



October 2026

SERVICE MEMBER RECORDS

DOD Needs to Address Improper and Delayed Releasing of Personnel and Health Information

DOD Needs to Address Improper and Delayed Releasing of Personnel and Health Information

GAO-27-107784

October 2026

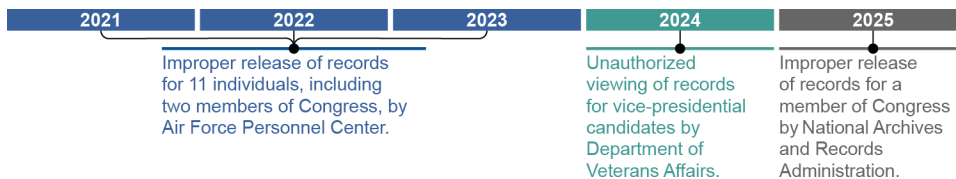
A report to the Committee on Armed Services, House of Representatives

Contact: Kristy Williams at williamsk@gao.gov

What GAO Found

Service members can accrue a large volume of personnel and health records during their military careers. The custodians of these records are the Department of Defense (DOD) and the Department of Veterans Affairs. DOD and the military services developed policies and procedures to properly adhere to federal laws for safeguarding records and timely processing records requests. However, the risk of breaches and delays exists. For example, GAO covertly tested 26 requests for records from DOD; of the 18 processed requests, one was improperly released and did not redact personally identifiable information.

Examples of Breaches of Military Records Among Record Custodians



Source: GAO analysis of Department of Defense, Department of Veterans Affairs, and National Archives and Records Administration information. | GAO-27-107784

Personnel records. The military services have procedures intended to safeguard records, such as redacting personally identifiable information. However, of the thousands of requests received during fiscal years 2021 through 2025, the services reported 49 breaches. The Freedom of Information Act (FOIA) requires agencies to respond to requests within 20 business days, and Privacy Act requests are generally processed within 20 business days. According to military service officials, staffing limitations across the military services contribute to challenges with the proper and timely processing of records requests. For example, during the time of GAO's review, the Navy had one employee processing FOIA requests, which officials stated contributed to an increased average processing time from 1.6 to 55.5 days. With a clearer understanding of the staffing levels needed to manage the volume and complexity of FOIA and Privacy Act requests, DOD and the services would be better prepared to improve response time, reduce the improper release of information, and minimize exposure to litigation costs.

Health records. GAO found that the Defense Health Agency (DHA) relies on a complex record processing system to access service member health records, which leads to challenges in processing requests. Request processors identify health records among multiple data systems and review them to redact personally identifiable information. DHA officials stated that system issues and complex workflows challenged request processing. Multiple officials stated that the redaction process can be the most cumbersome part of fulfilling requests, particularly if the record is large or contains scanned documents. GAO previously reported that DOD determined the multiple legacy electronic health record systems that it implemented over the past 3 decades to manage patient health information required modernization, and that DOD sought to replace these legacy systems with a comprehensive electronic health record system. However, DOD has not assessed the current framework and systems for processing health records requests to identify opportunities to streamline them.

Why GAO Did This Study

Accessing military service records can be complex, due partly to the number of entities involved in creating, retrieving, and maintaining this information. FOIA entitles the public to request access to federal agency records, while the Privacy Act of 1974 governs how personally identifiable information is released. The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards for safeguarding protected health information.

House Report 118-125, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2024, includes a provision for GAO to review DOD's release of service member records pursuant to FOIA or other requests. This report examines the extent to which DOD has established policies and procedures and has taken steps to address any challenges in the proper and timely release of service members' personnel and health records.

GAO reviewed relevant laws and DOD policies and processes governing the release of service member records. GAO also reviewed data on records requests and breaches; interviewed relevant officials; visited all four military services' personnel centers and selected military medical treatment facilities; and conducted a covert test of internal controls to protect personnel records for 26 records requests.

What GAO Recommends

GAO is making five recommendations, including that DOD conduct a workforce planning analysis to ensure staffing levels align with current and projected requests for processing personnel records, and identify opportunities to streamline systems used for processing health record requests. DOD generally concurred with the recommendations.

Contents

Letter		1
	Background	4
	Military Services Have Policies and Procedures for Processing Personnel Records, but Staffing Gaps Contribute to Challenges with Proper and Timely Records Release	8
	DOD Has Established Policies and Processes for Service Member Health Records but Has Not Fully Addressed Challenges with Their Proper and Timely Release	21
	Conclusions	30
	Recommendations for Executive Action	30
	Agency Comments	31
Appendix I	Objectives, Scope, and Methodology	34
Appendix II	Comments from the Department of Defense	40
Appendix III	GAO Contact and Staff Acknowledgments	42
Related GAO Products		43
Tables		
	Table 1: Known Personally Identifiable Information Breaches at Personnel Centers, by Military Service, Fiscal Years 2021–2025	10
	Table 2: Reported Freedom of Information Act (FOIA) Requests for Service Member Personnel Records, by Military Service, Fiscal Years 2020–2025	13
	Table 3: Reported Privacy Act Requests for Service Member Personnel Records, by Military Service, Fiscal Years 2020–2025	14
	Table 4: Defense Health Agency’s Data Systems Used for Health Records Processing	24
	Table 5: DOD and Non-DOD Locations Visited or Contacted by GAO	35

Figures

Figure 1: Military Services' Process for Releasing Service Member Personnel Records	9
Figure 2: Approval or Denial Results of GAO Nongeneralizable Testing of Third-Party Requests for Service Member Personnel Records	12
Figure 3: Processing Timeliness Results of GAO's Nongeneralizable Testing of Third-Party Requests for Service Member Personnel Records	16
Figure 4: Defense Health Agency's Health Records Request Processing	23

Abbreviations

DHA	Defense Health Agency
DOD	Department of Defense
FOIA	Freedom of Information Act
HIPAA	Health Insurance Portability and Accountability Act
medical facilities	military medical treatment facilities
National Archives	National Archives and Records Administration
OMB	Office of Management and Budget
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



October 16, 2026

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

During their military careers, service members can accrue a large volume of personnel-related records, including performance records, health records, and training records. Many of these records contain sensitive information that requires proper safeguarding. A service member's personnel and health records can be requested by either the service member or by a third party for a variety of reasons, such as for background investigations and medical history for treatment purposes such as medical referrals. Accessing military service records can be a complex process, due in part to the number of entities involved in creating, retrieving, and maintaining the information. Depending on the status of a service member (i.e., active, separated, or retired), the entities retaining the records vary. The custodians of service member records include the Department of Defense (DOD), military services, Department of Veterans Affairs (VA), and National Archives and Records Administration (National Archives), as well as the military medical treatment facilities (medical facilities).¹ According to DOD, as an originator of service member records, the department must balance privacy with access when responding to record requests. Without the service member's consent, the release of personal information should be limited. The Freedom of Information Act (FOIA) establishes the framework for requesting documents from the federal executive branch, including service members' records.²

¹The National Archives is a government agency that preserves and provides access to the nation's historical records, documents, and materials from all three branches of government. It is the official recordkeeper for the U.S. federal government, safeguarding such documents as the U.S. Constitution; presidential papers for legal, historical, and genealogical research; and military service records.

²FOIA applies to all federal executive branch agency records, while the Privacy Act only applies to records kept on individuals by the federal government. Any member of the public can submit a FOIA request, but generally only the individual or their authorized representative can request records under the Privacy Act.

Despite safeguards established to protect the security and privacy of service members' records, there have been reported instances of records being improperly released (officially described as a breach).³ For example, after being informed of an improper release of military records in October 2022, the Air Force Personnel Center initiated an audit of third-party requests processed during calendar years 2021 through 2023. This audit revealed that the military records of 11 individuals, including two members of Congress and several congressional candidates, were released without proper authority. This improper release involved particularly sensitive information, some of which was related to a sexual assault. Additionally, in 2024, VA employees allegedly viewed the health records of vice-presidential candidates without proper authorization. More recently, in June 2025, an entity of the National Archives, the National Personnel Records Center, had an improper release of information for a member of Congress.⁴ While only information releasable to the public under FOIA should have been provided, the veteran's comprehensive record, including personal information such as social security number and date of birth, was released.

We have previously reported on the challenges federal agencies face in addressing backlogs of FOIA requests, such as the complexity of requests, staffing challenges, and increased litigation.⁵ In 2024, we made recommendations to the Department of Justice aimed at specifying the elements to be included in backlog reduction plans and enhancing data reliability, which have since been implemented. In 2022, we reported on challenges federal agencies faced in implementing their privacy programs, including the hiring and retention of privacy personnel and

³DOD defines a breach as: "Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected. Such incidents also are known as breaches." Department of Defense Directive 5400.11-R, Department of Defense Privacy Program (May 14, 2007).

⁴The National Personnel Records Center is one of the National Archives' largest operations. It is the central repository for the nation's military and civil service personnel records.

⁵In this 2024 report, we state that generally, a request is considered backlogged if it is pending beyond the statutory time frames. *Freedom of Information Act: Additional Guidance and Reliable Data Can Help Address Agency Backlogs*, [GAO-24-106535](#) (Washington, D.C.: Mar. 7, 2024).

training for privacy professionals.⁶ Among the recommendations was one directed to DOD to establish a time frame for fully defining a process to ensure the involvement of senior privacy officials in assessing and addressing hiring, training, and professional development needs regarding privacy. In response, DOD officials stated that they had drafted an update to the policy that assigns responsibility for hiring, training, and professional development of privacy staff to the Senior Component Officials for Privacy. However, as of October 2026, this policy had not been finalized. According to an OSD official, implementation of actions in response to the recommendation has been delayed due to administrative procedures and organizational realignments. An official noted that the department expects the policy to be finalized by March 2027.

House Report 118-125, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2024, includes a provision for us to review DOD's release of service member records pursuant to FOIA or other requests.⁷ This report examines the extent to which DOD has established policies and processes and has taken steps to address any challenges in the proper and timely release of service members' (1) personnel records and (2) health records.

For both objectives, we reviewed relevant laws and DOD policies and processes regarding the release of service member personnel and health records to third parties, including data available on completed requests for records and breach reports reported by the services for fiscal years 2015 through 2025, which was most current at the time of the review. While we were not able to verify the reliability of all FOIA and Privacy Act data reported by the military services, we are reporting them because they are the best available data and are reported to DOD.

We also interviewed relevant officials from DOD, VA, National Archives, and the military services concerning the implementation of policies and laws for the release of personnel and health records. We conducted interviews with each of the military services' personnel centers and selected four medical facilities in proximity to the personnel centers to interview officials concerning their role in releasing the service members' military health records. We also conducted a nongeneralizable testing of third-party personnel records requests processed by each of the military

⁶*Privacy: Dedicated Leadership Can Improve Programs and Address Challenges*, GAO-22-105065 (Washington, D.C.: Sept. 22, 2022).

⁷H.R. Rep. No. 118-125, at 137 (2023).

services. Posing as a nongovernmental third-party requester, we submitted 26 FOIA and Privacy Act requests to each of the military services that, in some instances, contained flaws to assess if service member records were approved or denied in accordance with applicable laws and policies, as well as the timeliness of these decisions. See appendix I for more details on our scope and methodology and the related GAO products section for relevant work in the area.

We conducted this performance audit from August 2024 to October 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. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Background

Federal Law and Guidance Regarding Service Member Records

Federal law establishes the framework for both governing access to and safeguarding service members' personnel and health records.

FOIA entitles the public to request access to federal agency records, subject to nine statutory exemptions.⁸ FOIA generally requires agencies to respond to requests within 20 business days. As required of all federal agencies, DOD must

- determine the scope of records to be released;
- identify any exemptions applied to withheld information, such as classified national defense information or information prohibited from disclosure by another federal law; and
- provide responsive records promptly.⁹

⁸5 U.S.C. § 552. Agencies may withhold information if it falls under the following nine categories: (1) classified information, (2) internal personnel rules, (3) exempted by other statutes (4) trade secrets, (5) privileged communications, (6) personal privacy, (7) law enforcement records, (8) financial institutions, and (9) geological information. For details regarding these exceptions, see § 552(b).

⁹5 U.S.C. § 552.

When an agency denies a request, it must notify the requester of the reasons for denial and inform them of their right to appeal the decision.

The Privacy Act of 1974 establishes the legal framework for federal agencies to collect, maintain, use, and disseminate an individual's personally identifiable information.¹⁰ Unless a statutory exception applies, the law limits disclosure of records without the individual's consent, such as a disclosure required under FOIA or a court order, and requires agencies to maintain records that are relevant, accurate, timely, and complete. The Privacy Act also entitles individuals to procedural rights regarding their personal data, including access to records, amendment of records, and accounting of disclosures.

Under HIPAA and its implementing regulations, health-related records are subject to additional requirements. HIPAA provides national standards for safeguarding protected health information and regulates the use and disclosure of such information by covered entities, such as medical facilities.¹¹ HIPAA's requirements align and work in conjunction with the Privacy Act and other DOD-specific authorities.¹²

Roles and Responsibilities

The Office of the Director of Administration and Management, as the Oversight and Compliance Directorate; the military services; and the Defense Health Agency (DHA) all have responsibilities for managing and safeguarding service members' personnel and health records during

¹⁰Privacy Act of 1974, Pub. L. No. 93-579 (1974) (codified as amended at 5 U.S.C. §552a). The Office of Management and Budget (OMB) defines personally identifiable information as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017). OMB Circular No. A-130, serves as a policy guide for federal agencies to implement the Privacy Act of 1974. OMB Circular No. A-130, *Managing Information as a Strategic Resource*, 81 Fed. Reg. 49,689 (revised on July 28, 2016).

¹¹Protected health information is individually identifiable health information, including demographic information, that is created or received by a health care provider, health plan, employer, or health care clearinghouse, related to the (1) past, present, or future physical or mental health conditions, (2) provision of health care to an individual or (3) past, present, or future payment for the provision of health care. Pub. L. No. 104-191, (1996) (codified as amended at 42 U.S.C. § 1320d).

¹²DOD 5400.11-R. Department of Defense Instruction 5400.11, *DOD Privacy and Civil Liberties Programs* (Jan. 29, 2019) (incorporating change 1, effective Dec. 8, 2020); and Department of Defense Manual 5400.07, *DOD Freedom of Information Act (FOIA) Program* (Jan. 25, 2017).

active service. These entities are also responsible for ensuring compliance with FOIA, the Privacy Act, HIPAA, and applicable DOD policies when responding to records requests. The Oversight and Compliance Directorate and DHA provide overarching oversight of the compliance with the guidance issued to safeguard service member records and properly process records requests.

Multiple entities process requests for personnel and health records, depending on the type and age of the records and on the service member's status. These entities include the military services, medical facilities, VA, and the National Archives. Specifically:

- The military services are responsible for establishing procedures for maintaining, accessing, and releasing personnel records throughout a service member's period of service. Specifically, the military services must follow implementing guidance that provides further detail on the proper release of records, including procedures for processing requests and actions required in the event of a breach involving personally identifiable information. Each military service relies on its personnel center to process personnel records requests, and each personnel center has established standard operating procedures or guidebooks to assist staff in processing incoming requests.¹³
- Medical facilities process health records for over 700 medical facilities. These facilities are centrally managed by DHA, and the officials are responsible for implementing DHA guidance to process records requests instead of the military service where the facility is based.
- VA assumes responsibility for certain personnel and health records after service members separate or retire, particularly those records used to support veterans' benefits and health care.
- National Archives is responsible for preserving military personnel records and, up until 1992, medical records that have been transferred to archival custody for long term preservation, typically 62 years after a service member's separation.

¹³There is a personnel center designated for four of the military services—Army, Navy, Marine Corps, and Air Force. Space Force personnel records are processed at the Air Force personnel center.

Overview of DOD's Record Release Policies and Processes

DOD's authority to release records varies based on the requester. First-party requests are submitted by the service member or an authorized legal representative. Third-party requests, such as those from spouses, dependents, employers, attorneys, or insurance companies, are subject to additional restrictions and generally require written consent or another legal basis for disclosure. Access to service member personnel records is governed primarily by FOIA and the Privacy Act, as implemented through DOD-wide regulations and military service-specific policies. These laws and guidance are implemented across all DOD components. Specifically, DOD's guidance defines roles and responsibilities for releasing personnel records and requires DOD components, including the military services, to identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to manage privacy risks and ensure compliance with privacy requirements.¹⁴

Personnel records. DOD's FOIA program is governed by DOD Manual 5400.07, which establishes uniform procedures for processing FOIA requests, applying exemptions, conducting consultations and referrals, and responding to appeals.¹⁵ The guidance also assigns responsibilities to DOD components and requires FOIA offices to document determinations and ensure timely communication with requesters.

DOD implements the Privacy Act through DOD Manuals 5400.11-R and 5400.11, volume 2, which establish policies and procedures for maintaining systems of record for processing first- and third-party requests.¹⁶ Under DOD guidance, third-party requests generally require the written consent of the individual to whom the records pertain, unless disclosure is authorized under a Privacy Act exception, such as routine use or a law enforcement request. DOD components are required to verify requester identity, review consent documentation, and ensure disclosures are limited to the minimum necessary information.

Health records. Access to health records is governed primarily by HIPAA and the Privacy Act, along with DOD, DHA, and military service policies. These authorities define the conditions under which protected health

¹⁴DOD Instruction 5400.11; DOD Manual 5400.07; and DOD Manual 5400.11-R.

¹⁵DOD Manual 5400.07.

¹⁶DOD Manual 5400.11-R; DOD Manual 5400.11, vol. 2.

information may be accessed or disclosed and the responsibilities of entities that maintain such records.

Military Services Have Policies and Procedures for Processing Personnel Records, but Staffing Gaps Contribute to Challenges with Proper and Timely Records Release

The military services have established policies and procedures—such as training employees in properly processing records, verifying signatures, requesting identification, and requiring multiple levels of review—to safeguard the processing of personnel records. However, our nongeneralizable testing of third-party personnel records requests to the services demonstrated improper release of records and processing delays. Furthermore, the military services have experienced increases in the volume and complexity of requests and face challenges ensuring the proper and timely processing of records with the limited staff available to complete these tasks.

Military Services Have Policies and Procedures for Properly Processing Record Requests but Experience Breaches as Confirmed by Our Testing

The military services have established policies and procedures to properly release service member records. Properly releasing records includes ensuring that safeguards exist to protect personally identifiable information and unauthorized releases. Accordingly, these policies and procedures are intended to ensure information is appropriately safeguarded and released without impediments and include training on laws and guidance related to records releases. For instance, the Army's FOIA guidance outlines specific objectives—such as familiarizing personnel with requirements of FOIA and its implementation specified in the law, DOD guidance, and Army guidance—and advising personnel on noncompliance with FOIA and the consequences.¹⁷ Similarly, the Army's Privacy Act guidance outlines responsibilities; insight on handling and safeguarding personally identifiable information; and training requirements, including annual and specialized courses.¹⁸

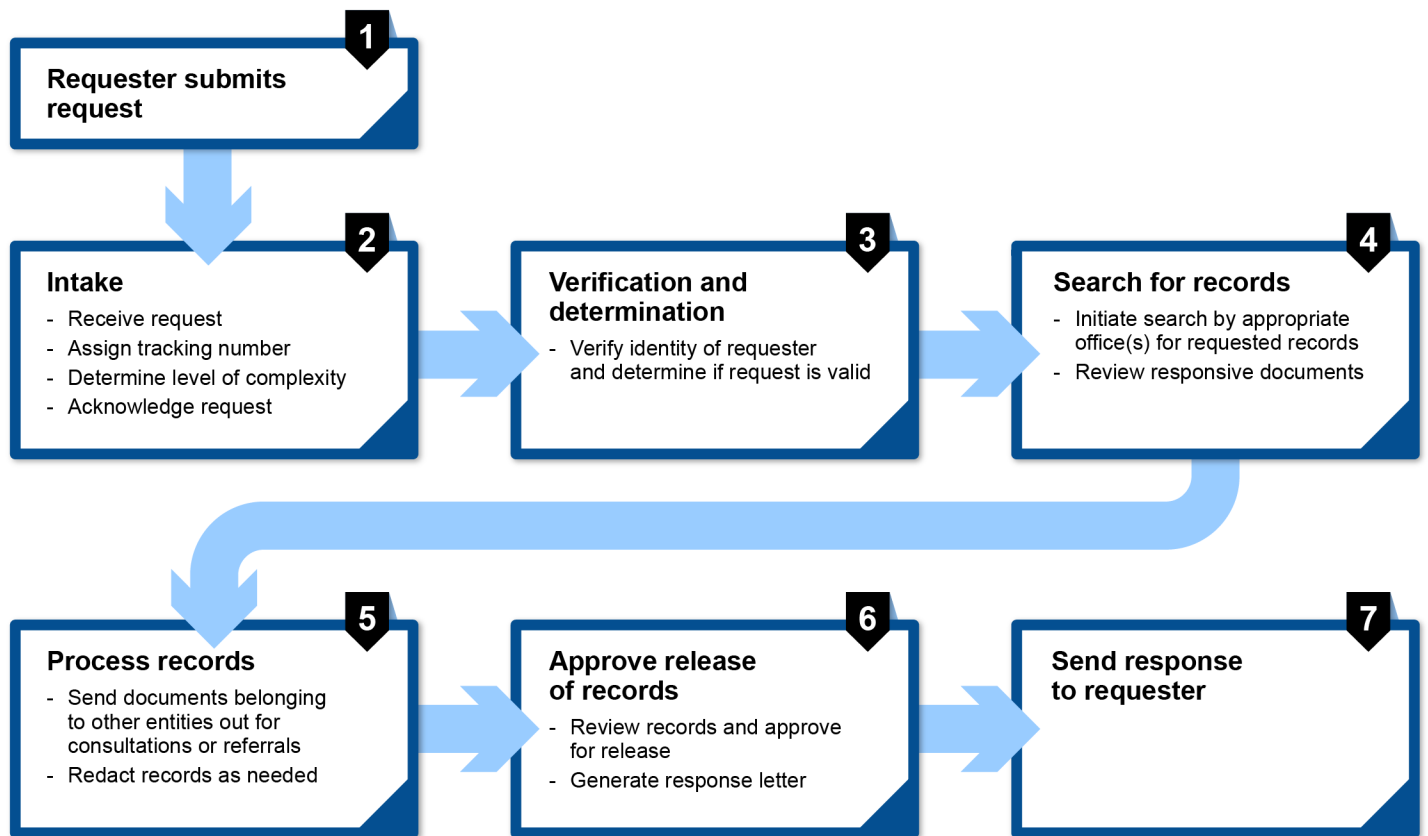
While the military services each have their own specific steps in releasing service member personnel records, the overall processing of records to be released at the Army, Navy, Marine Corps, and Air Force personnel

¹⁷Army Regulation 25-55, *The Department of the Army Freedom of Information Act Program* (Oct. 19, 2020).

¹⁸Army Regulation 25-22, *The Army Privacy and Civil Liberties Program* (Sept. 30, 2022).

centers can be summarized in seven steps. See figure 1 for an illustration of the process.

Figure 1: Military Services' Process for Releasing Service Member Personnel Records



Source: GAO analysis of Department of Defense information. | GAO-27-107784

Despite establishing procedures intended to properly process records, such as ensuring that information is released to the appropriate parties and properly redacting information, the services have reported breaches. According to military service officials, there are several ways that breaches can occur. For example, breaches may occur by failing to verify a service member's signature, inadequately confirming third-party authorization, or releasing records to the wrong individual. Information that can be improperly released includes information that was not authorized for disclosure, such as personally identifiable information (e.g., social security number or home address), reference to another service member's name or information, or disciplinary actions.

During fiscal years 2021 through 2025, the military services' personnel centers processed over 390,000 FOIA and Privacy Act requests. During this same time frame, the personnel centers collectively reported 49 breaches involving the improper release of personally identifiable information (see table 1).¹⁹

Table 1: Known Personally Identifiable Information Breaches at Personnel Centers, by Military Service, Fiscal Years 2021–2025

Service	2021	2022	2023	2024	2025	Total
Army	—	1	2	3	2	8
Navy ^a	—	—	10	5	2	17
Marine Corps	—	—	—	—	—	0
Air Force ^b	2	9	6	3	4	24
Total	2	10	18	11	8	49

Source: GAO analysis of Defense Privacy Information Management System data. | GAO-27-107784

Notes: Breach data provided are designated as potential or confirmed breaches. No data were reported for the years without an entry.

^aWhile Oversight and Compliance Directorate officials provide the data, Navy officials stated that 15 of the 17 breaches that occurred at the personnel center included unauthorized releasing of personally identifiable information but were not a result of a breach due to the processing of a records request. Rather, the breaches included the unauthorized release of information through unsecure email.

^bAccording to officials, Space Force data are included in Air Force data.

These breaches affected more than 1,000 service members. However, because officials said breaches are self-reported by the military service officials, these figures may understate the actual number of incidents.

Although reported breaches account for a small fraction of the number of requests processed, the implications of the improper release of personally identifiable information are far reaching. A single breach may include the unauthorized release of multiple service members' personally identifiable information, and this protected information can be used for nefarious purposes. In cases where a breach has occurred due to human error, each military service may ensure staff involved is retrained to ensure an understanding of existing policies and procedures related to records release. Additionally, after the Air Force's breach of 11 individuals, including two members of Congress and several congressional

¹⁹We did not assess the individual risk level associated with each of the 49 breaches, though the risk levels can vary. According to a DOD official, over 90 percent of these incidents were low-risk administrative errors.

candidates, the service added an additional reviewer to ensure that information provided to requesters included the appropriate redactions.

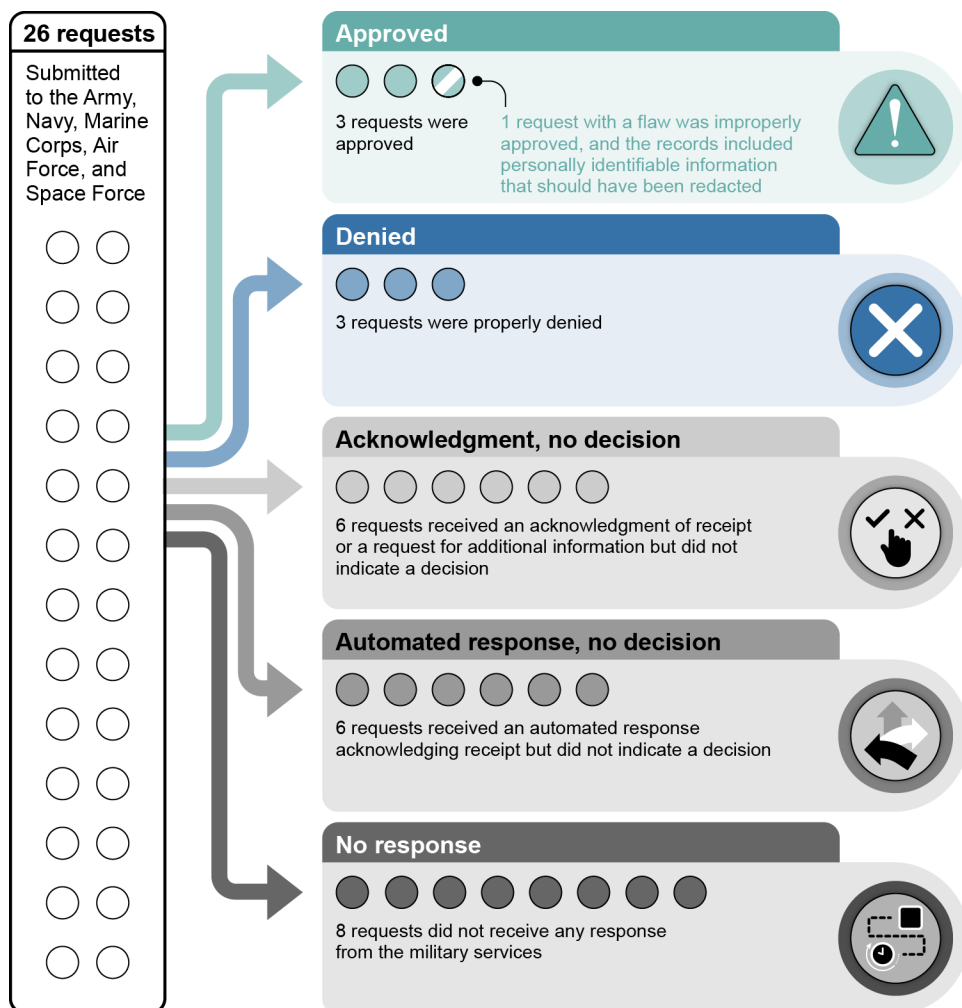
According to our review of data from the Defense Privacy Information Management System, Oversight and Compliance Directorate's system for capturing breach data, most breaches occur due to human error. Of the 49 reported breaches that occurred during fiscal years 2021 through 2025, 44 of the breaches listed in the data cited failure to adhere to policy or human error as the cause of the breach. Officials we interviewed also noted that record reviews and redactions are performed manually without an automated program to search and remove information not authorized for disclosure. Further, manually reviewing large files with numerous pages related to many years of service increases the risk that sensitive information not authorized for disclosure may be overlooked and improperly released.

To determine if requests for service member records were approved or denied in accordance with applicable laws and policies, we conducted a nongeneralizable testing of third-party personnel records requests processing by the services. Posing as a fictitious individual, (e.g., a private attorney), we sent 26 requests for personnel records to the five military services. Submitted forms intentionally contained flaws we were told were used as methods for validating requests. The incorrect or missing information should have led to the denial or request for additional information. Further, if a request was approved, we observed the extent to which personally identifiable information was properly redacted.

In response to our submissions, three requests were approved by the services; we received the requested information about service members. Two of these were FOIA requests that did not contain flaws, and their approval by the Marine Corps was appropriate. The other approval was by the Army in response to a submission that intentionally contained missing details and should have led the Army to request that we provide the missing information or to deny our request. Furthermore, the Army provided us with personally identifiable information that should have been redacted.

We also received three denials due to deliberate flaws in our requests, and for the remaining 20 of 26 requests, we either received a response with no decision or no response. We also used this testing to assess timeliness of record request processing, as discussed below (see figure 2).

Figure 2: Approval or Denial Results of GAO Nongeneralizable Testing of Third-Party Requests for Service Member Personnel Records



Source: GAO analysis of Department of Defense Information; and GAO (icons). | GAO-27-107784

Volume and Complexity of Requests Contribute to Processing Delays and Reported Backlogs, as Confirmed by Our Testing

The military services have processes in place to complete service member requests for records, but according to service officials, the amount of incoming requests, type of requests, and size of service member records can affect the processing time and result in backlogs of requests not fully processed. FOIA requires agencies to respond to requests within 20 business days, and according to service center officials, the general processing practice for responses to Privacy Act requests is within 20 business days. As of July 2025, the military services'

personnel centers reported having received 20,452 FOIA requests for fiscal years 2020 through 2025 and having processed 19,545 of those requests.²⁰ The personnel centers also reported a combined backlog of 508 FOIA requests not processed. See table 2 for service-reported data for FOIA requests received, requests processed, and backlogs reported.

Table 2: Reported Freedom of Information Act (FOIA) Requests for Service Member Personnel Records, by Military Service, Fiscal Years 2020–2025

Service	Fiscal year	FOIA requests received	FOIA requests processed	Backlogs reported
Army	2020	1,932	1,967	0
	2021	1,969	1,908	0
	2022	2,250	2,288	0
	2023	2,224	2,182	14
	2024	1,900	1,846	68
	2025	1594	1447	96
Navy	2020	665	668	0
	2021	580	547	0
	2022	534	514	0
	2023	685	641	0
	2024	897	709	19
	2025	935	622	-
Marine Corps	2020	91	91	0
	2021	64	64	0
	2022	98	98	0
	2023	206	206	0
	2024	791	788	3
	2025	861	857	4
Air Force ^a	2020	294	294	0
	2021	350	350	1
	2022	375	375	0
	2023	413	408	6
	2024	378	369	14
	2025	366	306	**

²⁰We were not able to verify the reliability of all FOIA and Privacy Act data reported by the military services. We are reporting these data because they are the best available and were reported to DOD by the military services. Additionally, at the time of our review, we requested fiscal year 2025 data from the services, but they were unable to provide the data. For more details about data reliability and limitations, see appendix I.

Service	Fiscal year	FOIA requests received	FOIA requests processed	Backlogs reported
Total	—	20,452	19,545	

Source: GAO analysis of Military Service provided data. | GAO-27-107784

Note: Data reported for 2025 were available through July 2025, except Marine Corps. No data were reported for the backlogs without an entry. GAO was not able to verify the reliability of the data. GAO is reporting these data because they are the best available and were reported to the Department of Defense by the military services.

^aAccording to officials, Space Force data are included in Air Force data.

The military services' personnel centers also reported 409,497 Privacy Act requests processed and 28,957 backlogs for the same period.²¹ The volume of requests has fluctuated across the military services, with some experiencing increases in both incoming requests and associated backlogs. See table 3 for service reported data for Privacy Act requests received, requests processed, and backlogs reported.

Table 3: Reported Privacy Act Requests for Service Member Personnel Records, by Military Service, Fiscal Years 2020–2025

Service	Fiscal year	Privacy Act requests received	Privacy Act requests processed	Reported backlogs
Army ^a	2020	495	495	—
	2021	2,580	2,580	—
	2022	1,881	1,881	—
	2023	280	280	—
	2024	390	390	—
	2025 ^b	495	397	—
Navy ^c	2020	33,074	33,074	0
	2021	48,083	48,083	1,021
	2022	51,827	51,827	2,869
	2023	54,747	54,747	1,083
	2024	120,917	120,917	16,034
	2025	71,519	71,519	6,278
Marine Corps ^d	2020	470	433	94
	2021	439	429	89

²¹According to military service officials, the difference in the reported number of FOIA requests received and processed does not match the reported combined backlog because the combined backlog reflects what is reported at the end of the year and could include carry over. Further, subtracting the processed requests from the incoming requests does not always equate to the backlog size reported at the end of a fiscal year if there are requests that remain unfilled from previous years or not fully processed in the year received.

Service	Fiscal year	Privacy Act requests received	Privacy Act requests processed	Reported backlogs
Air Force ^e	2022	828	793	118
	2023	1,097	1,075	155
	2024	497	375	284
	2025	—	—	—
	2020	110	92	17
	2021	—	—	—
	2022	—	—	—
	2023	5,758	5,232	32
	2024	9,081	9,342	260
	2025 ^b	5,895	5,536	623
Total	—	410,463	409,497	

Source: GAO analysis of military service data. | GAO-27-107784

Note: No data were reported for the years without an entry. GAO was not able to verify the reliability of the data. GAO is reporting these data because they are the best available data and were reported to the Department of Defense by the military services. Additionally, at the time of GAO's review, GAO requested fiscal year 2025 data from the services but they were unable to provide the data

^aArmy officials stated that their office generally answers Privacy Act requests within 20 days, and the recordkeeping system, FACTs, does not log Privacy Act requests to a backlog.

^bArmy and Air Force data were available through July 2025.

^cData include 106 Privacy Act requests processed by the Navy's Freedom of Information Act office during the timeframe.

^dData provided for the Marine Corps Manpower Management Performance Branch were not incorporated in the table because we could not confirm if the requests in the data they eventually provided were limited to third-party requests.

^eAccording to officials, Space Force data are included in Air Force data. Also, Air Force officials stated that they transitioned to a new tracking system in 2023 and could not provide portions of the data prior to that time because they were no longer available.

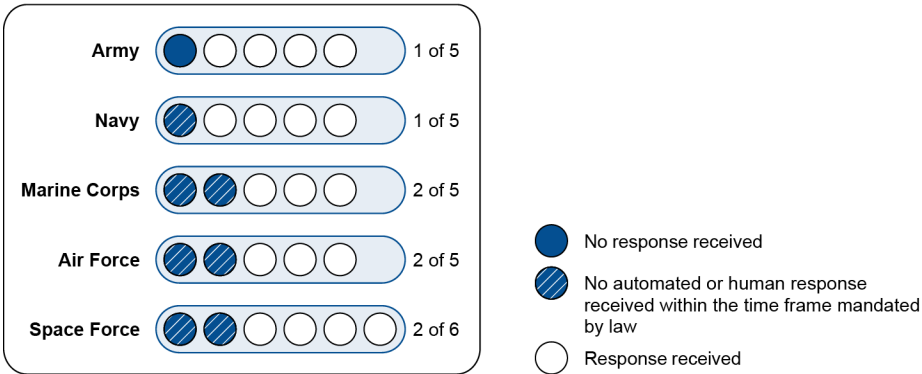
Officials from the military services stated that certain events—such as national, state, and local elections—can drive surges in records requests, which can increase delays in processing requests and thereby lead to a backlog. For example, Army officials reported increased requests from the media and the public for records of individuals running for public office during election years.

In addition, officials stated that the complexity of requests affects processing times. If a service member has an extensive record due to extended years of service that incorporates many honors or disciplinary actions, the records may be voluminous. In addition to vetting the request for records to ensure release validity, according to officials, records must be reviewed to remove disciplinary actions and all instances of personally identifiable information, such as social security numbers or addresses.

This redaction process is generally scanned by the processor digitally and then the information is electronically redacted. Factors such as the need for legal or supervisory review, the extent of required redactions, and the length of an individual's service—which can increase the volume of records to be reviewed—can significantly delay completion. Additionally, officials from all of the military services noted that requests for records that are considered “hot topics,” such as high-profile military justice cases and voting-related issues, add complexity to the processing because the records require additional layers of review.

Our nongeneralizable testing of third-party personnel records request processing demonstrated that the military services experienced some delays in providing responses to submitted requests that were contrary to the law and DOD guidance, although our testing was not designed to confirm the exact cause of the delays. Specifically, of the 26 requests we submitted over a 90-day timeframe, we received 18 responses within the appropriate timeframes—20-day response time for FOIA requests and generally accepted 20-day response time for Privacy Act requests. We did not receive a decision, acknowledgment of receipt, or request for additional information for eight of the requests we submitted, as the law and guidance requires. Figure 3 displays the results assessing the timeliness of the record requests processing.

Figure 3: Processing Timeliness Results of GAO’s Nongeneralizable Testing of Third-Party Requests for Service Member Personnel Records



Source: GAO analysis of Department of Defense information. | GAO-27-107784

Note: The testing included five requests—three Privacy Act and two Freedom of Information Act requests—submitted to each of the military services, totaling 25 requests. However, GAO submitted an additional request to the Space Force because it found that after its submission, one of the individuals for whom there was a record request transitioned from the Space Force to the Army. Therefore, GAO had to identify an additional Space Force service member for whom to submit a record request.

Staffing Gaps Contribute to Timeliness and Accuracy Challenges

According to military service officials, staffing limitations across the military services contribute to challenges with the proper and timely processing of requests for service member records. Each military service identified challenges with the availability of staff to complete these requests. Specifically,

- **Army.** In March 2025, Army personnel center officials reported that there were 16 unfilled positions within its personnel records servicing department, including positions dedicated to processing Privacy Act requests. Officials stated that these roles are filled exclusively by federal employees due to DOD and the Office of Management and Budget's (OMB) interpretation that much of this work constitutes an inherently governmental function. Officials also explained that the unfilled positions increase the workload and could cause challenges to the processing time and accuracy of fulfilling records requests. While Army FOIA data shows that there was not a FOIA backlog reported for unprocessed requests until fiscal year 2023 when 14 unprocessed requests were reported, the number of unprocessed requests that were reported increased to 68 in fiscal year 2024 and then to 96 by July 2025. Officials stated Privacy Act requests are typically processed within 30 days.

In March 2026, Army officials noted that the request process has changed since our visit to the personnel center. Officials stated that to ensure compliance, the personnel records center now submits all requests to the command's FOIA/Privacy Act Office for processing. Specifically, an Army official stated that the service recently conducted a review of the organization and reassigned duties among remaining staff. This reassignment included consolidating duplicative tasks, eliminating non-mission essential activities, centralizing the receipt and tracking of FOIA requests, standardizing procedures and quality checks, and automating workflow routing. According to the official, while no new staff were hired for FOIA request processing, this new process has improved timeliness and accuracy.²²

- **Navy.** Navy officials said they use contracted support under the supervision of a federal civilian employee to process Privacy Act requests. For FOIA requests, at the time of our review, all Navy Personnel Command requests were processed by one federal civilian employee, because the senior official that assisted with processing recently retired and there were currently no plans to replace the

²²This new process was not yet in place at the time of our testing of the processing of servicemember personnel records requests.

official. According to officials, this has contributed to significant delays and reported backlog of unprocessed requests, as well as ongoing litigation related to delayed responses. Processing data provided by the Navy showed that the time to process FOIA requests increased from an average of 1.64 days in fiscal year 2018 to an average of 55.5 days in fiscal year 2024. As of July 2025, the time to process requests increased to an average of 77.4 days. In late December 2025, Navy Personnel Command hired an assistant to help with the increasing workload and to manage reducing the backlog. As of April 2026, Navy officials told us that a backlog reduction plan is in place using the two federal civilian employees with supplemental help from reserve officers and other internal assets.

- **Marine Corps.** In July 2025, Marine Corps officials reported that while they have seen an increased workload of records request and some delays in processing time of records requests, they did not have a backlog of FOIA records requests. They noted that they had a shortage of one administrative staff member. According to a Marine Corps official, this staffing shortfall increased the workload of remaining staff as administrative duties had to be redistributed and affected the processing time of requests and remained as of March 2026. However, in September 2026, another official stated that there was a FOIA backlog of 75 requests due to an inability to fill a vacancy for a government administration position. The Privacy Act backlog data provided by Marine Corps officials shows an increase of unprocessed requests from 12 to 284 from fiscal year 2018 to fiscal year 2024 due to an increase of incoming requests and thereby workload of staff available to process them.²³
- **Air Force.** Air Force officials, who also process records requests for the Space Force, reported that contractors process all FOIA requests under the supervision of a federal civilian employee who provides final approval. For Privacy Act requests, the Air Force has five personnel processing requests, but one redaction reviewer position remains unfilled. According to officials, one attorney processes all nongovernmental requests following the retirement of three civilian attorneys under DOD's Deferred Resignation Program.²⁴ Officials explained that this additional review step increases the processing time of those non-governmental requests. While the Air Force's FOIA

²³At the time of our review, we requested comparable data for fiscal year 2025 but the Marine Corps was unable to provide them.

²⁴See GAO, *Civilian Workforce: DOD Should Assess Lessons Learned to Better Understand Reduction Impacts*, [GAO-26-108100](#) (Washington, D.C.: May 29, 2026).

backlog data show an increase in the amount of unprocessed requests from one in fiscal year 2018 to 14 in fiscal year 2024, data on the backlog for Privacy Act requests show a higher quantity and increase—from 165 in fiscal year 2018 to 623 in July 2025.²⁵ Air Force officials at the personnel center explained that over the last 5 years, they noticed that records requests rose. FOIA officials stated that the availability of the online submission portal and ease of use may have contributed to the increase in FOIA requests.

Military service officials stated that without sufficient staff to process FOIA and Privacy Act records, there will be slower response time to fulfill requests. For example, the Air Force data show an increase in days to process FOIA requests from 6.68 in fiscal year 2019 to 8.57 in July 2025. According to Navy officials, while reservists can be used to temporarily fulfill low priority FOIA workloads, there is no backup employee to process requests that require increased access information. Therefore, when the FOIA official goes on extended leave, there is no one available to process those requests.

In more critical cases, limited staff can contribute to the risk of litigation due to slower processing that does not meet legal timeframe guidelines. For example, during fiscal years 2020 through 2024, DOD spent nearly \$500 million processing over 266,000 FOIA requests. From that total, \$21 million was spent on litigation involving FOIA lawsuits filed by requesters.²⁶ As an extenuating consequence of slower processing time, in 2025, the Navy's FOIA office had four lawsuits related to the processing of third-party requests. To reduce future lawsuits regarding not meeting the legal timeframe, Navy officials explained that they included a new step in the processing of requests to acknowledge receipt of the request. Specifically, the official sends a letter to the requester stating that the request has been received but not yet processed. Navy officials explained that they believed sending this letter before the 20 days of receipt of the request attempts to meet the intent of the law.

²⁵At the time of our review, we requested comparable data for fiscal year 2025 but the Air Force was unable to provide them.

²⁶Generally, these lawsuits occur when requests are not processed within the required time frames or if the requester believes information is being withheld without cause. DOD Annual FOIA Reports, Fiscal Years 2020-2024.

OMB guidance states that management should identify, analyze, and respond to risks that may impede achieving objectives.²⁷ Further, DOD Directive 1100.4, *Guidance for Manpower Management*, states that personnel requirements are driven by workload and shall be established at the minimum levels necessary to accomplish mission and performance objectives.²⁸ In addition, *Standards for Internal Control in the Federal Government* state that management should recruit, develop, and retain competent personnel, and assess and address pressures—such as excessive workloads—that may hinder staff performance, as well as use quality information.²⁹ In this case, a workforce analysis would achieve the entity’s objectives.

DOD faces challenges in processing requests for service member personnel records. Although the Army and Navy have taken some steps to address these challenges through staffing efforts, the military services have generally not conducted a workforce planning analysis to clearly identify staffing requirements and align resources with current and projected needs, including any existing delays and reported backlogs. Officials from across DOD stated that FOIA and Privacy Act programs are often viewed as lower staffing priorities, which can delay hiring and prolong vacancies.

These challenges have been exacerbated by recent DOD-wide civilian workforce reductions and hiring freezes, which limit the ability to fill unoccupied positions.³⁰ During our initial discussions with officials at each of the military services’ personnel centers, there was no determination about whether or when a workforce planning analysis would be conducted to address workload backlogs and staffing shortages within the Privacy Act or FOIA divisions. Despite the breach that occurred during our review, Army officials stated that the timeliness and accuracy of the records processing have recently stabilized because of the assessment of

²⁷OMB Circular No. A-123, *Management’s Responsibility for Internal Control* (Mar. 10, 2026).

²⁸Department of Defense Directive 1100.4, *Guidance for Manpower Management* (Feb. 12, 2005).

²⁹GAO, *Standards for Internal Control in the Federal Government* [GAO-25-107721](#) (Washington, D.C.: May 2025).

³⁰See, e.g., Secretary of Defense Memorandum, *Immediate Civilian Hiring Freeze for Alignment with National Defense Priorities* (Feb. 28, 2025). See [GAO-26-108100](#).

and changes to the processes, workload distribution, and staff assignments.

By ensuring there is a clearer understanding of the staffing levels needed to manage the volume and complexity of FOIA and Privacy Act requests, DOD and the military services would be better prepared to reduce delayed responses, improper withholding or release of information, and exposure to litigation costs. Additionally, efforts to expedite processing to meet statutory deadlines may further increase the risk of errors and improper disclosures.

DOD Has Established Policies and Processes for Service Member Health Records but Has Not Fully Addressed Challenges with Their Proper and Timely Release

DOD and DHA have taken steps to safeguard and facilitate the proper and timely release of service member health records through established policies and processes. However, some challenges remain for DHA's medical facilities. These facilities rely on a complex record processing system to access and process requests for service member health records, and some facilities are experiencing increasing requests for health records.

DOD and DHA Have Policies and Processes Intended to Safeguard Health Record Requests

DOD and DHA have established policies and procedures that are intended to safeguard and facilitate the proper release of service member health records. For example, DOD guidance directs the safeguarding of private health information through an accurate and thorough assessment of potential risks and vulnerabilities regarding the confidentiality, integrity, and availability of protected health information.³¹ DHA guidance further directs medical facilities to conduct a random review of health records transactions to ensure record accountability.³²

These policies and processes are intended to ensure that DOD is adhering to appropriate laws on accessing and releasing health records.

³¹Department of Defense Instruction 8580.02, *Security of Individually Identifiable Health Information in DoD Health Care Programs* (Aug. 12, 2015).

³²Defense Health Agency Procedures Manual 6025.02, vol. 1, *DOD Health Record Lifecycle Management, Volume 1: General Principles, Custody and Control, and Inpatient Records* (Nov. 23, 2021).

For example, DOD and DHA issued guidance related to the implementation of HIPAA within the department, as well as procedures to be followed in the event of a breach of protected health information. Additionally, DHA issued guidance on health records management, among other related guidance.³³ DOD and DHA also have established annual privacy training requirements that must be completed by personnel prior to handling protected health information, such as courses available through the Joint Knowledge Online platform.³⁴

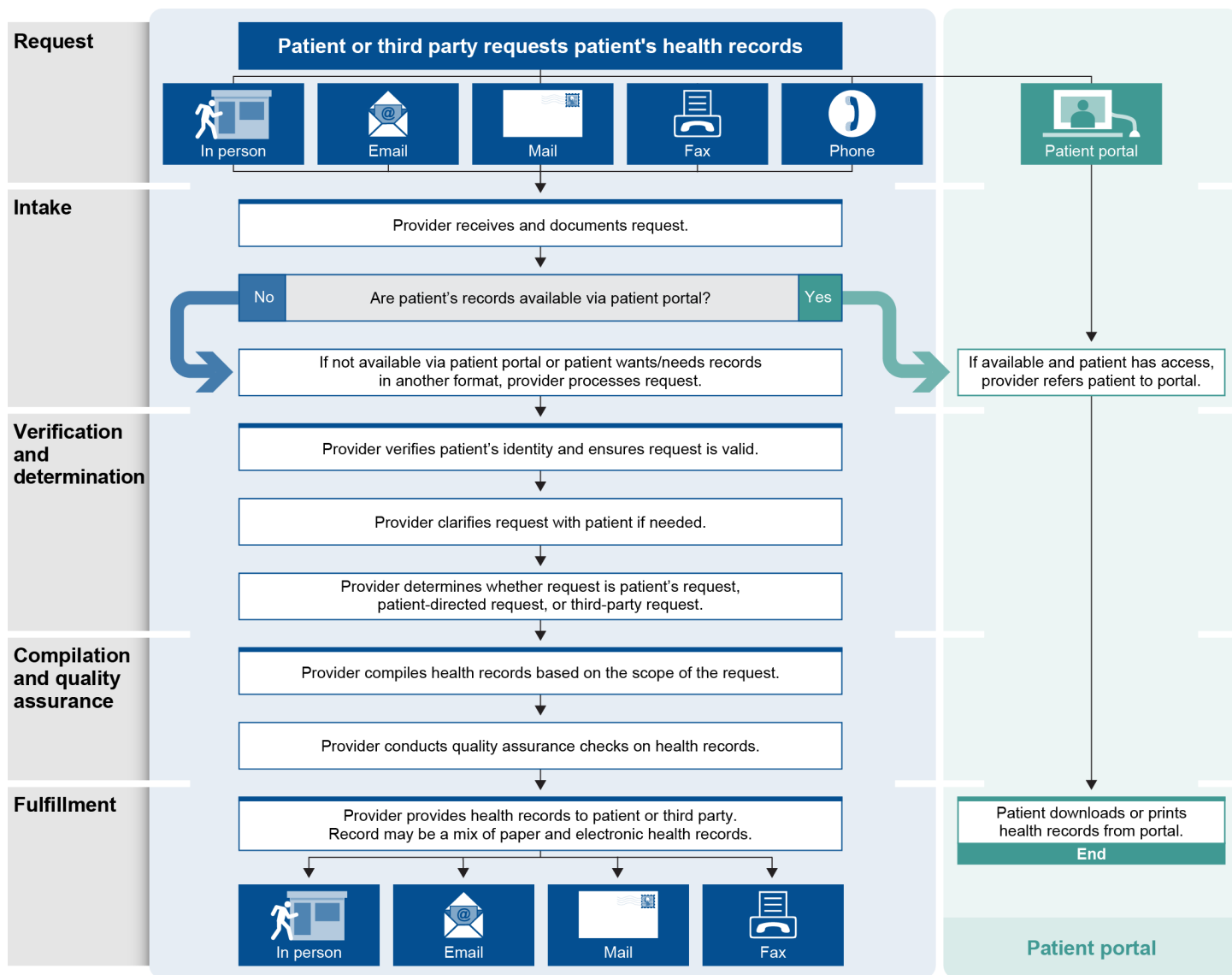
Requests for health records for the 9.5 million service members, retirees, and their beneficiaries can be processed at any of DHA's 547 medical facilities worldwide, according to officials. These requests are required to be fulfilled within 30 days according to HIPAA implementing regulations but may be extended to as much as 60 days.³⁵ The procedures for fulfilling health records requests can vary between medical facilities. However, based on our observations at three of the medical facilities we visited and on our prior work, the process generally involves the steps outlined in figure 4.

³³DHA Procedures Manual 6025.02, vol. 1.

³⁴DOD Instruction 8580.02.

³⁵45 C.F.R. § 164.524.

Figure 4: Defense Health Agency's Health Records Request Processing



Source: GAO analysis of Department of Defense information. | GAO-27-107784

The systems that providers use to access service member health records include new and legacy systems such as the Military Health System (MHS) Genesis, which can be used to document both inpatient and outpatient care, and the Health Artifact and Image Management Solution, which provides access to artifacts and images generated during the

health care delivery process.³⁶ See table 4 for additional information on these and other data systems involved.

Table 4: Defense Health Agency’s Data Systems Used for Health Records Processing

Data system	Description
Military Health System Genesis	- Federal electronic health records for service members and their families - Integrates inpatient/ outpatient medical and dental solutions - Deployed to all Department of Defense (DOD) hospitals and clinics worldwide in 2024
Armed Forces Health Longitudinal Technology Application	- Stores outpatient health care and clinical documentation “Web print” tool can create and upload a report to the Veterans Benefits Administration via another data system— the Health Artifact and Image Management Solution. This report serves as the base electronic record composing a service member’s health records
Essentris	- Inpatient component of current electronic health record for certain military hospitals since 1987 - Allows health care providers to document clinical care, procedures, and patient assessments occurring in both inpatient and emergency settings
Health Artifact and Image Management Solution	- Provides DOD health care and Department of Veterans Affairs providers access to artifacts and images generated during health care services - Serves as authoritative data repository for the health records, providing access to radiographs, clinical photographs, electrocardiographs, audio files, video files, documents, etc.
Paper Record Tracking	- Manages and tracks physical medical records stored in record rooms at military hospitals and clinics - Supports record transfers between military hospitals and clinics, borrowing of records by clinician staff, and retirement of records based upon National Archives and Records Administration disposition requirements

Source: GAO analysis of DOD Information. | GAO-27-107784

Providers generally must rely on multiple systems to obtain a complete set of records when responding to records requests because there is not a single system that houses all health records. In addition to having to search multiple systems for health records, providers might also have to search for and digitally scan paper records to fulfill a request. For example, while individuals who retired or separated from military service after January 1, 2014, had their health records digitized, records for those who retired prior to that time may remain in paper form. Paper records

³⁶Other systems include the Joint Longitudinal Viewer, Paper Record Tracking, Essentris, and Armed Forces Health Longitudinal Technology Application Web Print. MHS Genesis has a patient portal that provides service members with direct access to a portion of their health records. One official estimated that about 40 percent of an individual’s health records may be available through the patient portal.

can also be generated by non-DOD providers or in special circumstances such as during combat operations.³⁷

DOD Is Working to Address Previously Identified Challenges to Processing Health Records Requests

We previously reported that extracting health records from electronic systems is not a simple “push of a button” and often requires providers or contractor personnel to search through multiple systems to compile the records.³⁸ In 2019, the Congressional Research Service reported that DOD operates a number of legacy electronic health record systems.³⁹ Each system has separate capabilities and functions as a result of new or changing requirements over the past 5 decades. In April 2024, we reported that DOD determined that the multiple legacy electronic health records systems it implemented over the past 3 decades to create, maintain, and manage patient health information required modernization and that DOD sought to replace these legacy systems with a comprehensive, real-time electronic health records system.⁴⁰

We also reported in April 2024 that DOD had taken steps to incrementally deploy its federal electronic health records system at military facilities, and that the final system deployment took place in March 2024. We reported that DOD’s 2023 survey of user experiences demonstrated improved satisfaction from 2022, but results indicated that MHS Genesis system users continued to be generally dissatisfied with the system’s response time, ability to work as efficiently as possible, and ability to deliver high-quality care.⁴¹ As a result of this work, we recommended, among other things, that DOD establish user satisfaction targets (i.e., goals) for MHS Genesis and ensure that the system demonstrates improvement toward meeting those targets. DOD partially concurred with this recommendation. In January 2026, the department described planned targets for the survey response rate and a potential target for the

³⁷DHA uses the Paper Record Tracking application to manage and track medical records physically stored in record rooms at military hospitals and clinics.

³⁸GAO, *Medical Records: Fees and Challenges Associated with Patients’ Access*, [GAO-18-386](#) (Washington, D.C.: May 14, 2018).

³⁹Congressional Research Service, *MHS Genesis: Background and Issues for Congress*, R45987 (Washington, D.C.: Oct. 28, 2019).

⁴⁰GAO, *Electronic Health Records: DOD Has Deployed New System but Challenges Remain*, [GAO-24-106187](#) (Washington, D.C.: Apr. 18, 2024).

⁴¹[GAO-24-106187](#).

user satisfaction rate. The department expects to complete the efforts by January 2027.

In April 2025, we also reported on DHA's "health informatics," which is a business function that determines how to troubleshoot information technology challenges and improve processes related to DOD's electronic records system.⁴² Specifically, we reported that officials stated that health informatics reviews whether MHS Genesis can appropriately document health care delivery and ensure these data are integrated across the medical facilities. Based on this work, we recommended that DHA develop an implementation plan with timelines and key milestones and deliverables to track its progress in consolidating business functions, once studied, to manage and support its medical facilities. DOD concurred with this recommendation but as of May 2026, had not taken action in response.

Complex Processing and Increasing Requests May Challenge Proper and Timely Release of Health Records

Complex Processing of Health Records Requests

DHA's medical facilities rely on a complex record processing system comprised of multiple data systems to access service member health records, resulting in numerous steps that complicate processing health records requests. When processing requests, records are identified among multiple data systems; however, the processor must review the records to redact unnecessary personal information. For example, according to one official, social security numbers are often contained in health records and must be redacted. Multiple officials stated that the redaction process can be the most cumbersome part of fulfilling requests, particularly if the health records are large or contain scanned documents. Officials at another facility told us that the number of systems they need to obtain records can be cumbersome because depending on the age of the records, they can reside on different systems or even in hard copy. Furthermore, the complexity of these requests can vary significantly, with one medical facility official stating they processed a request for a health

⁴²GAO, *Defense Health Care: Actions Needed to Address Long-Standing Management Challenges with Medical Facilities*, [GAO-25-107432](#) (Washington, D.C.: Apr. 10, 2025).

record that was about 10,000 pages long and took approximately 6 days to complete.

DHA has worked to integrate these multiple data systems. For example, in 2013 DOD implemented the Joint Longitudinal Viewer, a system that allows DOD and non-DOD health care providers who are treating a patient to view a comprehensive read-only version of that patient's treatment history when providing medical care. However, to provide these records as part of a record request, staff processing the records would need to access each individual system to retrieve the needed information. DHA is also currently embarking on a multiyear digital transformation strategy to consolidate and improve information systems across the entire military health system, including its medical facilities.⁴³ The ongoing strategy includes employing artificial intelligence and other automation tools, which may also improve the process by which health record requests are processed and fulfilled and ultimately reduce the burden of using multiple data systems. DHA estimates that strategy will be fully implemented sometime in 2029.

DOD's 2023 Records Strategy states that the department seeks to employ the latest technologies, such as artificial intelligence and cloud-based services, to reduce the administrative burden associated with records management, while creating an environment where DOD records are automatically identified and captured, expertly curated, and systemically governed.⁴⁴ Further, to prevent breaches, the HIPAA security rule states that each regulated entity must implement administrative actions to safeguard protected health information, such as conducting an accurate and thorough assessment of the potential risks and vulnerabilities regarding the confidentiality, integrity, and availability of protected health information that it owns or manages.⁴⁵

If a breach of protected health information does occur it is reported via the Defense Privacy Information Management System. From 2019 through September 2025, DHA reported a total of approximately 7,332 breaches of either protected health information or other personally identifiable information, of which they classified 84 as breaches related to third party requests. While some of these breaches may be attributed to something

⁴³Military Health System, *Digital Transformation Strategy 2023 – 2028* (Mar. 26, 2025).

⁴⁴Deputy Secretary of Defense Memorandum, *Records Strategy* (May 10, 2023).

⁴⁵45 C.F.R. Part 164.

other than human error, such as computer hacking, multiple DHA officials cited human error as the primary cause.

DHA has not taken steps to streamline its complex record processing system comprised of multiple data systems to access service member health records because it has not studied its business functions to determine which ones to consolidate to ensure the efficient delivery of services. As stated above, in our April 2025 report on management challenges with DHA medical facilities, DHA officials identified “health informatics” as a business function related to electronic health records that improves related processes to ensure workload is allocated across the entire military health system.⁴⁶ We recommended that DHA study its medical business functions to determine which ones it would consolidate to manage and support its medical facilities, and DHA concurred. However, that recommendation did not specifically call for an assessment of its health informatics business function.

In addressing our prior recommendation, including in its study of “health informatics” business function an assessment of the current framework and systems for processing health records requests, would better position DHA to identify opportunities for improvement. These improvements may include consolidating data systems or using artificial intelligence, among others, to reduce the burden and resources needed to fulfill health records requests. By including an assessment of its complex record retrieval system comprised of multiple data systems to access service member health records in its assessment of business functions to determine which ones it will consolidate, DHA will be better positioned to ensure that these functions are structured to manage and support the proper and timely release of service member health records.

Increasing Requests at Some Medical Facilities

Some of DHA’s medical facilities are experiencing annual increases in the number of third-party health records requests they process. We requested health records requests and associated backlog data from DHA for all of its medical facilities spread among its nine defense health networks.⁴⁷ This resulted in data from 133 medical facilities out of a total of 547, according to officials. While we could not determine the reliability

⁴⁶[GAO-25-107432](#).

⁴⁷We were not able to determine the reliability of the health request data because of missing information, variation in methods for collection, storage, and retrieval of the data across the medical facilities, among other reasons. Please see appendix one for additional details.

of the data on health records, the data showed that a small proportion of the medical facilities were experiencing an increase in health record requests. According to the data, most (99, or about 75 percent) of the 133 medical facilities did not see a consistent increase in the number of health records requests, while 34 (about 25 percent) did.

While two of the four medical facilities we visited cited staffing challenges for request processors, another medical facility we visited stated that they had an excess of personnel processing health records requests and that they established a cost sharing agreement to use their processors to assist another medical facility in processing requests.

In December 2023, DOD issued a memorandum requiring the Under Secretary of Defense for Personnel and Readiness to conduct a comprehensive review of all medical personnel requirements, including medical facilities and other entities by June 30, 2024.⁴⁸ In June 2024, DOD issued another memorandum outlining requirements for the Under Secretary of Defense for Personnel and Readiness, in coordination with DHA and the secretaries of the military departments, to conduct an annual review of all validated and funded military medical and dental personnel requirements.⁴⁹ The memo also directed DHA to forecast and recommend uniformed manpower resourcing requirements to the secretaries of the military departments. According to officials, DOD completed this review in December 2025. Additionally, in April 2026, DHA officials stated that they were working to finalize a Human Capital Distribution Plan, which is a staffing plan for military medical personnel assignments at medical facilities that will be conducted annually.⁵⁰

In July 2025, we reported on military medical personnel shortfalls across DOD's medical facilities. At that time, we found that the number of assigned military personnel had declined by about 16 percent from fiscal year 2015 through fiscal year 2023. We made seven recommendations to DOD to improve its monitoring of military medical personnel staffing at the facilities, which may help address the demand for health care services

⁴⁸Deputy Secretary of Defense Memorandum, *Stabilizing and Improving the Military Health System* (Dec. 6, 2023).

⁴⁹Directive-Type Memorandum 24-003, *Military Health System Manpower Requirements Determination, Resourcing, and Assignment* (June 28, 2024) (incorporating change 1, May 20, 2025).

⁵⁰Assistant Secretary of Defense for Health Affairs Memorandum, *Military Health System Human Capital Distribution Plan Business Rules* (July 1, 2024).

while personnel remain in short supply. As of July 2026, six of seven recommendations had not been implemented.⁵¹

Conclusions

Although DOD and the military services have established policies and procedures to guide the proper release of service members' personnel records, they have not taken steps to determine the appropriate levels of staff needed to ensure the proper release of records and they risk not meeting statutory time frames for records release. These challenges are workload driven due to the volume and complexity of FOIA and Privacy Act requests, the increased risk of human error associated with manual processing and redaction, and staffing limitations across military service personnel centers. The general absence of workforce planning analysis to identify staffing requirements and align resources with current and projected workloads has contributed to persistent backlogs, processing delays, and the risk of improper disclosure or withholding of information. Addressing these workforce planning gaps would better position DOD to align resources with current and projected workloads and to identify opportunities for streamlining the record request process.

DOD and DHA also have established policies and procedures to assist in the proper and timely release of service member health records and have sought to improve their complex record retrieval process. However, challenges remain with the use of multiple data systems and an increasing number of health records requests. As a result, there is an increased risk of delays in processing requests and of human error that could lead to a breach of private information. DHA can alleviate the burden of using multiple data systems and reduce the potential for delays and human error by analyzing and implementing tools for increased efficiency, such as using artificial intelligence or improving workflow processes.

Recommendations for Executive Action

We are making the following five recommendations to DOD:

The Secretary of Defense should ensure that the Secretary of the Army, in consultation with the Director of Administration and Management's Oversight and Compliance Directorate, ensures that the functional review recently conducted adequately aligns with a workforce planning analysis that ensures the number of staff available for processing requests for

⁵¹GAO, *Defense Health Care: Information Needed to Improve Monitoring of Military Personnel Staffing at Medical Facilities*, [GAO-25-106988](#) (Washington, D.C.: July 21, 2025).

service member personnel records aligns with current and projected needs. (Recommendation 1)

The Secretary of Defense should ensure that the Secretary of the Navy, in consultation with the Director of Administration and Management's Oversight and Compliance Directorate, conducts a workforce planning analysis to ensure that the number of staff available for processing requests for service member personnel records aligns with current and projected needs. (Recommendation 2)

The Secretary of Defense should ensure that the Commandant of the Marine Corps, in consultation with the Director of Administration and Management's Oversight and Compliance Directorate, conducts a workforce planning analysis to ensure that the number of staff available for processing requests for service member personnel records aligns with current and projected needs. (Recommendation 3).

The Secretary of Defense should ensure that the Secretary of the Air Force, in consultation with the Director of Administration and Management's Oversight and Compliance Directorate, conducts a workforce planning analysis to ensure that the number of staff available for processing requests for service member personnel records aligns with current and projected needs. (Recommendation 4).

The Secretary of Defense should ensure that the Assistant Secretary of Defense for Health Affairs, in coordination with the DHA Director, includes an assessment of the current framework and systems for processing health records requests in the agency's study of the "health informatics" business function to identify opportunities for improvement, such as consolidating databases or using artificial intelligence. (Recommendation 5)

Agency Comments

We provided a draft of this report to DOD, VA, and the National Archives for review and comment. In written comments, DOD stated it concurred with the recommendations but stated it had concerns related to the data used in the report, the scope of our review, and how our report characterized the department's governance structure. DOD's comments are summarized below and reprinted in appendix II. DOD also provided technical comments, which we incorporated as appropriate. VA also provided verbal and written technical comments, which we incorporated as appropriate. In an email, the National Archives stated that it did not have comments.

Related to the data, DOD raised concerns with our characterization that data on FOIA and Privacy Act requests were of undetermined reliability. DOD requested that we reconcile the report's metrics with data from the department's annual FOIA reports submitted to the Department of Justice. We used data provided by the military services' personnel centers instead of the annual FOIA report because the data that DOD submits in that report were insufficient to meet the needs of this review. Specifically, that data did not disaggregate FOIA requests for all four services and are not limited to third-party requests, which is how we presented the information in our report. While we were not able to independently determine the reliability of these data, we are reporting them because they are the data reported by the military services for the department's annual report and because they were the best available data for purposes of highlighting information in the manner reflected in this report. Moreover, the data presented in the report does not solely form the basis for any recommendations made to the department. We have adjusted the language in the report to more clearly reflect the fact that the data were not unreliable, but that we were not able to independently determine the reliability of these data

DOD also stated that our draft report inaccurately portrays the management of service member records as a fragmented effort, omitting the centralized statutory governance and compliance architecture administered by the department's Director of Administration and Management and the Oversight and Compliance Directorate. We recognize the importance of these entities in providing enterprise-wide direction specific to records management and agree that training, compliance monitoring, and program reviews would impact the processing and safeguarding of records. However, our focus was to assess the military services' processing and safeguarding of service member records and not the broader operational framework for records management. In addition, the Director of Administration and Management and the Oversight and Compliance Directorate are generally not involved in individual decisions to release—or not release—information in response to a request. As discussed in our report, that is an action conducted at the level of the relevant military service office.

DOD also stated that our draft report aggregates the 49 breaches without taking into account the risk level of the breaches by applying the federal risk-of-harm framework. Additionally, DOD stated that over 90 percent of the incidents were low-risk administrative errors, which resulted in no harm to individuals. DOD further stated that the draft report conflates general administrative incidents with breaches stemming directly from the

FOIA and Privacy Act release processes, which mischaracterizes the department's security posture. By law the department is required to report all breaches independent of their risk level and type of release. We are unable to independently verify DOD's assertion of risk for these incidents because we did not analyze each of the breaches to determine the associated risk level. However, we added language to the report indicating that risk levels can vary and that, according to DOD, over 90 percent of these incidents were low-risk administrative errors. Moreover, we state in the report that these 49 breaches account for a small fraction of the total number of requests processed, but the implications of the improper release of personally identifiable information are far reaching.

Lastly, DOD commented that our draft report implies that the department has not taken action on a recommendation from a 2022 GAO report for DOD to establish a time frame for fully defining a process to ensure the involvement of senior privacy officials in assessing and addressing hiring, training, and professional development needs regarding privacy.⁵² We modified the report to reflect that DOD has drafted a policy to address this recommendation but that the policy is not expected to be complete until the end of March 2027.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Defense and Veterans Affairs, and the Administrator of the National Archives and Records Administration. In addition, the report is 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 williamsk@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found at the end of this report. GAO staff who made key contributions to this report are listed in appendix III.

//SIGNED//

Kristy E. Williams
Director, Defense Capabilities and Management

⁵²[GAO-22-105065](#).

Appendix I: Objectives, Scope, and Methodology

This report examines the extent to which the Department of Defense (DOD) has established policies and procedures and has taken steps to address any challenges in the proper and timely release of service members' (1) personnel records and (2) health records.

To address both objectives, we reviewed applicable statutes such as the Freedom of Information Act (FOIA), the Privacy Act of 1974, and the Health Insurance Portability and Accountability Act (HIPAA). We also reviewed DOD and military service policies and guidance governing the release of service members' personnel and health records; and interviewed officials at DOD, the military services, the Department of Veterans Affairs, and the National Archives and Records Administration.

We also conducted three in-person site visits and a teleconference site visit with the four military service personnel centers and a non-generalizable sample of four medical treatment facilities close to the personnel centers to obtain information and perspectives on the release of service members' records.¹

To develop our non-generalizable site visit sample, we selected all of the military services' personnel centers as well as four medical facilities that were co-located with the military services' personnel centers. We selected the military service personnel centers because they are the primary entities that fulfill requests for service member personnel records, according to officials.² We selected the medical facilities because

¹Department of Defense Manual 5400.07, *DOD Freedom of Information Act (FOIA) Program* (Jan. 25, 2017); Department of Defense Instruction 5400.11, *DOD Privacy and Civil Liberties Programs* (Jan. 29, 2019) (incorporating change 1; Dec. 8, 2020); Department of Defense 5400.11-R, *DOD Privacy Program* (May 14, 2007).; Department of Defense Instruction 6025.18 *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DOD Health Care Programs* (Mar. 13, 2019); Department of Defense Manual 6025.18, *Implementation of the Health Insurance Portability And Accountability Act (HIPAA) Privacy Rule in DOD Health Care Programs* (Mar. 13, 2019).; Army Regulation 25-55, *The Department of the Army Freedom of Information Act Program* (Oct. 19, 2020); Army Regulation 25-22, *The Army Privacy and Civil Liberties Program* (Sept. 30, 2022); Secretary of the Navy Instruction 5720.42G, *Department of the Navy Freedom of Information Act Program* (Jan. 15, 2019); Secretary of the Navy Instruction 5211.5F, *Department of the Navy Privacy Program* (May 20, 2019); and Air Force Instruction 33-332, *Air Force Privacy and Civil Liberties Program* (Mar. 10, 2020).

²According to Air Force officials, Space Force uses the Air Force Personnel Center to process requests for their personnel records.

requests for military health records can be made to any medical facility. See table 5 for a list of the locations we visited or contacted.

Table 5: DOD and Non-DOD Locations Visited or Contacted by GAO

Organization	Location visited or contacted
Department of Defense	Office of the Director of Administration and Management, as the Oversight and Compliance Directorate, Alexandria, Virginia
Department of the Army	- U.S. Army Human Resources Command, Fort Knox, Kentucky - Chief, Army Privacy and Civil Liberties, Fort Belvoir, Virginia - Office of the Chief Legislative Liaison, Washington D.C.
Department of the Navy	- Naval Personnel Command, Millington, Tennessee - Chief Information Officer, Washington D.C.
United States Marine Corps	Manpower Management Performance Branch, Quantico, Virginia
Department of the Air Force	- Air Force Office of the Chief Information Security Officer, Arlington, Virginia - Air Force Personnel Center, Joint Base San Antonio-Randolph, Texas - Air Force Office of Special Investigations, Quantico, Virginia
Defense Health Agency	- Defense Health Agency, Privacy & Civil Liberties Office, Falls Church, Virginia - Brooke Army Medical Center, Joint Base San Antonio, Texas - Ireland Army Health Clinic, Fort Knox, Kentucky - Naval Hospital Pensacola, Pensacola, Florida - Wilford Hall Ambulatory Surgical Center, Joint Base San Antonio, Texas - Naval Branch Health Clinic Memphis, Millington, Tennessee
Department of Veteran Affairs	- Veterans Health Administration, Washington D.C. - Veterans Benefits Administration, Washington D.C. - Office of Information & Technology, Washington D.C.
National Archives and Records Administration	- National Personnel Records Center, St. Louis, Missouri - Office of the Inspector General, College Park, Maryland

Source: GAO. | GAO-27-107784

For each of the military service personnel centers in our sample, we requested data regarding the number of third-party FOIA and Privacy Act requests for personnel records from fiscal years 2015 through 2025. We selected this time frame to identify trends, if any, in recent years in the volume of requests received, processed, and backlogged.

To assess the reliability of the data obtained from the military service personnel centers, we reviewed related documentation, asked knowledgeable officials to complete questionnaires about how the data were retrieved, and conducted interviews with knowledgeable officials. We also reviewed the data for missing or out of range values. However, we were not able to verify the reliability of all FOIA and Privacy Act data reported by the military services. Due to the migration of information to

new systems, at times, some data may not have been transferred according to service officials. For instance, the Air Force transitioned to a new tracking system in 2023 and could not provide portions of the data prior to that time because they were no longer available. Additionally, backlog data were not always captured in the system of record capturing the processed requests. While we were not able to determine, the reliability of these data, we are reporting them because they are the best available data and are reported to DOD.

For our first objective, we reviewed FOIA and the Privacy Act, as well as DOD and military service policies and guidance regarding the release of service member personnel records. We also interviewed DOD and service FOIA and Privacy Act officials, and officials from the National Archives and Records Administration, National Personnel Records Center to better understand other avenues for obtaining service member records outside DOD. Further, we observed the processing of both Privacy Act and FOIA requests from three of the four military service personnel centers we interviewed.

We also compared the request fulfillment processes that we observed against Standards for Internal Control in the Federal Government and Office of Management and Budget guidance.³ Specifically, we determined that the control environment and risk assessment components were significant to this objective, along with recruiting, retaining, and developing competent personnel and that management should identify, analyze, and respond to risks that may impede achieving objectives. In addition, we collected and reviewed the data mentioned above for the number of Privacy Act and FOIA requests processed by each military personnel center to identify any trends or potential workload challenges.

We also collected and reviewed data regarding the number of breaches at each military service personnel center from fiscal years 2021 through 2025 to identify the overall quantity, potential causes, and any trends. The data included the date of the breach, the organization holding the data, and DOD determined causes, among other elements. To assess the reliability of the breach data obtained from DOD's Oversight and Compliance Directorate for the military service personnel centers, we reviewed related documentation, questionnaires completed by knowledgeable officials on how the data were retrieved, and we

³GAO, *Standards for Internal Control in the Federal Government*, [GAO-25-107721](#) (Washington, D.C.: May 2025); Office of Management and Budget Guidance Circular No. A-123, *Management's Responsibility for Internal Control* (Mar. 10, 2026).

conducted interviews with the knowledgeable officials. Based on these steps, we determined that these data were sufficiently reliable for the purposes of describing the number and any associated trends of FOIA and Privacy Act personnel records requests at these facilities.

To assist in determining the sufficiency of internal controls designed to safeguard service member personnel records, we assessed these controls using 26 nongeneralizable tests in which we submitted 16 Privacy Act requests and 10 FOIA requests. To determine if requests were approved or denied in accordance with applicable laws and policies, we posed as a fictitious individual (e.g., a private attorney) and sent requests for personnel records to the Army, Navy, Marine Corps, Air Force, and Space Force. We submitted requests that did not contain errors that should have been approved and processed with appropriate redaction within the required timeline. We also submitted forms that intentionally contained flaws, which should have led to their denial or request for additional information, in accordance with FOIA and Privacy Act statutes.

The testing included five requests for each of the military services—three Privacy Act and two FOIA requests for each service—totaling 25 requests. However, we submitted an additional request to the Space Force because the individual switched from the Space Force to the Army and thus records were maintained by the Army. Of these 26 requests, one request was fulfilled with records containing personally identifiable information. While this information should not have been sent to us, we protected the record by downloading it and then placing it into our secure database with no further distribution and restricted access to the file.

To provide additional context for interviews and site visits and to better understand the breach process, we selected two nongeneralizable instances of high-profile breaches because both had information regarding the breach process that we could review. We reviewed information on these breaches to better understand the processes involved and the underlying causes based on the investigation of the breach. We interviewed agency officials who had knowledge of the breaches or conducted investigations of the incidents.

For our second objective, we reviewed applicable statutes such as HIPAA, FOIA, and the Privacy Act. We also reviewed DOD and DHA policies and guidance regarding the release of service member health records. We interviewed DOD Privacy Act, HIPAA, and FOIA officials, as well as officials from the Defense Health Agency (DHA). Further, we

conducted interviews at each of the four military medical treatment facilities we visited and observed the processing of health records requests at three of these. We requested health records request data from all DHA's 547 medical facilities (excluding dental and public health facilities, and the National Intrepid Center of Excellence) as reported by DHA. We received data from 133 medical facilities, on the number of third-party health record requests processed and any backlogs of requests to identify any trends or potential workload or timeliness challenges. These facilities vary in size and capabilities and consist of large "parent facilities"—such as ambulatory surgery centers, hospitals, and medical centers—and small "child facilities," such as behavioral health clinics. Of the 133 facilities that responded to our data request, 119 are parent facilities. While we requested 10 years of data, DHA and most of the medical facilities that provided data were able to provide data for fiscal years 2023 through 2025 during the period of our audit.

In addition, we collected and analyzed data regarding the number of breaches throughout all of the military medical treatment facilities from calendar year 2019 through September 8, 2025, to identify the overall quantity and any trends. To assess the reliability of the data obtained from DHA's medical facilities, we reviewed related documentation and asked knowledgeable officials at 133 medical facilities to complete questionnaires about how the data were retrieved. However, some of these questionnaires were incomplete. We also reviewed the data for missing values and errors, among others. We also spoke with knowledgeable officials regarding missing and inconsistent data, and the variation in methods used to collect, store, and retrieve the data. Based on these steps, we could not determine that these data were reliable for the purposes of describing the number of health record requests, trends, and any associated backlogged requests at these facilities. However, we are reporting high-level results because these data are the best available and may be used by decision-makers.

To assess the reliability of DHA breach data obtained, we reviewed related documentation, asked knowledgeable officials to complete questionnaires about how the data were retrieved, and conducted interviews with knowledgeable officials. Based on these steps, we determined that these data were sufficiently reliable for the purposes of describing the number of breaches and any trends at DHA's medical facilities.

We conducted this performance audit from August 2024 to October 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. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Appendix II: Comments from the Department of Defense



OFFICE OF THE DIRECTOR OF ADMINISTRATION AND MANAGEMENT
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

September 21, 2026

Ms. Kristy Williams
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Williams,

This letter is in response to your request for comments on the Government Accountability Office (GAO) draft report, GAO-26-107784, "SERVICE MEMBER RECORDS: DOD Needs to Address Improper and Delayed Releasing of Personnel and Health Information." The Department of War (DoW) appreciates the opportunity to review and comment on the draft report. We are committed to safeguarding service members' records and ensuring timely public access in accordance with federal law.

The Department concurs with the report's overarching goal of improving the processes for the release of personnel and health information. We are pleased that the draft report recognizes that the Department and its components have processes in place for the safeguarding and processing of service member records. However, we respectfully submit that the final report would be significantly enhanced by addressing key concerns related to data integrity, audit scope, and the characterization of the Department's governance structure. The Department's formal position is to concur with the recommendations, with comments. The primary concerns are as follows:

1. **Use of Unreliable Data:** Our most significant concern is that the report's findings and conclusions rely on data of "undetermined reliability," as acknowledged in Footnote 19 on page 18. Drawing definitive conclusions about systemic failures from unverified, ad-hoc data conflicts with Government Auditing Standards. We request GAO reconcile the report's metrics with the Department's official, legally certified Annual Freedom of Information Act (FOIA) Reports submitted to the Department of Justice Office of Information Policy.
2. **Omission of Enterprise Governance:** The report inaccurately portrays records management as a fragmented effort, omitting the centralized statutory governance and compliance architecture administered by the Director of Administration and Management and my office, the Oversight and Compliance Directorate. This existing framework, operating under the oversight of the DoW Chief FOIA Officer and Senior Agency Official for Privacy, provides robust enterprise-wide direction through standardized training, quarterly compliance monitoring, and continuous programmatic reviews. The final report should reflect this active governance structure.
3. **Mischaracterization of Data Breaches:** The report aggregates 49 data breaches without applying the federally mandated risk-of-harm framework (OMB M-17-12). As we

**Appendix II: Comments from the Department
of Defense**

documented in our formal response to GAO's Request for Information (RFI-05, August 2025), over 90% of these incidents were low-risk administrative errors with no resulting harm to individuals. The report appears to conflate general administrative incidents with breaches stemming directly from the FOIA/Privacy Act release process, which is the stated scope of this audit. This mischaracterizes the Department's security posture and penalizes our transparent self-reporting culture. Request that GAO provide this important context and these distinctions.

4. Context of Prior Recommendations: The report implies departmental inaction on a prior 2022 recommendation (GAO-22-105065). The Department has, in fact, already provided GAO with mutually agreed-upon Corrective Action Plan (CAP) language. The delay in formal publication is due to administrative issuance lifecycles and organizational realignments, not a substantive failure to act. Request that GAO include this important context.

We have provided detailed substantive and technical comments in the attached matrix to assist you in producing a final report that is factually accurate and provides a comprehensive view of our operations.

The Department appreciates the professionalism and support of the GAO audit team. My point of contact for this matter is Ms. Rahwa Keleta, who can be reached at (571) 256-1408 or rahwa.a.keleta.civ@mail.mil.

Sincerely,

KREMLACEK.MIC
HAEL.118798446
3



Digitally signed by
KREMLACEK.MICHAEL.118798446
Date: 2026.09.21 12:57:22 -04'00'

Michael Kremlacek
Acting Director
Oversight and Compliance

Attachment:
As stated

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Kristy E. Williams williamsk@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff members made key contributions to this report: Vincent Balloon (Assistant Director), Natasha Wilder (Analyst in Charge), Paul Seely, James Arp, Nicole Ashby, Sharon Ballinger, Joshua Hatter, Jeff Larson, Mark R. Macpherson, Mike Shaughnessy, Mike Silver, and Theologos Voudouris.

Related GAO Products

Artificial Intelligence: OMB Action Needed to Address Privacy-Related Gaps in Federal Guidance. [GAO-26-107681](#). Washington, D.C.: March 26, 2026.

Electronic Health Records: DOD Has Deployed New System but Challenges Remain. [GAO-24-106187](#). Washington, D.C.: April 18, 2024

Freedom of Information Act: Additional Guidance and Reliable Data Can Help Address Agency Backlogs. [GAO-24-106535](#). Washington, D.C.: March 7, 2024.

Privacy: Dedicated Leadership Can Improve Programs and Address Challenges. [GAO-22-105065](#). Washington, D.C.: September 22, 2022

Freedom of Information Act: Actions Needed to Improve Agency Compliance with Proactive Disclosure Requirements. [GAO-21-254](#). Washington, D.C.: March 10, 2021

Freedom of Information Act: Update on Federal Agencies' Use of Exemption Statutes. [GAO-21-148](#). Washington, D.C.: January 12, 2021.

Medical Records: Fees and Challenges Associated with Patients' Access. [GAO-18-386](#). Washington, D.C.: May 14, 2018.

Information Management: The Challenges of Managing Electronic Records. [GAO-10-838T](#). Washington, D.C.: June 17, 2010.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

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

General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.