US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2026

OPDIV:

IHS

Name:

Nurse Call System

PIA Unique Identifier:

P-3062590-278744

The subject of this PIA is which of the following?

General Support System (GSS)

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?

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 Nurse Call system serves as a critical communication link between patients and caregivers, enabling patients to quickly request assistance and supporting timely responses, patient safety, and staff efficiency. Commonly used in hospitals, nursing homes, and other healthcare settings, the system enhances care coordination, workflow management, and response tracking. At Northern Navajo Medical Center (NNMC), the system is a traditional configuration using call cords, push buttons, or pull cords connected to a central master station within each inpatient nursing unit. This setup provides a reliable and secure means for staff to respond to patient needs while optimizing workflow and reducing unnecessary steps.

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

The Nurse Call System operates independently and is not integrated with internal clinical systems such as Resource Patient Management System (RPMS)/Electronic Health Record (EHR) that maintain patient medical records. Patient information is entered manually at the time of admission for individuals placed in inpatient units and is removed upon discharge.The system collects and uses

limited personally identifiable information (PII) solely to support patient identification and safety, including:

Patient name
Chart number (medical record number)
Room/location information
Fall risk indicator (if applicable)

This information is used only to identify the origin of a call and to inform staff of any associated safety risks (e.g., fall risk).

In addition to PII, the system processes operational and non-PII data, including:

Call event data (e.g., time, type, priority)
Staff response and assignment information
System audit logs and operational records

All patient information is manually removed from the system upon discharge to ensure it is not retained beyond its operational need."

If the system collects information (i.e. user credentials) about system users/administrators in order to control access or for a similar purpose, please describe the information that is collected about those users/administrators.

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

he Nurse Call System is a critical communication tool that connects patients with caregivers, enabling timely assistance, enhancing patient safety, and improving staff efficiency and care coordination. At Northern Navajo Medical Center, the system operates as a traditional configuration using call cords, push buttons, or pull cords linked to a central master station within each inpatient nursing unit, supporting reliable response tracking and workflow management.

The system operates independently and is not integrated with clinical systems such as RPMS/EHR. It relies on manually entered, limited personally identifiable information (PII)—including patient name, chart number, room/location, and fall risk indicator—used solely to identify the origin of calls and support patient safety. In addition, the system processes operational data such as call event details, staff response information, and system audit logs. All patient information is manually removed upon discharge to ensure it is not retained beyond its operational need."

If the system collects information (i.e. user credentials) about system users/administrators in order to control access or for a similar purpose, please describe the information that is collected about those users/administrators.

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

Yes

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

Name
Medical Records Number
Patient room/location information/origination point
Call event data (time, type, priority)
Staff response and assignment information
System audit and operational logs

User credentials

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

Employees
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

he Nurse Call System is a critical communication tool that connects patients with caregivers, enabling timely assistance, enhancing patient safety, and improving staff efficiency and care coordination. At Northern Navajo Medical Center, the system operates as a traditional configuration using call cords, push buttons, or pull cords linked to a central master station within each inpatient nursing unit, supporting reliable response tracking and workflow management.

The system operates independently and is not integrated with clinical systems such as RPMS/EHR. It relies on manually entered, limited personally identifiable information (PII)—including patient name, chart number, room/location, and fall risk indicator—used solely to identify the origin of calls and support patient safety. In addition, the system processes operational data such as call event details, staff response information, and system audit logs. All patient information is manually removed upon discharge to ensure it is not retained beyond its operational need."

If the system collects information (i.e. user credentials) about system users/administrators in order to control access or for a similar purpose, please describe the information that is collected about those users/administrators.

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

Secondary use of Protected Health Information (PHI) refers to the use of patient health information for purposes other than direct patient care. While the primary use of PHI is to support diagnosis and treatment, secondary use supports healthcare operations, quality improvement, and regulatory oversight.Examples of secondary use include evaluating response times and care delivery, identifying trends in patient services, supporting staff training, conducting audits, and ensuring adherence to policies and procedures. PHI may also be used for reporting and compliance purposes, including meeting requirements under the Health Insurance Portability and Accountability Act (HIPAA). In certain cases, limited or de-identified PHI may be used for research or public health activities to improve healthcare outcomes.Secondary use is strictly controlled and limited to the minimum necessary information. Access is restricted to authorized personnel, and appropriate administrative, technical, and physical safeguards are implemented to protect patient privacy and prevent misuse.In summary, secondary use of PHI supports operational efficiency, compliance, and continuous improvement in healthcare delivery while maintaining strong privacy protections.

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

The NNMC Nurse Call System operates under the statutory authorities governing the provision of health services by the Indian Health Service, including the Snyder Act (25 U.S.C. § 13) and the Indian Health Care Improvement Act (25 U.S.C. § 1601 et seq.).The system maintains patient identifiers consistent with the Privacy Act of 1974 (5 U.S.C. § 552a) and the applicable IHS System of Records Notice (SORN) for patient medical records. Use and disclosure of information are permitted pursuant to published routine uses in the SORN and in accordance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164), which authorizes disclosures for treatment, payment, and

healthcare operations.The system is further governed by the Federal Information Security Modernization Act (FISMA), the E-Government Act of 2002 (PIA requirements), and applicable HHS and IHS privacy, security, and records management policies.

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 Number: 09-17-0001. Title: Indian Health Service Medical, Health, and Billing Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

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 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. A copy of the notice is given to the patient upon establishing a record or when requested. The staff member providing the notice has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed Acknowledgment of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record. The notices are displayed in the facility as well as on IHS website. IHS employees are notified at the time of hire that their Personally Identifiable Information (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.

Per the policy provided in the Indian Health Manual Part 2 Chapter 7 Section 22, "Under the HIPAA Privacy Rule, patients have the right to request restriction(s) of the use and/or disclosure of their PHI to carry out treatment; payment and health care operations; inpatient hospital directory; and disclosures to relatives, family members, personal representatives, close friends, health care givers, and any other person involved in the patient's care or payment who is identified by the patient. The IHS is not required to agree to the request. However, a patient still may object to the disclosure of information for the inpatient hospital directory and to relatives, friends, and others involved in patient care under 45 CFR 164.510(b). See Section 2-7.19, "Procedure for the Uses and Disclosures of Protected Health Information for Involvement in the Patient's Care and for Notification Purposes."

The initial collection of PII occurs at the various healthcare facilities at the point of registration and is required to determine eligibility for services. All patients at all facilities are provided with a Notice of Privacy Practices. They are also offered Form IHS-810, "Authorization for Use or Disclosure of

Protected Health Information". By completing and signing this document, patients may consent to or decline sharing of their protected health information with external entities outside the I/T/U ecosystem through the 4DH and eHealth Exchange.

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.

According to IHS policy all complaints regarding HIPAA Privacy and Privacy Act violations shall be addressed to the Chief Executive Officer or designee. Complaints must be documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Individuals may also file complaints directly to the Secretary, Department of Health and Human Services (HHS).

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

NNMC/IHS implements periodic administrative and technical reviews to ensure the integrity, availability, accuracy, and relevancy of PII maintained in the Nurse Call System. Patient identifiers (name and Medical Record Number) originate from the official medical record and are verified during the registration process.Periodic access reviews are conducted to ensure only authorized personnel and approved vendor staff retain system access. Audit logs, including remote vendor access logs, are maintained and reviewed to detect unauthorized activity.The vendor performs preventative maintenance and applies security updates in accordance with contractual and Business Associate Agreement requirements. Backup and recovery procedures are in place to ensure system availability.The system maintains only the minimum data elements necessary for treatment operations, and records are retained in accordance with applicable federal records management requirements.

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.

Access to PII in the NNMC Nurse Call System is determined based on role and documented need-to-know. Access requests require supervisory approval and system owner authorization prior to account provisioning. Users are assigned role-based permissions consistent with the least privilege principle and must complete required privacy and security training before access is granted.Vendor (Baxter) access is governed by contract and a HIPAA-compliant Business Associate Agreement and is limited to authorized personnel performing maintenance and operational support. Vendor remote access is authenticated, logged, and periodically reviewed. NNMC/IHS conducts periodic access reviews to ensure continued appropriateness of access and promptly removes access when no longer required.

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.

NNMC/IHS enforces the HIPAA minimum necessary standard through role-based access controls, supervisory approval of access requests, and assignment of permissions based on job function. The Nurse Call System maintains only limited patient identifiers (name and Medical Record Number), which inherently restricts the amount of PII accessible.Users are granted the least privilege necessary to perform their duties, and administrative access is restricted to designated personnel. Vendor (Baxter) access is limited to maintenance and troubleshooting functions under a HIPAA-compliant Business Associate Agreement. Access activity is logged and subject to periodic review to ensure compliance with minimum necessary requirements.

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.

All NNMC/IHS personnel with access to the Nurse Call System are required to complete annual Privacy Act and HIPAA training, as well as annual Information Security Awareness training. Training addresses responsibilities for safeguarding PII/PHI, applying the minimum necessary standard, and reporting suspected incidents.Personnel with elevated privileges receive additional role-based training appropriate to their responsibilities. Vendor (Baxter) personnel are required under contract and a HIPAA-compliant Business Associate Agreement to complete privacy and security training and comply with confidentiality requirements.Access to the system is contingent upon completion of required training and acknowledgment of Rules of Behavior.

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

All employees of IHS and direct contractors are required to complete HIPAA Privacy, HIPAA Security, Privacy Act Basics, and 42 CFR Part 2 training modules on an annual basis.

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.

The NNMC Nurse Call System maintains limited patient identifiers (name and Medical Record Number) solely for the duration of an active inpatient stay. PII is manually entered at admission and removed from the system upon patient discharge. The system is not the official medical record and does not retain patient data long term.

Records maintained within this system are managed in accordance with General Records Schedule (GRS) 5.2-010: Transitory Records. These records are temporary in nature and will be destroyed when no longer needed 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: 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.