U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	DOI Medical Support (NextGen) System
System or Project Acronym:	DMS (NextGen)
Bureau or Office:	Office of Wildland Fire Service
Date submitted for review:	March 23, 2026
System Operational Status:	Operational

Point of Contact

Name:	Adrienne Brooks-Hill
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

☐ New System
☐ New Electronic Collection
☒ Significant Modification
☐ Other: Describe below

New vendor/contractor taking over the application, implementing new infrastructure and use of new FedRAMP authorized cloud system.

2. What is the purpose of the system or project?

The DOI Medical Support (NextGen) system is a comprehensive occupational medical exam tracking system that is used to track medical examination information and medical determination for applicants, employees, and/or contractors of the Department of the Interior. The system maintains medical examination information from contracted exam providers and medical qualification determinations for personnel in arduous duty positions and

those with physical fitness clearances. The system allows authorized agency users to enter examinee information and request exams, determinations, and clearances. The system allows authorized agency users to view and track examinee medical qualifications status. The system provides an additional portal for examinees to enter personal medical information and access their exam information, medical qualification determinations and clearance status.

3. Is the system registered in BisonGRC?

☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

UII Code: 010-000002880 DOI Medical Support (NextGen) system.

4. What legal authorities authorize the collection and use of data in this system or project?

Federal Records Act of 1950, 44 U.S.C. §§ 31; The Freedom of Information Act (FOIA) of 1966, 5 U.S.C. § 552; The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Managers Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. § 3512; Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030; Government Performance and Results Act (GPRA) of 1993, as amended by the Government Performance and Results Modernization Act (GPRA Modernization Act) of 2010, 5 U.S.C. § 306 and 31 U.S.C. §§ 1115 et seq.; Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35; Clinger-Cohen Act – Information Technology Management Reform Act of 1996, 40 U.S.C. § 11101-11703; Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3111; National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030; Government Paperwork Elimination Act (GPEA) of 1998, 44 U.S.C. § 3504; E-Government Act of 2002, 44 U.S.C. Chapters 35 and 36.; Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. Chapter 35, Subchapter II; Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. 113-291; Office of Federal Procurement Policy Act, 41 U.S.C. Chapter 7; Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936; Sarbanes-Oxley Act of 2002, SOX, Pub. L. 107-204, 116 Stat 745; Section 508 of the Rehabilitation Act of 1973, 29 U.S.C. § 794D; Executive Order 10450, Security Requirements for Government Employees, April 1953; Executive Order 13011, Federal Information Technology, July 1996; Executive Order 13103, Computer Software Piracy, September 1998; Presidential Decision Directive 63: Critical Infrastructure Protection, May 1998; Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001; A-11, Section 53, Information Technology and E-Government; A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, as revised July 15, 2016; A-130, Managing Information as a Strategic Resource; A-130, Appendix I, Responsibilities for Protecting and Managing Federal Information Resources, July 28, 2016; A-130, Appendix II, Responsibilities for Managing Personally Identifiable Information, July 28, 2016.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: If yes, list the applicable citations below.
☐ No

OPM/GOVT-10, Employee Medical File System Records, 75 FR 35099 (June 21, 2010); modification published 87 FR 5874 (February 2, 2022).

6. Does this project involve an information collection that requires OMB approval under the Paperwork

Reduction Act?

☐ Yes
☒ No

N/A.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

None

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last)	☒ Home telephone number	☒ Employment or resume info
☐ Aliases/nickname	☒ Personal Email	☒ Full or Truncated SSN
☐ Driver's license	☒ Mailing or home address	☐ Physical characteristics
☐ Citizenship	☐ Religious preference	☐ Biometrics/facial recognition
☐ Legal Status	☐ Mother's maiden name	☐ Vehicle information
☒ Sex	☐ Marital status	☐ Passport information
☒ Race or ethnicity	☐ Spouse Information	☐ Travel information
☒ Date of birth	☐ Child or family information	☐ Parent's name
☐ Place of birth	☒ Emergency contact info	☐ Credit card number
☒ Personal cell phone number	☐ Financial information	☐ Nationality
☒ Username / user ID / acct ID	☒ IP address / network ID	☒ Device ID / online ID
☐ Geolocation / GPS / location	☐ Photos / video / audio	☒ Health / medical information
☐ Tribal or other ID number	☐ Education information	☒ Disability Information
☐ Criminal / disciplinary info	☐ Military records	☒ Other: Describe below

Employee's work email address collected and used to generate Examinee ID within system.

2. What is the source for the PII collected? Check all that apply.

☒ Individual	☒ DOI Records
☒ Federal Agency	☐ Third Party Records
☐ Tribal Agency	☐ State Agency
☐ Local Agency	☐ Other: *Describe Below*

PII is collected from the individual examinee, DOI records, authorized DOI users, contractor medical service providers, and subcontracted health clinics performing occupational medical examinations. Information may also be derived from medical examination results, medical qualification reviews, and supporting documentation submitted by examinees or medical providers.

3. How will the information be collected? Check all that apply.

☐ Paper Format
☐ Email
☒ Face-to-Face Contact
☒ Website
☒ Fax
☒ Telephone Interview
☐ Shared Between Systems: *Describe*
☐ Other: *Describe*

Information is collected through the DMS (NextGen) web portal, authorized user entry, examinee self-entry, contracted medical provider submission, subcontracted clinic submission, fax, telephone contact, face-to-face contact, and encrypted email where authorized for medical examination documentation. Information may also be transferred to approved DOI records repositories for retention and disposition.

4. What is the intended use of the PII collected?

Collecting PII facilitates REPORTS, where authorized users can track the status for examinees based on name, email address, and Examinee ID. Using the PII in this manner helps users verify that an exam matches the examinee, furthering efficiencies. Because DMS collects medical data, it triggers certain records retention requirements. Please see Section 4.1 for more details.

5. How does this project limit the collection and use of PII to only what is necessary?

Data collected by the system is limited to required information only. System profile data fields and collected health information have been reviewed to ensure that only necessary information is collected. Required fields are identified within the system and all privileged users receive privacy training.

Section 3: Data Sharing and Individual Rights

1. With whom will the PII be shared, both within DOI and outside DOI? Check all that apply.

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☐ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☒ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☐ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☒ **Other Third-Party Sources:** Describe how the data will be used below.

Within the Bureau/Office: Specific PII elements are shared within the Office of the Secretary to prevent file duplication, verify the accuracy of an employee profile, and to reconcile Office of Personnel Folder (OPF) records. For instance, after initial entry, SSN will only be used to prevent profile duplication, facilitate records archive, and retrieve records upon request. PII such as DOB is shared within DOI by employees with DMS access to verify the correct employee profile during transfers or when updating documentation. Personal medical information is shared within DOI by employees with DMS access on a limited basis when an examinee's medical condition does not meet the established medical standard for their position and the individual requests a waiver. This information is shared only with those individuals that have a bona fide business need to know. Individuals with a business need to know include a Human Resources (HR) representative, a Fire Management Officer (FMO), and a deciding management official from within DOI. The HR rep and FMO would discuss the medical information during a risk assessment, and the management official would have access to the medical information to make a risk and waiver decision.

Other Bureaus/Offices: As stated above, some PII is shared between bureau programs to verify profiles when the individual transfers within the agency (DOI).

Contractor: The medical system service provider of the DMS application receives information from personnel needing medical qualifications and pre-fitness clearings as part of using the application, and shares determinations with the requesting DOI bureau. The contractor has access to all the PII collected, including sensitive PII.

Other Third-Party Sources: Health clinics are subcontracted by the primary medical service provider. PII including medical information necessary for performing a medical exam is shared with the third-party clinics within the medical service provider's network via the system portal or encrypted email. DMS does not maintain any PII from the employees of third-party clinics.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

DMS (NextGen) does not have an MOU, MOA, or ISA with other Federal, State, local, or Tribal agencies for information sharing. The system is used by DOI and its authorized contractor medical service provider to support DOI occupational medical examination tracking, medical qualification determinations, and physical fitness clearance processes.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Refusals to provide the information would terminate the hiring process or opportunity to participate in positions subject to medical standards or pre-fitness screening.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

☒ Privacy Act Statement:
☒ Privacy Notice:
☐ Other: *Describe Below*
☐ None: *Example - law enforcement cases.*

Notice is provided through a Privacy Act Statement presented at or before the point of collection, the applicable published SORN(s), this PIA, and system warning banners. The Privacy Act Statement must identify the legal authority for collecting the information, the purpose of the collection, the routine uses that may apply, and whether providing the information is mandatory or voluntary, including the consequences of refusing to provide the information.

The system banner and Privacy Rules of Behavior Acknowledgement provide notice to users regarding system monitoring and responsibilities for protecting information, but they do not replace the Privacy Act Statement required for the collection of personal and medical information from examinees.

5. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data can be retrieved by first name, last name, email, and system generated Examinee ID. Please see Section 2 about how the Examinee ID is created.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

Authorized system users can generate reports within DMS that provide medical determination information. These reports are utilized to verify qualification status and exam periodicity. For example, a report is generated showing a list of individuals that are due for an exam between January and June, or a report can be generated for the Work Capacity Test (WCT) administrator showing a list of individuals who are medically qualified and eligible to participate in the WCT.

These authorized users fall into one or more of the four levels of system users: “individual examinee”, “read-only”, “limited access”, and “standard access”. Limited and standard users have access to reports, but only standard users can access reports with medical determination information that may include individuals’ personal medical information. Limited users can access more limited PII, including profile data and medical qualification status. Individual examinee users can only access their own data.

The DMS also generates system audit records that include user activities such as accessing and using the application. Audit records can include unsuccessful/successful logon attempts, access to data and location (IP address) of access, tracked by individual User ID. These audit records are part of the DMS (NextGen) continuous monitoring program, supporting security investigations and compliance.

7. How will data collected from sources other than DOI records be verified for accuracy?

No PII data is collected from non-DOI sources.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

Records are retained by the contractor for the duration of each five-year contract cycle or until exported. At the end of each contract cycle, and depending upon the contractor selected, records for current and active individuals are retained by the incumbent contractor or transferred to the next contracted system. This data also facilitates long term retention and retrieval of records upon employee separation. 5 CFR 293 Subpart E

provides guidance on the establishment of the Employee Medical File (EMF) which contains all the occupational medical records (both long-term and short-term records) designated for retention. The EMF must be kept separately from the Official Personnel Folder (OPF). EMF records are held by the system contractor, always accessible by DMS (NG) personnel, and migrated as necessary with each five-year contract cycle.

Exported (inactive) records, such as those for former or inactive employees, are transferred to the DOI Enterprise Content System upon employee separation or when the employee no longer requires medical qualifications or clearances and maintained according to the established GRS.

GRS 2.7 060 – Long-term records are kept for 30 years after employee separation or for the duration of the OPF, whichever is longer.

DRS 1.2.1 – Short-term HR records are retained for 3 years after employee separation or transfer.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

Data is reviewed by the appropriate system management user (Fire Center Manager, Human Resource Officer, etc.) at entry. The system identifies and prompts for required fields. Individual examinees also verify their data prior to each exam.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes
☐ No

DMS audit records log user activities within the application, including all file access. Further details are discussed in Section 7.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

As an information system, DMS NextGen has privacy risks within the information lifecycle. The DMS (NextGen) system is classified as FISMA Moderate and has all the required system security documentation. In accordance with OMB Circulars A-123 & A-130, the DMS system has controls in place to prevent the misuse of the data by those having access to it.

Collection: DMS NextGen collects PII directly from the individual, mitigating inaccuracies at collection point. Data fields also limit inaccuracies, collecting only the required information, so DMS (NextGen) does not collect more PII than needed.

Use/Sharing: Security measures and controls consist of passwords, user identification, IP addresses, database permissions and software controls to mitigate the risk of misuse. These technical controls safeguard the information. Section 7 contains a more detailed discussion of access controls. Audit trails also captured within

the system determine who has added, deleted or changed data. Furthermore, all DOI employee users and contractor employee users must meet the administrative requirements for protecting Privacy Act information, such as annual completion of Role-based Privacy Training (RBPT). For contractors, Privacy Act contract clauses are included in their agreement with DOI. Contractors are expected to uphold all privacy provisions regarding PII. Subcontracted clinics are also contractually obligated by a confidentiality, privacy, and security agreement outlining privacy laws, information disclosure and disposal of examinee data.

There is also risk of user PII exposure within system audit records. System audits maintain a record of system and user activities including successful/unsuccessful logon attempts, user activities and user access to data. Audit reports of user activity are provided to DOI for review. Exposure risk is mitigated through the implementation of system audit activities in accordance with the system security plan, which describes the management of audit records in accordance with security controls, applicable laws and regulations for Personally Identifiable Information and Personal Health Information.

Disclosure of PII: To mitigate the risk of unauthorized disclosure, all DOI privileged users (users with access to other employees' information) must complete RBPT and affirm their responsibility to protect sensitive system data annually. DOI privileged users are authorized by each bureau's national Medical Standards Lead after submitting a request form to the DOI Medical Standards Program Lead, outlining their requested level of access, unit(s) access required, and relevant job position. All DOI employee users and contractor employee users must meet the requirements for protecting Privacy Act information. Privacy Act contract clauses governing contract employees include 52.224-1 Privacy Act Notification (Apr 1984), 52.224-2 Privacy Act (Apr 1987), and 52.227-17 Rights in Data – Special Works (Dec 2007).

Retention/Destruction: Retaining data past its operational use could increase the risk of unauthorized access. Adherence to DOI data destruction and record retention policies ensures secure and timely deletion of data when it is no longer needed, reducing the risk of unauthorized access or misuse. These policies prevent the DOI Medical Support (NextGen) system from keeping PII longer than necessary. The contractor retains the records for the duration of a five-year contract cycle or until exported. Exported (inactive) records are transferred to the DOI Enterprise Content System and maintained according to the established GRS.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☒ No

The system does not generate new data or inferences through automated aggregation or analytics. However, DMS (NextGen) maintains new occupational medical examination records, medical review results, qualification determinations, waiver-related information, clearance status, and related workflow records entered by examinees, authorized DOI users, contractor medical personnel, or reviewing medical officials. These records may influence hiring, qualification, assignment, clearance, or participation decisions for positions subject to medical standards or physical fitness requirements. Risks are mitigated through role-based access, medical confidentiality controls, contractor privacy obligations, audit logging, human review, and retention under applicable employee medical records requirements.

3. Will the new data be placed in the individual's record?

☒ Yes: *Provide explanation below*
☐ No

Data from this system will be used for validation of medical fitness to serve in a multitude of DOI and bureau positions and placed in the Employee Medical Folder.

4. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Provide explanation below*
☒ No

The system does not make automated determinations about individuals. Medical qualification determinations and clearance statuses are entered or reviewed by authorized medical or program personnel and may be used by hiring officials, human resources personnel, fire management officials, and other authorized officials to make employment, assignment, waiver, or participation decisions consistent with applicable medical standards and program requirements.

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

New data is verified through examinee review, required-field validation, medical provider review, contractor medical review, and authorized DOI program review. Examinees may review and correct demographic information and submit supporting documentation for correction of medical information. Medical examination results and qualification determinations are reviewed by authorized medical or contractor personnel before being used for qualification, waiver, clearance, or fitness-related decisions.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☐ Yes
☒ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

DMS (NextGen) does not use AI or machine-learning models. Accuracy is managed through human review, required-field validation, examinee review, medical provider review, contractor medical review, and program review, rather than model validation.

3. Are individuals notified of AI-based decisions that affect them?

☐ Yes
☐ No

DMS (NextGen) does not make AI-based decisions. Individuals are not subject to AI-generated determinations.

Notice for collection and use of personal and medical information is provided through the Privacy Act Statement, applicable SORN(s), this PIA, and system notices.

4. Are safeguards in place to prevent bias or unintended consequences?

☐ Yes
☐ No

DMS (NextGen) does not use AI, machine learning, or automated decision-making. Non-AI safeguards include human review, medical standards review, role-based access, privacy training, contractor confidentiality obligations, audit logging, and individual access/correction processes.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☐ Yes
☐ No

There are no AI or machine-learning models to review, retrain, or validate. System reliability is addressed through security authorization, FedRAMP cloud controls, application testing, audit logging, contractor oversight, and program review.

6. Is federated learning used for privacy-preserving model training?

☐ Yes
☐ No

DMS (NextGen) does not use federated learning or any other model-training approach. The system does not train models using examinee medical information, employee records, or system activity data.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe below*

Examinee access is restricted to their own individual medical exam and personal profile data. Authorized users such as hiring officials, program managers, and unit administrators will be granted access based on business need to select bureaus, organizations and units within their purview. Primary contractor users such as reviewing medical officers, nurses, customer service representatives and system administrators will be authorized access commensurate with their individual roles.

Contractor developers involved in the design, development and maintenance of DMS (NextGen) may have access to system data. Privacy Act clauses are included in the contract for DMS (NextGen) services provided.

2. What data protection policies apply to cloud-based PII storage?

PII stored within the DMS (NextGen) application is subject to NIST SP800-53 security and privacy controls through application of risk management processes within the DOI Authority to Operate (ATO) process. DMS (NextGen) use of the Cority cloud application within the system implements FedRAMP controls through the FedRAMP authorization process required for systems to retain "FedRAMP Authorized" status. The DMS (NextGen) contract includes requirements provided in the DOI Cloud Computing Policy.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

The system monitors system access and use, through review of audit logs from system resources and consolidated within the enterprise SIEM (Splunk). Vendor security personnel also monitor intrusion detection systems and firewall logs for evidence of unauthorized access or data exfiltration.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

The system monitors user activity such as successful logon, logoff and file access as part of required security compliance. Access to system audit log information is restricted to only system administrators and security personnel. The system tracks individual Examinee users through their medical standards process to provide arduous duty qualification status to authorized personnel. This information is only available to the authorized personnel assigned to track Examinees within their area of responsibility.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

Privacy training and IT security awareness training are required by contract for all contractor employees involved with the system. Role-based training is also required for employees with specific security-related system roles. Contractor employees undergo initial background checks that include criminal history (federal, state, local), education, previous employment, drug testing and review against the national sex offender registry.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

☒ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Lock
☐ Other: *Describe Below*

Technical Controls

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Other: *Describe Below*

☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

Data is encrypted in transit using TLS1.2 and encrypted at rest through database encryption of both Oracle and MSSQL databases, as well as hardware enables encryption of virtual machines.

Administrative Controls

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Other: *Describe Below*

☐ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☐ Regular Monitoring of Users' Security Practices

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

As a DOI application, DMS follows DOI Privacy policy and procedures for complaints or requests to amend records that implicate protected information. These procedures are outlined in the DOI Privacy Act regulations at 43 CFR 2.246, in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, and the DOI ISE Privacy Policy. Additional information is available on the DOI Privacy and Civil Liberties webpage at: Privacy and Civil Liberties | U.S. Department of the Interior.

8. What processes are in place for individuals to access their information?

Individuals with a user account in DMS can access their own information by default. Examinee account access allows users to see their personal health and demographic information.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals can correct basic demographic information by contacting the privileged user responsible for their unit or by contacting DOI program management. Identity is verified by confirming current information and contact methods with the requestor. Individuals can request correction of medical information by submitting documentation of requested changes directly to their profile within the system. Documentation is reviewed by the contractor and updated as appropriate.

10. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The Contractor's Information System Security Manager (ISSM) for the DOI Medical Support system will report all known or suspected breaches in electronic or physical form to the CO, COR, and the DOI CIRC or bureau or office point of contact no later than one hour following discovery via email at DOICIRC@ios.doi.gov or (703) 648-5655.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

Loss, compromise, unauthorized disclosure, or unauthorized access of PII is considered a "security incident". The ISO and all authorized users must report to DOI Cyber Incident Report Council (DOI-CIRC) within one hour of discovery. Upon notification of a privacy breach, the DMS Information System Security Officer (ISSO) will work with the Office of the Secretary Privacy office personnel to follow procedures within the DOI Privacy Breach Response Plan. Those procedures consist of:

1. Immediate Reporting within one (1) hour of discovery;
2. Containment and mitigation to prevent further loss;
3. Risk Assessment to determine the scope and nature of the breach;
4. Notification, if required;
5. Oversight reporting, if required; and
6. Remediation and prevention to prevent recurrence.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

This PIA will be reviewed every three (3) years, in accordance with E-Government Act of 2002, or whenever major changes occur to the system's technology, data, or operations that could affect privacy risks.