US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/05/2025

OPDIV:

NIH

Name:

Cority

PIA Unique Identifier:

P-3041894-227549

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The PIA has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

Describe the purpose of the system.

Cority is a workflow and database system that manages occupational safety and health data for regulatory compliance and auditing purposes that supports the NIH Occupational Safety and Health Program. Cority will be used to collect, store, and create data on industrial hygiene, safety, and ergonomics activities.

MyCority, a component of Cority, will be available to all NIH staff with NIH network access and allows personnel to submit event reports, conduct investigations assigned to them, perform inspections and surveys, complete questionnaires, and access records.

NIH must comply with federal regulations and provide information when necessary, or as described in the applicable Code of Federal Regulations (CFR).

Personally Identifiable Information (PII) provided to Cority comes from a daily demographic feed of data (export/import) from the NIH Enterprise Directory (NED).

Describe the type of information the system will collect, maintain (store), or share.

The collected PII are: Department of Health and Human Services (HHS) identification (ID) number, NIH network login ID, name (first, middle, last, and preferred name), work email address, phone number (desk, work cell phone, and home), date of birth, emergency contact person, their relationship, and their phone number(s), mail stop, work location (campus, building, and room), home postal address, sex, employment status, staff category, job type, employee type, institute/center/office (ICO), organization, supervisor, job title, job classification, bargaining unit status, summer student status, emergency tier designation, date of hire, date of termination (inferred from when the record no longer appears in NED), NED active status, and NED last update date.

Additional information collected pertaining to individuals will be to capture details about the work they conduct, the hazards they may be exposed to, the protections that are or should be in place, their work environment conditions. The reason why this information will be collected is to detect or correct workplace hazards.

MyCority will serve as a mechanism for the reporting of events to, or the requested services from, the Division of Occupational Health and Safety (DOHS). The event report/request types, which are currently in development, include indoor air quality concerns, safety suggestions, lab clearances, and asbestos abatement. It is also the system through which questionnaires, inspections, surveys, assigned tasks, investigations, and actions can be completed, and personal records pertaining to occupational health and safety can be retrieved.

Users log into Cority using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

MyCority users log in using IAM Services or using MobileIron (a mobile device management tool that NIH uses to secure and manage apps, documents, and other business content on mobile phones and tablets) and Derived Personal Identity Verification credentials (PIV-D) through Government Furnished Equipment (GFE) mobile devices. Mobileiron has its own PIA, including all legal authorities documented.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

Cority is a workflow and database system that manages occupational safety and health data for regulatory compliance and auditing purposes that supports the NIH Occupational Safety and Health Program. Cority will be used to collect, store, and create data on industrial hygiene, safety, and ergonomics activities.

MyCority, a component of Cority, will be available to all NIH staff with NIH network access that allows personnel to submit event reports, conduct investigations assigned to them, perform inspections and surveys, complete questionnaires, and access records. PII provided to Cority from a daily demographic feed of data (export/import) from NED.

The collected PII: HHS ID number, NIH network login ID, name (first, middle, last, and preferred name), work email address, phone number (desk, work cell phone, and home), date of birth, emergency contact person, their relationship, and their phone number(s), mail stop, work location (campus, building, and room), home postal address, sex, employment status, staff category, job type, employee type, ICO, organization, supervisor, job title, job classification, bargaining unit status, summer student status, emergency tier designation, date of hire, date of termination (inferred from when the record no longer appears in NED), NED active status, and NED last update date.

Additional information collected pertaining to individuals will be to capture details about the work they conduct, the hazards they may be exposed to, the protections in place, and their work environment. MyCority will serve as a mechanism for the reporting of events to, or the requested services from, DOHS.

Users log into Cority using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format.

MyCority users log in using IAM Services or using MobileIron (a mobile device management tool that NIH uses to secure and manage apps, documents, and other business content on mobile phones and tablets) and PIV-D through GFE mobile devices. Mobileiron has its own PIA, including all legal authorities documented.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Employment Status
Badge number
Job type/title/occupational series, date of hire, date of termination, emergency tier designation, organization
sex
Emergency contact person and relationship, event report

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PII is used for employee contact and tracking for regulatory compliance and risk management.

Describe the secondary uses for which the PII will be used.

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

5 C.F.R. § 339.205, 42 U.S.C. 241, 42 U.S.C. 2201, 5 U.S.C. 7902, 44 USC 3101 and 3102, and 5 U.S. Code Sec. 301 and 302, 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, Public Law 91-596 (The Occupational Safety and Health Act of 1970), Executive Order 12196, and 13407 – NIH Occupational Safety and Health Management Program.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

SORN: 09-25-0166 Administration: Radiation and Occupational Safety and Health Management

SORN: OPM/GOVT-1, General Personnel Records

SORN: 09-25-0216 Administration: NIH Electronic Directory, HHS/NIH

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

An OMB collection approval number is not needed as Cority and MyCority only use PII of federal employees and direct contractors for internal use only.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

NIH, as a federal agency, is covered by the Occupational Safety and Health (OSH) Act, the same as any other federal agency or private sector employer that OSHA might interact with and request PII. NIH must comply with federal regulations and provide information when necessary, or as described in the applicable Code of Federal Regulations (CFR).

Information is shared only if an OSHA investigator requests a record. For example, OSHA may request a record of a toxic chemical exposure, and that information is exported into Portable Document Format (PDF) and sent by encrypted email to the OSHA investigator.

Describe the procedures for accounting for disclosures.

A record of what is disclosed is kept by the DOHS responsible official for reporting injuries and illnesses that meet OSHA’s mandatory reporting requirements, and who also would normally be designated to oversee responses to informal complaints or inspections, and their

associated information disclosures where necessary.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

All persons who enter in business relationships with the NIH are fully informed in writing prior to the beginning of the transaction that PII is required in order to proceed.

Users log into the system using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no opt-out of the collection of PII. PII is required for the use Cority in order to meet regulatory requirements. If individuals do not want to provide their information, they cannot use the system and participate in NIH programs and certain occupations.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Individuals are notified of major changes that occur in the IAM through official notices sent out or if an Administrative Officer updates or changes PII within the system.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals concerned their PII has been inappropriately obtained, used, disclosed, or is inaccurate, may contact the Division of Occupational Health and Safety.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The NIH privacy policy requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

The system applies role based access to ensure that users are only provided access to data that is required to complete their duties. System administrators assign roles to users based on their need-to-know.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job. An IAM or Monileiron account login is required to gain access to the data

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

System owners, and those with significant information technology responsibilities, are required to take additional annual role based training.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

06-704 Workplace environmental monitoring and exposure records. OSHA-regulated substance monitoring and exposure records.
Results or measurements of monitoring workplace air, toxic substances, or harmful physical agents, including personal, area, grab, wipe, or other methods of sampling results. Area/general occupational exposure records and select carcinogen exposure records from hazardous chemical use in laboratories. Includes the Chemical Hygiene Plan.
Destroy no sooner than 30 years after monitoring is conducted, but longer retention is authorized if needed for business use.
Disposition Authority: DAA-GRS-2017-0010-0004.

06-709. Occupational individual medical case files.
Records of health and safety-related training on topics such as cardiopulmonary resuscitation (CPR), automatic external defibrillators (AED), personal protective equipment (PPE) use, safe sampling techniques, personal decontamination procedures, and emergency response procedures
Long-term records. Destroy 30 years after employee separation or when the Official Personnel Folder (OPF) is destroyed, whichever is longer.
Disposition Authority: DAA-GRS-2017-0010-0009.

07-204 System access records.
These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Includes records such as: User profiles, log-in files, password files, audit trail files and extracts, system usage files, cost-back files used to assess charges for system use.
Systems requiring special accountability for access. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
Disposition Authority: DAA-GRS-2013-0006-0004.

07-201 Systems and data security records.
These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific
systems for which they were written. This series also includes analysis of security policies,

processes, and
guidelines, as well as system risk management and vulnerability analyses.
Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
Disposition Authority: DAA-GRS-2013-0006-0001.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.