A

U.S. Government Accountability Office

Electronic Health Records: Better Goals and Measures Would Improve Interagency Cybersecurity Collaboration

GAO-26-107673
Q&A Report to Congressional Committees
June 2, 2026
Accessible Version

Why This Matters

The federal electronic health record (EHR) system supports the delivery of healthcare to millions of beneficiaries across multiple federal agencies, including the Department of Defense (DOD) and the Department of Veterans Affairs (VA). At full deployment, the system will have more than 500,000 users providing care to over 18 million servicemembers, veterans, and their families, making it one of the nation's largest electronic health record systems.

Increasing cyberattacks in the healthcare sector put the system at high risk from threats to privacy, cybersecurity, and patient care. For example, in February 2024, a ransomware cyberattack on a health payment and commercial prescription processor disrupted healthcare services across the country. At DOD this led to delays in military pharmacies being able to process claims and fill some prescriptions. At VA, health information exchange and prescription orders were impacted, resulting in a backlog of about 1 million prescription claims.

The Further Consolidated Appropriations Act, 2024, includes a provision for us to report on aspects of the federal EHR. This report describes the federal EHR system and its management, identifies the roles and responsibilities for the cybersecurity of the system and protecting the privacy of the data within it, and examines how agencies are collaborating to keep the system and its data secure.

Key Takeaways

- The Federal Electronic Health Record Modernization office (FEHRM), a joint DOD-VA decision-making authority, is responsible for providing direction and oversight of the federal EHR, and DOD has primary responsibility for ensuring its cybersecurity.
- All four partner agencies using the federal EHR are responsible for managing their networks, following federal privacy laws related to managing health data, and alerting DOD in the event of a suspected breach.
- The FEHRM has generally facilitated collaboration among the federal partners; however, the collaboration would be improved by fully addressing leading practices.
- We recommend that DOD and VA leadership ensure that the FEHRM's efforts to coordinate cybersecurity and privacy protection are fully meeting leading interagency collaboration practices.

What is the federal electronic health record and who uses it?

The federal EHR is a single system used by federal health providers to store, share, and analyze patient care information. The system is used by DOD, VA, the United States Coast Guard, and the National Oceanic and Atmospheric Administration (NOAA).[1] These are referred to as partner agencies. DOD, Coast

Guard, and NOAA refer to the system as MHS GENESIS, while VA refers to it as the federal EHR. However, the federal EHR is the same commercial product (Oracle Health Millennium) purchased by the other agencies. We have previously reported on DOD's and VA's efforts to implement the federal EHR.[2]

DOD was the first agency to implement the system that would become the federal EHR in February 2017. DOD completed deployment of the system to all military treatment facilities in 2024, and its clinics and hospitals use the system to care for over 9 million patients worldwide.[3] Additionally, the system has been implemented at VA, Coast Guard, and NOAA health care facilities. The federal EHR currently has over 200,000 users (e.g., physicians, nurses, and other health care providers) and will have more than 500,000 users when VA completes its deployment.[4] See table 1 for details on the number of users at each agency, as of December 2025, and when the system was first implemented.

Table 1: Users and Implementation Dates of the Federal Electronic Health Record (EHR), as of December 2025

Agency	Current federal EHR users[a] (approximate)	Date of first implementation at agency
Department of Defense	191,400	February 2017
Department of Veterans Affairs	13,000[b]	October 2020
United States Coast Guard	1,000	August 2020
National Oceanic and Atmospheric Administration	18	June 2023

Source: GAO analysis of Federal Electronic Health Record Modernization office, Department of Defense, Department of Veterans Affairs, United States Coast Guard, and National Oceanic and Atmospheric Administration data. I GAO-26-107673

[a]For example, users include physicians, nurses, and other health care providers.

[b]VA plans to have 350,000 users when the system is fully deployed.

Providers at these facilities use the federal EHR to document care, view health information, and order labs, referrals, and prescriptions for patients. Additionally, providers can use the patient portal to communicate with patients. Patients can use the portal to view their health information, request appointments, and communicate with their care team.

DOD, VA, and Coast Guard connect to the federal enclave, which is the Oracle Health data center where the system resides, using a shared network environment called the Medical Community of Interest (MedCOI). NOAA accesses the system using a Citrix connection and does not connect to MedCOI. Access to the system is governed by agreements between DOD and the three partner agencies. Specifically, DOD has individual agreements with VA, NOAA, and Coast Guard, which establish responsibilities of the parties and the security requirements for connecting to the network and the federal enclave.

What is the Federal Electronic Health Record Modernization office (FEHRM)?

The FEHRM was chartered in December 2019 as the single decision-making authority and point of accountability in the delivery of a common federal EHR. The charter—which was signed by the Deputy Secretaries of Defense and Veterans Affairs—describes the FEHRM's responsibilities and the authorities of the office. The charter assigns the FEHRM decision-making authority for DOD and VA to provide unified direction on joint functions to ensure that the departments deliver an interoperable EHR system.[5] Additionally, the National Defense Authorization Act (NDAA) for Fiscal Year 2020, which was enacted in December 2019, establishes requirements and authorities of the office.[6]

According to the FEHRM charter, the office is to manage the risks and the operation of the federal enclave, and identify opportunities for efficiency, standardization, and process optimization. The charter also identifies several joint functions over which the FEHRM is to provide direction and oversight. See table 2.

Table 2: Selected Joint Functions Requiring Federal Electronic Health Record Modernization Office (FEHRM) Direction and Oversight

Function	Description
Federal enclave management	Management of the joint hosting environment housing the federal electronic health record (EHR).
Configuration management	Management of the process for making changes to the configuration of the federal EHR.
Cybersecurity	Manage the cybersecurity program including medical devices and associated interfaces consistent with cybersecurity requirements and the risk management framework.
Network security	Ensure compliance with security requirements for joint networks to protect the usability and integrity of the network and data.
Disaster recovery	Development of a joint business and technical plan for the resumption of work after man-made or natural disasters.
Access management	Development of processes, policies, and technologies to ensure proper user identity and access of providers and patients.

Source: GAO analysis of FEHRM charter. | GAO-26-107673

Leadership

The Fiscal Year 2020 NDAA requires the FEHRM to be led by a Director and Deputy Director who report to the Deputy Secretary of Defense and the Deputy Secretary of Veterans Affairs. The law also establishes the term, minimum qualifications, and appointment process for the positions and requires that a succession plan be developed. The former FEHRM Director was appointed in August 2020 and the former Deputy Director was appointed in December 2021.[7] In May 2025, FEHRM officials stated that both terms would expire in December 2025 and that a draft succession plan was under development. However, in December 2025, FEHRM officials stated that the current Director and Deputy Director would remain in their positions until a succession plan is developed and approved. They told us that the plan should be approved in 2026. In May 2026, a FEHRM official told us both positions were currently vacant and that they could not provide a timeline for when new leadership will be in place.

Funding and staffing

The Fiscal Year 2020 NDAA requires that DOD and VA assign personnel and other resources to the FEHRM. The law also requires both departments to enter into a cost-sharing agreement for operations and staffing of the office. To that end, the FEHRM charter defines shared responsibilities and funding.[8] Table 3 provides a summary of FEHRM funding by year and source. These funds were allocated towards civilian employees and Public Health Service officers' salaries; general management and administration; program management; functional community requirements; and software licenses and maintenance.

Table 3: Federal Electronic Health Record Modernization Office (FEHRM) Funding by Agency

Agency	Fiscal year 2023	Fiscal year 2024	Fiscal year 2025 (planned)	Fiscal year 2026 (requested)
Department of Defense	$20,273,000	$21,985,000	$22,993,000	$23,231,000
Department of Veterans Affairs	$30,672,000	$19,460,000	$19,890,000	$22,695,410
Total	**$50,945,000**	**$41,445,000**	**$42,883,000**	**$45,926,410**

Source: GAO Analysis of FEHRM and Department of Veterans Affairs data. I GAO-26-107673

Pursuant to the Fiscal Year 2020 NDAA and FEHRM charter, DOD and VA staff have been assigned to the FEHRM to carry out its responsibilities. Additionally, the FEHRM relies on contractors for support. Table 4 provides a count of staff (including contractor personnel) by agency.

Table 4: Federal Electronic Health Record Modernization Office (FEHRM) Staffing Counts, as of December 2025

Agency	Approximate number of full-time equivalents
Department of Defense	33
Department of Veterans Affairs	13
Contractor	95

Source: GAO Analysis of FEHRM data. I GAO-26-107673

Who is responsible for ensuring the cybersecurity of the federal EHR?

DOD has primary responsibility for ensuring the cybersecurity of the enclave, which includes protecting the personal information of millions of beneficiaries. The other partner agencies have limited cybersecurity responsibilities. These responsibilities are documented in agreements between DOD, VA, Coast Guard, and NOAA. See table 5 for more details.

Table 5: Key Federal Electronic Health Record Cybersecurity Responsibilities

Federal agency	Key responsibilities
Federal Electronic Health Record Modernization office (FEHRM)	The FEHRM is responsible for providing direction and oversight of the management of the federal enclave, cybersecurity, network security, and joint disaster recovery plans, among other things. While the FEHRM does not manage cybersecurity incidents directly, it coordinates with federal partners and facilitates shared incident response efforts.
Department of Defense (DOD)	DOD has primary responsibility for ensuring the cybersecurity of the federal electronic health record (EHR) and the network used to access it. To that end, DOD is responsible for authorizing partner agencies to access the system, conducting monitoring of the network, and maintaining the network used to access the system, among other things.
Department of Veterans Affairs (VA)	VA has responsibility for the cybersecurity of its own network. VA maintains mechanisms for information sharing with and visibility into cybersecurity measures implemented by DOD.
United States Coast Guard	Coast Guard does not have a cybersecurity role inside the federal EHR hosting environment. Cybersecurity protections are provided as a service from DOD. To that end, the memorandum of agreement between DOD and Coast Guard states that DOD will provide Coast Guard with governance, infrastructure deployment, operations and sustainment, and cybersecurity of the network used to access the federal EHR. Coast Guard is to comply with all technical and cybersecurity governance requirements communicated by DOD. Coast Guard is also responsible for configuring and securing devices that enable its use of the federal EHR and ensuring that all users have authorization and need-to-know consistent with federal requirements. Coast Guard also enforces least privilege access and physical access controls for those requiring use of the system.
National Oceanic and Atmospheric Administration (NOAA)	NOAA does not have a cybersecurity role inside the EHR hosting environment. NOAA is responsible for configuring and securing devices that enable its use of the federal EHR. NOAA is also responsible for ensuring that all users have authorization and need-to-know consistent with federal requirements. Additionally, NOAA enforces least privilege access and physical access controls for those requiring use of the system.

Source: GAO analysis of FEHRM, DOD, VA, Coast Guard, and NOAA data. I GAO-26-107673

Within DOD, several components share responsibilities for ensuring the cybersecurity of the federal EHR. These include the Defense Health Agency (DHA) Program Executive Office, Medical Systems; the Program Executive Office, Defense Healthcare Management Systems; and the DHA Cybersecurity Service Provider. Table 6 describes key federal EHR cybersecurity responsibilities of DOD components.

Table 6: Key Federal Electronic Health Record Cybersecurity Responsibilities of Department of Defense (DOD) Components

DOD component	Key responsibilities
Defense Health Agency (DHA)	• DHA is responsible for establishing and maintaining the DHA cybersecurity program that governs all DHA systems, including the Medical Community of Interest (MedCOI), which is the network used to access the federal electronic health record (EHR), and the federal EHR itself. For example, according to program officials, DHA is responsible for establishing security requirements for the federal EHR and defining compliance requirements. • Additional DHA responsibilities include reviewing and approving authorization packages for any system connecting to the federal EHR hosting environment.
DHA Cyber Operations Center	• The DHA Cyber Operations Center is responsible for consolidating oversight and coordination of cybersecurity activities to protect DHA systems including the federal EHR. To that end, the center issues cyber orders and directives on behalf of DHA. • The center also investigates incidents by collecting data in and around the affected device to determine the actor and root cause.

DOD component	Key responsibilities
DHA Program Executive Office, Medical Systems	• The Program Executive Office for Medical Systems is led by the DHA Chief Information Officer. This office is responsible for managing access to the network used to access the federal EHR and has responsibility for granting approval to partner agencies that connect to the system, on the condition that they have demonstrated compliance with DOD security standards included in agreements with vendors and partner agencies. • The Chief Information Security Officer is responsible for authorizing the use of the system and acts as the authorizing official for entities connecting to the federal EHR. The Chief Information Security Officer reports to the Chief Information Officer.
DHA Risk Management Executive Division	• The DHA Risk Management Executive Division reports to the DHA Chief Information Officer. • The division produces the final Risk Management Framework Security Authorization Package used for authorizing the operation of systems and maintains guidance for completing information system risk assessments within DHA.
Program Executive Office, Defense Healthcare Management Systems	• According to the Chief Information Security Officer, the program office is tasked with leading cybersecurity efforts for the federal EHR. • According to program officials, the office has responsibility for continuous monitoring, incident management, risk management, and system security. • The office also monitors all activities carried out by the EHR vendor to ensure compliance with standards.
DHA Cybersecurity Service Provider	• The Cybersecurity Service Provider is responsible for monitoring, detection, and incident response for the MedCOI network. For example, the provider conducts penetration testing, malware scans, and cyber environment evaluation. • The provider also controls the collection of security tools and technology that manages connections to the federal EHR hosting environment. Additionally, the provider assists the Program Executive Office, Defense Healthcare Management Systems to ensure that systems comply with cybersecurity standards.

Source: GAO analysis of DOD data. I GAO-26-107673

What responsibilities do DOD and partner agencies have for protecting the privacy of data in the federal EHR?

DOD and its partner agencies have varying responsibilities for protecting the privacy of personal and health information in the federal EHR. To that end, each agency is responsible for managing its network and following federal privacy laws related to managing health data. Additionally, each is responsible for alerting DHA in the event of a suspected breach. See table 7 for additional details.

Table 7: Key Federal Electronic Health Record Privacy Responsibilities of Participating Agencies

Agency	Key responsibilities
Federal Electronic Health Record Modernization office (FEHRM)	• According to FEHRM officials, the office plays a critical role in coordinating privacy protection efforts between agencies by ensuring that unified privacy standards and policies for the federal electronic health record (EHR) system are implemented. • Additionally, in the event of a major cybersecurity incident, the FEHRM is to facilitate cross-agency incident response protocols to ensure that federal partners can effectively collaborate during a breach.
Department of Defense (DOD)	• DOD coordinates with its partner agencies and its own components to protect the privacy of personal information by implementing interagency agreements such as memoranda of agreement and interconnection security agreements, which include responsibilities related to information sharing. • Additionally, the Defense Health Agency (DHA) is responsible for implementing agency policies to safeguard the privacy and security of personal information entrusted to DHA. It is also to ensure that adequate safeguards are maintained for all sensitive data that is maintained, received, or transmitted through its systems. • The DHA Privacy and Civil Liberties Office develops and administers policies and procedures governing the collection, maintenance, use and disclosure of personal information for DHA. The office also reviews the federal EHR Privacy Impact Assessment which documents the types of information being shared and proposed privacy controls, among other things. • In the event of a suspected breach, DHA has a dedicated team that responds to address it. The team follows a process to: (1) ensure timely notification to appropriate authorities, (2) contain the breach by limiting its impact, (3) employ mitigation tactics through communication with potentially affected entities, and (4) eradicate the cause of the breach while alleviating vulnerability to future breaches. The team then works to restore business operations.

Agency	Key responsibilities
Department of Veterans Affairs (VA)	• VA has an agreement with DOD establishing key responsibilities related to sharing personal information. Per the agreement, suspected unauthorized access to information is to be reported to the VA Privacy Office, and VA will collaborate with DOD regarding any interagency incidents that involve sensitive health information. • VA is also to comply with applicable laws and policies related to assessment and notification of a potential breach. Once a breach is determined to have occurred, VA is responsible for following relevant agreements that specify the manner, time frame, and mechanism for alerting applicable federal partners regarding the involvement of any joint data in the incident. • VA also conducts privacy reviews for the federal EHR. Additionally, VA is to track and enforce required privacy awareness training. To that end, VA officials stated that relevant staff are trained on accessing personal information and that VA has disciplinary policies in place for responding to unauthorized access.
United States Coast Guard	• According to Coast Guard officials, the agency is responsible for implementing Department of Homeland Security-directed privacy controls and roles and responsibilities documented in Department of Homeland Security policies pertaining to privacy and incident handling. • Coast Guard is also to ensure compliance with relevant privacy laws and policies and provide privacy awareness training to all personnel with access to patient information. • Coast Guard is also to treat any potential compromise of personal or sensitive information as a cybersecurity and privacy incident and initiate required reporting, notification, remediation, and mitigation activities. Additionally, it is to notify the DHA Privacy Office of a breach within 24 hours.
National Oceanic and Atmospheric Administration (NOAA)	• According to NOAA officials, NOAA does not have a direct role for ensuring the privacy of patient information inside the federal EHR. • NOAA facilitates the secure transmission of data into the federal EHR. NOAA also ensures that NOAA users have authorization and a need-to-know and that all government-furnished equipment used by providers to access the federal EHR has the appropriate configuration and controls. • In the event of a breach, NOAA would follow the Department of Commerce Breach Notification Plan. The plan provides guidance to Commerce staff on responsibilities related to reporting and investigating breaches.

Source: GAO analysis of FEHRM, DOD, VA, United States Coast Guard, and NOAA data. I GAO-26-107673

What efforts has the FEHRM undertaken to improve interagency cybersecurity and privacy collaboration?

The FEHRM has undertaken multiple efforts to improve interagency cybersecurity and privacy collaboration, and the efforts have resulted in varying levels of progress. For example, the FEHRM hosts a number of formal and informal meetings that provide opportunities for partner agencies to coordinate and agree upon system changes. Additionally, the FEHRM has initiated activities intended to enhance the security posture of the federal enclave and improve coordination across entities. While some of these efforts have been completed as intended, others remain in progress or have required alternative strategies to better support the cybersecurity of the enclave.

Meetings and exercises

The FEHRM hosts the weekly Joint Cybersecurity Team Meeting, which provides all federal partners and other stakeholders, such as contractors, a forum to discuss and track cybersecurity guidelines, requirements, best practices, and issues that impact the confidentiality, integrity, and availability of the federal enclave. The FEHRM also conducts cyber tabletop exercises with federal partners and contractors to enhance their cybersecurity posture. The FEHRM also manages the Joint Sustainment and Adoption Board, which is a joint governance body responsible for the approval of all federal EHR configuration changes, some of which could be cybersecurity or privacy related. The board is chaired by representatives from DOD and VA with Coast Guard and NOAA represented by DOD.

Joint Security Operations Center

Since 2019, when DOD and VA began working together to implement the federal EHR, the agencies planned for a joint organization responsible for EHR

cybersecurity. The FEHRM reported in public progress reports that the office had been working to create a Joint Security Operations Center. The Center was intended to bolster the resilience of the data center housing the federal EHR and facilitate cyber incident information sharing between DOD and VA. To that end, the FEHRM had developed a draft memorandum of agreement that defined proposed responsibilities for the two agencies. The original plan called for a shared physical facility where VA security personnel would be collocated with DOD staff at a DOD facility. In November 2024, FEHRM officials stated that differing personnel security requirements between DOD and VA had impeded the creation of a shared physical Joint Security Operations Center. However, the FEHRM told us that DOD and VA agreed that the objectives of the Joint Security Operations Center have been met with alternative collaboration mechanisms, as of April 2025. These include joint agreement reviews, tabletop exercises, and a near real-time data feed from the DOD security operations center to VA's security operations center.

Interagency cyber assessment

FEHRM documentation shows that, as early as October 2023, the FEHRM had planned an interagency cybersecurity assessment. The assessment was intended to integrate VA and DOD cyber teams to improve cybersecurity detection and response abilities within the federal EHR environment by allowing penetration testers to cross agency boundaries. By November 2024, however, the assessment had been indefinitely paused, with the FEHRM citing personnel security requirements and associated resource constraints as the reason for the pause. In December 2025, FEHRM officials told us that the effort was permanently suspended. However, according to the officials, the interagency cyber testing efforts were a pilot and DOD and VA conduct their own penetration testing.

Memoranda of agreement and understanding consolidation

Since 2022, the FEHRM has reported in public progress reports on its efforts to review, update, and consolidate memoranda of understanding and agreements between DOD and the partner agencies related to accessing the federal enclave. In November 2024, the FEHRM told us that working sessions had resulted in a strategy outlining procedures to review agreements. Despite taking these steps, as of May 2025, FEHRM officials had not completed this effort and expressed interest in creating a repository of interagency agreements in order to improve monitoring. In December 2025, FEHRM officials reported that the effort is ongoing and does not have an end date as they are continuously adding documents to the repository.

Joint Incident Management Framework

In 2021, the FEHRM reported in public progress reports that it had begun working on a Joint Incident Management Framework that it described as foundational to the cybersecurity posture of the federal EHR. An initial draft of the framework was developed in May 2021 and there were multiple revisions to the framework between May 2021 and November 2022. Despite those efforts, in May 2025, FEHRM officials stated that the framework was not complete; however, officials anticipated it would be completed by September 2025. In February 2026, FEHRM officials reported that the framework would be completed by April 2026. The officials also reported that when a breach happens the FEHRM works to bring all parties together through existing mechanisms such as conference calls.

How can partner agency collaboration be enhanced to protect the federal EHR?

While the FEHRM has generally facilitated joint efforts among the federal partners, collaboration could be improved by fully addressing leading practices. Our prior work has shown that implementing these collaboration practices can be effective in enhancing and sustaining federal agency coordination toward common outcomes.[9] The FEHRM's efforts to coordinate cybersecurity and privacy protection with its federal EHR partners generally aligned with five of the eight leading practices. The FEHRM's efforts partially aligned with two of the practices and did not align with one practice (see figure 1).

Figure 1: Extent to Which the Federal Electronic Health Record Modernization Office Followed Leading Interagency Collaboration Practices

Leading collaboration practice	Selected key considerations	GAO assessment
Define common outcomes	• Have the crosscutting challenges or opportunities been identified? • Have the short- and long-term outcomes been clearly defined? • Have the outcomes been reassessed and updated, as needed?	◐
Ensure accountability	• What are the ways to monitor, assess, and communicate progress toward the short- and long-term outcomes?	○
Bridge organizational cultures	• Have participating agencies established compatible policies, procedures, and other means to operate across agency boundaries?	●
Identify and sustain leadership	• Has a lead agency or individual been identified? • If leadership will be shared between one or more agencies, have roles and responsibilities been clearly identified and agreed upon? • How will leadership be sustained over the long term?	◐
Clarify roles and responsibilities	• Have the roles and responsibilities of the participants been clarified? • Has a process for making decisions been agreed upon?	●
Include relevant and diverse participants	• Have all relevant participants been included?	●
Leverage resources and information	• How will the collaboration be resourced through staffing? • How will the collaboration be resourced through funding? If interagency funding is needed, is it permitted? • Are methods, tools, or technologies to share relevant data and information being used?	●
Develop and update written guidance and agreements	• If appropriate, have agreements regarding the collaboration been documented? • Have ways to continually update or monitor written agreements been developed?	●

● = Generally aligned with leading practice ◐ = Partially aligned with leading practice ○ = Not aligned with leading practice

Sources: GAO analysis of Department of Defense, Federal Electronic Health Record Modernization office, and Department of Veterans Affairs data; warmworld/stock.adobe.com (icons). I GAO-26-107673

Define common outcomes

The FEHRM's activities partially aligned with this leading practice. Identifying challenges and defining goals toward intended results can guide actions and

allow decision-makers and stakeholders to assess performance by comparing planned and actual results. Our prior work has shown that defining common goals and outcomes and clearly articulating how the goals align with each other can help organizations illustrate and assess the contribution of individual activities toward broader outcomes.[10] FEHRM documentation defines cross-cutting challenges and opportunities. For example, the FEHRM charter describes objectives, including actively managing the risks and operation of the federal enclave, identifying standardization opportunities, and advancing interoperability. Additionally, FEHRM officials stated that they have the broad cybersecurity goals of protecting private patient information and the shared network.

Moreover, in January 2026, the FEHRM provided documentation describing goals and activities related to cybersecurity and collaboration for fiscal year 2025. For example, there was a goal to conduct joint cybersecurity tabletop exercises and to foster a joint process for mitigating risk. While the FEHRM reported that the tabletop exercise occurred and progress was made on the joint process for mitigating risk, the goals did not identify the resources, skills, or time needed.

However, the FEHRM has not fully articulated specific short- or long-term goals or intended outcomes related to the cybersecurity of the federal EHR or the privacy of health data within it. Specifically, the FEHRM told us in January 2026 that goals for fiscal year 2026 were still under development and the FEHRM did not provide information on specific, short-term or long-term planned cybersecurity or collaboration outcomes beyond the goals and activities provided for fiscal year 2025.

Without clear goals and outcomes, the FEHRM has limited insight into the specific resources, skills, or time needed to address any shared cybersecurity responsibilities. It will also not be well positioned to provide assurances to agency leadership and Congress that the health information in the federal enclave is as secure as possible. Further, progress on planned efforts, such as the Joint Incident Management Framework, may be impeded or further delayed. Implemented fully, establishing goals and outcomes could allow the FEHRM, DOD, VA, and other partner agencies to have a clearer understanding of the value of collaboration efforts and how they can help achieve secure and private health records.

Ensure accountability

The FEHRM's activities did not align with this leading practice. Ensuring accountability relies on monitoring, assessing, and communicating progress toward the short- and long-term outcomes by using performance measures. The FEHRM told us that it did not have performance measures for its fiscal year 2025 goals, and it did not have performance measures for the fiscal year 2026 goals that were reportedly under development. Since the FEHRM has not defined the planned outcomes for the current fiscal year and it did not define performance measures in the prior year, it cannot monitor progress towards achieving planned outcomes. As a result, the FEHRM may not have critical information needed to assess and communicate progress and may be at risk of failing to achieve shared cybersecurity responsibilities.

Bridge organizational cultures

The FEHRM's activities generally aligned with this leading practice. The partner agencies have in place compatible policies and procedures to operate across agency boundaries. For example, DOD and VA signed a charter establishing the FEHRM which outlined responsibilities and objectives, among other things.

Additionally, DOD and VA officials stated that they were able to collaborate to mitigate challenges associated with different personnel security requirements across agencies.

Identify and sustain leadership

The FEHRM's activities partially aligned with this leading practice. The charter signed by DOD and VA establishing the FEHRM identifies it as the lead organization for joint issues. Additionally, as previously noted, the Fiscal Year 2020 NDAA established the term, minimum qualifications, and appointment process for FEHRM leadership. The Fiscal Year 2020 NDAA also called for the creation of a leadership succession plan. As of January 2026, FEHRM officials anticipated approval of the plan in 2026. However, as of May 2026, the FEHRM Director and Deputy Director positions are vacant. Having this succession plan should improve the FEHRM's ability to maintain its efforts and provide continuity.

Clarify roles and responsibilities

The FEHRM's activities generally aligned with this leading practice. As previously mentioned, DOD and VA signed a charter to establish the FEHRM that outlined roles and responsibilities. There is also a support agreement between DOD, VA, and the FEHRM that provides additional information on roles and responsibilities. Additionally, the FEHRM has established a process for making decisions related to the system, including those related to cybersecurity issues. Partner agencies are responsible for maintaining private health data for patients within their own networks and participating in joint mechanisms for information sharing when breaches are detected.

Include relevant participants

The FEHRM's activities generally aligned with this leading practice. The FEHRM told us that all partner agencies are included in cybersecurity meetings and collaboration efforts. Additionally, no partner agencies conveyed to us any concerns about their level of involvement in cybersecurity collaboration efforts related to protecting the federal EHR.

Leverage resources and information

The FEHRM's activities generally aligned with this leading practice. Specifically, the Fiscal Year 2020 NDAA requires the Secretaries of Defense and Veterans Affairs to provide resources to the FEHRM and both have been funding and staffing it accordingly.

Develop and update written guidance and agreements

The FEHRM's activities generally aligned with this leading practice. The FEHRM has a charter that calls for re-evaluation every two years and modification as necessary. According to FEHRM officials, the charter has been reviewed and there has not been a need to update it. The charter also calls for the creation of an implementation plan to document joint functions for direction and oversight by the FEHRM. The FEHRM updated the implementation plan most recently in July 2024 and it was reviewed again in November 2025. Further, as noted above, the FEHRM stated that it is currently undertaking a review of all partner agency agreements related to the use of the federal EHR.

Conclusions

Collaboration among federal EHR partners is essential to protecting the health records of millions of beneficiaries worldwide. While the FEHRM has initiated a number of efforts to promote collaboration between DOD, VA, the Coast Guard, and NOAA and secure the network and privacy of health data in the federal enclave, it has done so without well-defined common goals and outcomes. Further, the FEHRM does not monitor, assess or communicate on performance measures to which it and the partner agencies can be held accountable. Articulating clear and measurable goals would better position the FEHRM to oversee the coordinated cybersecurity of the federal EHR by providing insight into the specific resources, skills, or time needed to address shared responsibilities. Further, these goals would help hold the FEHRM accountable for demonstrating how its activities, such as the development of the Joint Incident Management Framework, align with the common outcomes it seeks to achieve. In addition, performance measures associated with these planned outcomes would provide critical information needed to more effectively monitor, assess, and communicate the progress made on collaborating and overseeing efforts to protect the security of the system and its data. Further, addressing these practices could allow the FEHRM, partner agencies, and Congress to have greater assurance that appropriate actions are being taken to keep the system and its data secure and to prevent its exploitation by adversaries.

Recommendations for Executive Action

We are making two recommendations, one to DOD and one to VA. Specifically:

The Secretary of Defense should ensure that the Deputy Secretary of Defense directs the FEHRM to define common goals, outcomes, and associated performance measures, and monitor, assess, and communicate progress on collaboration efforts toward ensuring the cybersecurity and privacy of the federal enclave. (Recommendation 1)

The Secretary of Veterans Affairs should ensure that the Deputy Secretary of Veterans Affairs directs the FEHRM to define common goals, outcomes, and associated performance measures, and monitor, assess, and communicate progress on collaboration efforts toward ensuring the cybersecurity and privacy of the federal enclave. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD, VA, Coast Guard, and NOAA for review and comment. DOD disagreed with our report. VA neither agreed nor disagreed with the recommendations, and Coast Guard and NOAA did not provide formal comments on the report. DOD, VA, and Coast Guard also provided technical comments, which we incorporated into this report as appropriate.

In written comments, reproduced in Appendix I, DOD did not concur with the report, as written.

We stand by our findings and continue to affirm that our recommendations—which are intended to strengthen collaboration that already exists among DOD, the FEHRM, and the other partner agencies—would help the partners and Congress have greater assurance that joint actions taken to secure the system and its data not only operationalize the existing set of agreements but also produce intended results. Further, having clear goals and associated performance measures to monitor progress on collaboration efforts will ensure that all agencies that use the common EHR system continue to focus their

actions on those efforts that collectively allow them to keep their health data secure.

In written comments, reproduced in Appendix II, VA generally agreed with the findings in the report. Specifically, VA's response reiterated that initial actions have been taken to focus on building trust required for genuine collaboration with partner agencies. Further, they noted that joint readiness was tested and improved through cyber tabletop exercises and advancement of the incident management framework.

In written comments, reproduced in Appendix III, the FEHRM agreed that DOD has primary responsibility for ensuring the cybersecurity of the enclave and stated that, given the collaborative nature of the deployment effort, implementation of the report's recommendations requires concurrence from DOD and VA on the report's findings and recommendations. We agree that both DOD's and VA's support are necessary to ensure that the FEHRM is well-positioned to define common goals, outcomes, and performance measures to which it can be held accountable.

How GAO Did This Study

We focused our review on DOD and the partner agencies that were using the federal EHR as of October 2024. This included VA, Coast Guard, and NOAA. We also focused on the FEHRM, which has oversight responsibilities for the federal EHR. To describe the FEHRM's oversight responsibilities, we reviewed the December 2019 FEHRM Charter, the June 2023 FEHRM support agreement between DOD and VA, the Fiscal Year 2008 NDAA, and the Fiscal Year 2020 NDAA.[11] We also met with FEHRM officials, including the Director and Chief Technology Officer, to understand the office's cybersecurity and privacy responsibilities and the status of its cybersecurity and privacy collaboration efforts.

To describe the cybersecurity and privacy roles and responsibilities for the federal EHR, we reviewed relevant laws, interagency agreements, and agency policies. For DOD, VA, Coast Guard, and NOAA, we reviewed various interagency agreements documenting roles and responsibilities of the individual agencies, such as the DOD and VA memorandum of understanding for using MedCOI, the memorandum of agreement between the DOD and Coast Guard for implementing the Federal EHR at Coast Guard sites, and the DOD and NOAA interagency agreement establishing NOAA's use of the federal EHR. Furthermore, we reviewed relevant agency policies for cybersecurity and privacy such as DOD's privacy impact assessment policy, VA cybersecurity program guidance, the Coast Guard EHR cybersecurity plan, and the Department of Commerce breach notification plan. We also interviewed officials from DOD, VA, Coast Guard, and NOAA to discuss the agencies' cybersecurity and privacy responsibilities.

To evaluate the extent to which the FEHRM was collaborating with federal partners to ensure the cybersecurity and privacy of data within the federal EHR, we used the eight leading collaboration practices and selected key considerations identified in our prior work.[12] We then compared the FEHRM's collaboration efforts with agencies to these leading practices. We used a three-point scale to assess whether the FEHRMs efforts generally aligned, partially aligned, or were not aligned with the leading practices. For those leading practices where evidence described actions that reflected selected key considerations associated with the practice to a large or full extent, we determined the activities generally aligned with the leading practice. For those

leading practices where evidence described actions that reflected some, but not all, selected key considerations associated with the practice, we determined the activities partially aligned with the leading practice. For those leading practices where evidence demonstrated that actions did not reflect, or minimally reflected, selected key considerations associated with the practice, we determined the activities were not aligned with the leading practice.

Additionally, we reviewed annual and quarterly FEHRM public progress reports from 2020 to 2025 describing its efforts to safeguard the systems and data that comprise the Federal EHR. We also interviewed relevant officials from the FEHRM and reviewed written responses from partner agencies about cybersecurity and privacy practices and collaboration efforts.

We conducted this performance audit from June 2024 to June 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.

List of Addressees

The Honorable Mitch McConnell
Chair
The Honorable Christopher Coons
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Ken Calvert
Chairman
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Secretary of Veterans Affairs, the Secretary of Commerce, and the Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

GAO Contact Information

For more information, contact: Carol C. Harris, Director, Information Technology and Cybersecurity, HarrisCC@gao.gov.

Media Relations: Sarah Kaczmarek, Managing Director, Media@gao.gov.

Congressional Relations: David A. Powner, Acting Managing Director, CongRel@gao.gov.

Staff Acknowledgments: Jennifer Stavros-Turner (Assistant Director), Thomas Murphy (Analyst in Charge), Prisca Anyiam, Donna Epler, Sarah Glenn, Anthony Gray, Jess Lionne, Philip Menchaca, and Sarah Veale.

Visit GAO on the web at https://www.gao.gov.

Appendix I: Comments from the Department of Defense

DEFENSE HEALTHCARE MANAGEMENT SYSTEMS
PROGRAM EXECUTIVE OFFICE
1700 NORTH MOORE STREET, ROSSLYN, VIRGINIA, 22209

April 24, 2026

Ms. Carol Harris
Director, Information Technology Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Ms. Harris,

Thank you for the opportunity to review the Government Accountability Office (GAO) Draft Report GAO-26-107673, titled "ELECTRONIC HEALTH RECORDS: Better Goals and Measures Would Improve Interagency Cybersecurity Collaboration," dated March 23, 2026 (GAO Code 107673). I non-concur on this report, as written. The report was reviewed by my office, the Defense Health Agency (J6/Chief Information Officer), and the Federal Electronic Health Record Modernization office, comments are enclosed. My point of contact for this matter is Ms. Karla Carnemark, who may be reached at 703-969-1762 or karla.g.carnemark.civ@health.mil.

Sincerely,

PERKINS.JAMES.A.1162254312 Digitally signed by PERKINS.JAMES.A.1162254312 Date: 2026.04.24 10:43:22 -04'00'

James A. Perkins
Acting Program Executive Officer
Defense Healthcare Management Systems

Enclosure:
As stated

Appendix II: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

May 4, 2026

Ms. Carol C. Harris
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***ELECTRONIC HEALTH RECORDS: Better Goals and Measures Would Improve Interagency Cybersecurity Collaboration*** (GAO-26-107673).

The enclosure contains general and technical comments to the draft report. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Curt Cashour
Chief of Staff

Enclosure

Attachment

The Department of Veterans Affairs (VA) Response to the
Government Accountability Office (GAO) Draft Report
Electronic Health Records: Better Goals and Measures Would Improve Interagency Cybersecurity Collaboration
(GAO-26-107673)

General Comments:

The Federal Electronic Health Record Modernization (FEHRM) program office thanks the GAO for its professional engagement and its work to strengthen the cybersecurity of this vital national asset.

Regarding the report's findings, VA's initial focus was to establish a unified culture and build the trust required for genuine collaboration with our partner agencies. VA believes this foundational work was the essential first step. VA's success in this area is demonstrated by concrete outcomes, including the harmonization of interagency security agreements and the joint analysis of national cybersecurity frameworks, like Trusted Exchange Framework and Common Agreement. Furthermore, our joint readiness was tested and improved through cyber tabletop exercises and the continuous advancement of our incident management framework.

VA agrees the Department of War (DoW) has primary responsibility for ensuring the cybersecurity of the enclave, which includes protecting the personal information of millions of beneficiaries.

Given the collaborative nature of the deployment effort, implementation of the report's recommendations by the FEHRM requires concurrence from both DoW and VA.

The FEHRM is fully committed to the security of the Federal EHR and to continuous improvement. VA thanks the GAO for its diligent work, which reinforces our strategic direction.

Appendix III: Comments from the Federal Electronic Health Record Modernization office

Better Goals and Measures Would Improve Interagency Cybersecurity Collaboration

Draft Report GAO-26-107673

FEHRM Response:

The Federal Electronic Health Record Modernization (FEHRM) program office thanks the Government Accountability Office (GAO) for its professional engagement and its work to strengthen the cybersecurity of this vital national asset.

Regarding the report's findings, our initial focus was to establish a unified culture and the trust required for genuine collaboration between our partner agencies. We believe this foundational work was the essential first step. Its success is demonstrated by concrete outcomes, including the harmonization of interagency security agreements and the joint analysis of national cybersecurity frameworks like Trusted Exchange Framework and Common Agreement. Furthermore, our joint readiness has been actively tested and improved through cyber tabletop exercises and the continuous advancement of our incident management framework.

We agree as stated on page 4 of draft report, that DOD has primary responsibility for ensuring the cybersecurity of the enclave, which includes protecting the personal information of millions of beneficiaries.

Given the collaborative nature of the deployment effort, implementation of the report's recommendations by the FEHRM requires concurrence from both DOD and VA on the report's findings and recommendations.

The FEHRM is fully committed to the security of the federal EHR and to continuous improvement. We thank the GAO for its diligent work, which reinforces our strategic direction.

Endnotes

[1]In addition to DOD, VA, Coast Guard, and NOAA, there are plans to deploy the system to the Armed Forces Retirement Home.

[2]GAO, *Electronic Health Records: DOD Has Made Progress in Implementing a New System, but Challenges Persist*, GAO-21-571 (Washington, D.C.: Sept. 20, 2021); *Electronic Health Records: Additional DOD Actions Could Improve Cost and Schedule Estimating for New System*, GAO-22-104521 (Washington, D.C.: June 8, 2022); *Electronic Health Records: VA Needs to Address Management Challenges with New System*, GAO-23-106731 (Washington, D.C.: May 18, 2023); *Electronic Health Records: DOD Has Deployed New System but Challenges Remain*, GAO-24-106187 (Washington, D.C.: Apr. 18, 2024); and *Electronic Health Records: VA Making Incremental Improvements in New System but Needs Updated Cost Estimate and Schedule*, GAO-25-106874 (Washington, D.C.: Mar. 12, 2025).

[3]The federal EHR is used at fixed military treatment facilities and not in deployed or in-theatre locations. These capabilities are being managed by the Joint Operational Medicine Information Systems program management office. The office's mission is to provide interoperable medical information technology capabilities across the full range of military operations.

[4]VA currently plans to accelerate deployments to complete approximately 170 sites by 2031. According to VA officials, VA will have more than 350,000 users of the federal EHR at full deployment.

[5]Interoperability refers to the ability to exchange and use electronic health information.

[6]National Defense Authorization Act (NDAA) for Fiscal Year 2020, Pub. L. No. 116-92, § 715, 133 Stat. 1198, 1446 (2019). The Fiscal Year 2020 NDAA revised the requirements for the interagency program office established in the Fiscal Year 2008 NDAA. Pub. L. No. 110-181, § 1635, 122 Stat. 3, 460 (2008).

[7]The former Director and initial Deputy Director were appointed in August 2020 to four-year terms. The initial Deputy Director departed before the end of the term and the former Deputy Director was appointed in December 2021 to a 4-year term. According to FEHRM officials, the DOD and VA Deputy Secretaries agreed to align the Director and Deputy Director's terms to end in December 2025.

[8]The charter states that each department is responsible for all expenses of its respective personnel and contracts. Other administrative expenses are to be shared equitably or as otherwise agreed by the departments.

[9]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

[10]GAO, *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts*, GAO-23-105460 (Washington, D.C.: July 12, 2023) and GAO-23-105520.

[11]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 715, 133 Stat. 1198, 1446 (2019). National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-181, § 1635, 122 Stat. 3, 460-463 (2008).

[12]GAO-23-105520. We selected key considerations that were most relevant to the FEHRM's collaboration efforts.