involving PII that have affected millions of people.[2]

Among the key risks facing the nation's health IT systems are cybersecurity risks. Specifically, information systems supporting federal agencies and our nation's critical infrastructures are inherently at risk. These systems, including those of VA, are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks. Accordingly, since 1997, we have designated federal information security as a government-wide high-risk area. This area was expanded to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of PII in 2015. In addition, we

[1]In general, PII is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number, or that otherwise can be linked to an individual.

[2]A breach is an unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information.

designated VA health care as a high-risk area for the federal government in 2015, in part due to the department's IT challenges.[3]

Health data, such as those managed by VA's electronic health record (EHR) system and its EHR Modernization (EHRM) program, are essential to VA's ability to deliver health care services to about nine million veterans annually. In particular, the health care sector, including VA, uses a wide array of information systems and technologies across multiple settings, such as physician offices and hospitals. Further, the Veterans Health Administration (VHA) uses the services of external entities to help carry out its mission of providing veterans with healthcare. While the increasing use of health IT systems can improve health care quality, these systems are also vulnerable to the loss or unauthorized disclosure of patients' PII.

VA collects other sensitive information in support of its mission. For example, its Million Veteran Program (MVP) collects veteran participants' genomic data and health records for research to improve health care for veterans. VA uses information systems to host MVP's sensitive data and research environments. The cybersecurity of these systems and the data in them is imperative to the protection of veterans' health information.

You asked us to review VA's privacy and cybersecurity efforts. The objectives for the review were to determine the extent to which (1) VHA has developed and documented PII and Protected Health Information (PHI) policies in accordance with federal privacy guidance, (2) VHA oversees the privacy of veterans' health information shared with external entities, including those associated with its EHRM program, (3) VA protects the confidentiality and integrity of veterans' health information in selected systems for its MVP, and (4) VA has taken corrective actions to address identified control deficiencies and related recommendations.

[3]We highlighted VA's IT issues in our 2015 high-risk report and subsequent high-risk reports. See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015); *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017); *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019); *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021); *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023); and *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

To address the first objective, we reviewed VHA organization charts and privacy policies against selected privacy controls from National Institute of Standards and Technology (NIST) special publication (SP) 800-53 revision 5.[4] Specifically, we selected three controls due to their applicability to the sharing of PHI among VHA and external entities. Additionally, we also reviewed other documentation and interviewed cognizant VHA officials as necessary.

To address our second objective, we selected a random generalizable sample of 73 external entities (i.e., national business associates).[5] We excluded from our target population any business associates (BA) that were internal VA entities or other federal agencies, and associates that did not have electronic access to veterans' protected health information (PHI).[6] We identified 12 requirements from the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule for business associate agreements (BAA).[7] We then examined the agreements for each of the sampled BAs to determine whether they contained clauses that address these requirements. We also evaluated the BAAs between VHA and the EHRM Integration Office (EHRM-IO), as well as the BAA between EHRM-IO and the EHRM contractor, to determine if they included clauses that address the requirements. Additionally, we examined meeting minutes and interviewed agency officials to determine the plans VHA had for improving its approach for

[4]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, special publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

[5]A business associate is an entity that creates, receives, maintains, or transmits protected health information on behalf of a covered entity for a covered function or performs certain services to or for a covered entity that involve the use or disclosure of PHI. At VHA, business associates are classified as either local or national business associates. A local business associate agreement (BAA) is negotiated and executed between a single VA Health Care Facility and a single business associate. There are two types of national BAAs: (1) agreements between two or more VA health care facilities, or a regional or VHA Program Office and a business associate; or (2) agreements between VHA and a VA component as a business associate.

[6]Protected health information (PHI) means individually identifiable health information and includes information that (1) is created or received by a covered entity; (2) relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) identifies the individual or presents a reasonable basis to believe that the information can be used to identify the individual (45 C.F.R. § 160.103).

[7]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9) and the HIPAA Privacy Rule, 45 C.F.R. § 164.504.

conducting independent performance audits of national business associates.

Regarding our third objective, we focused on a selected information system that supports the MVP.[8] We based our methodology primarily on our Cybersecurity Program Audit Guide.[9] We evaluated VA's implementation of selected control objectives related to (1) asset and risk management, (2) configuration management, (3) identity and access management, and (4) continuous monitoring and logging. We selected control objectives related to ensuring the confidentiality and integrity of information.

To address these control objectives, we compared system documentation and security controls in place against agency policy, NIST security control guidance, and Office of Management and Budget (OMB) requirements. We also interviewed relevant agency officials and assessed additional supporting documentation as necessary.

We issued a report in September 2025 that addressed the first three objectives.[10] In that report, we identified security control deficiencies associated with a system supporting MVP (our third objective). As a result, we made 13 recommendations for VA to correct these deficiencies. We designated that report as "limited official use only" and did not release it to the general public because of the sensitive information it contained.

To address our fourth objective, we examined supporting documents to assess the effectiveness of the actions taken to address the security control deficiencies and related recommendations stemming from our third objective, which we reported on in September 2025. We also interviewed relevant agency officials as necessary.

This current report publishes the findings discussed in our September 2025 report, but we have removed sensitive information. We also provided a draft of this report to VA officials to review and comment on

[8]We are not naming the selected system in this report due to the sensitive nature of the information.

[9]GAO, *Cybersecurity Program Audit Guide*, GAO-23-104705 (Washington, D.C.: Sept. 28, 2023).

[10]GAO, *Privacy and Cybersecurity: VA Provides Oversight of Protected Health Information but Needs to Enhance Security Controls*, GAO-25-107381SU (Washington, D.C.: Sept. 25, 2025).

the sensitivity of the information contained herein and to affirm that the report can be made available to the public without jeopardizing the security of VA's systems. Appendix I provides additional details on our objectives, scope, and methodology.

We conducted this performance audit from January 2024 to May 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

VA is responsible for providing a variety of services to veterans including health care, disability compensation, and vocational rehabilitation. Within the department, VHA oversees the delivery of health care services, including primary care, specialized care, and related medical and social support at approximately 170 medical centers and 1,200 clinics located throughout the country. According to VA's website, about 9.1 million veterans are enrolled in the VA health care system.

The use of IT is crucial to helping VA effectively serve the nation's veterans. Specifically, VA uses the Veterans Health Information Systems and Technology Architecture to manage health care for its patients, which contains the department's electronic health record (EHR). However, this system is technically complex, costly to maintain, and does not fully support the department's need to exchange EHRs with other organizations, such as the Department of Defense (DOD) and private health care providers.

As such, in June 2017, VA initiated the EHRM program to replace its existing EHR system with the Oracle Health EHR system—the same commercial system that the Department of Defense was implementing across the military health system—and configure it for VA.[11] In April 2023, after deploying the new system to five sites, VA decided to delay

[11]VA and DOD use the same Oracle Health Millennium system with agency-specific configuration differences. VA refers to its EHR system as the Federal EHR, while DOD refers to its system as Military Health System GENESIS. VA contracted with Cerner Government Services, Inc. for the department's new EHR system in May 2018. Subsequently, in June 2022, Cerner was acquired by Oracle Health Government Services, Inc. We use Oracle Health throughout this report.

upcoming deployments to address feedback from users at the initial sites who identified patient safety and system reliability issues.

## HIPAA Established Safeguards for Protected Health Information

HIPAA authorized the Secretary of Health and Human Services to establish standards to protect the privacy of certain health information and required the Secretary to adopt security standards for that health information. The Department of Health and Human Services (HHS) implemented the HIPAA provisions through its issuance of the Privacy, Security, and Breach Notification Rules. The HIPAA Privacy Rule establishes national standards for safeguarding PHI, which includes most individually identifiable health information transmitted or maintained in any form by a covered entity or its business associates.[12]

Many health care providers and health plans do not carry out all their health care activities and functions by themselves. Instead, they often use the services of a variety of other businesses. The Privacy Rule allows covered providers and health plans to disclose PHI to these business associates. Business associates (BA) are defined, in part, as a person who, on behalf of a health care provider or another business associate, creates, receives, maintains, or transmits protected health information. The HIPAA Privacy Rule requires that covered entities, such as VHA, enter into agreements with their business associates (frequently referred to as business associate agreements) to ensure that the BAs appropriately safeguard the protected health information.[13]

## VHA Shares Information with National Business Associates

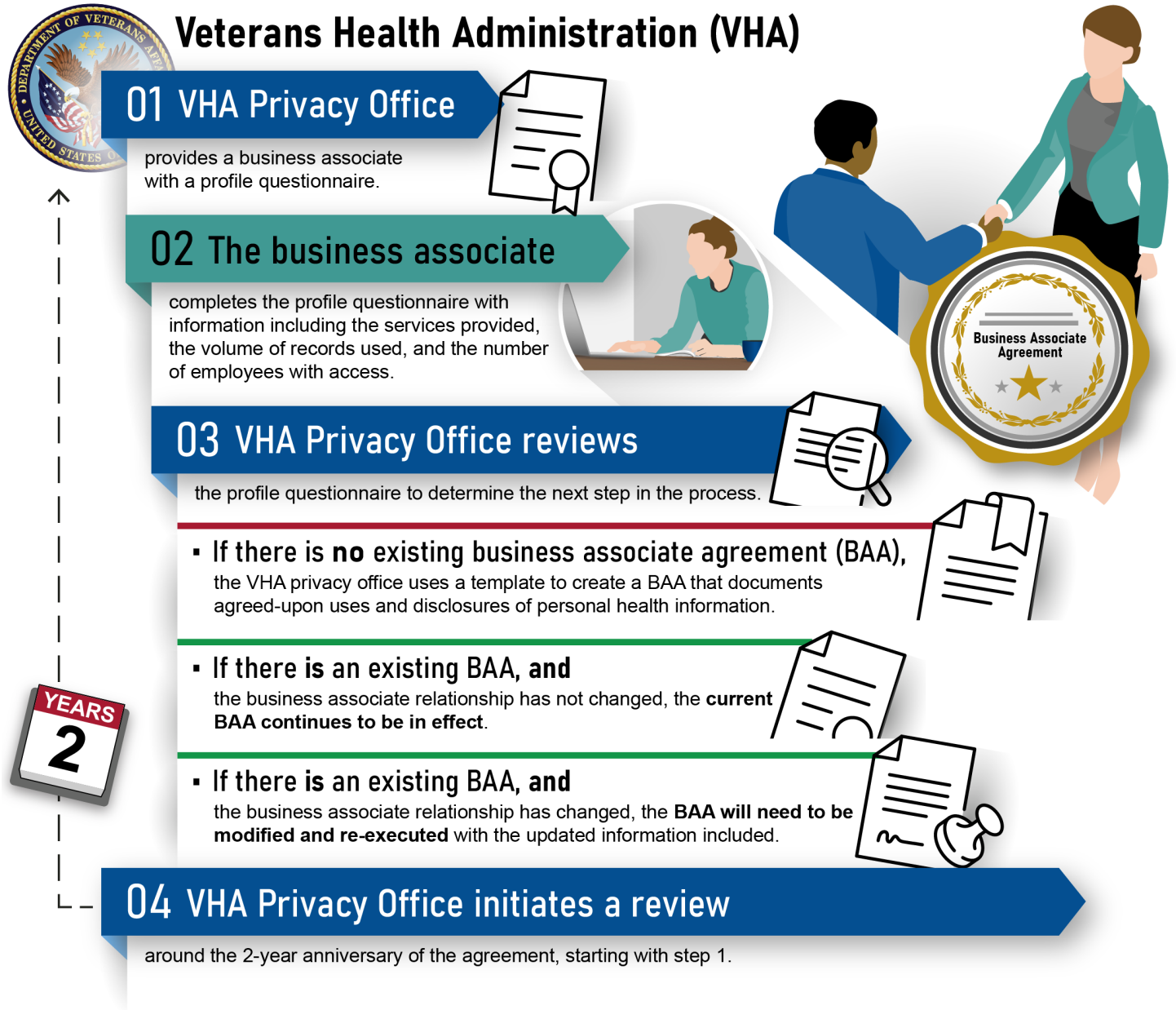
VHA has about 450 national BAs to help support its mission of providing veterans with healthcare. VHA establishes a relationship with national BAs by providing the external entity with a business associate profile questionnaire. In turn, the external entity provides responses to VHA. If the external entity will require access to veterans' PHI, then VHA and the external entity enter into a business associate agreement (BAA), which, among other things, requires the business associate to follow the requirements of the HIPAA Privacy Rule when dealing with PHI. The provisions of VHA's BAAs state that they are reviewed every 2 years.

[12]Covered entities include health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a transaction for which HHS has adopted standards.

[13]45 C.F.R. § 164.502. HIPAA-covered entities include health plans, health care providers who conduct certain transactions electronically, and health care clearinghouses. Business associates are third parties that (1) create, receive, maintain, or transmit PHI on behalf of a covered entity for a covered function; or (2) provide certain services to or for a covered entity that involve the disclosure of PHI. 45 C.F.R. § 160.103.

According to VHA, in that review, the relationship is examined to determine if the business associate relationship is still in effect. If so, then the business associate submits an updated profile questionnaire, and the agreement is either renewed or updated to reflect current VHA requirements. If not, then BAAs are cancelled, and business associates no longer have access to PHI. Figure 1 depicts the process of establishing a BAA with a business associate and reviewing and updating the agreements biennially.

**Figure 1: National Business Associate Agreement Establishment and Review Process**

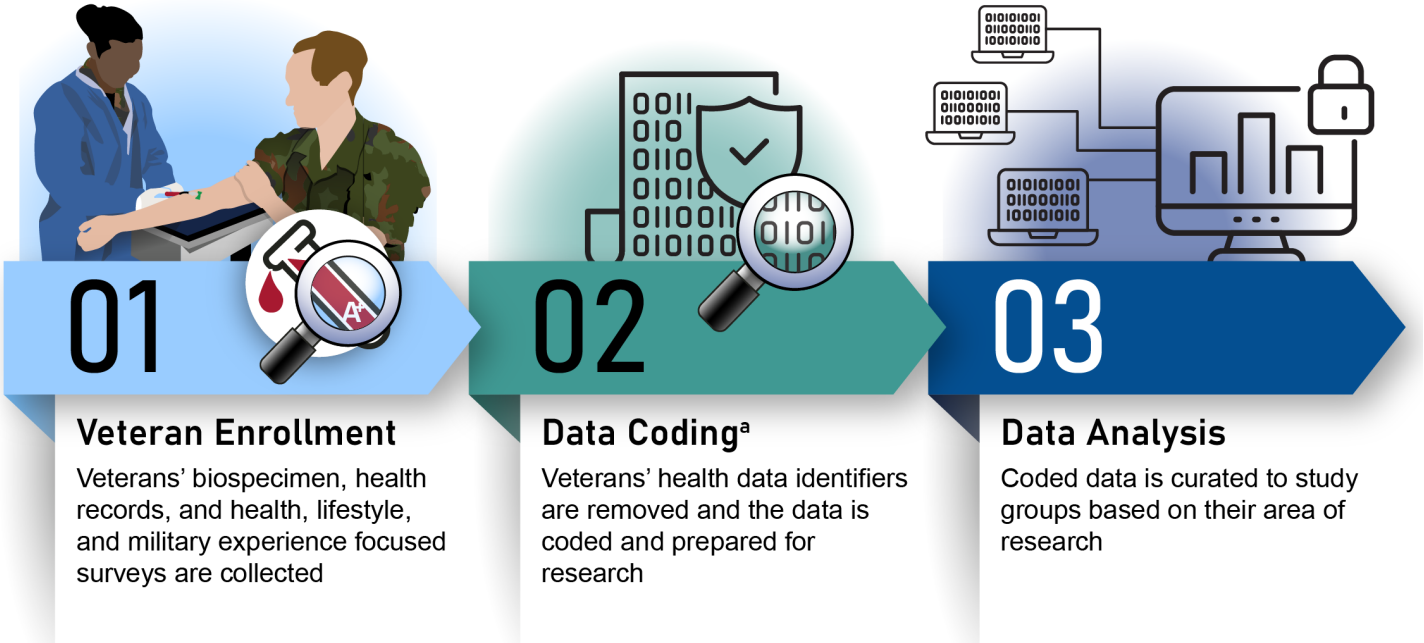



Sources: GAO based on VHA information; GAO (person on computer, people shaking hands, and calendar illustrations); Cetacons/stock.adobe.com (all other icons); Veterans Affairs (logo). | GAO-26-108651

## The Million Veteran Program Collects Sensitive Health Information

MVP is a national research program looking at how genetics, lifestyle, military experiences, and exposures affect health and wellness in veterans. Since launching in 2011, about 1 million veterans have joined the program, making it the nation's largest biorepository of veteran data. Figure 2 depicts MVP's process of veteran enrollment, data coding, and analysis.

**Figure 2: Million Veteran Program**




Sources: GAO based on Veterans Affairs information; GAO (#1 icon and illustration, and #2 magnifying glass icon); Cetacons/stock.adobe.com (all other icons). | GAO-26-108651

[a]According to Veterans Affairs (VA) officials, data coding involves removing identifiable information and replacing it with a unique code, which may be a numeric code or a bar code so that research participants cannot be identified. VA removes participant identifiers, such as date of birth, name, and Social Security number.

MVP is supported by a scientific computing system for genomic medical research. Components in the system serve as a data repository where genomic information is analyzed and stored. To protect veterans' information, personally identifiable information is coded in the system before use in research.[14]

## Federal Law, Policy, and Guidance Establish Requirements for Protecting PHI and Securing Federal Systems and Information

In addition to HIPAA and the Privacy Rule, federal laws, along with executive branch policy and federal guidance, establish agency requirements and responsibilities for ensuring the protection of PHI and other sensitive personal information. These laws, policy, and guidance include:

- **Privacy Act of 1974.** This act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[15] It requires agencies to issue system of records notices to notify the public when they establish or make changes to systems of records. The notices identify, among other things, the types of data collected, the types of individuals about whom information is collected, the intended "routine" uses of the data, and procedures that individuals can use to review and correct personal information.
- **E-Government Act of 2002.** The act requires that agencies conduct, where applicable, a privacy impact assessment for each system.[16] This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system.
- **OMB Memorandum M-22-09.** In January 2022, OMB published this strategy that requires agencies to meet specific cybersecurity standards and objectives intended to reinforce the government's defenses against sophisticated and persistent threat campaigns. The strategy outlines actions that agencies are to take by the end of fiscal

[14]The HIPAA Privacy Rule governs the de-identification of data, including demographic data that could be used to identify an individual, such as name, address, birth date, and Social Security number. The HIPAA Privacy Rule specifies two ways to de-identify information: (1) expert determination that risk of identification is very small and (2) removal of specified identifiers of the individual and no actual knowledge that residual information can identify the individual. 45 C.F.R. § 164.514.

[15]Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974) (codified as amended at 5 U.S.C. § 552a). A system of records is a collection of information about an individual under control of an agency from which information is retrieved by the name of an individual or other identifier. 5. U.S.C. § 552a(a)(4), (5).

[16]E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921-22 (Dec. 17, 2002).

year 2024 that are intended to form a starting point to implementing zero trust architecture.[17]

- **OMB Memorandum M-21-31.** In August 2021, OMB published this memorandum that requires agencies to implement various logging, log retention, and log management requirements by August 2023. The memorandum establishes requirements for agencies to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of federal information and executive branch departments and agencies.[18]
- **NIST Privacy Framework.** This voluntary tool was developed to help organizations identify and manage privacy risk to provide services while protecting individuals' privacy. The framework supports organizations in building customers' trust, fulfilling compliance obligations, and facilitating communication about privacy practices.[19]

In addition to laws and policy focusing specifically on PII, agencies are subject to laws and guidance governing the protection of information and information systems, which includes implementing privacy protections. For example:

- **Federal Information Security Modernization Act of 2014 (FISMA).** The act requires each agency to develop, document, and implement an agency-wide information security program. FISMA requires agency Inspectors General to annually assess the effectiveness of the information security policies, procedures, and practices of their parent agency. Further, FISMA gives NIST responsibility for developing standards for categorizing information and information systems,

[17]Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022). A zero-trust architecture is a set of cybersecurity principles stating that organizations must verify everything that attempts to access their systems and services.

[18]Office of Management and Budget, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (Washington, D.C.: Aug. 27, 2021).

[19]National Institute of Standards and Technology, *The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (Gaithersburg, MD: Jan. 2020)

security requirements for information and systems, and guidelines for detection and handling of security incidents.[20]

- **NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations.** This document provides a catalog of security and privacy controls for systems and organizations.[21] Previous revisions of this publication included a separate appendix detailing specific privacy controls. In September 2020, NIST issued revision 5, which aims to fully integrate privacy controls into the security control catalog, creating a consolidated and unified set of controls.

## Previous GAO and VA OIG Work Highlights Need for Controls over PHI and Management of EHRM

In May 2022, we reported that between 2015 and 2021, HHS had seen an increase in reported breaches of unsecured PHI while the number of affected individuals varied each year from approximately 5 to 113 million.[22] The HHS Office for Civil Rights (OCR) is charged with developing and managing the breach reporting process. However, OCR did not have a method for covered entities to provide feedback on the breach reporting process, nor did the office indicate that it had plans to develop one. We made one recommendation to HHS to ensure that OCR establishes a mechanism for covered entities and business associates to provide feedback on OCR's breach reporting process. HHS has implemented the recommendation.

In May 2023, we reported that the VA organizational change management activities for the EHRM program were partially consistent with seven organizational change management leading practices and not consistent with one leading practice.[23] We also reported that most users have expressed dissatisfaction with the new EHR system. Additionally,

[20]The Federal Information Security Modernization Act of 2014 (FISMA 2014) Pub. L. No.113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[21]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, special publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

[22]GAO, *Electronic Health Information: HHS Needs to Improve Communications for Breach Reporting*, GAO-22-105425 (Washington, D.C.: May 27, 2022).

[23]GAO, *Electronic Health Records: VA Needs to Address Management Challenges with New System*, GAO-23-106731 (Washington, D.C.: May 18, 2023).

VA did not adequately identify and address system issues. Specifically, VA did not ensure that trouble tickets for the new EHR system were resolved within timeliness goals. We made 10 recommendations to VA to address change management, user satisfaction, system trouble ticket, and independent operational assessment deficiencies. As of February 2026, VA has partially implemented four recommendations and has not yet provided evidence that it has implemented the other six recommendations.

In a September 2024 report, the VA Office of Inspector General (OIG) reported that VA lacked sufficient controls to prevent, respond to, and mitigate the impact of major incidents in the EHR system.[24] From October 24, 2020 through March 31, 2024, the system was affected by incidents including outages, performance degradations, and incomplete functionality for 1,909 total hours. Additionally, VA OIG found that VA and Oracle Health did not have adequate controls in place to prevent system changes from causing major incidents or responding to and mitigating the impact of those incidents. The OIG made nine recommendations. As of February 2026, VA has implemented two recommendations and has not yet implemented the remaining seven recommendations.

## VHA Developed and Documented PII and PHI Policies in Accordance with NIST Guidance

NIST guidance states that organizations should develop, document, and disseminate a PII processing and transparency policy.[25] This policy should address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The policy should also include procedures to facilitate the implementation of the policy and the associated controls. NIST also recommends that organizations designate an official to manage the development, documentation, and dissemination of the policy and procedures. Additionally, NIST states that organizations should (1) determine and document the authority that permits the processing of PII; (2) identify and document the purposes for processing PII; (3) describe the purposes in public privacy notices and policies; and (4) restrict the processing of PII to only that which is compatible with the identified purposes.

[24]VA Office of Inspector General, *VA Needs to Strengthen Controls to Address Electronic Health Record System Major Performance Incidents*, Audit 22-03591-231, September 23, 2024.

[25]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, special publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

VHA has developed, documented, and disseminated organization-level PII and PHI information processing and transparency policy. A VHA directive addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The directive also contains organizational policy for collecting, using, and disclosing PII and PHI based on federal statutes and regulations. Additionally, the directive includes procedures to facilitate the implementation of the policy and associated controls.

Multiple VHA directives also establish roles and responsibilities for overseeing and implementing the VHA Privacy Program. For example:

- The VHA Chief Privacy Officer is the director of the VHA Information Access and Privacy (IAP) Office and is responsible for administering the VHA privacy program and the VHA Privacy Compliance and Accountability (PCA) program, and for developing, issuing, reviewing, and coordinating privacy policy for VHA.
- The VHA Privacy Operations Officer manages the VHA Privacy Office, which is a component of the IAP office. The Privacy Officer is responsible for implementing the VHA Privacy Program and VHA-wide privacy policies and procedures through the Privacy Office.
- The Chief Privacy Compliance and Accountability Officer is responsible for conducting independent performance audits of national business associates for compliance with the terms of BAAs.

VHA has also sufficiently documented its authority to process PHI and the approved uses of PHI, provided adequate public notice of those uses, and documented policy to restrict processing of PII to those uses. Specifically:

- A VHA directive documents the authority that permits the collection, use, and disclosure of PII and PHI by VHA. For example, the directive lists the Privacy Act, the HIPAA Privacy Rule, and other VA regulations related to use and disclosure of PHI.
- The directive also states that VHA employees may use information contained in VHA records required for the performance of their official job duties for treatment, payment, or healthcare operations purposes. This directive is posted on VA's public website.
- The privacy impact assessment for the EHRM system is publicly available on VA's website and describes the purposes for processing PII. Specifically, the assessment states that the EHRM program enables VA to provide the delivery of quality healthcare to veterans.

Additionally, the assessment identifies, and lists the use of, the information collected or maintained in the system.

- Use and disclosure restrictions for external entities are implemented through BAAs. These agreements document the permitted uses and disclosures of the shared data. A VHA directive states that all VHA personnel will make reasonable efforts to limit requests for, use of, or disclosure to the minimum necessary to accomplish the intended purpose of the request, use, or disclosure. This directive is also publicly available on the VA's website.

## VHA Oversees the Privacy of Shared Health Information and Plans to Improve Its Performance Audit Approach

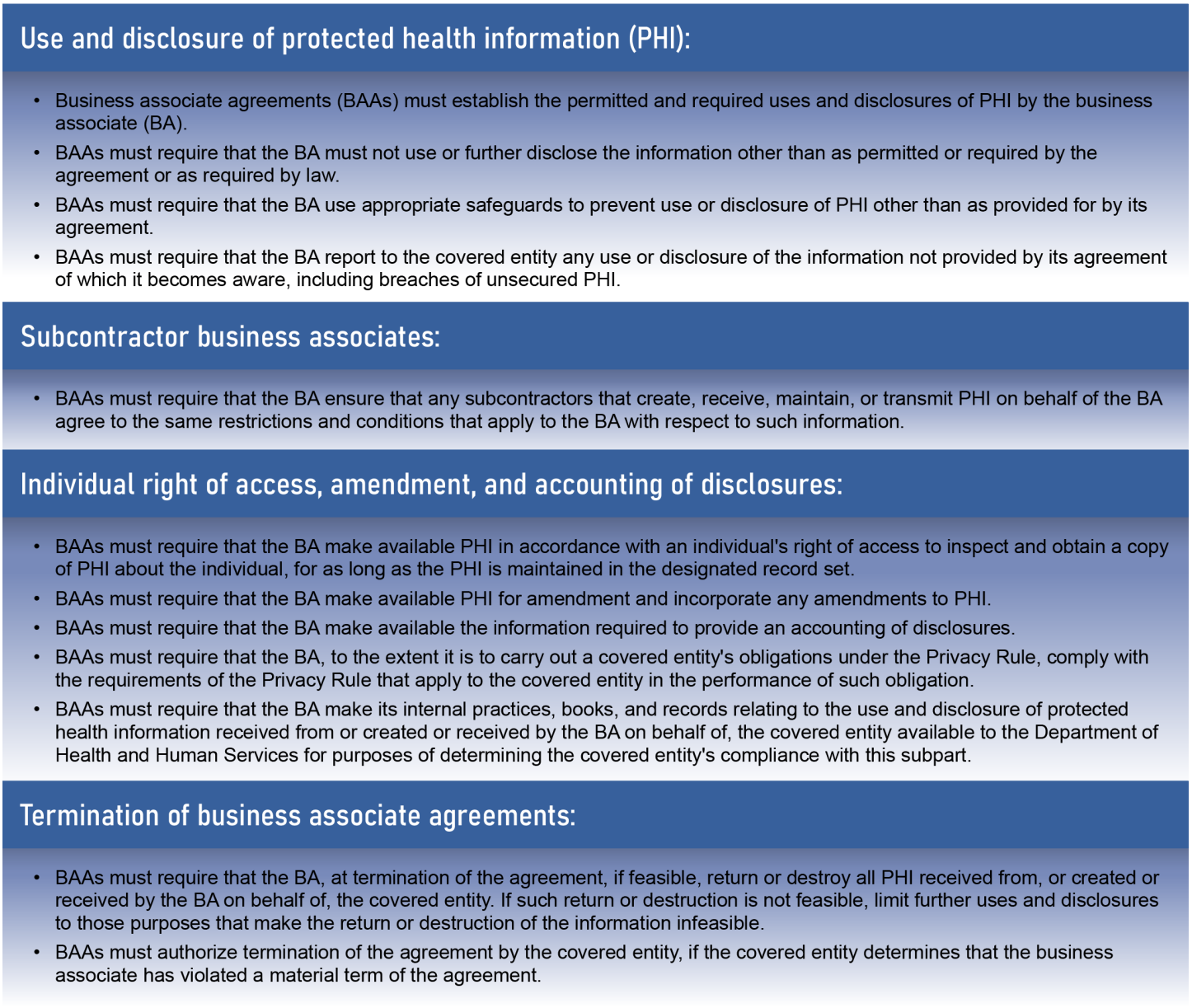
VHA provided oversight of information shared with external entities (i.e., national BAs) by ensuring that business associate agreements with national BAs addressed requirements from the HIPAA Privacy Rule. It also ensured that its business associate agreements associated with the EHRM program met these requirements. Additionally, the agency monitored changes in the processing of PHI by reviewing business associate agreements every 2 years. Further, VHA documented responsibilities for conducting independent performance audits to confirm that national BAs are meeting their obligations. Finally, VHA is developing an approach for selecting associates for independent performance audits based on risk.

### VHA Ensured That National BAAs Addressed HIPAA Privacy Rule Requirements

Under HIPAA, HHS has established rules to protect the privacy and security of PHI.[26] The HIPAA Privacy Rule applies to covered entities and their BAs. Covered entities may disclose PHI to a BA if they first enter into a BAA that provides assurances that PHI will be appropriately safeguarded and establishes what uses and disclosures of PHI are permitted by the associate. Figure 3 lists requirements from the Privacy Rule that are to be addressed in BAA clauses.

[26]The HIPAA Rules refer to the Privacy, Security, Enforcement, and Breach Notification Rules—the regulations that implement HIPAA and set out requirements governing covered entities, such as VHA, and business associates' disclosure, use, maintenance, and transmission of PHI. Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) as amended, 45 C.F.R. pts. 160 and 164 subpts C (Security Rule), and E (Privacy Rule). PHI is individually identifiable health information and includes information that (1) is created or received by a covered entity; (2) relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) identifies the individual or presents a reasonable basis to believe that the information can be used to identify the individual.

**Figure 3: Health Insurance Portability and Accountability Act Privacy Rule Requirements to be Addressed in Business Associate Agreements**




Sources: Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. § 164.504. | GAO-26-108651

VHA used templates to create BAAs with national business associates. Each of the four templates used since 2019 included clauses that addressed all the selected HIPAA Privacy Rule requirements. BAA templates are updated as needed; the most recent template from September 2024 included a new provision for compliance audits. According to agency officials, during each BAA's biennial review, the VHA Privacy Office will use the most recent template to update the agreement. As a result, all BAAs are updated to the most recent template within 2 years.

In addition, the 73 national BAAs in our random sample included clauses that addressed all the HIPAA Privacy Rule requirements. Based on sample results, we estimate that 100 percent of BAAs include clauses that address all of the HIPAA Privacy Rule requirements and the 95 percent confidence interval ranges from 96 to 100 percent.[27] Further, the BAA between VHA and the EHRM-IO as well as the BAA between the Integration Office and the EHRM contractor included clauses that addressed all the Privacy Rule requirements.

By ensuring that BAAs address key requirements of the HIPAA Privacy Rule, VHA has greater assurance that business associates have procedures and controls intended to protect the privacy of veterans' protected health information.

## VHA Monitored Changes in PHI Processing Through Biennial Reviews of BAAs

NIST states that organizations should monitor changes in processing PII and implement mechanisms to ensure that any changes are made in accordance with appropriate requirements.

The VHA Privacy Office monitors changes in the processing of PII and ensures that changes are made in accordance with VHA requirements. According to agency officials and the provisions of the BAAs, VHA monitors changes in the processing of PII by reviewing BAAs every 2 years. The office uses a database to track significant dates in the review process such as when the agreement was initiated and executed. At the beginning of each fiscal year, the office pulls a report from the database that includes the agreements that are due for a 2-year review based on the date of the last signature on the agreement. As a result, VHA has

[27]The population of national BAs from which we drew our sample included only the 331 national business associates that are non-federal entities and that have electronic access to veterans' PHI.

better assurance that changes in how BAs are processing and using PHI are made in accordance with VHA requirements.

## VHA Documented Audit Responsibilities and is Developing a Risk-Based Approach for Performance Audits

NIST states that, as part of managing privacy risk in the processing of PII, data processing ecosystem parties, including service providers and partners, should be routinely assessed.[28] Assessments may include using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or other obligations.

VHA established responsibilities for conducting independent performance audits of BAs to ensure that they are meeting their contractual obligations. Specifically, a VHA directive states that the VHA Chief PCA Officer is responsible for conducting periodic independent performance audits of the operations of VA's national BAs for compliance with the terms of the BAA.

During the period of August 1, 2023 to July 31, 2024, the PCA Office performed one independent performance audit of a business associate because it had reported multiple data breaches of veterans' PHI.[29] VHA officials stated that the identification of the associate for an audit was not based on a risk-based approach, but highlighted the need for such an approach to help better identify potential risk.

To address this concern, IAP's Business Associate Program Improvement Workgroup was tasked with creating a risk-based approach to identify high risk business associates to submit to the PCA Office for potential audit. Officials stated that the approach is expected to be completed by the end of calendar year 2025. If implemented effectively, such a risk-based approach can provide greater assurance that its BAs are meeting privacy requirements.

[28]National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*, Version 1.0 (Gaithersburg, MD: January 2020).

[29]According to an IAP Office official, during the period of August 1, 2023, to July 31, 2024, VHA had 18 reported privacy incidents for eight national business associates. Of those 18 privacy incidents, officials determined that, based on VA criteria, four were breaches. Those four breaches occurred at three different business associates.

## VA Took Steps to Protect Health Information in Its Million Veteran Program, but Work Remains

VA took steps to protect the health information used in MVP. Specifically, the agency assessed potential risks and secured data in transit and at rest in the selected system. However, VA did not fully implement all security controls related to risk management, configuration management, identity and access management, and continuous monitoring. As a result, VA had less assurance that the controls over confidentiality and integrity are effective. Due to their sensitive nature, GAO's detailed findings and recommendations related to MVP are not included in this report. The next section discusses the status of the recommendations that GAO made in the September 2025 limited distribution report.

### VA Implemented Asset and Risk Management Controls but Further Actions Needed

VA fully implemented one element and partially implemented four elements of NIST guidance on risk management.[30] Specifically, VA determined the potential security impacts in the selected system. However, VA did not fully establish system-level procedures, conduct risk or security control assessments, or implement remedial action plans.

#### VA Categorized the Confidentiality, Integrity, and Availability of Information Appropriately

Security categories describe the potential adverse impacts or negative consequences to organization operations, assets, and individuals if information and systems are compromised through the loss of confidentiality, integrity, or availability. NIST states that organizations should categorize information systems and the information they use.

VA identified and categorized information that is used in the system. The agency documented this categorization in the system's categorization report and system security plan. As a result, VA assessed potential impacts and consequences to the organization due to the loss of confidentiality, integrity, or availability of information used in the system.

#### VA Partially Established System-Level Procedures

Policies and procedures contribute to security and privacy assurance. NIST states that agencies should develop, document, and disseminate system-level procedures to address scope, roles, responsibilities, coordination, and to facilitate the implementation of the policy and associated security controls.

VA partially documented system-level procedures. Specifically, VA has procedures that outline roles and responsibilities for the system owner, administrators, security officer, and stewards. However, not all procedures contain system-level security control implementations. Until VA has such procedures, the agency would have limited assurance that it

[30]NIST special publication 800-53 revision 5.

has implemented its policy and that security controls are operating as intended.

### VA Conducted a Limited Scope Risk Assessment

Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets. NIST states that agencies should conduct a risk assessment to identify threats and vulnerabilities and determine their likelihood and impact to information systems. It also recommends that agencies integrate risk assessment decisions from other organizational perspectives. Further, it states that the assessment should be updated when there are changes to the operating environment that may impact the security or privacy state of the system.

VA's risk assessment showed its analysis of some but not all threats and vulnerabilities to the system. For example, the assessment outlines various examples of threats, such as system intrusion and break-in and power failure, and the threats' assessed likelihood, impact, and risk. It also documents risk mitigation against some of these vulnerabilities. In addition, the agency integrated mission perspectives into risk management decisions to ensure the continuity of research.

However, the risk assessment did not document changes to the environment such as vulnerabilities identified in all system components. Without updating the risk assessment when there are changes that may impact the security or privacy state of the system such as vulnerabilities, the agency would not be making fully informed decisions or considering all threats and vulnerabilities.

### VA Conducted Limited Scope Control Assessments

Security control assessments provide essential information needed to make risk-based decisions as part of the authorization process. OMB requires that, among other things, agencies use high-quality firms specializing in application security for independent third-party evaluations.[31] In addition, NIST states that agencies should plan, conduct, and report on assessments of the system's control implementation to determine the extent to which the controls are implemented correctly, operating as intended, and producing desired results.

VA requested and conducted control assessments of the system. However, the assessments did not effectively evaluate all system components. As a result of the limited scope of the assessments, the

[31]OMB M-22-09.

agency would have less assurance that controls are operating as intended.

### VA Documented Its Remedial Action Management Process but Did Not Fully Implement It

Plans of action and milestones (POAM) are useful to track remedial actions. NIST states that agencies should implement a process to ensure that POAMs are developed, maintained, and reported in accordance with agency requirements.[32] Additionally, the VA POAM Management Guide requires that all remedial action plans include information such as the vulnerability description, milestones, and mitigations, and be reviewed and approved quarterly. Further, VA policy requires POAMs to include tasks that need to be accomplished to remediate or mitigate deficiencies and specify resources required to accomplish tasks, including roles and responsibilities.[33]

VA implemented a process to ensure that POAMs are developed, maintained, and reported on, and documented active POAMs for the system. Specifically, VA established the POAM Management Guide which describes step-by-step processes to create, edit, review, approve, and close POAMs. The guide states that POAMs are required to be reviewed on a quarterly basis. However, VA did not review and approve the active remedial action plans quarterly. In addition, VA did not always document all required POAM information. Until VA includes required information in remedial action plans to record and monitor control deficiencies and reviews them quarterly, the agency would have limited ability to effectively remediate or mitigate deficiencies.

## VA Partially Implemented Configuration Management Guidance

VA partially implemented two elements of configuration management NIST guidance. Specifically, VA partially implemented configuration-controlled change guidance and server baselines in the selected system.

### VA Did Not Always Fully Document Configuration-Controlled Changes to the Selected System

Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. NIST states that agencies should determine the types of changes to the system that are configuration controlled. Additionally, it states agencies should review proposed changes, document change decisions, implement approved changes, and retain records of

[32]According to NIST, a POAM is a document that identifies elements of the plan, milestones for meeting the elements, and the scheduled completion dates for the milestones that need to be accomplished.

[33]VA, *VA Handbook 6500: Risk Management Framework for VA Information Systems* (Washington, D.C.: Feb. 24, 2021).

configuration control activities. In addition, the system configuration management procedure requires that a change approval board approve configuration-controlled changes in the system.

VA determined the types of changes that should be configuration controlled but had shortcomings in the implementation of its configuration change control processes. Specifically, decisions made during change board meetings were not documented, and documentation of a configuration-controlled change to the selected system was incomplete. Without such documentation, the agency would have limited oversight of changes to the system.

### VA Implemented Baselines for One Server on the Selected System but Not All

Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. NIST states that agencies should establish, document, and implement configuration settings for components employed within the system that reflect the most restrictive mode using organization-defined common secure configurations.[34] Additionally, the system's configuration management procedure states that configuration settings are inherited and managed by the enterprise using baselines.[35]

For the selected system, VA baselined one server but did not do so for other servers that support research. Without establishing, documenting, and implementing baselines for all servers, VA would have limited its ability to ensure that system components are established in the most restrictive mode.

## VA Encrypted in Transit and at Rest Data, but Shortcomings Exist in Other Identity and Access Management Controls

VA protected data in transit and at rest in the selected system with encryption. However, weaknesses existed in VA's implementation of other identity and access management controls.

### VA Protected Data in Transit

Unprotected communication paths are exposed to the possibility of interception and modification. OMB requires that agencies use encrypted

[34]NIST states that common secure configurations provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for IT products.

[35]NIST defines a baseline as a set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk.

internet traffic in their environment. Additionally, NIST states agencies should implement cryptographic mechanisms to protect the confidentiality and integrity of transmitted data.

VA encrypted internet traffic and data in transit in the system. Specifically, the system's firewall restricted insecure traffic between the VA network and system network. Additionally, VA enforced the use of secure versions of cryptographic communication and data transfer protocols in the system. As a result, VA has greater assurance of the confidentiality and integrity of internet traffic and data in transit in the system.

### VA Secured Data at Rest

Information at rest refers to the state of information when it is not in process or in transit and is located on system components and should be protected. NIST states that agencies should protect the confidentiality and integrity of data at rest and determine and implement cryptographic mechanisms to prevent unauthorized disclosure of information. Additionally, system procedure states that all cryptographic mechanisms implemented are to be Federal Information Processing Standards (FIPS) 140-2 compliant.[36]

VA determined and implemented cryptographic mechanisms to ensure that veterans' genomic data are protected at rest in the system. Specifically, a key component in the system is encrypted at rest and the key used to decrypt it is stored in a key manager. In addition, the component's firewall restricts the use of network protocols to limit communication and data transfer to and from itself. Further, the component is FIPS 140-2 compliant. As a result, VA has greater assurance of the confidentiality and integrity of sensitive data at rest in the system.

### VA Documented, but Did Not Fully Implement, Account Management Requirements

Privileged roles such as system administrators are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. NIST states that agencies should 1) document and define the types of accounts allowed, 2) assign account managers, and 3) require criteria for role membership within information systems. Additionally, the selected system's access control procedure states that system administrator accounts should be created by VA's electronic permissions

[36]The Federal Information Processing Standards (FIPS) are a series of computer security standards developed by NIST. FIPS 140-2 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems.

access system based on the user's role and then assigned to the appropriate security group.

VA documented account management requirements for the selected system. However, weaknesses existed in its implementation of certain account management controls over privileged accounts. Until it addresses these weaknesses, the department would face increased risk of unauthorized access to the system.

### VA Reviewed Some, but Not All, User Accounts in Accordance with Procedure

A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. NIST states that agencies should review the user privileges at an organization-defined frequency. Additionally, the selected system's access control procedure calls for supervisors to perform quarterly reviews of accounts to ensure least privilege, separation of duties, and continued need for access.

VA reviewed certain user accounts but did not review other accounts quarterly in accordance with its access control procedures. As a result, the agency would be less able to ensure that the rationale for assigning certain functions to individuals remains valid and least privilege and separation of duties are enforced.

### Other Identity and Access Management Controls Were Not Always Fully Implemented

Identity and access management controls involve limiting or detecting inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure. User identities may be authenticated through something they know (a traditional password), something they have (such as a token or card), or something about them that uniquely identifies them (such as a fingerprint). Multifactor authentication is a mechanism to verify an individual's identity by utilizing two or more of these elements. If authentication is successful, authorization grants or restricts user, service, or device access to resources based on the identity of the user, service, or device.

VA did not fully implement user authentication and authorization controls to access system resources.[37] Without these controls in place, the agency would limit its ability to manage users' access.

[37]Due to their sensitive nature, GAO's detailed findings and recommendations related to MVP are not included in this report.

## VA Partially Implemented Continuous Monitoring and Logging Controls in the Selected System

Although VA had a department-level continuous monitoring strategy, it did not implement its policy related to having a system-level strategy for the selected system. In addition, it partially addressed OMB logging requirements for a key system component.[38]

### VA Did Not Establish a System-Level Information System Monitoring Strategy

Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture. VA policy requires the development and implementation of a system-level strategy for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system.

VA has a department-level continuous monitoring strategy but did not establish one for the selected system. As a result, the agency may be limited in its timely response to incidents and effective defense of the system.

### VA Logged Events in the System but Did Not Fully Implement Selected Monitoring Requirements

Event logging supports monitoring and auditing needs. OMB required agencies to implement various logging capabilities by August 2023, such as logging certain events.

VA logged certain important events in the selected system. However, the department did not fully implement selected OMB monitoring and logging requirements in a key system component. Until VA fully implements these requirements, the agency would be limited in its ability to detect and respond to threats in real-time.

## VA Has Made Progress in Addressing GAO Recommendations to Resolve Security Control Weaknesses

In September 2025, GAO reported on and made 13 recommendations to VA to address weaknesses identified in the selected MVP system. Specifically, we recommended that the agency take action to resolve security control deficiencies related to asset and risk management, configuration management, identity and access management, and continuous monitoring and logging. As of March 2026, VA has made progress to address the majority of our recommendations. Specifically, VA addressed nine recommendations, partially addressed three others, and did not address one recommendation. Figure 4 summarizes the status of VA's efforts to implement the 13 recommendations to resolve the security control deficiencies.

[38]OMB M-21-31.

**Figure 4: Status of Efforts by the Department of Veterans Affairs to Implement GAO's Recommendations for the Selected System's Security Control Deficiencies, as of March 2026**

| Security control area | Recommendation | Status of recommendation |
|---|---|---|
| Asset and risk management | 1 | ✓ |
| | 2 | ✓ |
| | 3 | ! |
| | 4 | ✓ |
| | 5 | ✓ |
| Configuration management | 6 | ✓ |
| | 7 | ! |
| Identity and access management | 8 | ✓ |
| | 9 | ✓ |
| | 10 | ✓ |
| | 11 | ✗ |
| Continuous monitoring | 12 | ✓ |
| | 13 | ! |

✓ = Implemented: VA successfully completed actions to implement the recommendation.

! = Partially implemented: VA had made progress but had not completed implementation.

✗ = Not implemented: VA had not provided sufficient evidence that it had implemented the recommendation.

Sources: GAO analysis; Veterans Affairs (VA) logo; Ka Han/stock.adobe.com (icons). | GAO-26-108651

By implementing nine of these 13 recommendations and partially implementing three, VA has further protected the confidentiality and integrity of health information in its MVP.

Although VA has made progress, fully implementing these recommendations is essential to ensuring the confidentiality and integrity of sensitive health information. GAO will continue to monitor VA's progress in implementing the remaining recommendations.

## Agency Comments

We requested comments on a draft of this report from the Department of Veterans Affairs (VA). In written comments, which are reprinted in appendix II, the department stated that it takes security very seriously and works to ensure veterans' data is always protected in the continuously changing threat scenarios. We will continue to monitor VA's progress in implementing the remaining recommendations outlined in this report. VA also provided technical comments, which we addressed as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Veterans Affairs, the VA Office of Information and Technology, the department's Inspector General, and interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at FranksJ@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Sincerely,

//SIGNED//

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

# Appendix I: Objectives, Scope, and Methodology

The objectives for this review were to determine the extent to which (1) the Veterans' Health Administration (VHA) has developed and documented personally identifiable information (PII) and protected health information (PHI) policies in accordance with federal privacy guidance, (2) VHA oversees the privacy of veterans' health information shared with external entities including those associated with its Electronic Health Record Modernization (EHRM) Program, (3) the Department of Veterans Affairs (VA) protects the confidentiality and integrity of veterans' health information in selected systems for its Million Veteran Program (MVP), and (4) VA has taken corrective actions to address identified control deficiencies and related recommendations.

To address the first objective, we reviewed VHA organization charts and privacy policies against selected privacy controls from National Institute of Standards and Technology (NIST) special publication (SP) 800-53 revision 5.[1] We selected three controls due to their applicability to the sharing of PHI between VHA and external entities. Specifically, we selected the following controls associated with protecting personally identifiable information and its processing:

- policy and procedures;
- authority to process PII; and
- PII processing purposes.

Additionally, we reviewed other documentation and interviewed cognizant VHA officials as necessary.

To address the second objective, we focused on PHI that VHA shares with national business associates (i.e., external entities). We focused on national business associates (BA) due to their potential impact on the privacy of veteran's protected health information.[2]

[1]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, special publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

[2]There are two types of national business associate agreements: (1) agreements between two or more VA health care facilities, or a Regional or VHA Program Office and a business associate; or (2) agreements between VHA and a VA component, as a business associate. The national agreements we selected for this review are agreements between the VHA Privacy Office and external business associates. A local agreement is negotiated and executed between a single VA health care facility and a single business associate.

To select the associates for a generalizable random sample, we first determined the population. We obtained responses to the business associate profile questionnaires for all 459 VHA national business associates as of August 30, 2024. Each profile questionnaire represented a national business associate with an active business associate agreement (BAA).

We excluded from our target population any BAs that were internal VA entities or other federal agencies, associates that did not have electronic access to veterans' PHI, and duplicate profile questionnaire records. To determine whether BAs had electronic access to PHI, we examined each profile questionnaire to determine whether it stated that the associate had electronic access. In some cases, the questionnaires were unclear, and we had to use our own discretion and other information in the questionnaires to determine whether the BA had electronic access. Based on these exclusions, the final sample frame included 331 BAs with active BAAs. We next selected a random sample of 73 of the 331 associates. The sample size of 73 was computed to ensure a margin of error of plus or minus 10 percentage points or fewer, at the 95 percent confidence level.

We identified 12 requirements from the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule that BAAs are to include.[3] We then examined the agreements for each of the sampled business associates to determine whether they contained clauses that address these requirements.

In addition to our sample, we evaluated the BAAs between VHA and the EHRM Integration Office (EHRM-IO) and between the integration office and the EHRM contractor. We included these organizations in our scope because of the importance of the EHRM program to VA's mission and the large amount of veterans' PHI processed by EHRM. We reviewed the business associate agreements between VHA and EHRM-IO, and the integration office and the contractor (Oracle Health), to determine whether the agency has privacy oversight of veterans' PHI shared with EHRM.

Additionally, we obtained and examined documentation of VHA privacy incidents, and the one independent performance audit of a national business associate conducted in calendar years 2023 and 2024. We then

[3]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9) and the HIPAA Privacy Rule, 45 C.F.R. § 164.504.

compared the documentation to one selected control related to evaluating whether data processing ecosystem parties are meeting their privacy-related obligations from the NIST Privacy Framework, as well as VHA policy on conducting independent performance audits. We did so in order to determine whether VHA was conducting such audits in accordance with NIST controls and agency policy. Further, we examined meeting minutes and interviewed agency officials to determine the plans VHA had for improving its approach for conducting independent performance audits of national business associates.

We also determined that the control environment component of internal control was significant to this objective, along with the underlying principle that management should assign responsibility and delegate authority to achieve the entity's objectives.[4] We assessed VHA policies and procedures, reviewed organizational charts, and interviewed officials to determine whether the agency had assigned responsibility and delegated authority for overseeing the privacy of veterans' PHI shared with national business associates.

We further determined that the control activities component of internal control was significant to this objective, along with the underlying principle that management should implement control activities through policies. We assessed VHA policies and examined the one performance audit report of a national business associate that VHA conducted. We did this to determine if the agency had implemented its policy to create a program for evaluating business associates for compliance with BAAs.

To address our third objective, we first gained an understanding of the operating environment by reviewing network diagrams and system documentation such as system security plans. Our scope focused on a selected information system that supports the MVP.

We used our Cybersecurity Program Audit Guide to facilitate our methodology.[5] We selected control areas and control objectives in them based on their relevancy to the confidentiality and integrity of information.

[4]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

[5]GAO, *Cybersecurity Program Audit Guide*, GAO-23-104705 (Washington, D.C.: Sept. 28, 2023).

We evaluated the implementation of requirements and guidance related to the following Cybersecurity Program Audit Guide control areas:

- Asset and Risk Management,
- Configuration Management,
- Identity and Access Management, and
- Continuous Monitoring and Logging.

To address asset and risk management, we evaluated the system's documentation including system categorization, risk assessment, and control assessment reports and compared them to NIST SP 800-53 revision 5 security control guidance. We also determined the extent to which VA established a process for and documented and updated system plans of actions and milestones (POAM) in accordance with agency requirements and NIST guidance. To do so, we reviewed the agency's POAM Management Guide and system's active POAMs. We examined the POAMs to determine whether the agency had documented all required fields and had updated them quarterly as required by VA's guide.

To address configuration management, we evaluated system documentation. Specifically, we compared system configuration management procedures to NIST guidance. Additionally, we reviewed evidence of configuration changes in the system to determine if agency officials had documented their review and approval and retained records of these changes in accordance with system procedures and NIST guidance. Also, we reviewed the implementation of configuration baselines for servers in the system to determine if VA had established, documented, and implemented restrictive and secure configuration settings in accordance with NIST guidance. The servers we selected host key functions and services that support MVP research.

To address identity and access management, we reviewed the system's identification and authentication and access control documentation. Specifically, we evaluated related procedures against NIST guidance. In addition, we reviewed system account management artifacts to determine if VA had implemented system-level procedures and NIST guidance.

To do so, we selected a stratified sample of five of the 66 MVP research studies in the system. We divided the 66 studies into three groups based on the number of researchers in the study: those with five or fewer researchers, between six and 20, and more than 20. We randomly

selected two studies from each of the first two groups and one from the last. We assessed evidence of the review of researcher accounts from each of the selected research studies to determine if VA had complied with its procedures. We also reviewed evidence of the creation and review of system administrator accounts in the system to determine if VA had followed its procedures for these accounts.

Additionally, we reviewed documentation and observed evidence of encryption mechanisms for data in transit and at rest in the system and compared it with NIST guidance. Specifically, we reviewed the system's firewall rules that restrict insecure network traffic and use of secure cryptographic mechanisms and communication protocols. We also reviewed VA's use of encryption for data at rest and access restrictions in a key system component.

To further address identity and access management, we reviewed VA's implementation of selected requirements from Office of Management and Budget (OMB) M-22-09.[6] We selected these requirements based on their relevance to the confidentiality and integrity of data, asset and risk management, and identity and access management.

To address continuous monitoring and logging, we evaluated system documentation. Specifically, we reviewed the system's audit and accountability procedure against NIST guidance. In addition, we compared VA's implementation of a system-level continuous monitoring strategy in the system to agency risk management policy.

Further, we evaluated VA's implementation of monitoring and logging requirements from OMB M-21-31 in a key component of the system.[7] We selected these requirements because of their relation to the confidentiality and integrity of genomic data in the system. We selected the component because it is critical to the confidentiality and integrity of data in MVP. We reviewed the server's configuration baseline and compared it to OMB's monitoring and logging requirements.

[6]Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

[7]Office of Management and Budget, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (Washington, D.C.: Aug. 27, 2021).

We also determined that the control environment component of internal control was significant to this objective, along with the underlying principle that management should assign responsibility and delegate authority to achieve the entity's objectives. We assessed VA cybersecurity policy and procedures and interviewed cognizant agency officials to determine whether the agency had assigned responsibility and delegated authority for the security of veterans' health information in the system.

Additionally, we determined that the risk assessment component of internal control was significant to this objective, along with the underlying principle that management should identify, analyze, and respond to risks related to achieving the defined objectives. We assessed agency cybersecurity policy, procedure, and control implementations, and interviewed cognizant agency officials to determine whether the agency implemented processes to address risk related to the system.

We further determined that the control activities component of internal control was significant to this objective, along with the underlying principles that management should design the entity's information system and related control activities to achieve objectives and respond to risks and implement control activities through policies. We evaluated VA cybersecurity policy, procedure, and control implementations to determine whether the agency designed and implemented security controls to protect the system.

In September 2025, we reported on our results of evaluating the first three objectives.[8] In that report, we made 13 recommendations to the department to resolve shortcomings in the selected MVP system. We designated that report as "limited official use only" and did not release it to the general public because of the sensitive information it contained. In this report, we removed all references to the sensitive information that was included in our September 2025 report.

To address our fourth objective—to determine the extent of VA's actions to address the previously identified security control deficiencies and related recommendations—we examined documentation provided by VA. Specifically, for each recommendation that VA indicated it had implemented or partially implemented as of March 2026, we examined supporting documents to assess the effectiveness of the actions taken to

[8]GAO, *Privacy and Cybersecurity: VA Provides Oversight of Protected Health Information but Needs to Enhance Security Controls*, GAO-25-107381SU (Washington, D.C.: Sept. 25, 2025).

implement the recommendation and resolve the control deficiency. Based on this assessment, we categorized the status of each recommendation into one of three categories:

- **Implemented:** VA successfully completed actions to implement the recommendation.
- **Partially implemented:** VA had made progress but had not completed implementation.
- **Not implemented:** VA had not provided sufficient evidence that it had implemented the recommendation.

We conducted this performance audit from January 2024 to May 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

May 6, 2026

Ms. Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report, ***PRIVACY AND CYBERSECURITY: VA Has Made Progress Enhancing Security Controls for Protected Health Information*** (GAO-26-108651).

VA values the effort by GAO to evaluate privacy and cybersecurity protections implemented to protect the Million Veteran Program. VA takes security very seriously and works to ensure Veterans data is always protected in the continuously changing threat scenarios.

VA's technical comments on the draft report are enclosed.

Sincerely,

Curt Cashour
Chief of Staff

Enclosure

# Appendix III: GAO Contact and Staff Acknowledgments

## GAO Contact

Jennifer R. Franks, FranksJ@gao.gov

## Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: West Coile and Jeffrey Knott (Assistant Directors), Luis Alicea, James Ashley, Chris Businsky, Bill Cook (Analyst in Charge), Jonnie Genova, Shane Homick, Smith Julmisse, Koushik Nalluru, Monica Perez-Nelson, Nolan Roosa, Walter Vance, and Merry Woo.