US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/06/2026

OPDIV:

IHS

Name:

EKG ECG Machines IHS-wide

PIA Unique Identifier:

P-2402931-714191

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Requirements Analysis

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 Electrocardiogram (EKG/ECG) machine records the electrical activity of the heart to assess: heart rhythm, heart rate, electrical conduction abnormalities, evidence of ischemia or prior heart injury to rule out cardiac problems when a patient is experiencing chest pain, dizziness or shortness of breath. EKG is also used as a diagnostic tool and establishes cardiac baseline for future comparisons.

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

The EKG/ECG system collects, stores, and shares patient and staff information to support cardiac testing and clinical care. Patient data includes Personally Identifiable Information (PII) (e.g., name, date of birth, patient sex, phone number, medical record number (MRN), and demographics) and Protected Health Information (PHI) such as EKG waveforms, heart rate and rhythm data, test dates, ordering provider information, electronic signature, device identifier, and clinical interpretations. The system also maintains limited staff Personal Identifiable Information (PII), including name, user ID, role, and audit logs that track access and actions within the system. This information is used to

accurately link test results to patients, support clinical review and diagnosis, maintain longitudinal medical records, and ensure accountability through audit logging. Information may be shared with authorized users and integrated systems, such as Electronic Health Records (EHRs), for continuity of care. Records are routinely retrieved using MRN, patient name, and date of birth, and by user ID for staff access.

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

The EKG/ECG system records and manages information related to a patient's heart activity to support diagnosis and treatment. It collects Protected Health Information (PHI) , including name, date of birth, patient sex, phone number, mailing address, medical record number (MRN), along with such as EKG waveforms, heart rate and rhythm data. Personal Identifiable Information (PII) collected are staff name preforming the EKG/ECG or user ID, role, test date and time, ordering provider, clinical interpretations, device ID, test location, and electronic signature. The system maintains audit logs of system access and actions. Information is used to link test results to the correct patient, support clinical review, maintain medical records, and ensure security and accountability. Data may be stored and shared with authorized systems, such as Electronic Health Records (EHRs). Records are routinely retrieved using MRN, patient name, and date of birth, and by user ID for staff.

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

Yes

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

Date of Birth
Name
Mailing Address
Phone Numbers
Medical Records Number
Device Identifiers
EKG waveforms
Heart rate and rhythm data
Ordering provider name and/or Technician name, user ID, electronic signature, role and demographics

Patient Sex
Date & time of test

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

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

To accurately identify the patient and correctly associate the clinical results with the right individual so the information can be used safely for diagnosis, treatment, and continuity of care.

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

Secondary uses of PII is used in healthacare operations:
Quality assessment and improvement
Clinical performance reviews
Patient safety investigations

Peer review activities
Accreditation and compliance audits

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

Departmental Regulations (5 U.S.C.301); Privacy Act of 1974 (5 U.S.C. 552a); Federal Records Act (44 U.S.C. 2901); Section 321 of the Public Health Service Act, as amended (42 U.S.C. 248); Section 327A of the Public Health Service Act, as amended (42 U.S.C. 254a); Snyder Act (25 U.S.C. 13); Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.); Transfer Act of 1954 (42 U.S.C. 2001–2004); HIPAA, HITECH (and subsequent regulations); and 21st Century Cures Act, 42 CFR Part 2.

Privacy Act of 1974; Report of Amended or Altered System; Medical, Health and Billing Records System. https://www.govinfo.gov/content/pkg/FR-2010-01-12/pdf/2010-285.pdf.

IHS SORN for Medical, Health and Billing Records System. 09-17-0001

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.

SORN 09-17-0001, BAA Required. Include the following: FAR 52.224-1, 52-224-2, 52-239.1,

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Government Sources
Within the OPDIV

Identify the OMB information collection approval number and expiration date

Exempt from an OMB Information Collection Number through Public Law 114-255, the 21st Century Cures Act, Section 2035: Exemption for IHS from the Paperwork Reduction Act requirements.

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.

Indian Health Manual - Part 2, Chapter 7 - It is IHS policy to provide adequate notice of its uses and disclosures of 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.
HS employees are notified at the time of hire that their PII will be collected and give consent as it is part of the on-boarding process.

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.

The Individual is given the opportunity to opt-in to the test, if they opt out of testing the risk are communicated to the patient.

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 in every facility. 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 Acknowledgement form and files the signed "Acknowledgement 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)).

IHS employees are notified at the time of hire that their PII will be collected and give consent as it is part of the on-boarding process.

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.

PII will only appear in EKG if an order is placed by provider. For any reason, if PII was entered and no EKG was preformed, order will be discontinued and PII will be discarded.

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.

IHS employees will only obtain PII if ordered by provider and patient consent.

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.

PII will only be access with pass code to protect patient privacy.

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.

Training will be held by contractor, train the trainer, and train employees who will be operating EKG.

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

Training will be held by contractor, train the trainer, and train employees who will be operating EKG.

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.

PHI/PII is stored temporarily on the machine based on system settings and managed in accordance with Records Retention Schedule Number DAA-GRS-2022-0009-0002, titled "Intermediary Records cites the Retention Period as follows: "Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later."

The electronic or paper report is transmitted to Electronic Health Record where the report becomes part of the patient's official medical record and managed in accordance with Records Retention Schedule Number DAA-0513-2014-0003, sequence 0003, titled "Health Records File. Electronic Health Record." cites the Retention Period as follows: "Destroy/delete 75 years after last episode of patient care or date of death."

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

Administrative Controls: All personnel who access IT systems 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.

Technical Controls: 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.

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured IHS 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.