US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/11/2026

OPDIV:

NIH

Name:

CRSS: Patient Call-Rauland Responder 5

PIA Unique Identifier:

P-3031997-109853

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)?

Yes

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The Clinical Center (CC) has been undergoing an Information Technology (IT) restructuring. This assessment incorporates the following systems and services under one system, Patient Call Services:
Responder
Enterprise Converge
Zebra Extension Manager
Zebra Provisioning Manager
Zebra Workcloud Push to Talk (PTT) Pro
Patient Call-Forward Thinking Locate+
Patient Call-Zebra
Navenio Intelligent Locator Service

Describe the purpose of the system.

Patient Call Services is a collection of computer software and hardware devices intended to facilitate efficient communication between patients and healthcare staff, streamline response times, and enhance patient care coordination in accordance with hospital safety and operational protocols. The Patient Call software integrates with hospital admission, discharge, and transfer (ADT) systems to display patient names and room numbers on staff terminals for quick identification during responses.

Hardware devices, which include staff stations and wireless phones, allow caregivers to receive and prioritize patient call alerts based on urgency or location. The system logs call data, including response times and call types, in a secure database to support clinical reporting and workflow analysis.

Except where noted, the software and devices are produced by Rauland Responder Systems. Patient Call Services includes:

Responder is a multi-faceted call system for Clinical Center (CC) patients. It can call clinical staff to their room for assistance, act as a television (TV) Remote, a bathroom emergency call, and facilitates patient-to-staff and staff-to-staff communications, and performs “Code Blue” calls in the event of cardiac arrest. Responder also allows for tracking certain medical devices that are mobile using Radio-frequency identification (RFID) tags to determine the location of the devices.

Enterprise Converge is a digital control center that integrates nurse call, real-time location, and workflow management into patient rooms, enhancing clinician communication and patient care efficiency. It offers comprehensive visibility of unit activities and streamlines processes through a mobile app-inspired interface.

Zebra Extension Manager simplifies the deployment and management of applications on Zebra mobile devices, ensuring seamless updates and configurations.

Zebra Provisioning Manager automates the configuration and deployment of Zebra devices, reducing setup time for healthcare information technology (IT) teams.

Zebra Workcloud PTT Pro Messaging provides secure, instant push-to-talk and multimedia messaging over Wi-Fi or cellular networks for healthcare staff. It supports location tracking and emergency alerts.

Patient Call-Zebra is a healthcare-specific, handheld Android based cellular phone with the cellular function disabled. It is only able to make calls over the NIH wireless network system. It supports patient call applications, enabling secure communication and real-time staff coordination.

Patient Call-Forward Thinking Locate+, developed by Forward Thinking Systems, provides real-time location tracking for healthcare staff and assets, optimizing patient care workflows. It integrates with nurse call systems to enhance response times and operational efficiency.

Navenio Intelligent Locator Service, developed by Navenio Limited, is a smartphone-based Real-Time Location Service (RTLS). It provides infrastructure-free indoor tracking for staff and assets in hospitals, optimizing task allocation and workflow. It integrates with systems like patient call to improve response times and operational efficiency, requiring minimal setup.

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

Patient Call Services collects patient information from the Admissions Travel and Voucher (ATV)

system, which maintains its own privacy impact assessment (PIA). Patient information includes name, medical record number (MRN), Visit Identification (ID), sex, race, ethnicity, attending and primary doctor, and CC room number.

Patient Call Services also collects NIH staff information, specifically, name and NIH Enterprise Directory (NED) ID. Clinical Center Nursing Department (CCND) staff log-in and assign themselves to a patient unit. This is used by Patient Call Services to contact staff when a patient identifies the need for assistance. Nurses also identify their NED ID badge for Forward Thinking, a subcomponent of Patient Call Services identified earlier, so as they go into a room it automatically turns off the alert.

Staff using Patient Call Services log in using the NIH Identity, Credential, and Access Management (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.

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

Patient Call Services is a collection of computer software and hardware devices intended to facilitate efficient communication between patients and healthcare staff, streamline response times, and enhance patient care coordination in accordance with hospital safety and operational protocols.

Hardware devices allow caregivers to receive and prioritize patient call alerts based on urgency or location. The system logs call data, including response times and call types, in a secure database to support clinical reporting and workflow analysis.

Patient Call Services includes:
Responder
Enterprise Converge
Zebra Extension Manager
Zebra Provisioning
Zebra Workcloud PTT Pro
Patient Call-Zebra
Patient Call-Forward Thinking Locate
Navenio Intelligent Locator Service

Patient Call Services collects patient information from the ATV system. Patient information includes name, MRN, Visit ID, sex, race, ethnicity, attending and primary doctor, and CC room number.

Patient Call Services also collects NIH staff information, specifically, name and NED ID. CCND staff log-in and assign themselves to a patient unit. Nurses also identify their NED ID badge for Forward Thinking.

Staff using Patient Call Services log in using the NIH IAM Services which maintains its own unique PIA on record, including all legal authorities documented.

NED, ATV and NIH IAM Services maintain their own unique PIA, with all legal authorities documented.

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
CC room number, Visit ID, sex, race, ethnicity
NED ID

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

Employees
Public Citizens
Patients

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The personally identifiable information (PII) is used primarily to identify the patient who request assistance or call and for patient care.

The primary purpose of the NIH staff PII is to identify the nurse assigned to care for the patient during the shift.

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

There are no secondary uses specified by the system owner.

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

42 U.S.C. §§ 241, 248, 282 and 284.

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.

09-25-0099; Clinical Research: Patient Medical Records, HHS/NIH/CC

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Government Sources
Within the OMB
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) 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.

Every patient must voluntarily execute a protocol consent and authorization prior to entry into an intramural research protocol and treatment at the Clinical Center. In addition, each patient is provided a formal notification of Information Practices at the Clinical Center and must certify that they have been so advised.

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.

General admission and protocol consent forms are signed by each patient. Additionally, an information practices notification form is reviewed and acknowledged in writing by each patient at the time of initial admission to the CC. Enrollment in a clinical research trial is voluntary and the collection of PII and medical notes is necessary to conduct research and provide clinical care. Therefore, a patient may not opt out of the collection or use of their PII while participating in research at the CC, only prior to participating in research at the CC.

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

All patients are notified of information practices upon admission. Each patient would be advised at the time of the next admission about major system changes and the CC Information Practices Notice would be revised and provided to each patient again.

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.

A Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The CC Department of Clinical Research Informatics (DCRI) Privacy Office will review the complaint and coordinate with the NIH Office of the Senior Official for Privacy (OSOP) to respond to the concern. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC DCRI Privacy Office.

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

Information, including PII, is reviewed when queries are performed, and data is provided to the clinical research team. Modifications to patient PII such as name, MRN, or Visit ID are sent from NIH Clinical Research Information System (CRIS) to the clinical information systems, including ATV and Patient Call Services, to keep the patient PII in synchronization across the ancillary clinical information systems. CRIS maintains its own PIA.

CC Nurses review their name and NED ID when assigning themselves to a unit. Any discrepancies would be reported to the system owner for investigation. Major discrepancies or errors in PII are entered in the CC Safety Tracking and Reporting System (STARS) for investigation.

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 is based on the user's role. Application administrators assign account permissions based on the user's role and current job 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.

Appropriate access is granted to the system based on predefined roles and job descriptions. Administrative access is limited to authorized NIH CC staff based on current roles. A NIH IAM Systems account is required to gain access to 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.

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

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

The CC Nursing Professional Development educators update staff when there are new features or modifications to the Responder system.

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 retained and disposed of under the authority of the NIH Intramural Records Retention Schedule.

Item 03-001: Clinical Care Services Records
These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Exclusions and exceptions are noted and cross referenced to their appropriate item numbers within this schedule.
Disposition: Cut off annually at end of fiscal year. Destroy 7 years after cutoff. DAA-0443-2019-0001-0001

Item 03-005: Patient Medical Records.
These records document admissions and medical treatment for a patient accepted in a research project.
Disposition: Cut off patient case file annually after 5 years of inactivity. Destroy when case file is no longer needed for scientific reference. DAA-0443-2012-0007-0010

Item 03-006: Medical Staff Credentialing Records
Medical Staff credentialing records documenting approval of physicians, dentists, and other health professionals for involvement in patient treatments or other patient contacts. These records document participation in patient care and include signed agreements to abide by Medical Staff bylaws, delineations of clinical privileges, and related records. Information is collected from individual

members of the Clinical Center Medical Staff and is used to document their credentialing and privileging.
Disposition: Cut off annually after medical staff member leaves patient care. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff. DAA-0443-2012-0007-0011

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

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

Technical Controls: IT hardware and software is segregated from public networks to prevent unauthorized or malicious access. Access to the system is controlled by NIH login which authenticates the user prior to granting access. 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.

Administrative Controls: All technical 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.