US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/23/2024

OPDIV:

NIH

Name:

Division of Police Body Worn Camera (DPBWC)

PIA Unique Identifier:

P-3239643-236301

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 NIH Division of Police (DP) Directive 463 establishes a Body Worn Cameras (BWC) Program to ensure transparency and accountability in law enforcement activities. The BWC videos/recordings provide accurate and credible accounts of police interaction with individuals within the NIH, that can be used as evidence, and for training purposes for the NIH patrol officers. NIH DP uses the Axon Enterprise, Inc, (Axon) owned website, Evidence.com, as the Software-as-a-Service (SaaS) Central repository for evidence collected by BWC. The information processed and stored in Evidence.com includes audio and video recordings taken by the BWC and associated metadata. The metadata includes information about the footage that helps DP understand and manage the video, such as notes, clips, markers, and audit trails. While the BWC Program data in Evidence.com is stored on the cloud site, and the cloud vendor provides the infrastructure and platform services, that vendor has no access to the data. As a separate note, the cameras employed by DP do not have facial recognition capabilities and Evidence.com is not being used to conduct facial recognition on the recordings.

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

The DP patrol officer is mandated to use the BWC system to record interactions with individuals in NIH facilities during policing events and incorporate Personally Identifiable Information (PII) of involved parties to confirm the identification of individuals during investigative interviews.

The BWC recordings may collect through the video interview and maintain (store) in videos: Social Security Number (SSN), name, driver license, mother maiden name, email address, phone numbers, medical notes, certificates, education records, military status, foreign activities, taxpayer identification (ID), date of birth, photographic identifiers, biometric identifiers, vehicle identifiers, mailing address, medical records number, financial account info., legal documents, device identifiers, employment status, passport number, badge number, and geolocation information.

The PII, with exception of the officer badge number, is not individually recorded on the system, but rather is stored as part of a video recording. Access to these data will be available to specific DP officers for retrieval, review, and analysis. DP officers will label all BWC videos with an ID generated incident report number, a Title that includes the victim and primary suspect names or the incident address, and a Category number.

Users log in to the system through PIV based single-sign-on (SSO). This is done through 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 NIH Division of Police (DP) Directive 463 establishes a Body Worn Cameras (BWC) Program to ensure transparency and accountability in law enforcement activities. The BWC videos/recordings provide accurate and credible accounts of police interaction with individuals within the NIH, that can be used as evidence, and for training purposes for the NIH patrol officers. NIH DP uses the Axon Enterprise, Inc, (Axon) owned website, Evidence.com, as the Software-as-a-Service (SaaS) Central repository for evidence collected by BWC. The information processed and stored in Evidence.com includes audio and video recordings taken by the BWC and associated metadata. The metadata includes information about the footage that helps DP understand and manage the video, such as notes, clips, markers, and audit trails. While the BWC Program data in Evidence.com is stored on the cloud site, and the cloud vendor provides the infrastructure and platform services, that vendor has no access to the data. As a separate note, the cameras employed by DP do not have facial recognition capabilities and Evidence.com is not being used to conduct facial recognition on the recordings.

The DP patrol officer is mandated to use the BWC system to record interactions with individuals in NIH facilities during policing events and incorporate PII of involved parties to confirm the identification of individuals during investigative interviews.

The BWC recordings may collect through the video interview and maintain (store) in videos the following PII: SSN, name, driver license, mother maiden name, email address, phone numbers, medical notes, certificates, education records, military status, foreign activities, taxpayer ID, date of birth, photographic identifiers, biometric identifiers, vehicle identifiers, mailing address, medical records number, financial account info., legal documents, device identifiers, employment status, passport number, badge number, and geolocation information.

The PII, with exception of the officer badge number, is not individually recorded on the system, but rather is stored as part of a video recording. Access to these data will be available to specific DP officers for retrieval, review, and analysis. DP officers will label all BWC videos with an ID generated incident report number, a Title that includes the victim and primary suspect names or the incident address, and a Category number.

Users log in to the system through PIV based single-sign-on (SSO). This is done by 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.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Biometric Identifiers
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Device Identifiers
Military Status
Employment Status
Foreign Activities
Passport Number
Taxpayer ID
Badge number
Geolocation information

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?

100,000-999,999

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.

The recordings can also be used for DP Officer 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

Other HHS OpDiv

State/Local/Tribal

Foreign

Other Federal Entities

Other

Non-Governmental Sources

Public

Private Sector

Other

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.

For non-law enforcement agencies, information is shared in accordance with FOIA and/or Privacy Act requirements.

Under the Freedom of Information Act (FOIA) and Privacy Act regulations, video recording may be requested through NIH FOIA and Privacy Policy Branch (PPB) for disclosure.

Describe the procedures for accounting for disclosures.

All recording will be registered in metadata (audit log) within the BWC system and upon release.

For all releases to the public and other agencies, the NIH FOIA and PPB 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.

NIH facilities have signage throughout the campus that indicates video and audio surveillance. Off campus facilities in the states of Maryland and Montana requires that DP patrol officer provide verbal notice.

During an active police situation or event on NIH grounds, the DP patrol officer will initiate the recording and does not notify involved individuals of the use of the body cameras, except when interviewing a witness or victim, where they can request not to be recorded and can provide a signed written statement. However, if the individual is a suspect on a criminal situation, the video recording cannot be to stopped during the investigation. The individual can request their Fifth Amendment rights.

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.

During an active police situation, individuals cannot opt-out because video recordings are required for legal evidence as they collect objective and continuous records of events. The only exception is during an interview, when an eyewitness or victim can request to not be recorded, and agree to provide a signed written statement.

If the individual is a suspect on a criminal situation, the video recording cannot be stopped during the investigation. The individual can request their Fifth Amendment rights.

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

AXON is an evidence storage system that maintains the video and audio recordings of the body worn camera system. This system does not document the identity of individuals, but are stored within the video recordings themselves. Similarly, system changes or capabilities will not be able to identify individuals and if a capability was to be deployed with that feature, it will not be able to retroactively and redactively identify previous PII information.

Although individuals are notified (by signage or verbally) that video and audio surveillance is occurring, they cannot decline to have their PII collected in the system when they are subject to an active police investigation 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 ORS-ORF 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.

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. The system produces reports for review by the system administrator.

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 Chief of DP will provide decisions and approvals for all role based access controls based on 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.

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 and privacy awareness training. 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).

The NIH DP personnel receive on-the-job-training to use the BWC system by DO Training Officers and DP Designees.

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 in accordance with the following NIH record retention schedules:

Item 08-204, Information access and protection operational records. Records tracking and controlling access to protected information.
Records tracking and controlling access to protected information Includes: Records documenting receipt, internal routing, dispatch, or destruction of classified and controlled unclassified records, tracking databases and other records used to manage overall access program, and requests and authorizations for individuals to have access to classified and controlled unclassified records and information
Disposition: Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified or destroyed; or when an individual's authorization expires; whichever is appropriate. Longer retention is authorized if required for business use
Disposition Authority: DAA-GRS-2019-0001-0002

Item 08-228, Controlled Unclassified Information (CUI) Information sharing agreements.
Agreements in which agencies agree to share CUI with non-executive branch entities.
Disposition: Destroy 7 years after canceled or superseded, but longer retention is authorized if

required for business use.
Disposition Authority: DAA-GRS-2019-0001-0006

Item 09-413 Accident and incident records.
Records documenting accidents and incidents occurring on, in, or at government-owned or -leased facilities, vehicles (land, water, and air), and property used by federal agencies.
Disposition: 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.
Disposition Authority: DAA-GRS-2021-0001-0004

Item 09-422, Personnel suitability and eligibility investigative reports.
Investigative reports and related documents agencies create or use to support initial favorable eligibility determinations, fitness determinations, and periodic reinvestigations, or to implement a continuous evaluation program.
Disposition: Destroy in accordance with the investigating agency instruction.
Disposition Authority: DAA-GRS-2017-0006-0022
Item 09-423, Personnel security investigative reports. Reports and records created by agencies conducting investigations under delegated investigative authority. Investigative reports and related documents agencies create or use to support initial favorable eligibility determinations, fitness determinations, and periodic reinvestigations, or to implement a continuous evaluation program.
Disposition: Destroy in accordance with delegated authority agreement or memorandum of understanding.
Disposition Authority: DAA-GRS-2017-0006-0023

Item 09-427 Security Management Records
Information security violations records. Case files about investigating alleged violations of executive orders, laws, or agency regulations on safeguarding national security information. Includes allegations referred to the Department of Justice or Department of Defense. Includes final reports and products.
Dispositon: Destroy 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use.
Disposition Authority: DAA-GRS-2017-0006-0027

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

Administrative Controls: DP officers who have access to the BWC 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 BWC cloud provider rates an "A" in the Qualys Secure Socket Layer (SSL) Labs. The vendor maintains a highly secure cloud ecosystem with advanced protections that use advanced security tools and threat protection solutions. The body worn cameras are individually assigned to each patrol officer and the equipment are held within the secure DP Office area which requires PIV access as well as a manned front desk. These devices have been hardened to reduce potential attack surfaces and only allow necessary functionality.

Technical Controls: The BWC cloud based storage used to host protected information is located within a FEDRAMP high cloud system that requires NIH PIV based single-sign-on on Security Assertion Markup Language (SAML) that is audit logged. The DPBWC cloud utilizes Federal Information Processing Standards (FIPS) 140-2 ad Transport Layer Security (TLS) 1.2 (256 BIT connection, Rivest-Shamir-Adleman (RSA) 1048 bit key) in data encryption in transit. The data encryption at rest is Center for Internet Security (CIS) Compliant, National Security Agency (NSA)

Suite B 256 bit Advanced Encryption Standard (AES) encryption. The system utilizes granular role-based permission management for access control which is managed by the System Owner. Updates are provided when placed on the charging station.

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