US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/04/2025

OPDIV:

NIH

Name:

Computer Aided Dispatch/Records Management System (CAD/RMS).

PIA Unique Identifier:

P-8875202-376619

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.

Computer-Aided Dispatcher (CAD)/Records Management System (RMS) is a public safety software built in the cloud that collects police intervention information to help the NIH increase efficiency and accurate law enforcement results. CAD operates a natural extension of the NIH dispatcher, call taker, and in-field first responder during an emergency response. RMS is a safety reporting platform that has six core functions: Report Writing, Case Management, Property & Evidence, Booking, Stat Reporting & Crime Analysis, and System Administration.

CAD/RMS receives criminal history information, such as name, date of birth, fingerprints, crimes locations and court history, from the Maryland Electronic Telecommunications and Enforcement Resource System (METERS), VESTA 911 Emergency Call Handling Software and Geographic Information System (GIS) using a one-way Virtual Private Network (VPN) interface connection.

It also receives emergency information, such as name, driver's license number, phone numbers, geographic location, and medical notes, to assist 911 call takers/dispatchers to quickly determine the

appropriate Determinant Code for each case and to clearly display the response configuration and specifically assign that code by local agency authorities and individual centers.

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

CAD/RMS receives criminal history information, such as name, date of birth, fingerprints, crimes locations and court history, from the Maryland Electronic Telecommunications and Enforcement Resource System (METERS), VESTA 911 Emergency Call Handling Software and GIS using a one way VPN interface connection.

It also receives emergency information, such as name, driver's license number, phone numbers, geographic location, and medical notes, to assist 911 call takers/dispatchers to quickly determine the appropriate Determinant Code for each case and to clearly display the response configuration and specifically assign that code by local agency authorities and individual centers.

CAD/RMS will collect, maintain, store, and disclose Social Security Number (SSN), name, driver's license number, email address, phone numbers, date of birth, photographic identifiers, vehicle identifiers, mailing address, employment status, geo-location, and medical notes, and badge numbers only with the NIH Division of Police (DP) through the Axon Body Worn Camera (BWC) system and to the NIH Division of Fire Rescue Services (DFRS) to respond to events swiftly and efficiently.

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.

Computer-Aided Dispatcher (CAD)/Records Management System (RMS) is a public safety software built in the cloud that collects police intervention information to help the NIH increase efficiency and accurate law enforcement results. CAD operates a natural extension of the NIH dispatcher, call taker, and in-field first responder during an emergency response. RMS is a safety reporting platform that has six core functions: Report Writing, Case Management, Property & Evidence, Booking, Stat Reporting & Crime Analysis, and System Administration.

CAD/RMS receives criminal history information, such as name, date of birth, fingerprints, crimes locations and court history, from the Maryland Electronic Telecommunications and Enforcement Resource System (METERS), VESTA 911 Emergency Call Handling Software and GIS using a one way VPN interface connection.

It also receives emergency information, such as name, driver's license number, phone numbers, geographic location, and medical notes, to assist 911 call takers/dispatchers to quickly determine the appropriate Determinant Code for each case and to clearly display the response configuration and specifically assign that code by local agency authorities and individual centers.

CAD/RMS will collect, maintain, store, and disclose Social Security Number (SSN), name, driver's license number, email address, phone numbers, date of birth, photographic identifiers, vehicle identifiers, mailing address, employment status, geo-location, and medical notes, and badge numbers only with the NIH Division of Police (DP) through the Axon Body Worn Camera (BWC) system and to the NIH Division of Fire Rescue Services (DFRS) to respond to events swiftly and efficiently.

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.

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

Yes

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

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Employment Status
Geo-Location
Badge Number

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

For identification purposes in the investigation, review, and analysis of the incident or event.

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

These data can also be used for Division of Emergency Management (DEM) dispatchers, DP Officer and First Responder training.

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

40 U.S.C. § 1315 Law enforcement authority of Secretary of Homeland Security for protection of public property; General Administrative Delegation of Authority Number 08, Control of Violations of Law at Certain NIH Facilities (September 1, 2020).

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.

09-25-0224, NIH Division of Police Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Other

Government Sources

Within OpDiv

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not Applicable. Information collection is exempt from the Paperwork Reduction Act of 1995.

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.

Information is only shared between law enforcement agencies conducting a criminal investigations or under legal mandate with consideration from the NIH Chief of Police.

Describe the procedures for accounting for disclosures.

For all releases to the public and other agencies, the NIH FOIA and Privacy Policy Branch will review, redact (when necessary) the recording 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.

For information that is collected in person during the process of incident investigations, individuals are notified verbally by
the DEM representative and/or as part of the evidence-informed decision making (EIDM) application.

Information that is pulled from the Health and Human Services (HHS) Identity Management System (IDMS) and NIH Enterprise Directory (NED) have their own PIAs and processes for notifying individuals that their information will be collected. Both IDMS and NED maintain their own approved PIAs, with processes in place to notify individuals that their personally identifiable information (PII) will be collected.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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.

Individuals cannot 'opt-out' of providing their PII (name, phone number, home address, etc.) because it is required on the EIDM application as part of the incident investigation.

DP users cannot 'opt-out' of providing their PII as it is required to create an account to access CAD/RMS to process an incident.

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

Information that is pulled from the IDMS and NED have their own PIAs and processes for notifying individuals when changes to the system occur. Both IDMS and NED maintain their own approved PIAs, with processes in place to notify individuals that their PII will be collected.

For individuals whose information is collected outside of NED and IDMS, individuals are notified by a DEM representative through the investigation process and up to 3 years after the final investigation or reporting action as been processed. At that time, the record is removed from 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.

Information that is pulled from the IDMS and NED have their own PIAs and processes for resolving individuals' concerns. Both IDMS and NED maintain their own approved PIAs, with processes in place to notify individuals that their PII will be collected.

For individuals whose information is collected outside of NED and IDMS, individuals may reach out to a DEM representative throughout the investigation process and up to 3 years after the final investigation or reporting action as been processed. At that time, the record is removed from the system.

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

CAD/RMS has annual reviews of PII contained in the system, as well as audits of data logs to assure all information is accurate and relevant.

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.

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.

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.

Access to PII is assigned to personnel based upon current job responsibilities. Specific login credentials are required to access the stored PII 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. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials. Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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

The NIH DEM personnel receive on-the-job-training to use the CAD/RMS system by the System Owner.

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.

CAD/RMS records are retained and disposed of under the authority of the NIH Records Retention schedule Records Schedule System

NIH General Records Schedule (GRS) 5.6 Item 030, Security Records; Uniform and equipment tracking records: Disposition Authority Agency (DAA)-GRS-2017-0006-0004. Destroy 3 months after return of equipment, but longer retention is authorized if required for business use.

NIH GRS 5.6 Item 090, Security Records; Records of routine security operations: DAA-GRS-2017-0006-0012. Destroy when 30 days old, but longer retention is authorized if required for business use.

NIH GRS 5.6 Item 100, Security Records; Accident and incident records: DAA-GRS-2017-0006-0013. Destroy 3 years after final investigation or reporting action or when 3 years old, whichever is later, but longer retention is authorized for business use.

NIH GRS 5.6 Item 110, Security Records; Visitor processing records. Areas requiring highest level security awareness: DAA- GRS-2017-0006-0014. Destroy when 5 years old, but longer retention is authorized if required for business use.

NIH GRS 5.6 Item 111, Security Records; Visitor processing records. All other facility security areas: DAA-GRS-2017-0006-0015. Destroy when 2 years old, but longer retention is authorized if required for business use.

NIH GRS 5.6 Item 120, Security Records; Personal identification credentials and cards. Application and activation records:
DAA-GRS-2017-0006-0016. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor’s employment, but longer retention is authorized if required for business use.

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

Administrative Controls: DEM users that has access to the CAD/RMS cloud system 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 information technology (IT) hardware used to host protected information is located in a secured datacenter facility and not publicly accessible. 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: CAD/RMS is hosted on a cloud platform that is restricted to only NIH internet protocol (IP) addresses. CAD/RMS analyzes logs and alerts the team when unauthorized, suspicious or malicious activity is detected. Access to the system is controlled and granted based on the principle of least privilege access. Two Factor Authentication, which is an industry security standard that uses two different types of identity verification, is used for accessing the site. CAD/RMS has integrated file integrity monitoring and auditing capabilities.

Disaster recovery/business continuity is managed by the vendor and performs annual testing.