Version Number: 01-2019

U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)

Privacy Impact Assessment
for the
150-01 Office of Safety, Health, and Environment

Reviewed by: Claire Barrett, Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 02/03/2022

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 150-01

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The Office of Safety, Health, and Environment (OSHE) supports NIST in carrying out its mission safely and in maintaining safety as an integral core value and vital part of the NIST culture. The OSHE information system supports this role and includes the following components:

- **The Radiation Monitoring System (RMS) is used to monitor radioactive sources above a certain level. The RMS has detectors, processors, cameras, and network connectors monitoring sensitive equipment and their surrounding physical locations. The monitoring provides unidirectional information to NIST Emergency Services consoles. This component does not contain PII records that are retrievable by a unique identifier.**

- **The Health Physics System (a.k.a., HAPPY) provides inventory of radioactive material, ionizing machines, radiation equipment, physical radiation laboratories. HAPPY has also been used since 2007 to track NIST staff radiation exposure. In addition, required safety training is made available through the internal, web-based Safety Education and Training (SET) site to ensure training prior to access to radioactive material, machines, equipment, or laboratories. SET is an OSHE application used to provide and track training.**

- **The Health Unit (HU) provides health services to federal employees/contractors, member of the public, foreign nationals, or visitors who require care related to**

their position or while on Gaithersburg's campus. The HU is not a Covered Entity under HIPAA. Both Occupational Health Records and Personal Health Records are maintained in case files. Case files dated 2018 and prior are maintained as paper records, whereas case files dated 2019 to present are maintained in the Health Unit's Electronic Medical Records System (EMRS).

- **The EMRS is a COTS cloud-based application used to enable online scheduling of appointments, tracking patient visits, storing health data, such as audiometer and spirometer test results, vaccination and test results, photographs of wounds or injuries, prescriptions, etc., and includes information related to maintenance of a Commercial Driver's License. All staff may log into ERMS to access their own record, although only medical information collected during medical appointments made since 2019 is available in the system. Visits prior to 2019 are only on paper records, which patients can request to see.**

- **The Tort process and some safety incident investigations require collection of PII or PHI for claims for damage, injury, death, or motor vehicle accident reports. This process could include police reports if applicable. OSHE assists in the investigation and reporting processes but does not maintain any documents. Legal documents are sent to Human Resources, DOC, and/or physical security.**

a. Whether it is a general support system, major application, or other type of system
NIST 150-01 is a General Support System.

b. System location
The EMRS is a COTS cloud-based application hosted within the continental United States. All other system components are located at the NIST Gaithersburg, Maryland and Boulder, Colorado facilities within the continental United States.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The RMS is a standalone component and only communicates with devices located in the Emergency Services guard offices via a private network in Buildings 101 and 318 over OSHE's isolated Research Equipment Network (REN).

The HAPPY is a standalone database.

The EMRS is a standalone application housed in an encapsulated environment but obtains a weekly report from the Central People Repository (NIST 183-01) with NIST employee and associate data. This file is transferred to the EMRS via Secure FTP for purposes of account generation, allowing Single Sign On (SSO) to the ERMS with employment status, supervisor or host information, and contact information for staff.

All system connectivity to HAPPY and the Health Unit is via TCP/IP across the NIST Network Infrastructure (NIST 181-04) to encrypted file share (NIST 184-12). NIST 181-04 provides all services for physical cabling, network frame synchronization/flow

control/error checking, routing, switching, and DNS. All data is encrypted with FIPS 140-2 compliant technologies in transit and at rest.

d. The way the system operates to achieve the purpose(s) identified in Section 4
The RMS provides monitoring capabilities via a live video feed for Emergency Services to detect unauthorized access to radioactive material.

The HAPPY provides access and inventory of radioactive materials and related information, which are stored and tracked in the HAPPY database application. Owners of radioactive material access and update the database via secured, authorized computers.

The Health Unit (HU) component provides scheduling of appointments, tracking patient visits, storing health data, such as audiometer and spirometer test results, vaccination and test results, photographs of wounds or injuries, prescriptions, etc. The HU component includes maintaining legacy medical case files in paper form, and an Electronic Medical Record System (EMRS). With the implementation of EMRS, while all active NIST staff have access to ERMS, not all medical records were transitioned (i.e., scanned and uploaded).

- **For patients who received care from 2019 to present, Health Unit medical case files includes scans of all paper records generated during patient visit.**
- **For patients who have not received care since 2019 (e.g., calendar year 2018 and prior), medical case files remain as a paper record until the next time health services are rendered. At that time, some of the medical information may be transitioned to EMRS, while the majority will continue to remain in the paper medical case file.**

Access to medical case files, whether legacy paper files or within the EMRS, is restricted using role-based access controls. For example, the EMRS has role-based access controls restricting access and views for health practitioners, health unit administrative staff, and system administrators. Patients can log into EMRS to view their personal information and appointments. Supervisors can only see their employee and associates occupational health appointments to determine if required tests are scheduled. The legacy paper case files continue to be stored in a secured location and cabinets until they are needed by the patient or administrative staff, or it is time to archive or destroy. The National Archives and Records Administration (NARA) does not currently have the capability to receive electronic records for archival, so Occupational Health records are printed (as necessary) and archived with NARA according to the Records Schedule.

Tort claims are initiated with the forms:

- **SF-95 Claim for Damage, Injury or Death – to be used by a non-federal person making such claims against NIST pursuant to the Federal Tort Claims Act.**
- **SF-91 Motor Vehicle Accident Report – Used by operators of federal motor vehicles for every motor vehicle accident involving injury, fatality, and/or damage exceeding $500.**

- **GSA Form 1627 Motor Vehicle Accident Reporting Kit – to assist vehicle operators involved in an incident with a GSA leased fleet vehicle.**

e. How information in the system is retrieved by the user

The RMS is a live camera feed of radioactive material viewed by NIST Emergency Services on a continuous basis. In the event of an incident, the recorded feed and the timestamp are used for retrieval by NIST Emergency Services staff. Otherwise, the recorded feed is not retrievable by the end user.

HAPPY data is retrieved by authorized individuals by opening the database and retrieving the source by type of radioactive source. Radioactive source owners can retrieve their data by their name. SET information is available for retrieval by the end user. Otherwise, the HAPPY data is not retrievable by the end user.

The Health Unit paper case files are retrieved from secure file cabinets by authorized health practitioners or health unit administrative staff, by patient name. The online EMRS records are accessible by health practitioners, health unit administrative staff, and system administrators, and limited based on their role. They are retrieved by patient name or by employee ID. Online EMRS records are accessible by the end user through single sign-on (SSO).

Tort records are stored and retrieved by name and date of incident.

f. How information is transmitted to and from the system

The RMS is viewed by NIST Emergency Services over an encrypted isolated REN network via TCP/IP. The information is not transferred to another system on a routine basis. In the event of an incident, the recording may be required for investigative and prosecuting purposes and would be shared through secure means.

The HAPPY does not automatically transmit information to other systems. Annually, a mandatory report is generated to provide the Nuclear Regulatory Commission and is sent via encrypted secure file transfer to ensure the report is only available to NRC.

The EMRS information is stored in Health Unit databases and encrypted in transit to the EMRS interface via HTTPS. Paper-based medical case files are not electronically transmitted. Patients can request paper copies which are then given directly to them.

Paper records associated with Torts or workers' compensation are exchanged either in envelopes marked, "For XXXX's Eyes Only" or hand delivered to the recipient. To request information from the Emergency Services Office, an OSHE employee fills in a NIST-1226 with justification for requesting ESO physical security related information. The Police Chief reviews the police report to ensure it does not contain any law enforcement sensitive information, and then forwards to OSHE via an encrypted email. The report typically includes the names of personnel involved, contact information, and a synopsis of what occurred. Electronic records are exchanged via encrypted email or secure files shares such as Kiteworks or nfiles. The NIST claims

specialist who handles Tort claims and the Incident Investigation Specialist handling compensation claims have been trained on handling PII in electronic and paper format and provides detailed instructions on how to submit data to individuals involved. Information is gathered by OSHE for investigation purposes only. Information for Tort claims are sent to legal and/or finance and the claimant for retention. Working copies are destroyed or deleted. For OSHA recordables and Workers Compensation, investigative information is put into DOC and OSHA systems and PII is not retained by OSHE.

g. Any information sharing conducted by the system
The RMS data shared is what is captured on the live camera feeds that is viewed by NIST Emergency Services. In the event of an incident, the recording may be required for investigative and prosecuting purposes and would be shared through secure means.

The information in HAPPY is shared with the Nuclear Regulatory Commission (NRC) on an annual basis in support of radioactive licensing. The required information to be shared is individuals who have access to radioactive material, including their SSN, material, location, and amount.

The Health Unit shares information collected, stored, or generated as disclosed and consented to by a patient when entering the Health Unit, or accessing the EMRS. Occupational Health Records (OHR) are owned by NIST but regulated by the Occupational Safety and Health Administration (OSHA) and shared with other DOC and NIST business units as needed. Non-Occupational Health Records, or limited health information, are only shared as a circumstance or situation warrants, with the consent of the patient (if the medical condition permits consent). Of note, for vaccination status and administration and COVID testing, NIST is required to share information with the Maryland Department of Health, who then anonymizes and further shares with the U.S. Centers for Disease Control and Prevention.

Occupational Health records are archived with the National Archives and Records Administration as required by the General Records Schedule section 2.7: Employee Health and Safety Records https://www.archives.gov/files/records-mgmt/grs/grs02-7.pdf. Non-Occupational Health records (personal) are not otherwise shared.

TORT information is shared with the legal department when required and insured/representative receives information gathered on the following forms: SF-95, SF-91, SF-94, GSA-1627 in a package with a cover letter hand delivered in designated mail pouches labeled "eyes only" or sent to attention only OSC/DoC address. The finance department information is gathered on an SF-1145 with cover letter summary (they do not get a full investigative report package as it is not needed) and hand delivered in package labeled "eyes only." All documents are destroyed after claim is complete.

h. The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.

To retain and renew NIST's license to have radioactive material, we provide NRC with information required by the by reporting criteria based on adherence of the licensee and facility to the appropriate regulations described in the Code of Federal Regulations (CFR), Title 10. NRC is ordered to collect this by the Atomic Energy Act of 1954 (as amended) that allows the NRC to issue licenses for commercial power reactors.

Department of Labor, Occupational Safety and Health Standard 1910.501 - Vaccination, testing, and face coverings.

Department of Labor, Occupational Safety and Health Standard 1913.10 - Rules of agency practice and procedure concerning OSHA access to employee medical records.

Federal Tort Claims Act (28 U.S.C. 2671-2680) delegates authority to settle or deny claims and establishes procedures for the administrative adjudication of such claims.

The Federal Employees' Compensation Act (FECA) provides workers' compensation coverage to Federal workers for employment-related injuries and occupational diseases.

i. The Federal Information Processing Standards (FIPS) 199 security impact category for the system is **Moderate**.

Section 1: Status of the Information System

1.1 The status of this information system:

This is an existing information system with changes that create new privacy risks.

Changes That Create New Privacy Risks (CTCNPR)
Significant System Management Changes
Other changes that create new privacy risks:

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
Social Security Number (SSN) **Driver's License**
Other identifying numbers:

Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:
The collection of SSN is required for reporting to the Nuclear Regulatory Commission and is collected in HAPPY. **The paper copies of the Health Unit Occupational Health records will continue to collect the SSN in order to archive to NARA. When the EMRS is in use, the SSN will not be stored. Upon archival, a report will be run to generate a cover page for the medical record, printed, placed in the archival envelope, and sent to NARA.**

General Personal Data (GPD)
Name **Maiden Name** **Alias** **Gender** **Race/Ethnicity** **Age** **Date of Birth** **Home Address** **Telephone Number** **Medical Information** **Physical Characteristics** **Other**
Other general personal data:
Emergency Point of Contact **Medical Information to include vaccination information (verification and testing) for current employees**

Work-Related Data (WRD)
Occupation **Job Title** **Work Address** **Work Telephone Number** **Work Email Address** **Work History** **Other**
Other work-related data:
Supervisor

Distinguishing Features/Biometrics (DFB)
Photographs
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID **IP Address** **Date/Time of Access**
Other system administration/audit data:

Other Information

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
In Person
Online
Other (specify)
Other:
Diagnostic medical devices
Video surveillance

Government Sources
Other:

Non-government Sources
Other:

2.3 Describe how the accuracy of the information in the system is ensured.

The RMS component is inspected and calibrated quarterly by Department of Energy staff.

The HAPPY component information is collected from the source and integrity controls are built into the database.

The Health Unit requests update by the patient when appointments are made, or when visiting the Health Unit. Medical testing derived from spirometer and audiometer software have built-in calibration mechanisms that are run each time the software is launched. Additionally, the manufacturer ensures calibration, annually.

Investigations occur to validate information in TORT claims.

2.4 Is the information covered by the Paperwork Reduction Act?

Yes, the information is covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:
OMB number 0693-0080

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

Yes

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other (specify)

Other:
Electronic Medical Records System (EMRS)

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?
Yes

The IT system supported activities which raise privacy risks/concerns.

Activities
Other
Other:
Video surveillance

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
For administrative matters
Other:

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The RMS collects information (in form of video surveillance) about federal employee/contractor, member of the public, foreign national, or visitor (e.g., anyone entering the physical space).

The HAPPY collects information about NIST employees and associates to assure security and control of radioactive materials and to demonstrate license limit compliance.

The Health Unit collects information about federal employee/contractor, member of the public, foreign national, or visitor who requires care related to their position or while on Gaithersburg's campus.

The Tort forms collect information about federal employee/contractor, member of the public, foreign national, or visitor filing a claim.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating

unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Unauthorized access could result in a breach of users' information. Since OSHE does contain sensitive PII and PHI, a breach would not only have a significant impact on NIST, but also the individual. If released, there is a risk that individual health records could potentially be used to harm or embarrass an individual. **Information system security controls used to protect this data are implemented, validated, and continuously monitored. NIST user access is restricted to authorized users. Annual training and rules of behavior are provided to internal users on the appropriate handling of PII and PHI. The components also have records schedules and procedures in place to dispose of data accordingly.**

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared.

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Bulk Transfer - Federal agencies **Case-by-Case - DOC bureaus** **Case-by-Case - Within the bureau** **Other (specify)**
Other:
Bulk transfers provided from HAPPY to NRC for radioactive material. **Bulk transfers of Occupational Health Data folders are archived with the National Archives and Records Administration by the Health Unit.** **Health Unit information is shared with DOC Bureaus on a case-by-case basis for OSHA and Workman's Compensation. This must be logged as a reportable event and only shared through a DOC portal.** **General user information is transferred via a data feed from the NIST Central People Repository (NIST 183-01) to the Health Unit EMRS. Occupational Health Information and emergency status is shared with supervisors when needed.**

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
NIST 183-01 Applications Systems Division Moderate Applications System **Technical controls are described in Section 8.2.**

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
Government Employees **Contractors**
Other:

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

Yes, notice is provided pursuant to System of Records Notices published in the Federal Register as identified in Section 9. **Yes, notice is provided by a Privacy Act statement and/or privacy policy.** **Yes, notice is provided by other means.**
The Privacy Act statement and/or privacy policy can be found at:
For HAPPY and EMRS, the NIST site privacy policy is on the header and can be found at: https://www.nist.gov/privacy-policy.
The reason why notice is/is not provided:
For RMS, notice is provided on signage within the area where surveillance occurs. **For HAPPY, collection notice is provided on the requisite NIST Request for Personal Radiation Monitoring Services (NIST-366A).** **For Health Unit notifications, notice is provided through the Health Unit's Notice of Privacy Practices, Privacy Act Statements on forms, and the Patient Authorization and Consent for Use and Disclosure of Protected Health Information, in paper form and via the EMRS portal.** **Tort forms are submitted voluntarily by individuals.**

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

Yes, individuals have an opportunity to decline to provide PII/BII. **No, individuals do not have an opportunity to decline to provide PII/BII.**
The reason why individuals can/cannot decline to provide PII/BII:
For RMS, individuals do not have an opportunity to decline surveillance. If an individual enters the area, their actions are observed and recorded. They can choose not to enter the areas. **For HAPPY, individuals have an opportunity to decline providing information by not completing the requisite NIST Request for Personal Radiation Monitoring Services (NIST-366A); however, access to radioactive material will be denied.** **For Health Unit Intake, individuals have opportunity to decline providing information, however, care and services provided may be limited.** **Tort claims are voluntarily submitted by individuals.**

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

Yes, individuals have an opportunity to consent to particular uses of their PII/BII. **No, individuals do not have an opportunity to consent to particular uses of their PII/BII.**
The reason why individuals can/cannot consent to particular uses of their PII/BII:
For RMS, individuals do not have an opportunity to consent to particular uses of information captured by surveillance of the NIST facilities and equipment. **For HAPPY, consent to particular uses is obtained via a letter of request with signature authorization by an individual, Radiation Safety Division Chief, and supervisor before data can be released to any third-party entity other than the established regulatory agency (i.e., NRC). Authorization to release to the NRC is part of NIST Request for Personal Radiation Monitoring Services (NIST-366A). Individuals may choose not to allow for collection and use of this information, but their access to radioactive material would be denied.** **For Health Unit information, individuals have opportunity to consent to particular uses of their non-occupational health information (with the exception of vaccination information) and allowing the Health Unit to use the information for medical care and reporting. For occupational health information, they do not have the opportunity to consent to particular uses. For example, if a patient experiences hearing loss because of occupational exposure, this information must be shared with their supervisor. For personal health data, they have the opportunity to decline particular uses.** **Individuals do not have to file TORT claims, but if they do, information has to be shared with applicable offices or entities; e.g., legal, insurance.**

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

Yes, individuals have an opportunity to review/update PII/BII pertaining to them. **No, individuals do not have an opportunity to review/update PII/BII pertaining to them.**
The reason why individuals can/cannot review/update PII/BII:
For RMS, individuals do not have an opportunity to review/update their information as the collection is not specific to the individual. **For HAPPY, individuals have an opportunity to review/update their information by submitting a service request through safety.nist.gov.** **For Health Unit information, individuals have an opportunity to review/update their information upon each visit or by directly requesting an update to the Health Unit.** **For tort claims, individuals can request changes.**

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

Staff (employees and contractors) received training on privacy and confidentiality policies and practices **Access to the PII/BII/PHI is restricted to authorized personnel only.**

Access to the PII/BII/PHI is being monitored, tracked, or recorded.

The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate.

NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII/PHI are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M) for deficient controls.

An assessment report has been reviewed and determination made that there are no additional security and privacy risks.

Contractors that have access to the system are subject to information security and privacy provisions in their contracts as required by DOC policy.

Reason why access to the PII/BII is being monitored, tracked, or recorded:

RMS is required to ensure no unauthorized personnel have access to controlled materials. The surveillance is recorded to a DVR, and unsuccessful attempts to gain access to areas monitored by RMS trigger an alarm on the monitoring stations.

HAPPY contains sensitive information including the amount and location of radioactive materials, and thus NIST needs to ensure only authorized individuals have access to the materials.

Health Unit case files contain both occupational and non-occupational medical information related to patients and thus access must be monitored to ensure unauthorized access does not occur.

The tort process requires personal information on the incident in order to file a claim and to provide compensation. When the claim is satisfied, all paperwork and emails are destroyed/deleted.

The information is secured in accordance with FISMA requirements.

Is this a new system? No
Below is the date of the most recent Assessment and Authorization (A&A).
04/01/2021

Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

For the RMS and HAPPY components are administered on internal NIST networks protected by multiple layers of firewalls. Automated audit reduction, monitoring, and reporting is employed on each component. All data is encrypted in transit and at rest. For the EMRS, the component is located in an encapsulated isolated environment where data is encrypted in transit and at rest.

For all components, unauthorized access of the components is restricted by user authentication, and role-based access is employed.

For all components, the information sharing is transferred in a secure fashion using FIPS 140-2 validated encryption. Electronic files are maintained on secure file shares and/or encrypted databases.

Physical security controls are employed on Health Unit paper records. They are locked in file cabinets in secured areas.

Any emails sent for the TORT process are encrypted. Any files shared with anyone outside of NIST are performed through nfiles or kiteworks.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

Yes, PII is searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means 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."

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
RMS: **NIST-4, Employees External Radiation Exposure Records** **74 FR 50770 – October 10, 2009** **HAPPY & Health Unit:** **DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies** **72 FR 6200 - February 9, 2007** **OPM/GOVT-10: Employee Medical File System Records** **Health Unit:** **DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations** **86 FR 64448 – November 18, 2021**
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
RMS & HAPPY: **NIST Records Schedule Health Physics item 103 Regulatory Compliance Subject Files** **NIST Records Schedule Nuclear Reactor Program Records item 107 Employee Training and Indoctrination Records**

Health Unit: **GRS 2.7/60 Occupational individual medical case files. Long-term records.** **GRS 2.7/61 Occupational individual medical case files. Short-term records.** **GRS 2.7/70 Non-occupational individual medical case files.** **TORT** **Tort Claims are covered under the General Record Schedule 1.1/080 Administrative claims by or against the United States. GRS1.1/080 lists:** **31 CFR 900-904** **28 U.S.C. 2401** **28 U.S.C. 2415(a)** **31 U.S.C. 3716(c)** **31 U.S.C. 3716(e)**
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Overwriting **Degaussing** **Shredding**
Other disposal method of the PII/BII:

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Quantity of PII** **Data Field Sensitivity** **Obligation to Protect Confidentiality** **Access to and Location of PII**	**Identifiability: Identifying numbers can uniquely identify an individual. The information in HAPPY includes SSN, and the archival process for individual Health Unit medical records include SSN.** **Quantity of PII: As Personal Health**

	Information is maintained for every employee, Associate, or visitor, the quantity of PII is significant. **Data Field Sensitivity: Personal Health Information coupled with identifying information can present and increase risk to privacy with unauthorized disclosure. Information in Happy contains record of who has access to and the location and volume of radioactive material.** **Obligation to Protect Confidentiality: Personal Health Information is entrusted to NIST for patient care and by its nature requires confidentiality.** **Access to and Location of PII: Personal health information is documented in medical case files (both digitally in EMRS and in legacy paper records) for use by the Health Unit. However, controls are in place to protect unauthorized access and security of the information.**

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The threat of unauthorized access and/or misuse exists but is reduced by effective security and privacy controls, internal user training, and requiring internal users to sign the NIST rules of behavior agreements. Threats could arise from collecting more data than is necessary by not employing data minimization. Threats could exploit data secondary use (using personal information for a purpose other than the purpose for which it was collected). Only data required for the OSHE mission is used in OSHE.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

Yes, the conduct of this PIA does result in required business process changes.

Explanation

With migration to Health Unit EMRS, processes to collect. maintain, and archive information has changed.

With the implementation of EMRS, while all active NIST staff have access to ERMS, not all medical records were transitioned (i.e., scanned and uploaded).

- **For patients who received care from 2019 to present, Health Unit paper medical records will be transitioned to EMRS.**
- **For patients who have not received care since 2019 (e.g., calendar year 2018 and prior), the staff's medical record will remain as a paper record until the next time care is provided. At**

that time, some of the medical information may be transitioned, while the majority will continue to remain as a paper medical record. **In addition, to minimize collection/maintenance of SSN with the Health Unit EMRS, a process to obtain SSN for purposes of record archival has been established (i.e., obtaining SSN from HR at time of archival).**

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

Yes, the conduct of this PIA does result in required technology changes.
Explanation
With migration to Health Unit EMRS, legacy paper files will continue to be available, however, new technology is presented with EMRS.