US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2025

OPDIV:

IHS

Name:

Video Surveillance Systems

PIA Unique Identifier:

P-1258521-435773

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

Existing

Does the system have Security Authorization (SA)?

No

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

Describe the purpose of the system.

To ensure patient and staff security and to deter theft and misuse of facility equipment, medical supplies and medicines and narcotics.

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

The system will store and maintain photographic identifiers, vehicle identifiers, device identifiers, login time and date of staff accessing the system.

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

Cameras will be installed in strategic locations with the video and still image recordings stored on a network server. Data collected will be video and still images of everyone who comes within range of the cameras. Vehicles that pass within the camera range may have their license plates and make and model of the vehicle collected. The video and still images will collect the date and time of when the images were taken. The device identifiers are collected via identifier. e.g. "Main Entrance". The system will also collect the date and time of those who access and logs into the video control

system. The recorded video will be used to ensure staff and patient safety. The recordings will run 24 hours a day and will be stored temporarily, depending on the location, up to 60 days. The camera locations will be in public areas. Access to the live view and recordings will be enforced with specific access granted to Security, IT staff and administrators. There will be internal controls and separation of duties will be enforced ensuring that users cannot delete or manipulate the recorded videos.

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

Yes

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

Photographic Identifiers
Vehicle Identifiers
Device Identifiers
Other data collected will be login time and date of staff accessing the system.

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?

1,000,000 or more

For what primary purpose is the PII used?

To ensure patient and staff safety, law enforcement investigations and Freedom of Information Act.

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

Secondary use includes training and testing.

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

The Privacy Act of 1974.

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 DoD
Other DoD Components
Non-Government Sources
Public

Identify the OMB information collection approval number and expiration date

Not Applicable

Describe how the PII is used.

The PII are images of the public in the building. Proper signage is present. e.g. "Cameras in Use in this Building"

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.

N/A

Describe the procedures for accounting for disclosures.

The IHS, with respect to each system of records under its direct control (i.e., Privacy Act System of Record 09-17- 0001, Medical, Health, and Billing Records) must keep a record of the date, nature, and purpose of each disclosure of a record to any person or Agency under subsection (b) of the Privacy Act (5 U.S.C. § 552a) and the name and address of the person or Agency to whom the disclosure is made. This record must be kept for 5 years or the life of the record; whichever is longer, after the disclosure for which the accounting has been made. An individual (beneficiary) is entitled, upon request, to get access to this disclosure record of his or her own personal records with the exception for disclosures made under subsection (b)(7) of the Privacy Act (as a result of civil or criminal law enforcement activity). The IHS must inform any person or other Agency about any correction or notation of dispute made by the IHS in accordance with subsection (d)(4) of the Privacy Act (Access of Records) of any record that has been disclosed to the person or Agency if an accounting of the disclosure was made. This is a mandatory reporting requirement and may be recorded utilizing the IHS-505, "Disclosure Accounting Record" form.

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

Indian Health Manual - Part 2, Chapter 7 - It is IHS policy to provide adequate notice of its uses and disclosures of Protected Health Information (PHI) and of the individual's rights and IHS' legal duties with respect to PHI. A copy of the Notice is provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office provides a copy of the current Notice to the patient. The staff member has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed "Acknowledgement of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record.

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.

Patient can choose not to come to IHS and in the Kayenta Patient's Bill of Rights, patients have the option not to participate.

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

It is IHS policy to provide adequate notice of its uses and disclosures of PHI/PII and of the individual's rights and IHS' legal duties with respect to PHI/PII. The IHS prominently and clearly displays the Notice (2-7.18) in every facility (https://www.ihs.gov/sites/foia/themes/responsive2017/display_objects/documents/HIPAAPRIVACYPRACT.pdf). A copy of the Notice is also provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office or other appropriate department

provides a copy of the current Notice to the patient. The patient acknowledges receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. An IHS staff member signs and dates the Acknowledgment form and files the signed "Acknowledgment of Receipt of IHS Notice of Privacy Practices" into the patient's medical record. No less than every three years, IHS provides notification of the availability of the Notice and how to obtain the Notice. If the Notice is revised by a material change, the revised Notice must be posted in clear and prominent locations in every facility and on its web site, on or after the effective date of the revision. The revised Notice will be posted on the IHS website within the 60 days of a material revision. The revised Notice is also given to all patients who come into a facility after the effective date of the revision and is available upon request on or after the effective date of the revision. Additionally, IHS provides the revised notice to all eligible patients registered in the patient registration system within 60 days of the revision of the Notice. Any individual, whether or not a patient, has the right to request and receive a copy of the Notice at any time, except an inmate. Inmates have no rights to the Notice (45 CFR § 164.520 (a)(3)).

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.

All complaints are addressed to the Service Unit Chief Executive Officer or (his or her) designee for investigation. Complaints are documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Complaints may also be filed directly with the Secretary, DHHS.

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 Health Information Management Department has oversights and processes in place. They will be contacted to ensure there are periodic reviews to ensure the data's integrity, availability, accuracy and is relevant. To also ensure that only non-relevant data is deleted so that if deletion is in 30 days, that data will be reviewed. The Security Department who monitors the camera images will notify system owners to ensure images are clear.

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.

Indian Health Manual, Part 8, Chapter 21 - Access Control

The Information Technology Access Control (ITAC) supervisors are responsible for submitting appropriate access requests for IHS system users on their team and for reviewing their team members' access. The System Administrator then grants the most restrictive access privileges needed to perform job related roles and responsibilities.

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.

The system utilizes least privilege and role-based access controls. Access is granted to a limited number of authorized administrators and federal employees. Standard users do not have access to PII.

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.

Role-based training, IHS Rules of Behavior agreements, and Information System Security and Privacy Awareness training courses are required to be completed annually by all IHS users.

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

All staff with access to network servers and data require the Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Act trainings.

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.

DAA-GRS2013-0007-0020 - Destroy when 90 days old, 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.

Active Directory user access control, Microsoft BitLocker full disk encryption, and physical access controls in the Albuquerque Data Center (ADC) and facilities will be utilized to secure the images to include locked doors to the Server Farm and Building security locks for access.