US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/10/2025

OPDIV:

NIH

Name:

Division of Fire and Rescue Services Emergency Response System (DFRS ERS)

PIA Unique Identifier:

P-2345991-095980

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

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)?

No

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

Describe the purpose of the system.

The Division of Fire and Rescue Services (DFRS) Emergency Reporting Software (ERS) is a cloud-based system primarily used to collect, maintain (store), or share patient's information for the dispatch of the Fire and Rescue Services (FRS) for a National Institutes of Health (NIH) emergency response event. The secondary use of this information will be used to report cases to Occupational Medical Services (OMS) and the Occupational Safety and Health Administration (OSHA).

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

The DFRS ERS will collect, maintain (store), or share patient's name, driver's license number, address, age, phone number, medical notes, geo-location, employee's work schedule status (scheduling of shifts, on duty, off duty, annual leave, sick leave), patient's medical status (transport location, medical/injury, medication, medical history), badge number and Personal Identity Verification (PIV) card number.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM)

Services which maintains its own unique privacy impact assessment (PIA) on record, including 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 credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

The DFRS ERS is a cloud-based system primarily used to collect, maintain (store), or share patient's information for the dispatch of the FRS for an NIH emergency response event. The secondary use of this information will be used to report cases to OMS and OSHA.

The DFRS ERS will collect, maintain (store), or share patient's name, driver's license number, address, age, phone number, medical notes, geo-location, employee's work schedule status (scheduling of shifts, on duty, off duty, annual leave, sick leave), patient's medical status (transport location, medical/injury, medication, medical history), badge number and PIV card number.

Users log in to this system using the NIH IAM Services which maintains its own unique PIA on record, including 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 credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

Yes

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

Name
Driver's License Number
Mailing Address
Phone Numbers
Medical Notes
Age, Geo-location
Badge Number
PIV Card number
Employee's work schedule status (scheduling of shifts, on duty, off duty, annual leave, sick leave)
Patient's medical status (transport location, medical/injury, medication, medical history)

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

To identify the patient, incident location, and to pay insurance claims.

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

To report cases to OMS and OSHA.

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

42 U.S. Code § 282, Section 19 of the Occupational Safety and Health Act of 1970 (Pub. L. 91-596); 5 U.S.C. 7902; 29 CFR part 1960; Executive Order No. 12196

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the DOI

Other Federal Entities

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

The OMB collection approval number is not needed as the Division of Fire and Rescue Services (DFRS) Emergency Response Software (ERS) does not survey or solicit information. It's entered by responders during emergency incidents.

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.

OSHA and the Department of Labor require all federal agencies to create and post an annual summary of all OSHA-recordable work related injuries and illnesses. An MOU is not needed to satisfy this requirement.

Describe the procedures for accounting for disclosures.

For all releases to the public and other agencies, the NIH Freedom of Information Act (FOIA) and Privacy Policy Branch will review, redact (when necessary) and keep an electronic track of such disclosures.

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

At the time of a dispatch of an actual emergency response and rescue service, the DFRS will obtain the personally identifiable information (PII) from the individual employees, public citizens, vendors/suppliers/contractors, and patients assigned PIV Card Badges.

If individual employees, public citizens, vendors/suppliers/contractors, patients do not have a PIV Card Badge at the time of an emergency, then the individuals would be advised verbally that their information will be obtained and stored within the DFRS ERS.

There may be instances where the individual employees, public citizens, vendors/suppliers/contractors, patients cannot be notified because they may not be coherent or responsive or incapacitated, and as a result, the DFRS cannot notify nor obtain consent that their PII has been obtained and stored within the DFRS ERS.

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 method for individuals to opt-out of the collection or use of their PII because it is required to process their emergency request.

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

There is no method to notify or obtain consent to their PII collected in the system because they are subject to an emergency and/or in a location where there is no reasonable expectation of privacy.

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 may contact their NIH Privacy Coordinator or the NIH Senior Official for Privacy at Privacy@mail.nih.gov.

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

DFRS staff will perform quarterly reviews as part of DFRS Quality Assurance (QA) and Quality Improvement (QI) program. System owner will perform review of QA/QI reports and system security audit reports.

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.

ERS users are approved by DFRS management for access based on their technical/functional role in administering, developing, and supporting the daily job functions of DFRS ERS.

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 conform to 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. Annual review of system users' roles are done to assure access is current with user's technical/functional role in administering, developing, and supporting the daily job functions of DFRS ERS.

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 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).

Users with additional roles for system administration, risk management, leadership, continuity of operations and safety receive additional training for ethics, equal opportunity and diversity, No FEAR act, and use of strategic sourcing.

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.

DFRS ERS records are retained and disposed of under the authority of the NIH Records Retention.

Item 03-001: Clinical Care Services Records
These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Exclusions and exceptions are noted and cross referenced to their appropriate item numbers within this schedule. The records associated with this common schedule item include, but are not limited to, clinical care functions.
Disposition: Cut off annually at end of fiscal year. Destroy 7 years after cutoff.
Disposition Authority Agency (DAA): DAA-0443-2019-0001-0001

Item 09-102: Employee emergency contact information.
Employee emergency contact information.
Records used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations. Records include name and emergency contact information such as phone numbers or addresses. Records may also include other information on employees such as responsibilities assigned to the individual during an emergency situation.
Disposition: Destroy when superseded or obsolete, or upon separation or transfer of employee.
Disposition Authority: DAA-GRS-2016-0004-0002

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

Physical Controls: The information technology (IT) hardware used to host ERS protected information is located in a secured data center 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 provisioned for ERS 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.

Administrative Controls: All technical personnel who access ERS 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.