DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS BENEFITS ADMINISTRATION

Records Management Center Disclosed Third-Party Personally Identifiable Information to Privacy Act Requesters

REVIEW | REPORT #19-05960-244 | NOVEMBER 14, 2019

The mission of the Office of Inspector General is to serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs through independent audits, inspections, reviews, and investigations.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

The purpose of this review was to determine whether the Veterans Benefits Administration's (VBA) Records Management Center (RMC) staff disclosed third-party personally identifiable information (PII) when responding to Privacy Act requests. Both federal law and VA policy protect the privacy of PII, such as names, social security numbers, and dates and places of birth. VBA is required to allow any individuals or their representatives to review their claims files and have copies made under the Privacy Act.

Since 2015, VBA has generally centralized the processing of Privacy Act requests to its RMC in St. Louis, Missouri, where staff fulfill most requests electronically.[1] Many records in VBA's possession used to fulfill the Privacy Act requests include third-party PII. A third party is any individual, other than the person making the Privacy Act request, identified in that person's record. For example, military service records may contain the PII of multiple individuals such as the names and social security numbers of doctors who treated a veteran. The doctors' information would be third-party PII.

Prior to May 2016, VBA policy required staff to redact third-party PII for Privacy Act requests and provide information relating only to the requester. However, VBA reported the redaction requirement was a major contributing factor in its massive backlog of Privacy Act requests. VBA also had plans to provide veterans with online access to their records, which made the policy of redacting third-party PII prior to release infeasible.

In May 2016, VBA changed its Privacy Act release policy after VA's Office of General Counsel determined there was legal support for releasing unredacted records.[2] This new policy allowed the disclosure of third-party PII in response to Privacy Act requests if VBA purposely included the information in the requester's record. For example, staff were directed to no longer redact third-party PII in a requester's service records since VBA purposely included the requester's own service records in the requester's claims file. However, the May 2016 release policy did not allow disclosure of information belonging to other individuals that was erroneously misfiled in veterans' claims files. In May 2019, the chief of the RMC's centralized support division reported the RMC had completed about 379,000 Privacy Act requests since implementing this new policy.

[1] Examples of types of requests excluded from centralization at the RMC include requests for information other than veterans' records, requests for finance and payment information, and requests for business lines other than Compensation Service or Pension.

[2] VBA Letter 20-16-01, *Privacy Act – Requests for Records*, May 10, 2016. See Appendix A.

What the Review Found

The VA Office of Inspector General (OIG) reviewed a random sample of 30 Privacy Act responses out of about 65,600 Privacy Act requests that RMC staff completed from April 1, 2018, through September 30, 2018.[3] The review team found unrelated third-party names and social security numbers permitted under the May 2016 release policy in 18 of the 30 Privacy Act responses reviewed.[4] These 18 responses included 1,027 third-party names and social security numbers in records that VBA purposely included in requesters' claims files.

The review team determined disclosures under the May 2016 release policy raised legal concerns, and more importantly, put millions of people at risk of identity theft. The VA Office of General Counsel, however, provided legal support for the disclosure practice despite the risk of substantial harm to third parties whose PII is included in a veteran's claims file. The team also found that the May 2016 release policy did not require staff to inform third parties that their PII was released, meaning individuals at risk of identity theft might not be aware of that risk. VBA also did not communicate the policy change to external stakeholders, including veterans and service members.

VBA did not revise its mailing policy or practices after the May 2016 Privacy Act release policy became effective. In all 18 cases in which third-party PII was released pursuant to this policy, the review team found that staff failed to encrypt or protect with passwords the discs that staff mailed to requesters. These discs included the names and social security numbers of both the requesters and unrelated third parties. RMC leaders relied on an exception to the general encryption and password requirements in VA Directive 6609 that permitted staff to mail records without encryption when sending records containing a single individual's information to that person or that person's representative.[5] By its own terms however, this exception did not apply to responses sent under the May 2016 release policy, where multiple individuals' PII was disclosed to requesters.

RMC leaders stated they did not reassess their mailing procedures after the policy changed and did not realize that the exception no longer applied in some cases. However, a team from VBA's Office of Administration and Facilities raised a concern to RMC leadership about the lack of encryption when this team visited the RMC in September 2016. Although the Office of Administration and Facilities team subsequently prepared a report recommending the RMC encrypt and password protect discs, Office of Administration and Facilities managers told the review team that the RMC was not given a copy of the report. By not following procedures

[3] Based on initial sample results, the review team determined a sample size of 30 Privacy Act responses was sufficient to confirm RMC staff were releasing large amounts of third-party PII.

[4] The team focused on unrelated third-party names with social security numbers because VBA's prior policy already stated dependency documents containing PII of a spouse or child do not require redaction.

[5] VA Directive 6609, *Mailing of Sensitive Personal Information*, May 20, 2011.

established to protect information during the mailing process, the RMC put individuals at risk of identity theft if the individuals' PII was on discs that were lost, sent to the wrong recipient, or stolen.

The review team also found third-party names and social security numbers were erroneously disclosed in five of 30 Privacy Act responses reviewed. In these cases, third-party information was either misfiled in requesters' claims files, or RMC staff mistakenly provided the requester with records from another individual's claims file. These five responses erroneously disclosed 31 third-party names and social security numbers. VA's Data Breach Response Service determined each of these cases represented a data breach, and the RMC notified the 31 individuals affected and offered them credit protection services. These erroneous disclosures occurred in part because RMC managers did not effectively hold staff accountable for meeting quality standards when assessing fiscal year 2018 performance due to concerns with the consistency of local quality reviews and the number of reviews completed.

On December 11, 2018, based on the review team's preliminary findings, the OIG recommended in a formal memorandum that the under secretary for benefits, Dr. Paul Lawrence, immediately suspend VBA's release policy and reevaluate VBA's Privacy Act request program (Appendix B). On December 20, 2018, Dr. Lawrence responded that he did not concur with the OIG's recommendation (Appendix C). Dr. Lawrence stated that VBA's May 2016 policy was based on a thorough assessment of the need for requesters' timely and complete access to records. Dr. Lawrence further stated that the policy was issued after an extensive legal review by VA's Office of General Counsel and approval by the VA deputy secretary at the time, Sloan Gibson. Dr. Lawrence also indicated Mr. Gibson approved the proposed policy after a briefing that addressed associated risks. However, the review team interviewed VA and VBA officials with roles related to privacy who expressed serious concerns to the review team that the May 2016 release policy was inappropriate and did not protect third-party PII.

On June 19, 2019, Dr. Lawrence provided an updated response to the OIG, stating that VBA concluded that a Privacy Act policy update was necessary (Appendix D). He reported VBA was working toward both a long- and short-term solution to bring the program into compliance and protect PII. He noted the redaction of third-party PII would commence as soon as possible, but no later than October 1, 2019. Revised guidance was subsequently issued on September 27, 2019 (Appendix H).

What the OIG Recommended

The OIG recommended the under secretary for benefits implement VBA's commitment to update its Privacy Act release policy and ensure VA's website reflects current policy related to the release of third-party PII. The OIG also recommended the under secretary implement a plan to ensure the RMC complies with requirements in VA Directive 6609 for mailing Privacy Act responses and ensure RMC managers receive a report for any site visit of the RMC completed by

VBA and take corrective action as needed. The OIG also recommended the RMC director implement a plan to improve quality reviews and ensure staff are held accountable for the accuracy of their Privacy Act releases.

Management Comments

The under secretary for benefits concurred with Recommendations 1 through 5 and provided acceptable action plans for all recommendations. The OIG will monitor VBA's progress and follow up on the implementation of the recommendations until all proposed actions are completed.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

FY	fiscal year
IRS	Internal Revenue Service
OGC	Office of General Counsel
OIG	Office of Inspector General
PII	personally identifiable information
RMC	Records Management Center
VBA	Veterans Benefits Administration

Introduction

In passing the Privacy Act of 1974, Congress found that the right to privacy is a personal and fundamental right protected by the Constitution of the United States.[6] Similarly, VA policy states, "[t]he privacy of [personally identifiable information] PII is a personal and fundamental right that shall be respected and protected in all VA functions, services, and facilities."[7] PII is any information about an individual that can be used to distinguish or trace their identity, either alone or when combined with other information. For example, PII includes information such as an individual's name, social security number, date and place of birth, mother's maiden name, telephone number, and driver's license number.

Under the Privacy Act, individuals may request access to their Veterans Benefits Administration (VBA) claims files.[8] VBA is required to allow the individuals or their representatives to review the claims files and have copies made. These claims files include records in VBA's possession that often include third-party PII. A third party is any individual, other than the claimant, identified in the claimant's record. For example, military service records may contain the PII of multiple individuals such as the names and social security numbers of doctors who treated a veteran. The doctors' information would be third-party PII.

In 2015, VBA centralized processing of Privacy Act requests, with some exclusions, to its Records Management Center (RMC) in St. Louis, Missouri.[9] The RMC fulfills most Privacy Act requests electronically. Requested records are downloaded, placed on a compact disc, and mailed to the requester. A duplicate copy of the disc is retained for at least five years to satisfy legal retention requirements. The VA Office of Inspector General (OIG) conducted this review to determine whether RMC staff disclosed third-party PII when responding to Privacy Act requests.

VBA Historically Required Redaction of Third-Party PII

Prior to May 10, 2016, VBA's Privacy Act policy required staff to limit disclosure to information that pertained only to the requester, and staff were required to redact third-party information.[10] This practice required staff to conduct a page-by-page review of requested records and use software to block out the third-party information prior to release. In July 2014, VBA's

[6] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896.

[7] VA Directive 6502, *VA Enterprise Privacy Program*, May 5, 2008.

[8] 5 U.S.C. § 552a (d)(1) (2014).

[9] Examples of types of requests excluded from centralization at the RMC include requests for information other than veterans' records, requests for finance and payment information, and requests for business lines other than Compensation Service or Pension.

[10] VBA Handbook 6502, *Privacy and Release of Information*, July 11, 2012.

Compensation Service addressed the issue of documents containing PII for multiple claimants and stated, "VA may not provide information that includes 'personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy' in response to a request for records under the Privacy Act."[11] Further, VBA's Office of Administration and Facilities previously issued guidance acknowledging that veterans' claims files frequently contain PII about third parties.[12] The Office of Administration and Facilities stated these records could not be released unredacted without the permission of the third party. Although VBA representatives were unable to tell the review team how long this requirement had been in place, the team identified VBA policy documents requiring staff to redact as early as July 2012.[13]

VBA Changed Its Privacy Act Release Policy in May 2016

On May 10, 2016, Danny Pummill, the acting under secretary for benefits at the time, issued a new Privacy Act release policy.[14] A copy of this policy, which was drafted by VBA's former Office of Disability Assistance, is included in Appendix A.[15] Dr. Paul Lawrence, the under secretary for benefits at the time of the OIG review, was not in that position when the May 2016 release policy was being developed. He told the OIG that the individuals involved in the creation and implementation of the May 2016 policy were

- Sloan Gibson, former VA deputy secretary;
- Danny Pummill, former acting under secretary for benefits;
- David McLenachen, VBA's former deputy under secretary for disability assistance; and
- Robert Waltemeyer, VBA's former director of the Office of Management.

The May 2016 policy changed the practice of redacting third-party PII from VBA claims records prior to release. Under that policy, VBA staff would respond to Privacy Act requests without redacting PII of third parties that was "properly included" in requested records.[16] The policy described third-party PII that was properly included in the record as information that VBA

[11] Compensation Service Bulletin, July 2014. Compensation Service develops rulemaking and policy requirements in support of the compensation benefit program.

[12] Office of Administration and Facilities oversees policy development and procedures for VBA's Privacy Act activities.

[13] VBA Handbook 6502, *Privacy and Release of Information*, July 11, 2012.

[14] VBA Letter 20-16-01, *Privacy Act – Requests for Records*, May 10, 2016.

[15] The Office of Disability Assistance coordinated initiatives, projects, and procedural changes for VBA's Compensation Service, Pension and Fiduciary Service, Insurance Service, and Benefits Assistance Service.

[16] Criminal investigation records were an exception to the May 2016 policy and continued to require redaction of third-party PII.

purposely included. For example, staff were directed to no longer redact third-party PII in a requester's service records since VBA purposely included the requester's own service records in the requester's claims file. However, staff were still not allowed to disclose information to requesters that was erroneously placed in the records, such as misfiled documents for another veteran.

Results and Recommendations

Finding 1: VBA Policy Permitted RMC Staff to Disclose Third-Party Names and Social Security Numbers in Response to Privacy Act Requests

VBA's May 2016 Privacy Act release policy permitted RMC staff to disclose some unrelated third-party names and social security numbers to veterans or their representatives when responding to Privacy Act requests. The review team reviewed a sample of 30 Privacy Act responses and found that 18 included 1,027 unredacted third-party names and social security numbers allowed under the May 2016 release policy. On December 11, 2018, the OIG recommended that the under secretary for benefits, Dr. Paul Lawrence, immediately suspend VBA's Privacy Act release policy, but he did not agree, and the practice continued. Subsequently, on June 19, 2019, Dr. Lawrence provided an updated response indicating VBA had concluded that a Privacy Act policy update was necessary. He reported the redaction of third-party PII would commence as soon as possible, but no later than October 1, 2019.

VBA changed its Privacy Act release policy in 2016 to improve veterans' access to their records. At the time VBA implemented the policy, it had a large backlog of Privacy Act requests resulting in a growing number of appeals and litigation. VBA officials told VA's Office of General Counsel (OGC) that the requirement to redact third-party information was a major factor in the delays, and OGC provided alternative redaction options in response. Because VBA also wanted to provide veterans with online access to claims records, the release policy needed to change because it was not feasible to review and redact millions of records.

The review team obtained documents showing OGC determined that the Privacy Act did not specifically address third-party information, and there was case law that could be used as legal support to stop redacting third-party PII.[17] However, the OGC representative also noted VBA should be sensitive to those third parties who may also be veterans. The OIG contends that the May 2016 policy could place VBA at legal risk of penalties for Privacy Act violations based on other more recent case law.[18]

VBA officials made the decision to stop redacting information that was purposely included in claims files, despite the inherent risks of disclosing third-party PII in service records, as well as former spouse and dependent PII. Although the VA deputy secretary at the time, Sloan Gibson, approved the policy after being briefed of the associated risks, the review team interviewed VA

[17] Voelker v. IRS, 646 F.2d 332 (8th Cir. 1981).

[18] See Windsor v. A Federal Executive Agency, 614 F. Supp. 1255 (M.D. Tenn. 1983), aff'd 767 F.2d 923 (6th Cir. 1985). See also Sussman v. U.S. Marshals Service, 494 F.3d 1106 (D.C. Cir. 2007).

and VBA officials with roles specifically related to privacy who expressed serious concerns with the appropriateness of the May 2016 Privacy Act release policy.

In May 2019, the chief of the RMC's centralized support division reported staff had completed about 379,000 Privacy Act requests since implementing the May 2016 release policy. Based on the volume of third-party PII the review team found in the sample of 30 Privacy Act responses, the OIG determined that the RMC could have already released millions of third parties' names and social security numbers.

VBA officials considered that misuse of a third party's information could cause significant harm to the third party. VBA officials agreed that the policy could increase the risk for identity theft. However, VBA did not notify external stakeholders of the policy change or update its public website. Therefore, if individuals were harmed under this policy, they could be unaware that VBA staff released their information.

What the OIG Did

There were about 65,600 Privacy Act requests completed by the RMC during the review period from April 1, 2018, through September 30, 2018. The review team reviewed a random sample of 30 of those completed requests, which was sufficient to confirm RMC staff were releasing large amounts of third-party PII. The team obtained duplicate copies of discs from the RMC with the records released in response to the sampled Privacy Act requests. The team used these discs and VBA's electronic systems, including the Veterans Benefits Management System, to review the sample and assess whether RMC staff released unrelated third-party names with social security numbers as permitted under the May 2016 Privacy Act release policy.

Although the team identified additional types of PII in the sample that were released in accordance with the Privacy Act release policy—including military service numbers, addresses, and dates of birth—the team focused on unrelated third-party names with social security numbers. It did so because these numbers can be used to get other personal information and commit identity theft. Further, VBA's prior policy already stated dependency documents containing PII of a spouse or child do not require redaction.

The review team discussed the findings with VA and VBA officials and included their comments in the report, as appropriate. The review team performed a site visit at the RMC in St. Louis, Missouri, in February 2019. Appendix F provides additional details on what the review team did.

Details of this finding appear in the following sections:

- RMC staff released third-party names and social security numbers in accordance with VBA policy.
- VBA changed its release policy to improve veterans' access to their records with legal support from OGC, despite known risks.

- Individuals potentially harmed may be unaware of VBA's policy.

RMC Staff Released Third-Party Names and Social Security Numbers According to VBA Policy

RMC staff disclosed third-party names and social security numbers that were permitted under the May 2016 Privacy Act release policy in 18 of 30 Privacy Act responses reviewed. These 18 responses included 1,027 unredacted third-party names and social security numbers. The release policy in effect directed staff not to redact this PII from Privacy Act responses. Table 1 provides details of the responses reviewed and the number of third-party names and social security numbers disclosed.

Table 1. Responses with Third-Party Names and Social Security Numbers Allowed under the 2016 Release Policy

Requester	Responses reviewed	Responses with third-party names and social security numbers	Number of third-party names and social security numbers included
Veteran	19	10	426
Veteran's representative	11	8	601
Total	**30**	**18**	**1,027**

Source: OIG analysis of 30 Privacy Act requests completed from April 1, 2018, through September 30, 2018

Generally, the third-party names and social security numbers were contained in the requesters' service records—medical and personnel records created during an individual's military service. Medical records describe medical and dental care a service member received. Personnel records are administrative records containing information about a service member's service history. The following are examples of Privacy Act responses in which RMC staff disclosed third-party names and social security numbers in accordance with the release policy in effect.

Example 1

Staff sent a disc to a veteran's representative who requested the veteran's records. The disc contained the names and social security numbers of 259 other individuals. This PII was included in the veteran's personnel records, which contained military orders that listed the names and social security numbers of other service members.

Example 2

> *Staff sent a disc to a veteran who requested his records, and the disc contained the names and social security numbers of 197 other individuals. The disc included medical professionals' PII that was in the veteran's medical records, as well as other service members' PII listed in the veteran's personnel records.*

According to VA, the term "breach" generally includes the acquisition, access, use, or disclosure of PII in a manner not permitted by law or VA policy which compromises the security or privacy of the information.[19] Since VA's definition of a breach is dependent on its own policies, VA would not consider third-party PII disclosures allowed under the release policy in effect during the review period to be breaches although they may have been considered breaches under the prior policy. The review team asked the director of VA's Data Breach Response Service, who is also the chairman of VA's National Data Breach Core Team, whether the RMC sending veterans their own service records with third-party names and social security numbers would be considered a breach.[20] He reported that the scenario would more than likely have been considered a breach resulting in an offer of credit protection services under VBA's prior policy. However, since this was permissible by the May 2016 release policy, it would no longer be considered a breach.

On December 11, 2018, the OIG issued a memorandum to the under secretary for benefits, Dr. Paul Lawrence, notifying him that the RMC was releasing third-party PII and informing him of the potential legal impact of penalties for Privacy Act violations (Appendix B). The OIG recommended Dr. Lawrence immediately suspend VBA's release policy and reevaluate VBA's Privacy Act request program. On December 20, 2018, Dr. Lawrence responded that he did not concur with the OIG's recommendation (Appendix C). He replied that VBA's May 2016 policy was based on a thorough assessment of requesters' need for timely and complete access to records, and the policy was issued after an extensive legal review by VA's OGC and approval by the then VA deputy secretary, Sloan Gibson.

The review team continued its review, and on June 19, 2019, Dr. Lawrence provided an updated response to the OIG's December 11, 2018, memorandum (Appendix D). Dr. Lawrence stated that VBA had reviewed existing policies and processes and concluded that a Privacy Act policy update was necessary. He reported VBA was working towards both a long- and short-term solution to bring the program into compliance and protect PII. Dr. Lawrence noted VBA's comprehensive solution would require a phased approach, and VBA would request the additional

[19] VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, July 28, 2016.

[20] The Data Breach Response Service is responsible for handling all privacy and security-related events that are entered into the Privacy and Security Event Tracking System. Complex breaches are referred to VA's Data Breach Core Team.

resources needed through the budgetary process. However, he stated the redaction of third-party PII would commence as soon as possible, but no later than October 1, 2019.

VBA Changed Its Release Policy to Improve Veterans' Access to Their Records with Legal Support from OGC Despite Known Risks

In an email, the then deputy under secretary for disability assistance, David McLenachen, reported the primary reasons for issuing the May 2016 Privacy Act release policy were

- A massive backlog of Privacy Act requests caused by the past redaction requirement,
- Claimants' rights to their records under the Privacy Act, and
- A push by Mr. Gibson to provide veterans electronic access to their records.

Emails between VBA officials and OGC show VBA officials consulted with OGC when developing the May 2016 policy, and OGC determined there was legal support for disclosing unredacted records. However, OGC also noted there were some inherent risks such as disclosing third-party PII in service records and former spouse and dependent PII. Further, OGC noted the potential harm from misuse of such information could be substantial. Both Mr. McLenachen and VA's acting general counsel agreed that the decision was ultimately left up to VBA leaders.

Dr. Lawrence stated VBA did not take this change of policy lightly. He indicated that VBA and OGC briefed Mr. Gibson on the proposed policy change, as well as the risk that VBA could disclose third-party PII. The policy change was approved by Mr. Gibson, and the policy was issued by the acting under secretary for benefits serving at that time, Danny Pummill. VA and VBA officials with roles specifically related to privacy expressed serious concerns during interviews with the review team that the May 2016 Privacy Act release policy is inappropriate and does not protect third-party PII; however, some of them were not involved in creating the policy.

RMC's Growing Backlog of Privacy Act Requests

VBA conducted a pilot program to centralize the Privacy Act requests from five offices to the RMC from March to June 2014. Then, starting in August 2014, offices were added in groups to the RMC operations until the nation's workload was fully transferred to the RMC in March 2015. However, a large backlog of Privacy Act requests quickly developed. The chief of the RMC's centralized support division provided the review team data regarding the pending inventory and timeliness of the RMC's Privacy Act requests.

Figures 1 and 2 show the number of pending Privacy Act requests at the RMC and the average days they had been pending at the beginning of each month from January 2015 until VBA changed its release policy.

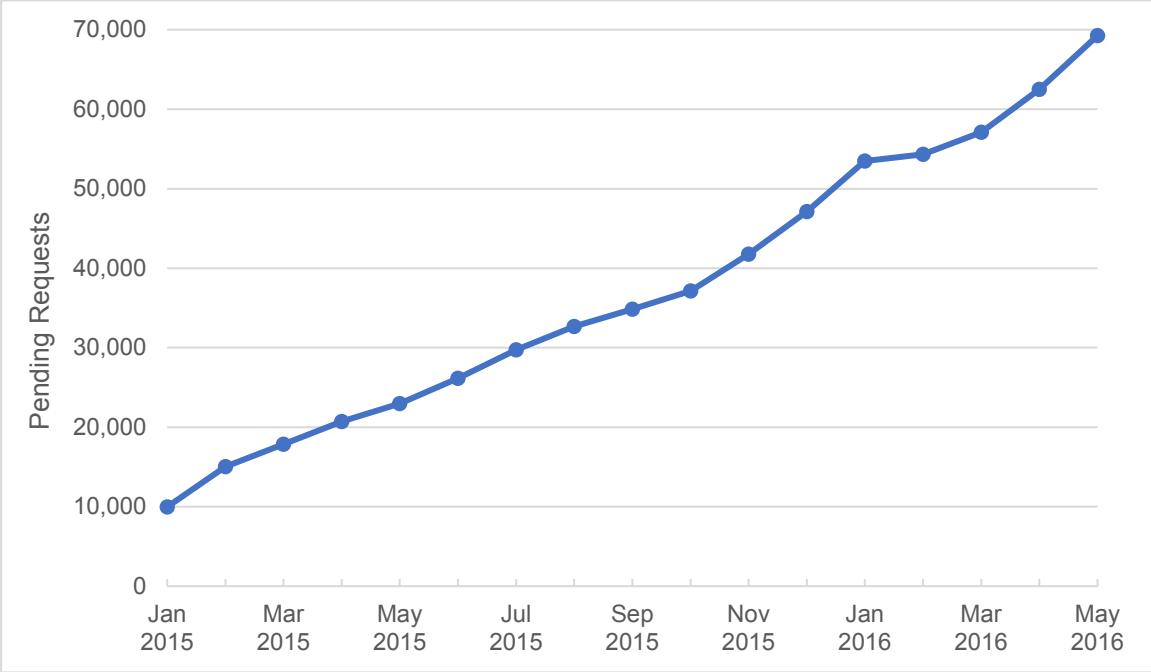

Figure 1. *Inventory of Privacy Act requests at the RMC from January 1, 2015, to May 1, 2016*
Source: VA OIG presentation of data provided by the chief of the RMC's centralized support division

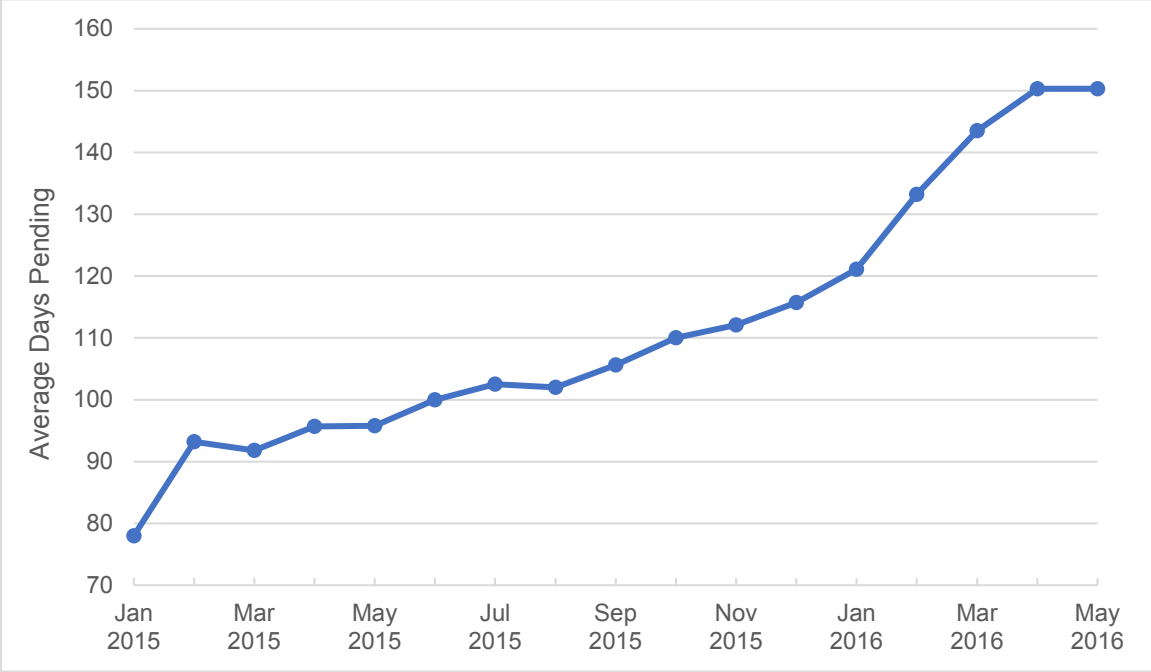

Figure 2. *Average days that Privacy Act requests were pending at the RMC from January 1, 2015, to May 1, 2016*
Source: VA OIG presentation of data provided by the chief of the RMC's centralized support division

The former RMC director told the review team the RMC was never sufficiently staffed to keep up with the Privacy Act requests prior to the issuance of the May 2016 release policy. In

May 2014, RMC managers assessed staffing needs for centralization; however, the former RMC director subsequently reported the RMC was only authorized to hire 62 of the 71 additional employees initially requested. In August 2014, the director at the time had already noted that without additional staffing, the RMC was at high risk of "finding itself in a hole out of which it will be difficult to climb."

In January 2015, the RMC's former lead management analyst notified the Office of Field Operations of a "rapid increase in inventory" over the past month and a half. He projected "exponential growth" of inventory if it moved forward without additional staff or technology enhancements. In July 2015, the former RMC director reported to the Midwest District that inventory and timeliness continued to worsen and could not be stabilized without additional staffing.[21] However, the RMC had been told by the Office of Field Operations that there were no additional staff available because of budget constraints at the time. The former RMC director also stated the situation was urgent enough to begin exploring alternative means to increase production.

Effect of Privacy Act Request Backlog on the OGC

VBA's backlog of Privacy Act requests was also affecting the OGC. OGC provided documents that indicated there was a meeting in May 2015 between OGC and VBA officials to discuss the growing number of appeals and litigation associated with Privacy Act access requests. OGC managers told the review team that the bulk of the Privacy Act appeals they received were because veterans did not get access to their records in a timely manner. Further, documents received from VBA and OGC showed that VA also faced litigation for access delays. The review team asked OGC for additional information quantifying these administrative appeals and litigation. However, OGC did not provide a response.

According to OGC documents, VBA reported it had a large backlog of Privacy Act requests at the May 2015 meeting, and the requirement to redact third-party information was a major contributing factor in the delays. VBA also indicated that not having to review each page of a claims file for third-party information would enable faster processing of Privacy Act requests. Because of the growing number of appeals and litigation, OGC shared an interest in resolving VBA's backlog of Privacy Act requests. In response to this meeting, OGC officials reassessed the law and judicial opinions regarding Privacy Act requests and provided VBA with options regarding whether to redact third-party information.

Although VBA officials indicated to OGC that not having to review each page of claims files for third-party information would enable faster processing of Privacy Act requests, the chief of the RMC's centralized support division told the OIG review team that staff must still conduct

[21] District offices are responsible for the effective management of VBA regional offices in an assigned geographical area.

page-by-page reviews to identify any misfiled documents in requesters' records. Therefore, she noted seeing some increased efficiency under the May 2016 release policy, but not a lot.

VBA's Plans to Modernize Claims Records Access

According to the May 2016 Privacy Act release policy, VBA planned to modernize its culture, improve or eliminate processes that impeded great customer service, and rethink internal structures to become more veteran-centric and productive. In addition, VBA was working toward giving veterans online access to their claims records. VBA concluded that providing veterans prompt and complete access to their claims records would increase transparency, improve customer service, and greatly benefit claimants.

The review team recognizes that providing veterans prompt access to their claims records could improve customer service and benefit claimants. However, providing veterans complete, unredacted access to records would place other individuals' PII at risk. Mr. McLenachen told the review team that it would not have been feasible for VBA to review and redact millions of records before providing this online access. Therefore, it was necessary for VBA to change its release policy before it could continue pursuing veterans' online access to claims records.

VA's Legal Analysis for Disclosing Unredacted Records

Officials with the former Office of Disability Assistance conferred with OGC regarding legal support for disclosing unredacted records to Privacy Act requesters. OGC prepared memorandums for VBA leaders in June and July 2015 that analyzed the law and judicial opinions related to Privacy Act access requests. Although OGC officials were unable to confirm whether the memorandums were delivered to VBA, in its analysis, OGC noted that since the Privacy Act does not address third-party information in an individual's record, courts have been forced to address this "gap." OGC discussed two primary judicial approaches that reached opposite conclusions concerning whether Privacy Act requesters have a right to access third-party information in the requesters' records.[22]

OGC and VBA then discussed the "legal support for a VBA business decision to disclose to Veterans completely unredacted copies of their claims files" through a series of email messages later in July 2015. Mr. McLenachen was specifically concerned about whether employees would be protected from Privacy Act disclosure penalties. OGC officials replied that staff were unlikely to be held personally liable for granting veterans access to their claims files consistent with a

[22] OGC noted that in Voelker v. IRS, the court held that if information is in a system of records and retrieved by the individual's name or other unique identifier, then it is about the individual, and the individual has a right to access it. See 646 F.2d 332, 333-35 (8th Cir. 1981). However, OGC also noted that in DePlanche v. Califano, the court held that although the information is maintained in a system of records and retrieved by the individual's name, if the information is not actually about the individual, then there is no right to access it. See 549 F. Supp. 685, 693-98 (W.D. Mich. 1982).

VBA policy that is sound and appropriately balances competing privacy interests. For example, OGC described balancing "the need for Veterans to be granted prompt access to their files against the expectation that VBA won't intentionally or willfully disclose third-party information." OGC also stated that although the Privacy Act doesn't speak to third-party information, VBA should still be mindful and sensitive to those third parties who may be veterans themselves.

OIG's Concerns with OGC's Legal Analysis

OGC cited *Voelker v. IRS*, a 1981 Eighth Circuit case as legal support for providing veterans unredacted copies of their claims files.[23] Dr. Lawrence also referenced *Voelker* when he initially disagreed with OIG's recommendation in December 2018 to suspend the Privacy Act release policy.

Because the *Voelker* case cited by OGC related to the Internal Revenue Service (IRS), the OIG contacted the IRS to determine whether it would release social security numbers of unrelated third parties to Privacy Act requesters. An official from the IRS Office of Chief Counsel's group that handles privacy law and disclosure matters indicated that no one in the group could remember an instance in which third-party PII was included in IRS Privacy Act requested records. He also noted the *Voelker* case concerned investigative records of an IRS employee, and it failed to indicate if any third-party social security numbers were present in the requested records.

Although *Voelker* has remained unchallenged in the Eighth Circuit, VBA's reliance on this case law is problematic given that other case law, such as *Windsor v. A Federal Executive Agency* in the Sixth Circuit and *Sussman v. U.S. Marshals Service* in the D.C. Circuit, have more recently held that releasing such information violates third parties' rights under the Privacy Act.[24] This distinction is noted on the Department of Justice's Office of Privacy and Civil Liberties website, which specifically notes that *Sussman* controls in the D.C. Circuit.[25] The OIG finds the Department of Justice's interpretation of the Privacy Act provisions particularly relevant because the Federal Programs Branch of the Department of Justice's Civil Division defends civil actions involving alleged violations of the Privacy Act against the VA.

The OIG also determined that the likelihood of Privacy Act litigation against the VA being filed in the Eighth Circuit is relatively low. Affected individuals are likely to file in the federal district courts in their home states or the D.C. District Court, which has universal venue for Privacy Act

[23] Voelker v. IRS, 646 F.2d 332 (8th Cir. 1981).

[24] Windsor v. A Federal Executive Agency, 614 F. Supp. 1255 (M.D. Tenn. 1983), aff'd 767 F.2d 923 (6th Cir. 1985) and Sussman v. U.S. Marshals Service, 494 F.3d 1106 (D.C. Cir. 2007).

[25] "Overview of the Privacy Act of 1974," DOJ Office of Privacy and Civil Liberties website, accessed April 26, 2019, https://www.justice.gov/opcl/individuals-right-access.

cases. Therefore, VBA could be at risk if such civil actions are filed in district courts in circuits that protect third-party PII under the Privacy Act. On February 11, 2019, the OIG provided its legal analysis to VA's acting general counsel and invited OGC to provide any comments or contrary arguments (Appendix E). However, OGC did not provide a response.

Disclosure Risks for Third-Party PII in Service Records

OGC noted a risk associated with releasing unredacted records to Privacy Act requesters was that some service records contain other individuals' social security numbers. Further, Mr. McLenachen stated he knew that service records often contained PII about other individuals. Before issuing the May 2016 Privacy Act release policy, VBA and OGC briefed the then VA deputy secretary Sloan Gibson regarding the risk of providing requesters their own service records with other individuals' PII. The briefing materials indicated many veterans already had access to this PII as part of their military records. For example, the RMC director told the review team that he assumed veterans received a copy of their own records while in the military, so the information had already been released. However, Mr. McLenachen stated he did not know how many veterans already had access to this information. Further, even if some veterans had received copies of their military records in the past, RMC managers agreed staff would not know whether a specific requester already had the information.

Disclosure Risks for PII of Dependents and Former Spouses

OGC also noted a risk associated with releasing dependents' or former spouses' information included in veterans' claims files. For example, in an apportionment case, for which VA pays all or part of a veteran's disability award to a former spouse on behalf of the veteran's child, the veteran's claims file could include the former spouse's current address and banking information. Before issuing the May 2016 Privacy Act release policy, VBA and OGC briefed Mr. Gibson regarding the risk of providing veterans access to a former spouse's otherwise unknown address. The briefing materials indicated the apportionment form includes notice that information provided may be disclosed when authorized under the Privacy Act. Although the form includes a general statement regarding the Privacy Act, it does not specifically state that the former spouse's current address would be disclosed to the veteran. Furthermore, for apportionment cases, VA's website states staff should furnish the information that is vital to the decision, which usually includes the income and expenses of each party.[26]

[26] VA Manual 21-1, part III, sub. v, chap. 3, sec. A, topic 1, "General Information on Apportionments," February 19, 2019, VA website, accessed July 11, 2019, https://www.knowva.ebenefits.va.gov/system/templates/selfservice/va_ssnew/help/customer/locale/en-US/portal/554400000001018/content/554400000014232/M21-1-Part-III-Subpart-v-Chapter-3-Section-A-Apportionment-Process.

Because the May 2016 release policy provides no exclusion for former spouses' current addresses, the OIG is concerned that former spouses could mistakenly believe that VBA would not disclose their addresses in response to a veteran's Privacy Act request. Thus, former spouses may trust VBA with information that could potentially be used to harm them if it were disclosed to a veteran.

OGC officials provided the review team memorandums prepared for VBA leaders stating that OGC could not recommend disclosure of former spouses' or dependents' bank account or other financial information for obvious reasons of potential harm to the third party. One memorandum strongly recommended that VBA take necessary steps to avoid inadvertent disclosure of this information. However, OGC officials were unable to provide documentation confirming whether these memorandums were delivered to VBA. OGC did not express any legal objections to such information being released in its review of the May 2016 release policy draft, and ultimately the policy specifically allowed for the release of third-party bank account information.

VA and VBA Privacy Officials' Concerns with the May 2016 Privacy Act Release Policy

Dr. Lawrence reported that VBA and OGC briefed Mr. Gibson on the risks involved with the proposed change to the Privacy Act release policy, but he approved the policy change anyway. The review team interviewed several VA and VBA officials with roles specifically related to privacy to obtain their perspectives on the Privacy Act release policy. These privacy officials expressed serious concerns to the review team, although some of them were not involved in creating this policy.

The former director of VA's Office of Privacy and Records Management provided the review team with a document that identified privacy and business-related concerns with the release of third-party information before the May 2016 Privacy Act release policy was issued.[27] He stated he was totally against the policy change and thought it would come back to "bite" VBA, but he was not a decision maker.

The director of VA's Privacy Service was not familiar with VBA's May 2016 Privacy Act release policy before the review team's interview.[28] However, she said the policy was not appropriate and anyone who reads it would question it based on common sense, even if he or she

[27] The Office of Privacy and Records Management integrated privacy considerations into the ways in which the VA used technologies and handled information. It also oversaw activities related to creation, maintenance, and use of records. It accomplished these tasks through the following Service Areas: VA Privacy Service, Enterprise Records Service, Freedom of Information Act Service, and Incident Resolution Service.

[28] The mission of VA's Privacy Service is to preserve and protect the PII and protected health information of veterans, their families, and VA employees by promoting a culture of privacy awareness and maintaining the trust of those they serve by embedding and enforcing privacy protections, transparency, and accountability into all VA activities.

was not a privacy expert. She also stated the policy conflicts with the fundamental tenets of the Privacy Act, safeguarding personal information. The privacy officer for VA's Office of Information and Technology within VA's Privacy Service stated she was not involved in creating VBA's May 2016 Privacy Act release policy, and she had grave concerns that it could be violating the Privacy Act.

VBA's privacy officer said she started in her position in July 2016, after Mr. Pummill had issued the May 2016 release policy. When she learned of the policy in September 2016, she had concerns and said it went against everything she knew as a privacy officer. She also stated she had been trying for two years to get the policy rescinded.

The OIG's first recommendation addresses the need for the under secretary for benefits to implement VBA's commitment to update its Privacy Act release policy to protect third-party PII.

Individuals Potentially Harmed May Be Unaware of VBA's Policy

In May 2019, the chief of the RMC's centralized support division reported staff had completed about 379,000 Privacy Act requests since implementing the May 2016 release policy. Based on the volume of third-party PII found in the sample of 30 Privacy Act responses, the 379,000 Privacy Act responses could contain millions of third parties' names and social security numbers.

Even though OGC determined there was legal support for disclosing unredacted records, OGC informed VBA that misuse of third-party information could cause those individuals significant harm. According to the frequently asked questions section on VA's Privacy Service website, individuals whose PII is misused by an identity thief may experience several adverse effects, including loss of money, damage to credit, threats, embarrassment, and harassment.[29]

According to VA's official blog, safeguarding PII is a veteran's best defense against identity theft, and veterans should never disclose their social security numbers to an unknown third party.[30] Mr. McLenachen and other VBA officials acknowledged that the May 2016 Privacy Act release policy could increase the potential for identity theft. The policy does indicate that VBA employees should redact information when there is evidence that the requester intends to use the information to commit a crime or harm another. The chief of the RMC's centralized support division indicated staff redact records before sending them to an incarcerated requester as a precautionary measure. However, she stated staff do not redact records for a previously incarcerated requester.

[29] "Privacy FAQs," VA website, accessed July 31, 2018, https://www.oprm.va.gov/privacy/faqs_privacy.aspx.

[30] "Protecting Yourself from Identity Theft," VA website, accessed May 8, 2019, https://www.blogs.va.gov/VAntage/50303/protecting-identity-theft/.

The May 2016 release policy in effect during this review does not require staff to inform third parties when their PII is released. VA's Privacy Service website indicates individuals have the right to have their personal information kept private, and to have some control over how their PII is released.[31] However, RMC staff confirmed that under the May 2016 release policy they do not ask third parties for permission before releasing the third parties' information to a Privacy Act requester, and staff do not inform third parties after their information is released. The policy also does not allow individuals to choose whether to allow VBA to disclose their PII to other Privacy Act requesters. Furthermore, RMC managers and staff stated that if they were asked, they would be unable to tell an individual whether the RMC had released the individual's information, or to whom. As a result, if individuals were harmed by this policy, they may not know that VBA released their information.

VBA also did not notify external stakeholders, including veterans and service members, of the May 2016 Privacy Act release policy change. VBA's Office of Administration and Facilities (OAF) oversees policy development and procedures for VBA's Privacy Act activities. The executive director of OAF told the review team that to the best of his knowledge, VBA did not notify external stakeholders of its change in policy, and that OGC did not tell VBA to provide such notice. He also confirmed that the policy change was not posted on any public-facing VA websites.

As of July 2019, VA's website still reflected VBA's previous redaction requirement. For example, the website stated staff may not provide information that includes personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy in response to Privacy Act requests.[32] It further states that documents containing PII for multiple individuals, such as service personnel records, must be reviewed for relevancy to a particular claimant's record and copies must be appropriately redacted before they are provided to a third party. However, under the current release policy, RMC staff generally released these types of records with unredacted third-party names and social security numbers. Until VA updates its website, veterans could mistakenly believe that VBA would not disclose their PII in response to someone else's Privacy Act request.

The OIG's second recommendation addresses the need for the under secretary for benefits to ensure VA's website is updated to reflect current VBA policy regarding the release of third-party PII.

[31] "Privacy FAQs," VA website, accessed July 31, 2018, https://www.oprm.va.gov/privacy/faqs_privacy.aspx.

[32] VA Manual 21-1, part III, sub. ii, chap. 4, sec. G, topic 3, "Folder Renovations," September 17, 2018, VA website, accessed July 11, 2019, https://www.knowva.ebenefits.va.gov/system/templates/selfservice/va_ssnew/help/customer/locale/en-US/portal/554400000001018/content/554400000014132/M21-1-Part-III-Subpart-ii-Chapter-4-Section-G-Folder-Maintenance#3d.

Conclusion

Although VA policy states that the privacy of PII is a fundamental right, VBA changed its Privacy Act release policy in May 2016 to allow the disclosure of third-party PII. This policy change created an increased risk of identity theft for individuals who may be unaware their information was disclosed in response to Privacy Act requests. By implementing VBA's commitment to update its Privacy Act release policy, the under secretary for benefits could respect the privacy of third-party PII and reduce the risk of identity theft for third parties. In addition, the under secretary for benefits should make sure VA's website is updated to reflect VBA's current release policy to help ensure individuals know when VBA may release their personal information.

Recommendations 1–2

1. The under secretary for benefits implement the Veterans Benefits Administration's commitment to update its Privacy Act release policy and begin redacting third-party personally identifiable information.
2. The under secretary for benefits ensure VA's website is updated to reflect current Veterans Benefits Administration policy regarding the release of third-party personally identifiable information.

Management Comments

The under secretary for benefits concurred with Recommendations 1 and 2 and provided acceptable action plans for the recommendations. To address Recommendation 1, the under secretary for benefits provided the revised Privacy Act release policy (VBA Letter 20-19-09), which was issued on September 27, 2019. Further, the under secretary stated the redaction of PII began on October 1, 2019. To address Recommendation 2, VBA uploaded the revised Privacy Act release policy to its VBA website on September 27, 2019. VBA has requested closure of both recommendations.

OIG Response

The under secretary for benefits' comments and actions are responsive to the recommendations. For Recommendation 1, the OIG acknowledges that the under secretary for benefits has issued a revised Privacy Act release policy. However, before closing the recommendation, the OIG will review documentation to ensure compliance with the redaction of PII. Although closure has been requested for Recommendation 2, VBA Letter 20-19-09 has not yet been uploaded to VA's website. The OIG will monitor VBA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

Finding 2: RMC Staff Mailed Privacy Act Responses without Encryption or Password Protection

The review team found RMC staff failed to encrypt or password protect the 18 discs discussed under Finding 1 that were mailed with the names and social security numbers of the requesters and unrelated third parties. Although RMC leaders relied on an exception to the general encryption and password requirements for mailing records with a single individual's information, this exception does not apply to responses covered by the May 2016 release policy under which multiple individuals' PII was disclosed to Privacy Act requesters.

On February 6, 2019, the review team notified RMC leaders of its concerns, but the leaders did not change RMC work processes, and staff continued to mail discs without encryption and password protection. The director of the RMC stated he informed OAF and his senior leaders of the OIG's concerns, and to his knowledge OAF was looking into the issue.

RMC leaders stated they did not reassess RMC mailing procedures after the release policy changed and did not realize the exception no longer applied in some cases. Although an OAF team raised a concern to RMC leadership in September 2016 about the lack of encryption, the RMC was not given a formal report on the issue. By not following procedures established to protect information during the mailing process, the RMC put individuals at risk of identity theft if their PII was on discs that were lost, sent to the wrong recipient, or stolen.

What the OIG Did

During a site visit at the RMC in St. Louis, Missouri, in February 2019, the review team interviewed and obtained testimonial information from RMC managers related to its mailing procedures associated with Privacy Act requests. The review team assessed whether the RMC's mailing procedures complied with VA policies based on the sample results described in Finding 1. Appendix F provides additional details on what the review team did.

Details of this finding appear in the following sections:

- RMC staff failed to properly protect discs they mailed to requesters.
- OAF officials did not provide RMC managers a site visit report that recommended protecting discs.
- The RMC's failure to follow VA Directive 6609 increased the risk of identity theft.

RMC Staff Failed to Properly Protect Discs They Mailed to Requesters

When mailing discs containing names and social security numbers, VA Directive 6609 (the directive) generally requires staff to encrypt and password protect the discs.[33] However, the review team found RMC staff mailed discs without encryption or password protection for the 18 of 30 Privacy Act responses that included the names and social security numbers of the requesters and unrelated third parties.

The directive includes an exception that encryption is not required when mailing a disc with records containing a single individual's information to that person or their representative. This exception would not apply to the 18 discs that included the names and social security numbers of multiple individuals. The directive also does not require encryption when mailing a disc to a person or entity that does not have the capability to decrypt it. However, the disc must be password protected, and the password must be provided separately from the disc. In February 2019, the chief of the RMC's centralized support division reported that RMC staff had completed over 352,000 Privacy Act requests since implementing the release policy in May 2016, and the RMC director stated staff had not encrypted or password protected the discs associated with those requests.

As discussed earlier, the review team notified RMC leaders of concerns regarding RMC staff's violation of the directive on February 6, 2019; however, leaders did not change the RMC's work processes and continued to mail discs without encryption and password protection. On March 12, 2019, the RMC director told the review team he had informed OAF and his senior leaders of OIG's concerns, and to his knowledge OAF was looking into the issue. He also stated that once he received information regarding a change in policy, it would be implemented as appropriate.

The OIG's third recommendation addresses the need for the under secretary for benefits to implement a plan to ensure RMC staff comply with requirements for mailing Privacy Act responses noted in the directive.

OAF Officials Did Not Provide RMC Managers a Site Visit Report that Recommended Protecting Discs

Before VBA changed its Privacy Act release policy, the RMC relied on the exception in the directive allowing discs with a single individual's information to be sent to the individual or their representative without encryption or password protection. RMC leaders stated they did not reassess RMC mailing procedures after the policy was changed and did not realize the exception no longer applied in cases where records contained multiple individuals' information. However, the review team obtained documentation that OAF notified RMC leadership of concerns

[33] VA Directive 6609, *Mailing of Sensitive Personal Information*, May 20, 2011.

regarding the lack of encryption in September 2016 when an OAF team visited the RMC to assess its records management and shredding programs.

A Midwest District management analyst's September 20, 2016, email noted that RMC leadership was notified during this site visit that the directive required discs to be encrypted. The email noted the RMC and Midwest District had concerns with moving forward with encryption, which would put the RMC further back on processing Privacy Act requests. The email requested guidance from VBA's Office of Field Operations regarding whether to act on these concerns or continue operations as normal. A subsequent Office of Field Operations email asked OAF for some insight regarding the disc encryption requirement. OAF's chief of administration directed his team to address the issue in the RMC site visit report.

The OAF team's report noted that records were saved to unencrypted discs and released to Privacy Act requesters. Further, the report noted the RMC misrepresented the exception outlined in the directive that applied when records contained only one person's information. OAF recommended RMC staff encrypt all discs and include the password in the acknowledgment letter prior to release of the encrypted disc. Although OAF reported having discussions with the Office of Field Operations, OAF officials were unable to provide any documentation to confirm whether the report was formally sent. The chief of the RMC's centralized support division told the review team she could not find evidence that the RMC received the report, and OAF managers confirmed the RMC was not given a copy of the report.

The OIG's fourth recommendation addresses the need for the under secretary for benefits to ensure RMC management receives a report for any site visit of the RMC completed by VBA and takes corrective action as needed.

Failure to Follow VA Directive 6609 Increased Risk of Identity Theft

The purpose of the directive is to ensure the protection of individuals' personal information, which is vital to the fulfillment of VA's mission. The directive established procedures to protect information during the mailing process, recognizing that mail that is lost, sent to the wrong recipient, or stolen can result in identity theft that may result in personal hardship. Therefore, RMC staff's failure to comply with the directive when mailing discs could increase the risk of identity theft for individuals whose PII is included.

Conclusion

RMC staff put individuals at increased risk of identity theft by violating requirements for encryption and password protection when mailing Privacy Act responses. Although an OAF team identified this issue in 2016 and detailed it in a site visit report, the practice has continued because OAF officials did not provide the site visit report to RMC managers. The under secretary for benefits can protect individuals' PII during the mailing process by implementing a plan to ensure RMC staff comply with requirements for mailing Privacy Act responses. Further,

the under secretary for benefits can ensure necessary corrective actions are taken when concerns are identified by ensuring that RMC managers receive reports for any VBA site visits conducted at the RMC.

Recommendations 3–4

3. The under secretary for benefits implement a plan to ensure the Records Management Center complies with requirements for mailing Privacy Act responses in accordance with VA Directive 6609.
4. The under secretary for benefits establish a plan to ensure that Records Management Center management receives a report for any site visit of the Records Management Center completed by the Veterans Benefits Administration and takes corrective action as needed.

Management Comments

The under secretary for benefits concurred with Recommendations 3 and 4 and provided acceptable action plans for the recommendations. To address Recommendation 3, VBA's Office of Administration and Facilities and the Office of Business Process Integration are developing a Freedom of Information Act Modernization procedure to integrate Freedom of Information Act processing with the Centralized Intake. The target completion date is June 30, 2020.

To address Recommendation 4, the under secretary for benefits stated the RMC and all business lines will receive an out-brief and draft summary report, as well as a list of observations, prior to the Office of Administration and Facilities team leaving the facility. Further, a final report will be provided within three weeks of completion of the site visit. VBA's Office of Administration and Facilities is developing a Site Visit Standard Operating Procedure/Checklist that will include guidelines and procedures for providing feedback to the RMC and VBA business lines. The target completion date is November 15, 2019.

OIG Response

The under secretary for benefits' comments and action are responsive to the recommendations. For Recommendations 3 and 4, the OIG will monitor VBA's progress and follow up on implementation of the recommendations until all proposed actions are completed.

Finding 3: RMC Staff Erroneously Disclosed Third-Party Names and Social Security Numbers in Response to Privacy Act Requests

Although the May 2016 Privacy Act release policy permitted RMC staff to release some third-party PII that VBA purposely included in the requesters' claims files, this policy did not permit RMC staff to send requesters information that was erroneously placed in requesters' claims files, like other people's service or VA claims records. The OIG's review of a sample of 30 Privacy Act responses revealed that RMC staff erroneously disclosed 31 third-party names and social security numbers in five of the responses.

Generally, errors occurred because RMC managers did not effectively hold staff accountable for meeting the quality standard when assessing staff's fiscal year (FY) 2018 performance, despite quality being listed as a critical element on their performance plans. Although the performance plan requires staff to ensure accurate information is provided to veterans, managers expressed concerns with the consistency of local quality reviews and stated some required reviews of staff members' work were not performed during FY 2018.

Improper disclosures potentially violated individuals' rights to privacy and confidentiality. After the review team notified RMC leaders of the five cases, VA determined all five represented data breaches, and all 31 individuals affected were offered credit protection services.

What the OIG Did

While reviewing the same sample of Privacy Act responses described in Finding 1, the OIG review team also assessed whether RMC staff erroneously released unrelated third-party names with social security numbers. The team identified additional types of PII in the sample that were erroneously released, including VA file numbers and addresses. However, as noted in Finding 1, the team focused on unrelated third-party names with social security numbers. The OIG review team also performed a site visit at the RMC in St. Louis, Missouri, in February 2019. Appendix F provides additional details on what the review team did.

Details of this finding appear in the following sections:

- RMC staff released names and social security numbers in violation of VBA policy.
- RMC managers did not effectively hold staff accountable for meeting quality performance standards.
- Data breaches potentially violated individuals' privacy and confidentiality.

RMC Staff Released Names and Social Security Numbers in Violation of VBA Policy

In five Privacy Act responses, RMC staff disclosed third-party names and social security numbers that should not have been released under the May 2016 policy because VBA did not

purposely include this information in the requesters' records. These five responses included a total of 31 third-party names and social security numbers. Table 2 shows how often Privacy Act responses improperly disclosed unrelated third-party names and social security numbers and how many third parties were affected, even in this small sample.

Table 2. Responses That Erroneously Disclosed Third-Party Names and Social Security Numbers

Requester	Responses reviewed	Responses that erroneously disclosed third-party names and social security numbers	Number of third-party names and social security numbers included
Veteran	19	3	28
Veteran's representative	11	2	3
Total	**30**	**5**	**31**

Source: OIG analysis of 30 Privacy Act requests completed from April 1, 2018, through September 30, 2018

In four cases, staff sent requesters third-party records that were misfiled in the requesters' claims files. In the remaining case, staff sent a requester records from another veteran's claims file. The following examples provide details on these cases.

Example 3

Staff sent a disc to a veteran who requested his records, and the disc contained the names and social security numbers of 21 other individuals on records that were misfiled in the veteran's claims file. The 21 names and social security numbers were listed on a misfiled service record that assigned their military occupational specialty. The disc also contained misfiled service records with medical information for one of the individuals.

Example 4

Staff sent a disc to a veteran who requested his records. The contents of the disc were from another veteran's claims file, other than the final Privacy Act response letter. The disc contained the names and social security numbers of the other veteran as well as his spouse and three children. The records on the disc also included the other veteran's claims information, banking information, medical information, service information, address, and date of birth.

Two of the five cases for which the review team identified errors had undergone a local review by a quality assurance specialist who did not identify all the misfiled records the review team found. The RMC director agreed with the errors identified in these five cases.

RMC Managers Did Not Effectively Hold Staff Accountable for Meeting Quality Performance Standards

RMC managers and staff gave a variety of reasons for why the errors the review team identified could have occurred. For example, the errors may have been due to inattention to detail, carelessness, the requirement to review a large number of pages, or simply human error. Managers reported that staff are held accountable for the quality of their Privacy Act releases through the RMC's quality assurance program. According to the staff performance plan, an expanded random monthly sample of the employee's work should be reviewed if the work demonstrated the need for quality improvement. However, managers expressed concerns with the consistency of the reviews completed by the quality assurance specialists, and stated expanded samples were not performed during FY 2018. Therefore, managers did not hold staff accountable for meeting the quality standard when assessing FY 2018 performance, despite quality being listed as a critical element on staff performance plans.

The OIG's fifth recommendation addresses the need for the RMC director to implement a plan to improve quality reviews and ensure staff are held accountable for the accuracy of their Privacy Act releases.

Data Breaches Potentially Violated Privacy and Confidentiality

Cases in which the RMC erroneously released third-party information potentially violated the third parties' rights under the Privacy Act and the confidential nature of claims, as VA is required to keep records pertaining to any claim confidential and privileged.[34] The review team identified five discs with unredacted third-party information including names, social security numbers, addresses, dates of birth, claims information, medical information, military service information, and banking information. This third-party information would have been accessible to the Privacy Act requesters once the requesters received their discs.

After the review team notified RMC leaders of the five cases, the RMC's privacy officer entered the cases into the Privacy and Security Event Tracking System. Ultimately, VA's Data Breach Response Service determined each of these cases represented a data breach, and the RMC notified the 31 individuals affected and offered credit protection services. However, these individuals may never have found out their data had been breached if not for the OIG's review.

[34] 38 U.S.C.A. § 5701 (2017).

Conclusion

RMC staff erroneously released third-party PII resulting in data breaches that potentially violated individuals' privacy and confidentiality. Holding staff accountable for the quality of their Privacy Act responses is critical to preventing these types of errors from recurring. By implementing a plan to improve quality reviews and hold staff accountable for their releases, the RMC director can reduce erroneous disclosures and help protect third-party privacy.

Recommendation 5

5. The Records Management Center director implement a plan to improve quality reviews and ensure staff are held accountable for the accuracy of their Privacy Act releases.

Management Comments

The under secretary for benefits concurred with Recommendation 5 and provided an acceptable action plan for the recommendation. To address Recommendation 5, the director of the RMC is developing a plan to improve quality reviews and ensure staff are held accountable for the accuracy of their Privacy Act releases. The target completion date is October 31, 2019.

OIG Response

The under secretary for benefits' comments and actions are responsive to the recommendation. For Recommendation 5, the OIG will monitor VBA's progress and follow up on implementation of the recommendation until all proposed actions are completed.

Appendix A: VBA Letter 20-16-01, "Privacy Act – Requests for Records"

May 10, 2016

VBA Letter 20-16-01

Director (00/21)

All VBA Facilities

ATTN: All VBA Regional Offices and Centers

SUBJ: Privacy Act – Requests for Records

Purpose

This letter establishes general Veterans Benefits Administration (VBA) policy for responding to Veterans' and their surviving spouse-claimants' requests for their VBA claim records.[1] Moving forward:

With the exception of the criminal investigation records identified below, VBA facilities should respond to requests for records under the Privacy Act without delaying the release by redacting personal identifiable information (PII) of third parties that is properly included in requested records.[2] A third party is any individual, other than the claimant, identified in the claimant's record.

VBA facilities will continue to redact third party PII from any federal or military criminal investigation record released in conjunction with a request for records.[3] Criminal investigation records include investigatory material compiled by any federal agency for law enforcement purposes ***or*** maintained by a federal agency or component thereof which performs as its principal function any activity pertaining the enforcement of criminal laws. *See* 5 U.S.C. § 552a(j)-(k).

NOTE: Except with the written consent of the Veteran or an individual with a right of access, VBA may not disclose any record by any means of communication to any third party that is not the Veteran or an individual with a right of access, unless authorized by law. Disclosures of the Veteran's records to the Veteran, or to an individual with a right to access under the Privacy Act, generally do not require a written request.

[1] A Veteran, his or her surviving spouse who has filed a claim for survivor benefits, an individual authorized by written consent of the Veteran or surviving spouse-claimant to access his or her record, an individual who has been substituted to continue the Veteran's or surviving spouse-claimant's claim, and/or the representative(s) of a deceased Veteran's estate have a right of access to the record. For purposes of this letter, a "spouse-claimant" includes survivors who received an automated award of dependency and indemnity compensation under 38 U.S.C. § 1318 without filing a claim for benefits.

[2] The policy set forth in this document does **not** apply to requests for information under the Freedom of Information Act (FOIA). VBA will continue to redact third-party PII when processing FOIA requests.

[3] This exception to the general policy of full disclosure remains in effect pending VA's coordination with other federal agencies regarding a long-term policy for releasing criminal investigation records. VBA will notify field employees of any future changes to this policy.

Authority

5 U.S.C. §§ 552, 552a; 38 C.F.R. §§ 1.550-1.582

Background

This policy represents a change from the prior VBA practice of redacting certain information from VBA claim records prior to release. VBA has concluded that principles of transparency and accountability demand that Veterans and their surviving spouse-claimants enjoy unfettered access to the information relied upon by VBA to decide their claims. Moreover, a policy of prompt and complete access is consistent with relevant legal authority.

a. VBA's Strategic Plan and MyVA Principles

VBA's strategic plan and vision for the future focus on achieving a Veteran-centric, readily accessible service organization. In addition, the MyVA Transformational Plan reiterates the importance of modernizing VBA's culture, improving or eliminating processes that impede great customer service, and rethinking internal structures to become more Veteran-centric and productive. VBA has concluded that providing Veterans and their surviving spouse-claimants prompt access to their complete claim records is critical to increase transparency and improve customer service.

In addition, VBA is working towards affording Veterans and their surviving spouse-claimants online access to their claim records, regardless of whether VBA has received a request for the records. VBA will notify field employees and external stakeholders when this access is available, and will provide additional instructions at that time to further improve customer service to Veterans and their surviving spouse-claimants.

b. The Privacy Act, 5 U.S.C. § 552a, implemented by 38 C.F.R. §§ 1.575-1.582

VBA must follow the Privacy Act, which protects "records" pertaining to individuals that a federal agency maintains in a "system of records." The Act defines "record" as any "item, collection, or grouping of information about an individual that is maintained by an agency" within its system of records. *See* 5 U.S.C. § 552a(a)(4). A system of records is a file, database, or program from which personal information is retrieved by the individual's name or other personal identifier. § 552a(a)(5). Importantly, the Privacy Act affords individuals the right to access records about them, as maintained by a federal agency. Upon request from an individual to access his or her record, VBA must provide the requestor an opportunity to review the record and have a copy made of all or any portion of the record. *See* 5 U.S.C. § 552a(d). As such, providing claimants complete access to their claim records is consistent with the Privacy Act. *See* Voelker v. IRS, 646 F.2d 332, 333-35 (8th Cir. 1981).

A VBA claims file, whether it is in an electronic format or is a paper record that has not yet been converted to electronic format, is a "record" within the Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA (58VA21/22/28) system of records and is therefore subject to the Privacy Act. In addition to information received by VBA in conjunction with a claim for benefits, a VBA claims file includes any military Service Treatment Records (STRs) in VA's possession, or available to VBA through its system of records. Among other matters, this system of records pertains to Veterans who have applied for disability compensation under 38 U.S.C. chapter 11, survivors who have applied for dependency and indemnity compensation under 38 U.S.C. chapter 13, and Veterans and survivors who have applied for pension under 38 U.S.C. chapter 15. Pursuant to the access provision of the Privacy Act, VA's implementing regulations, and relevant case law, these claimants have an absolute right of access to their VBA claims file.

VBA-Wide Access Policy

Other than the exception for criminal investigation records created by a federal agency or a military department, VBA will respond to requests for records under the Privacy Act without delaying the release by redacting third-party PII that is properly included in requested records.[4] When responding to requests for access by or on behalf of the claimant whose file is sought (i.e., first-party right of access under the Privacy Act), VBA will not redact third-party PII that is properly included in the claims file. Third-party PII that is "properly included" in the folder or record refers to information that VBA purposely included, and does **not** encompass information that was erroneously placed in the record as a result of a misfiled document(s). Examples of properly included third-party PII are:

- Social Security Numbers of individuals other than the Veteran, spouse-claimant, or other individual with a right to access;
- Names of Veterans Service Representatives (VSRs), Rating Veterans Service Representatives (RVSRs), Decision Review Officers (DROs), Veterans Health Administration employees, contracted VA examiners, or other third parties;
- Routing and account numbers for third parties' bank accounts;
- Tax ID numbers of third parties.

This general access policy applies to all VBA business lines.

Note: Except for the changes set forth above, current procedures for responding to requests for records remain unchanged. Any local procedures for processing records requests received from Veterans, their surviving spouse-claimants, and/or an individual with a right of access should incorporate the VBA-wide access policy established in this letter. This letter does not change current procedures for establishing end-product credit and claim dates for records requests.

Ensuring Accurate Folders

Existing safeguards incorporated in VBA's Veterans Claim Intake (VCIP) procedures, centralized mail procedures, and longstanding adjudication procedures provide protections to prevent the erroneous release of misfiled documents. In light of these safeguards, VBA has concluded that allowing Veterans and their surviving spouse-claimants prompt and complete access to their claim records is an appropriate policy that will greatly benefit claimants. As such, this letter does not require changes to existing claims intake, folder maintenance, or compensation and pension adjudication procedures.

Claims and Document Intake

VBA's longstanding claims intake processes require employees to review, classify, apply a date stamp, and place proper controls on all incoming mail, prior to associating the mail with a claims folder. This well-established process imposes an important, initial safeguard to ensure that mail is associated with the correct claims folder. *See* M21-1, Part III, Subpart ii, 1.B.1-3; *see also* M21-1, Part III, Subpart ii, 1.C.1.a-c.

[4] In cases where there is evidence that the requestor intends to utilize the requested information to commit a crime or harm another, VBA employees should withhold or redact information accordingly, and notify local management and other VA officials as appropriate.

More recently, VBA has implemented additional safeguards to support increased automation and paperless claims processing. For example, under both VCIP and centralized mail processing:

- Regional office personnel conduct folder maintenance prior to shipping files for scanning to ensure documents are routed to the appropriate claim file. *See* M21-1, Part III, Subpart ii, 1.E-F (VCIP and Centralized Mail procedures).
- Document conversion vendors review Document Control Sheets and Shipping Manifests against physical files to ensure that the correct documents are uploaded into the claim file. Vendors notify VBA when misfiles are discovered. *See* M21-1, Part III, Subpart ii, 1.E-F (VCIP and Centralized Mail procedures).
- Document conversion vendors conduct Quality Assurance and Quality Control reviews prior to VBMS upload to ensure that source material is associated with the proper claim file.
- Document conversion vendors conduct Independent Verification and Validation post-upload to the claim file, and notify VBA of potentially misfiled documents.
- Centralized mail processing requires document conversion vendors to extract indexing values (i.e., name and file number) from source material. These data elements are presented to VBA personnel who validate the entries prior to uploading documents into the claim file. *See* M21-1, Part III, Supbart ii, 1.E (centralized mail procedures).

Additional Safeguards

In addition to the safeguards against potential misfiles in VBA's claims and mail intake processes, VBA employees conduct multiple reviews that confirm the accuracy of the claim folder in the course of adjudicating claims. *See* M21-1, Part III, Subparts iii-v. Often, the claims adjudication process requires that a VSR review the claims folder when developing evidence, an RVSR again reviews the claims folder when rendering a decision, and an additional VSR reviews the folder at the time an award is authorized. These multiple reviews occur independent of any subsequent review of the claims folder by a DRO or the Board of Veterans' Appeals in the course of appeals processing.

Again, it should be noted that all employees retain responsibility for correcting misfiled documents immediately upon discovery, and VBA provides employees with detailed instructions for doing so. For specific instructions, see:

- *VBMS Standard Operating Procedures Editing Documents in the eFolder*;
- *Deleting Documents from the eFolder*;
- *Procedures for Handling Misfiled Documents*;
- *VBMS Job Aid – eFolder Fundamentals: Managing Duplicate Documents & Transferring Documents from One eFolder to Another*;
- *VBMS Job Aid – eFolder Fundamentals: Associating Documents to Claims (Tagging Documents) & Bookmarking Documents*;
- *Virtual VA User Guide*; and
- *VBMS User Guide*.

Questions

For questions, please contact Gwendolyn Smith at foia.vbaco@VA.gov.

/s/

Danny G.I. Pummill

Acting Under Secretary for Benefits

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

Appendix B: OIG Memorandum to the Under Secretary for Benefits, "Release of Third-Party Personally Identifiable Information Under the Privacy Act"

December 11, 2018

MEMORANDUM

TO:	Dr. Paul R. Lawrence, Under Secretary for Benefits
FROM:	Larry M. Reinkemeyer, Assistant Inspector General for Audits and Evaluations
SUBJECT:	Release of Third-Party Personally Identifiable Information Under the Privacy Act

The purpose of this memo is to inform the Under Secretary for Benefits that the VA Office of Inspector General, Office of Audits and Evaluations, discovered that Veterans Benefits Administration (VBA), specifically the Records Management Center (RMC) in St. Louis, Missouri, is releasing third-party personally identifiable information (PII) in response to Privacy Act (PA) requests. This letter serves to notify you that such releases are taking place, and to inform you of the potential legal impact of this practice.

Background

When VBA claim records are requested by an individual or their appointed representative, it is a PA request. When granting PA requests, VBA Handbook 6502, dated July 11, 2012, requires VBA to limit disclosure of information to that which pertains only to the individual making the request. It further states that third-party information that does not pertain to the requester will not be disclosed and must be redacted.

The majority of PA requests are processed by staff at the RMC, where VBA consolidated the processing of all such requests in March 2015. In May 2016, VBA modified its policy for processing PA requests in VBA Letter 20-16-01 to no longer require staff to redact third-party PII. The letter explicitly defined PII to include, among other information, social security numbers, tax ID numbers, and bank account information. The release of third-party PII represented a change from VBA's prior practice of redacting certain third-party information from VBA claim records prior to release.

OIG Preliminary Data Testing and Analysis

The RMC completed over 60,000 PA requests from April through September 2018. The Office of Audits and Evaluations conducted a review of 20 randomly selected PA responses to requestors and found that a majority disclosed unredacted third-party PII related to other individuals including veterans and service members. In some responses, staff disclosed the social security numbers of over 200 other veterans and service members.

Legal Concerns

The PA provides that ". . . [e]ach agency that maintains a system of records shall (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him . . . to review the record and have a copy made of all or any portion thereof . . ." 5 U.S.C. § 552a(d)(1). The government can only deny an individual access to his record if an exemption exists.[1] The PA, unlike the Freedom of Information Act, does not contain an independent exemption to protect another person's privacy interest. Due to this lack of exemption protecting third-party information, it has been left to the courts to determine which information should or should not be released to PA requesters.

In support of its decision to stop redacting third-party PII, the VBA, in its May 2016 letter, cited *Voelker v. IRS*, a 1981 Eighth Circuit case which held that, pursuant to a PA request, a government agency has no discretion to withhold information from a requester's file absent an exemption. 646 F.2d 332. While the ruling in *Voelker* has remained unchallenged in the Eighth Circuit, various District Courts, including the District Court for the District of Columbia, and the Sixth Circuit, have ruled in opposition to Voelker. These courts, in their various rulings, concluded that requesters are not entitled to third-party PII found in PA requested records.

In *DePlanche v. Califano,* the plaintiff sought the addresses of his minor children contained in his Social Security Administration (SSA) file. The SSA explained that while the addresses were located in the father's file, they were not about him and consequently did not constitute a "record" for purposes of the PA. 549 F. Supp. 685, 695-696 (W.D. Mich. 1982); accord, *Windsor v. A Federal Executive Agency*, 614 F. Supp. 1255, 1261 (M.D. Tenn. 1983), aff'd, 767 F.2d 923 (6th Cir. 1985) (in order to constitute a "record" subject to the PA, the information must have been "about" or "pertained to" the requester). As noted in the citation above, the *DePlanche* rationale was adopted by the U.S. District Court for the Middle District of Tennessee, and later affirmed by the U.S. Court of Appeals for the 6th Circuit.

The U.S. District Court for the District of Columbia has also ruled that requesters are not entitled to third-party PII located in PA requested records. In *Haddon v. Freeh*, the plaintiff requested from the FBI records related to him after the Bureau initiated an investigation in response to a report that the plaintiff posed a security threat to the First Family. The Court held that the identities as well as the telephone numbers of FBI agents and personnel were not "about" the plaintiff and therefore "outside the scope of the privacy act and not subject to disclosure." See 31 F. Supp. 2d 16 (D.D.C. 1998). In *Murray v. BOP*, the plaintiff, a federal prisoner, sought records related to "his" visitors during the time he was incarcerated. While the Bureau of Prisons (BOP) initially released a partial list of names, dates, and visits, BOP withheld the names, dates, and times associated with various third-party visitors. The Court held that the information requested was properly withheld because it was not "about" the plaintiff. See 741 F. Supp. 2d 156, 161 (D.D.C. 2010).

The U.S. Court of Appeals for the District of Columbia Circuit, which has universal venue for PA matters, has also weighed in on this issue, albeit somewhat indirectly, by adopting the *DePlanche* rationale. In *Sussman v. U.S. Marshals Service*, the plaintiff sought "any and all" records related to him. The Court held that the plaintiff was not entitled to information about him that was contained in a third party's record because that record was not "about" the plaintiff. See 494 F.3d 1106, 1121 (D.C. Cir. 2007). Factually, Sussman did not concern third-party information in a requester's case file; it was the reverse—a requester's information in a third party's file. However, if a requester is not entitled to his own information in another's file, how much more so is a third party's information in an access requester's file not about

[1] The PA provides that the government will provide access to records on individuals within its possession unless one of 12 exemptions applies. The exact language of the exemptions can be found in the PA, 5 USC 552a.

the requester? While the D.C. Circuit has not addressed this specific question, it seems likely that it would uphold the decisions in *Haddon* and *Murray*.

The PA specifically provides civil remedies, including damages, and criminal penalties, for violations of the Act. The civil action provisions are premised on agency violations of the Act or agency regulations promulgated thereunder. A civil action may be filed in the U.S. District Court in the district where the requester resides or has his/her principal place of business; in which the agency records are located; or in the District of Columbia. Because individuals may file civil actions outside of the Eighth Circuit, VBA could be at risk if such civil actions are filed in district or circuit courts that protect third-party PII under the PA.

Conclusion

Reliance on the *Voelker* opinion is problematic, as more recent law is moving to a contrary conclusion to *Voelker* and its analysis. *DePlanche v. Califano*, 549 F. Supp. 685 (W.D. Mich. 1982); *Windsor v. A Federal Executive Agency*, 614 F. Supp. 1255 (M.D. Tenn. 1983), aff'd 767 F.2d 923 (6th Cir. 1985); *Haddon v. Freeh*, 31 F. Supp. 2d 16 (D.D.C. 1998); *Sussman v. U.S. Marshals Service*, 494 F.3d 1106 (D.C. Cir. 2007). Given this more recent body of law, it is not prudent for VA to rely on *Voelker*. Moreover, not only is the weight of authority against VA's approach, requesters have the ability to file civil actions in multiple venues, which means they can tap into this more recent law. If this occurs, VA has put itself at risk of adverse rulings and has exposed VBA to possible civil penalties if it continues to release VBA claim records without first redacting third-party PII. We recommend you immediately suspend VBA's current release policy and reevaluate VBA's PA request program.

Please send a written response stating whether you concur with our recommendation by January 4, 2019. Additionally, we request that your response address the following questions concerning the implementation of VBA's current PA release policy:

1. What was the reason for VBA's new PA release policy?
2. Who was involved in the creation and implementation of the new policy?
3. Was VA Office of General Counsel consulted prior to the distribution of VBA Letter 20-16-01? If so, what guidance did they provide?

If you have questions, or wish to discuss the issues in this letter, please contact me at 202-461-4483.

(Original signed by Larry Reinkemeyer)

Assistant Inspector General for Audits and Evaluations

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

Appendix C: Under Secretary for Benefits' Response to OIG Memorandum

Department of Veterans Affairs Memorandum

Date: December 20, 2018

From: Under Secretary for Benefits (20)

Subj: OIG Memorandum – Release of Third-Party Personally Identifiable Information Under the Privacy Act. (2019-05960-SD-0001)

To: Larry M. Reinkemeyer, Assistant Inspector General for Audits and Evaluations

1. Attached is VBA's response to the OIG's December 11, 2018, Memorandum: Release of Third-Party Personally Identifiable Information Under the Privacy Act.
2. Questions may be referred to Renetta Johnson, Sr. Program Analyst, Office of Program Integrity & Internal Controls at (202) 632-8699.

(Original signed by)

Paul R. Lawrence, Ph.D.

Attachments

Veterans Benefits Administration (VBA)
Response to OIG's December 11, 2018 Memorandum:
Release of Third-Party Personally Identifiable Information Under the Privacy Act
(2019-05960-SD-0001)

VBA provides the following response to the OIG December 11, 2018 memorandum.

OIG Recommendation: We recommend you immediately suspend VBA's current release policy and reevaluate VBA's Privacy Act request program.

VBA Response: Non-concur. VBA's policy for releasing benefit claim records in response to Veterans' and survivors' requests under the Privacy Act is based upon a thorough assessment of their need for timely and complete access to these records. VBA issued the policy in VBA Letter 20-16-01 after an extensive legal review by the VA Office of the General Counsel (OGC) and approval by the VA Deputy Secretary.

Question 1: What was the reason for VBA's new PA release policy?

VBA Response: See the Background section of VBA Letter 20-16-01, which provides the complete rationale for the policy. Specifically, "principles of transparency and accountability demand that Veterans and their surviving spouse-claimants enjoy unfettered access to the information relied upon by VBA to decide their claims. Moreover, a policy of prompt and complete access is consistent with relevant legal authority." In this section of the letter, VBA also noted that the policy supported VBA's strategic plan and the modernization elements of the VA's transformational plan, such as "affording Veterans and their surviving spouse-claimants online access to their claim records." VBA concluded, "providing Veterans and their surviving spouse-claimants prompt access to their complete claim records is critical to increase transparency and improve customer service" consistent with these plans.

Question 2: Who was involved in the creation and implementation of the new policy?

VBA Response:

- Sloan Gibson, former VA Deputy Secretary
- Danny G.I. Pummill, former Acting Under Secretary for Benefits
- David McLenachen, Director, Appeals Management Office, VBA (former Deputy Under Secretary for Disability Assistance)
- Robert Waltemeyer, Chief Learning Officer (former Director, Office of Management, VBA)

Question 3: Was the VA Office of General Counsel consulted prior to the distribution of VBA Letter 20-16-01? If so, what guidance did they provide?

VBA Response: Yes. VBA did not take this change of policy lightly and collaborated extensively with OGC leadership, to include:

- Leigh Bradley, former General Counsel
- Tammy Kennedy, Chief Counsel, OGC (former Principal Deputy General Counsel)
- Richard Hipolit, Acting General Counsel

OGC advised that there are two lines of legal authority applicable to the issue of redacting Veterans' claim records prior to releasing them under the Privacy Act, and that OGC could defend a policy choice based upon either of these approaches subject to an exception for law enforcement investigative reports

that may be contained in a Veteran's claims record. One approach, represented by the Court's opinion in *Voelker v. IRS*, 646 F.2d 332, 333-35 (8th Cir. 1981), recognizes a claimant's absolute right of access to a record maintained by the Government if an agency used the information in the record to decide a claim. As stated in VBA Letter 20-16-01, VBA's policy is based upon the Court's holding in *Voelker*. On August 27, 2015, OGC completed its review of VBA's draft letter, and subject to certain tracked changes and comments, which VBA addressed in the final version of the letter, OGC had no legal objection to VBA's policy. See the attached email from Leigh Bradley to David McLenachen and the accompanying word document with OGC's tracked changes and comments.

In February 2016, VBA and OGC briefed the VA Deputy Secretary on VBA's proposed policy. See the attached PowerPoint presentation. The Deputy Secretary approved the policy after the briefing.

OIG correctly notes that there are lower court cases that VBA could have used to support a different policy, specifically continuing the policy of conducting a page-by-page review of claim records for purposes of redacting third-party information. However, VBA did not choose that policy as it was inconsistent with VA's Veteran-centric goals of improving transparency and customer service.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Note: The attachments were not included in this report.

Appendix D: Under Secretary for Benefits' Updated Response to OIG Memorandum

Department of Veterans Affairs Memorandum

Date: June 19, 2019

From: Under Secretary for Benefits (20)

Subj: Release of Third-Party Personally Identifiable Information Under the Privacy Act - Update

To: Assistant Inspector General for Audits and Evaluations

1. In reference to your memorandum dated December 11, 2018, regarding the Veterans Benefits Administration's (VBA) release of third-party personally identifiable information (PII) while processing Privacy Act requests, I provide the following update.
2. VBA continues to cooperate with the Office of Inspector General's (OIG) review into this matter by providing statements and relevant data. At my request, VBA has reviewed existing policies and processes related to the Privacy Act requests processed at the Records Management Center. This review has concluded that a Privacy Act policy update is necessary. The Office of Field Operations in conjunction with the Office of Administration and Facilities are working towards both a long- and short-term solution to bring the program into compliance and protect PII.
3. The comprehensive solution will require a phased approach as additional unfunded resources are needed to implement the required changes. VBA will request the additional resources through the budgetary process. However, the redaction of third-party information will commence as soon as possible, but no later than October 1, 2019.
4. My point of contact is Mr. Jeffrey Smith, Executive Director Office of Administration and Facilities, and can be reached at 202-461-9894 or Jeffrey.smith42@va.gov.

(Original signed by)

Paul R. Lawrence, Ph.D.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

Appendix E: OIG Letter to VA's Acting General Counsel, "Release of Third-Party Personally Identifiable Information Under the Privacy Act"

February 11, 2019

By Email

Richard Hipolit, Esq.

Acting General Counsel

Office of General Counsel

Department of Veterans Affairs

Re: Release of Third-Party Personally Identifiable Information Under the Privacy Act

Dear Mr. Hipolit:

Recently, in the course of reviewing the Veterans Benefits Administration's (VBA) current information release policies, the Office of Inspector General (OIG) discovered that VBA is releasing unredacted third-party personally identifiable information (PII) in response to Privacy Act (PA) requests. Specifically, VBA's Records Management Center (RMC) in St. Louis, Missouri is releasing such material in reliance on VBA Letter 20-16-01, dated May 10, 2016 (VBA Letter). The OIG understands that the Office of General Counsel (OGC) may have provided guidance to VBA prior to its decision to issue the VBA Letter. To complete our review of this matter, the OIG would like to understand any guidance OGC may have provided to VBA concerning the release of third-party PII in response to veterans' PA requests.

Further, the OIG's analysis of the law applicable to the protection of third-party PII in these circumstances is set forth briefly below and in more detail in the attached memorandum. The OIG invites OGC to review its analysis and to provide any comments or contrary arguments it deems applicable.

Background

In May 2016, VBA published the VBA Letter modifying its policy for processing PA requests to no longer require staff to redact third-party PII. The VBA Letter explicitly defined PII to include, among other information, Social Security Numbers, Tax ID Numbers, and bank account information. The release of third-party PII represented a change from VBA's prior practice of redacting certain third-party information from VBA claims records prior to release. During our current review, VBA staff informed the OIG that VBA collaborated extensively with OGC leadership when developing the policy set forth in the VBA Letter.

Legal Concerns

As outlined in detail in the OIG's December 11, 2018 Memorandum to VBA's Under Secretary for Benefits (attached), it is the OIG's position that VBA's reliance on Eighth Circuit case law to justify the release of third-party PII pursuant to PA requests is problematic given that other Circuits, including the D.C. Circuit, have held that PA requesters are not entitled to such information and that releasing such information violates the third-parties' privacy rights.

In support of its decision to stop redacting third-party PII, the VBA Letter cited *Voelker v. IRS*, a 1981 Eighth Circuit case holding that, pursuant to a PA request, a government agency has no discretion to

withhold information from a requester's file absent an exemption. 646 F.2d 332. While the ruling in *Voelker* has remained unchallenged in the Eighth Circuit, various District Courts, the Sixth Circuit, and the D.C. Circuit have since decided the issue contrary to *Voelker*. These courts, in their various rulings, concluded that requesters are not entitled to third-party PII found in PA requested records and that disclosing such information violates the Privacy Act. This distinction, specifically as it pertains to the D.C. Circuit,[1] is noted on the Department of Justice's (DOJ) Office of Privacy and Civil Liberties website.[2]

While DOJ does not provide policy guidance to executive agencies, as that role statutorily rests with the Office of Management and Budget (OMB), the Federal Programs Branch of DOJ's Civil Division defends civil actions involving alleged violations of the PA against virtually all of the approximately 100 federal agencies and departments of the Executive Branch, including the VA. In this respect, the OIG finds DOJ's interpretation of PA provisions particularly relevant in evaluating VBA's current PA release policy. That is especially the case where, as here, OMB has not provided guidance on the issue.

It is also important to note that the likelihood of Privacy Act litigation against the Department being filed in the Eighth Circuit is relatively low. First, the D.C. District Court has universal venue for Privacy Act cases. Second, aggrieved individuals are unlikely to bring an action in the federal district courts in the Eighth Circuit simply because the RMC is located there over the federal district courts in their home states or D.C. As such, only veterans living in Missouri and six other states are ever likely to be subject to the Eighth Circuit precedent. Because individuals may (and, overall, are more likely to) file civil actions outside of the Eighth Circuit, VBA could be at risk if such civil actions are filed in district courts in circuits that protect third-party PII under the PA.

Request for Information and Documentation

Considering the forgoing discussion and attached documents, the OIG respectfully requests that OGC provide a written description of its involvement in the creation and implementation of VBA Letter 20-16-01, including identifying the OGC personnel who were involved. The OIG also requests all records related to any guidance OGC may have provided to VBA regarding the policy articulated in the VBA Letter concerning the release of third-party PII in response to PA requests.

If you have questions or wish to discuss the issues in this letter, please contact me at 202-461-4753. We appreciate the cooperation your staff extended to us during our review.

[1] In Sussman v. U.S. Marshals Service, the court explained that "[i]f certain materials pertain to both Sussman and other individuals, from whom the Marshals Service has received no written consent permitting disclosure, the Privacy Act would both require (5 U.S.C. § 552a(d)(1)) and forbid (id. § 552a(b)) their disclosure." 494 F.3d at 1106, 1121 n.9 (D.C. Cir. 2007). In such a situation, subsection (d)(1) must give way because "the consent requirement in § 552a(b) is one of the most important, if not the most important, provisions in the Privacy Act." Id.

[2] See https://www.justice.gov/opcl/individuals-right-access.

Sincerely,

(Original signed by)

Christopher A. Wilber

Counselor to the Inspector General

Enclosures

1. VBA Letter 20-16-01
2. OIG Memo to USB, dated December 11, 2018
3. USB Reply to OIG, dated December 20, 2018

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Note: The enclosures were included in this report. See Appendices A, B, and C.

Appendix F: Scope and Methodology

Scope

The review team conducted its work from October 2018 through September 2019. The review covered a population of about 65,600 Privacy Act requests completed by RMC staff from April 1, 2018, through September 30, 2018.

Methodology

To accomplish the review objective, the review team identified and reviewed applicable laws, regulations, VA policies, operating procedures, and guidelines related to Privacy Act requests. The review team performed a site visit at the RMC in St. Louis, Missouri, in February 2019. The review team interviewed and obtained testimonial information related to work processes associated with Privacy Act requests from RMC managers and staff. The review team also interviewed and obtained relevant testimonial information associated with Privacy Act requests from managers and staff with VA's Office of General Counsel and Office of Information and Technology, as well as VBA's Central Office, including the former Office of Disability Assistance, Office of Administration and Facilities, Office of Field Operations, and Compensation Service.

In coordination with VA OIG statisticians, the team reviewed a random sample of 30 Privacy Act requests completed from April 1, 2018, through September 30, 2018, and determined whether RMC staff disclosed unrelated third-party names and social security numbers.

The review team obtained duplicate copies of Privacy Act response discs from the RMC to review the sampled responses. The team also used VBA's electronic systems, including the Veterans Benefits Management System, to review the sampled veterans' claims files and relevant documentation. The review team discussed the findings with VA and VBA officials and included their comments where appropriate in this report.

Fraud Assessment

The review team assessed the risk that fraud, violations of legal and regulatory requirements, and abuse could occur during this audit. The review team exercised due diligence in staying alert to any fraud indicators by taking actions such as

- Soliciting the OIG's Office of Investigations for indicators, and
- Completing the fraud indicators and assessment checklist.

The OIG did not identify any instances of fraud or potential fraud during this review.

Data Reliability

The review team used computer-processed data from VBA's Corporate Data Warehouse. To test for reliability, the review team determined whether any data were missing from key fields, included any calculation errors, or were outside the time frame requested. The review team also assessed whether the data contained obvious duplication of records, alphabetic or numeric characters in incorrect fields, or illogical relationships among data elements. Furthermore, the review team compared veterans' names, file numbers, social security numbers, action stations, dates of claims, and completion dates as provided in the data received for the 30 completed Privacy Act requests reviewed.

Testing of the data disclosed that they were sufficiently reliable for the review objectives. Comparison of the data with information contained in VBA's electronic systems and veterans' claims files did not disclose any problems with data reliability.

This report includes data provided by the chief of the RMC's centralized support division regarding the RMC's pending and completed Privacy Act requests. However, the review team did not verify the accuracy of the self-reported data.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.*

Appendix G: Management Comments

MEMORANDUM

Department of Veterans Affairs

Date: October 8, 2019

From: Under Secretary for Benefits (20)

Subj: OIG Draft Report – Records Management Center Disclosed Third-Party Personally Identifiable Information to Privacy Act Requesters (Project Number 2019-05960-SD-0001) - VIEWS 01482855

To: Assistant Inspector General for Audits and Evaluations (52)

1. Attached is VBA's response to the OIG Draft Report: Records Management Center Disclosed Third-Party Personally Identifiable Information to Privacy Act Requesters.

2. Questions may be referred to Renetta Johnson, Office of Program Integrity & Internal Controls, at (202) 632-8699.

/s/

Paul R. Lawrence, Ph.D.

Attachments

Attachment

Veterans Benefits Administration (VBA)
Comments on OIG Draft Report
Records Management Center Disclosed Third-Party Personally Identifiable Information to Privacy Act Requesters (2019-05960-SD-0001)

The Veterans Benefits Administration concurs with the findings in OIG's draft report and provides the following comments:

During the review, VBA acknowledged that the issues identified by the OIG were problematic and cooperated with OIG by providing statements and relevant data. On September 27, 2019, VBA Letter 20-19-09 was issued providing the revised Privacy Act release policy. VBA received concurrence on the revised policy letter from VA's Office of General Counsel. The policy letter provides updated guidance for all VBA District Offices, Regional Offices, Service Offices, Program Offices, Centers, and the Records Management Center (RMC) for Release of Information from Privacy Act Systems of Records. The guidance was effective upon issuance of the letter. The comprehensive process and automated solution will require a phased approach as additional resources are needed to implement the additional changes. However, the redaction of third-party information commenced on October 1, 2019 in accordance with the September 27, 2019 policy letter.

The following comments are submitted in response to the recommendations in the OIG draft report:

Recommendation 1: The Under Secretary for Benefits implements the Veterans Benefits Administration's commitment to update its Privacy Act release policy and begin redacting third-party personally identifiable information.

VBA Response: Concur. On September 27, 2019, the attached revised Privacy Act release policy (VBA Letter 20-19-09) was issued and redaction of Personally Identifiable Information (PII) began on October 1, 2019.

VBA requests closure of this recommendation.

Recommendation 2: The Under Secretary for Benefits ensures VA's website is updated to reflect current Veterans Benefits Administration policy regarding release of third-party personally identifiable information.

VBA Response: Concur. The revised Privacy Act release policy (VBA Letter 20-19-09) was uploaded to the VBA website on September 27, 2019.

VBA requests closure of this recommendation.

Recommendation 3: The Under Secretary for Benefits implements a plan to ensure the Records Management Center complies with requirements for mailing Privacy Act responses in accordance with VA Directive 6609.

VBA Response: Concur. VBA's Office of Administration and Facilities (OAF) and the Office of Business Process Integration (OBPI) are developing a Freedom of Information Act (FOIA) Modernization procedure to integrate FOIA processing with the Centralized Intake (Conceptual Framework). This procedure is expected to be implemented by the end of June 2020.

Target Completion Date: June 30, 2020

Recommendation 4: The Under Secretary for Benefits establishes a plan to ensure that Records Management Center management receives a report for any site visit of the Records Management Center completed by the Veterans Benefits Administration and takes corrective action as needed.

VBA Response: Concur. When preforming a site visit, the RMC and all business lines will receive an out-brief and draft summary report with a list of observations prior to the OAF team leaving the facility. A final report will be provided within three weeks of the completion of the site visit. OAF is developing a Site Visit Standard Operating Procedure (SOP)/Checklist that will include guidelines and procedures for providing feedback to the RMC and VBA business lines. The Site Visit SOP/Checklist will be complete by November 15, 2019.

Target Completion Date: November 15, 2019

Recommendation 5: The Records Management Center director implements a plan to improve quality reviews and ensures staff are held accountable for the accuracy of their Privacy Act releases.

VBA Response: Concur. The director of the RMC is developing a plan to improve quality reviews to ensure staff are held accountable for the accuracy of their Privacy Act releases. This plan is expected to be implemented by October 31, 2019.

Target Completion Date: October 31, 2019

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

Appendix H: VBA Letter 20-19-09, "Release of Information from a Privacy Act (5 U.S.C. § 552a) System of Records"

September 27, 2019

VBA Letter 20-19-09

Director (00/21)

All Facilities

ATTN: All VBA District Offices, Regional Offices, Program Offices, Service Offices, Centers, and the Records Management Center (RMC)

SUBJ: Release of Information from a Privacy Act (5 U.S.C. *§* 552a) System of Records

PURPOSE

This letter supersedes VBA Letter 20-16-01 Privacy Act - Requests for Records, dated May 10, 2016, and provides updated guidance for all Veterans Benefits Administration (VBA) District Offices, Regional Offices, Service Offices, Program Offices, Centers, and the Records Management Center (RMC) for Release of Information from Privacy Act Systems of Records (SORs). This guidance change is effective upon issuance of this letter and will be implemented in stages as delineated according to guidance issued by the Office of Administration and Facilities.

SUMMARY OF CONTENT

This letter provides guidance related to disclosure of records subject to the Privacy Act of 1974. The Privacy Act prohibits the disclosure of information contained in an SOR absent a written request by or with the prior written consent of the subject individual to whom the record pertains, unless the disclosure is pursuant to one (1) of twelve (12) statutory exceptions stated in the statute, and in the document enclosed. VA Handbook 6300.4 Procedures for Processing Requests for Records Subject to the Privacy Act, implements the statutory language.

Authority

5 U.S.C. § 552a, implemented by 38 C.F.R. §§ 1.500-1.582

Background

The Privacy Act of 1974 establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of Personally Identifiable Information (PII) about United States citizens or lawfully admitted permanent resident aliens (hereinafter referred to as "individual") in systems of records (SORs) generally maintained by an agency in the executive

VBA Letter 20-16-09

Director (00)

branch. The Privacy Act also allows individuals an access right to records about themselves contained in SORs, requiring agencies to provide an individual, upon request, an opportunity to review his or her Privacy Act records, and have a copy made of all or any portion of the records. In addition, the Privacy Act provides the right to individuals to request an amendment of their Privacy Act records that they believe are inaccurate, irrelevant, untimely, or incomplete, and an accounting of disclosures made to any person or entity outside the agency during the previous five years.

Exceptions to Prohibition Against Disclosure

The Privacy Act prohibits the disclosure of information from an SOR absent the written consent of the subject individual, unless the disclosure is pursuant to one of twelve (12) statutory exceptions to the general prohibition against release. The exceptions to the written consent rule that permit an agency to release an individual's Privacy Act records without his/her consent are releases:

1. To those officers and employees of the agency who have a need for the record in the performance of their duties, under Exception (b)(1);
2. As required by the Freedom of Information Act (FOIA), under Exception (b)(2);
3. Under a routine use as outlined in the System of Records Notice (SORN), under Exception (b)(3);
4. To the Bureau of the Census for purposes of planning or carrying out a census, survey, or related activity, under Exception (b)(4);
5. To a recipient who has provided advance written assurance that the record will be used solely as a statistical research or reporting record and transferred in a form that is not individually identifiable, under Exception (b)(S);
6. To the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation or evaluation, under Exception (b)(6);
7. To another agency or to an instrumentality of any governmental jurisdiction under the control of the United States for a civil or criminal law enforcement activity authorized by statute, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired, and the law enforcement activity for which the record is sought, under Exception (b)(7);
8. To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual, if upon such disclosure notification is transmitted to the last known address of the individual, under Exception (b)(8);
9. To either House of Congress, any committee or subcommittee thereof, to the extent of matter within its jurisdiction, any joint committee of Congress, or subcommittee of any such joint committee, under Exception (b)(9);
10. To the Comptroller General, or any of his authorized representatives, performing the duties of the Government Accountability Office, under Exception (b)(1O);
11. Pursuant to the order of a federal court or other court of competent jurisdiction, under Exception (b)(11); and
12. To a consumer reporting agency in accordance with 31 U.S.C. § 371l(e), Collection and compromise, under Exception (b)(l2).

Exemptions from Access, Amendment, and Other Requirements

VBA Letter 20-16-09

Director (00)

The Privacy Act also contains exemptions that exclude an SOR from one or more of the provisions, such as an individual's right of access or amendment. An agency may exempt an SOR if it contains:

1. Information compiled in reasonable anticipation of civil action or proceeding, pursuant to Exemption (d)(S);
2. Records maintained by the Central Intelligence Agency, pursuant to Exemption G)(l);
3. Records maintained by a criminal laws enforcement agency or agency component and consisting of (a) information compiled for the purpose of identifying criminal offenders, (b) information compiled for the purpose of a criminal investigation, and (c) reports compiled at any stage of the process of criminal law enforcement, pursuant to Exemption (j)(2);
4. Classified information under an Executive Order in the interest of national defense or foreign policy, pursuant to Exemption (k)(l);
5. Records compiled by non-principal function criminal law enforcement agencies for criminal investigative law enforcement purposes, or records compiled by any agency for other investigative law enforcement purposes, pursuant to Exemption (k)(2);
6. Secret Service records pertaining to the protection of the President of the United States or other individual pursuant to 18 U.S.C. § 3056, pursuant to Exemption (k)(3);
7. Statistical records that are required by statute, pursuant to Exemption (k)(4);
8. Source-identifying material in investigatory material used only to determine suitability, eligibility, or qualifications for Federal Civilian employment, military service, Federal contracts, or access to classified information when the material comes from confidential sources, pursuant to Exemption (k)(S);
9. Testing or examination material used to determine appointment or promotion of Federal employees when disclosure would compromise the objectivity or fairness of the process, pursuant to Exemption (k)(6); or
10. Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source who furnished information to the government, pursuant to Exemption (k)(7).[1]

NOTE: The following two VBA SORs are exempt from the Privacy Act provisions on access, amendment, and other requirements:

- Loan Guaranty Fee Personnel and Program Participant Records (l 7VA26); and
- Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records, Specially Adapted Housing Applicant Records, and Vendee Loan Applicant Records (55VA26).

Please consult your supervisor or FOIA/PA Officer to obtain further guidance on responding to requests for copies of records contained in these systems.

[1] One Special Exemption 5 U.S.C. § 552a (d)(S), two General Exemptions 5 U.S.C. § 552a G)(l-2), and seven Specific Exemptions (5 U.S.C. § 552a [k][l]-[k][7]).

VBA Letter 20-16-09

Director (00)

First Party Access to One's Own Records

The Privacy Act requires an agency to provide the subject individual of a record with access to or a copy of his/her own record upon request. A first-party requester must provide a written, signed, and dated request addressed to VBA or a component thereof. Unless the SOR is exempt from the access provision, VA must provide the first-party requester with:

- A copy of all files or a particular record pertaining to the subject individual and maintained in an SOR, such as a copy of his/her entire or partial VA claims folder, C-file, Vocational Rehabilitation plan, or correspondence sent to the individual's member of Congress; or
- An opportunity for the individual to visit the regional office to review his/her own record(s).

NOTE: The Privacy Act right of access may be exercised on behalf of the subject individual by a duly authorized representative, such as an accredited attorney, agent, or representative of a veterans service organization. Before such release, however, any information revealing treatment for drug or alcohol abuse, HIV, or sickle cell anemia and therefore protected by 38 U.S.C. § 7332 must be redacted unless the requester is the subject individual's court-appointed guardian or other court designated representative. Online access, from which§ 7332-protected information cannot be restricted, may not be granted to a representative who is not so designated by a court.

Access to Records Containing Third-Party Information

An individual's Privacy Act records may contain information pertaining to other persons, such as PII of dependents, other Veterans, or physicians. Some of these records originated from DoD, where Service member lists with PII of multiple Service members were filed within individual service members' records, and physicians' SSNs were used as identifiers. Such records may also include constructive claims folders of spouses and children; promotion rosters; military records; and medical records containing SSNs, names, and other PII of a person who is not the subject of the request.

NOTE: Records released pursuant to a first-party request for an individual's own records from a non-exempt SOR must not contain PII of other individuals. Therefore, such records must be reviewed by the FOIA/Privacy Officer prior to release to ensure appropriate redaction and removal of third-party information. If third-party information is commingled in the subject individual's records, that information will be processed under FOIA.

Third-Party Requests for Privacy Act Records

An individual's Privacy Act records may also be requested by a third party, such as a spouse, former spouse, military member, or other dependent. Records may be released to a third party pursuant to the subject individual's consent in any written format that includes a clearly legible signature.

NOTE: Records protected under 38 U.S.C. § 7332 require a special authorization consistent with 38 C.F.R. §§ 1.475-1.479. Note that while VA Form 3288, "REQUEST FOR AND CONSENT TO

VBA Letter 20-16-09

Director (00)

RELEASE OF INFORMATION FROM INDIVIDUAL'S RECORDS," permits VA to release an individual's Privacy Act records, it does not allow release of§ 7332-protected records under VA regulations. If an authorization is deficient for such disclosure, VA may ask the individual - but not the requester – to provide a § 7332-compliant authorization, such VA Form 10-5345, REQUEST. FOR AND AUTHORIZATION TO RELEASE HEALTH INFORMATION.

Absent a written consent, third-party requests must be processed under FOIA, which requires agencies to disclose records requested unless their withholding is permitted under one or more of the statutory exemptions. Although the Privacy Act permits disclosure of records requested under FOIA pursuant to Exception (b)(2), they are often redacted or withheld completely under one or more FOIA exemptions. Privacy Act records processed under FOIA are often withheld, in whole or in part, under Exemption (b)(6), which protects information about individuals when the disclosure "would constitute a clearly unwarranted invasion of personal privacy." Depending on the contents of such records, other FOIA exemptions may also apply. If no FOIA exemption applies to permit withholding, the records must then be released under FOIA.

Requests for Deceased Veterans' Records

Records of deceased individuals are not protected by the Privacy Act and do not require a Privacy Act exception for release to next of kin with the appropriate request. Because deceased individuals have no recognizable privacy interest, such records requested by other third parties are not subject to withholding under FOIA Exemption (b)(6). By contrast, information about living persons maintained in a deceased Veteran's file may require redaction under Exemption (b)(6) when processed under FOIA.

NOTE: Records that contain § 7332 information may be released to the next-of-kin only for the purpose of obtaining survivorship benefits or with the authorization of the administrator, executor, or other court-appointed representative of the deceased Veteran's estate.

Amendment of Records

Under the Privacy Act, an individual has the right to request an amendment of records retrieved by his/her name, claim number, or other identifier. An amendment request must be in writing, be signed, and adequately describe the specific information the individual believes to be:

- Inaccurate (i.e., faulty, or not conforming exactly to truth);
- Incomplete (i.e., unfinished, or lacking information needed);
- Irrelevant (i.e., inappropriate, or not pertaining to the purpose for which records were collected); or
- Untimely (i.e., before the proper time or prematurely)

and the reason for this belief. The individual may be asked to clarify a request that lacks specificity in describing the information for which an amendment is requested so that a responsive decision may be reached.

VBA Letter 20-16-09

Director (00)

Accounting of Disclosures

The Privacy Act requires an agency to maintain a list of all disclosures made from a subject individual's record to persons or entities outside of VA. Further, the agency must provide the individual upon request an accounting of all such disclosures within the previous five years that includes:

- The date, nature, and purpose of the disclosure; and
- The name and address of the person or entity to whom the disclosure was made.

An accounting is not required for releases:

- To the subject individual in response to a first-party access request to his/her own records;
- To those officers and employees of the agency who have a need for the record in the performance of their official duties, under the need-to-know exception of Exception (b)(I); or
- A FOIA request, under Exception (b)(2).

FOIA and Privacy Requests Tracking

In order to maintain transparency and openness, VBA utilizes FOIAXpress as its official tracking system for FOIA requests and Privacy Act access and amendment requests. All requests received by any VBA component shall be entered and assigned to the appropriate VBA component within the FOIAX press application. Any questions regarding assignment of requests should be directed to the VBA FOIA/Privacy Officer for assistance.

VBA Privacy Program Guidance

As outlined within VA Directive 6509, Duties of Privacy Officers, (2)(a) Policy - VBA Administration, staff, and regional (VBA) offices must each designate a Privacy Officer to ensure compliance with privacy laws guidance from the Office of Management and Budget and the National Institute of Standards and Technology, and VA and VBA guidance. Any updates to the designation should be reported via email to the Administrations Privacy, and Alternate Privacy Officers as soon as the information becomes available.

Each business line must dictate how corrections are made within their SORN to ensure compliance with privacy laws guidance from the Office of Management and Budget and the National Institute of Standards and Technology, and VA and VBA guidance.

Each business line must use registered mail to send Privacy and FOIA correspondence to ensure compliance with privacy laws guidance from the Office of Management and Budget and the National Institute of Standards and Technology, and VA and VBA guidance.

Upon implementation of this guidance, all proposed privacy guidance must undergo review and concurrence by the designated staff or regional Privacy Officer. The appointed Privacy Officer will

VBA Letter 20-16-09

Director (00)

share such guidance with the administration prior to implementation.

Definitions

Individual - a citizen of the United States or an alien lawfully admitted for permanent residence.

Record - any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history, and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph within an SOR)(4).

Routine Use - with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

System of Records (SOR) - a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Personally Identifiable Information (PII) - any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. VA Handbook 6500.

RESPONSIBLE OFFICE

If you have questions regarding this guidance, you may contact VBA, Office of Administration and Facilities (20M33) Privacy Officer, Yvonne Lynah, via email at VAVBAWAS/CO/Privacy.

Alternately, you may opt to contact Ms. Lynah via telephone at (202) 632-8956.

//Original signed by//

Paul R. Lawrence, Ph.D.

Under Secretary for Benefits

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG note: The enclosures were included in this report. See Appendices A, B, and C.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Review Team	Dana Sullivan, Director Michelle Elliott Jeffrey Myers David Pina Michael Stack Leslie Wheeler
Other Contributors	Michael Soybel, Attorney Advisor

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.va.gov/oig