US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/10/2020

OPDIV:

NIH

Name:

COVID-19 Reporting Tool

PIA Unique Identifier:

P-1512071-613355

The subject of this PIA is which of the following?

Electronic Information Collection

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

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?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The purpose of the system is to provide a tool for the NIH community to report unsafe conditions related to the COVID pandemic and return of staff to the physical workspace.

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

The system will collect information regarding safety violations: the location where the violation occurred (campus, building, room, Institute, Center, Office [ICO]), the name of the person violating procedures (optional), the name, title and email/phone number of the person to whom the issue was reported and the name of the person making the report, ICO, building, room, email/phone (optional). The Division of Occupational Health and Safety (DOHS) will maintain the system, and will only share the finding and location of these issues. DOHS will not share the information of the person making the report if it is volunteered.

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

The purpose of the system is to provide a tool for the NIH community to report unsafe conditions related to the COVID pandemic and return of staff to the physical workspace.

The system will collect information regarding safety violations: the location where the violation occurred (campus, building, room, Institute, Center, Office [ICO]), the name of the person violating procedures (optional), the name, title and email/phone number of the person to whom the issue was reported and the name of the person making the report, ICO, building, room, email/phone (optional). The Division of Occupational Health and Safety (DOHS) will maintain the system, and will only share the finding and location of these issues. DOHS will not share the information of the person making the report if it is volunteered.

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

Yes

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

Name

E-Mail Address

Phone Numbers

Building and room numbers

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

For follow up for additional information on the reports.

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.

29 CFR 1960.28; Executive Order 12196; Public Health Emergency Declaration:

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

No

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

An OMB collection approval number is not needed as the electronic information collection only uses the PII of federal employees for internal use only, and is exempt from the Paperwork Reduction Act due to the Public Health Emergency Declaration.

Is the PII shared with other organizations?

No

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

A description in the system lets users know that the inclusion of their information is completely voluntary. There is an option to leave an anonymous tip or users have the choice to leave their name and contact information in case they want someone to contact them.

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 a provision for users to opt-out of the collection or use of their PII. There is an option to leave an anonymous tip or users have the choice to leave their name and contact information in case they want someone to contact them.

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

There are no major changes anticipated to the system. This system is going to be in use for a limited period of time and will be decommissioned when the emergency conditions brought on by the pandemic have been resolved.

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.

It is anticipated that back end of this program will support two types of access . The first is access to the information without PII. The second level of access, which contains the PII , will only be accessible to limited staff who have additional permissions to view the data. The second level personnel will only access the PII when additional information is needed to resolve the complaint.

If a complaint is made the organization will determine the nature of the complaint, review the limited staff access and protocols to confirm the security processes were being followed. If the protocols are not followed or some other unanticipated hardware or application breach occurs, the appropriate remediation will be conducted to include: additional training and system changes as necessary.

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

There are no planned reviews of the PII anticipated. The system life is expected to be of limited duration. When the pandemic emergency has concluded, the system will be decommissioned and the data disposed of in a manner consistent with federal records management practices.

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

Users:

Users may need information for additional follow up to the complaint. These will be limited DOHS staff with permission to access the data.

Administrators:

The administrators are DOHS Federal staff who are the only ones who have access to the PII.

Contractors:

Direct contractors provide system development life cycle (SDLC) support and may have access to the PII for official support purposes.

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

Designated staff may need information for additional follow up of the complaint. These will be vetted DOHS staff only. The staff are tasked with the review, follow up and resolution tracking of these reports initially without the PII. If the PII is needed then another level of access will be necessary. That access will be provided by DOHS leadership on an as needed basis only.

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Authentication with NIH Personal Identity Verification (PIV) card will occur at time of login to the NIH Network.

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.

The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness).

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

Staff using this information will receive site specific training on privacy and response expectations by DOHS leadership.

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 maintained within 1 year after monitoring is conducted, but longer retention is authorized if needed for business use in accordance with NARA record retention schedule:

GRS 06-707, Employee Health and Safety Records; Workplace environmental monitoring and exposure records. Background data; DAA-GRS-2017-0010-0007.

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

Administrative controls: Elevated access requests can be made through the system or via email. Each individual requesting elevated access is contacted by a system administrator to determine the appropriate level of access to be granted. During monthly census uploads all accounts not on the NIH census are inactivated and their access level is reset to the lowest level. Permissions level is also reset if an account is inactivated manually by an admin. Elevated permissions can only be granted again via the approval system above.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.