US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/03/2025

OPDIV:

NIH

Name:

iRhythm

PIA Unique Identifier:

P-5259657-176280

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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.

iRhythm's Zio unit is a heart rate monitor that provides continuous, uninterrupted recording for up to 14 days. When the study is complete, the patient ships the unit directly to iRhythm for data extraction. This data is analyzed by iRhythm and entered into an online reporting system known as Ziosuite. The clinician can then interpret and sign the report, which is sent to the NIH Clinical Center (CC) Clinical Research Information System (CRIS) to finalize the study.

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

Patients in a NIH clinical trial can be asked to use the heart rate monitor by their doctor or clinical trial lead. Patient data is entered into CRIS, as well as Ziosuite. Information collected for monitoring include Name, Sex, Date of Birth, Telephone Number, Patient Address, Device serial number, medical notes, medical record number and primary indication(Reason for exam) are collected during registration. Access to the system requires specific Username and Password. CRIS maintains its PIA.

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

iRhythm's Zio unit is a heart rate monitor that provides continuous, uninterrupted recording for up to 14 days. When the study is complete, the patient ships the unit directly to iRhythm for data extraction. This data is analyzed by iRhythm and entered into an online reporting system known as Ziosuite. The clinician can then interpret and sign the report, which is sent to the (CC) (CRIS) to finalize the study.

Patients in a NIH clinical trial can be asked to use the heart rate monitor by their doctor or clinical trial lead. Patient data is entered into CRIS, as well as Ziosuite. Information collected for monitoring include, Name, Sex, Date of Birth, Telephone Number, Patient Address, Device serial number, medical notes, medical record number and primary indication(Reason for exam) are collected during registration. Access to the system requires specific Username and Password.

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
Medical Notes
Device Identifiers
Sex
Primary Indication
UserName
Password

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

Employees
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The primary purpose is for identification of the patient.

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

Research

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

42 U.S.C. 241, 42 U.S.C. 290dd-2, 42 CFR part 2

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.

09-25-0200 Clinical, Basic and Population-based Research Studies of the National Institutes of

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the OPDIV

Non-Government 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?

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.

iRhythm has an Information Sharing Agreement (ISA) with the NIH Clinical Center.

Describe the procedures for accounting for disclosures.

Patients enrolled in NIH Clinical trial are advised at the time of enrollment. If a request for an accounting is received, Integrated Data Management System (IDMS) has audit logs which would allow the system owner to provide that information. Specifically, a log of reports generated for purposes of FDA compliance and NIH Intramural Research Program (IRP) study compliance is recorded in IDMS has context menu.

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

For clinical center patients: Every patient voluntarily signs a protocol consent and a general admission consent prior to enrollment 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.

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.

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 Clinical Center's Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC Privacy Officer.

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.

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 is based on role of person and the need to use or have access to the system. All requests for access go through the system administrator after being approved by division directors.

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.

Determinations are made according to role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of Personally Identifiable Information necessary to perform their job.

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).

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

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 following NIH Records Retention Schedules .

Item 03-005- Patient Medical Records
Description: These records document admissions and medical treatment for a patient accepted in a research project. These
records are the primary source of evaluation and analysis for either clinical care or clinical research study

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

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

Administrative control: Access is based on role of person and the need to use or have access to the system. All requests for access go through the system administrator after being approved by division directors.

Technical control: PII data is stored on an a cloud environment which cannot be accessed except for authorized users who have a valid user-name and password

Physical Control: The information technology (IT) hardware used to host protected information is located in a secured datacenter facility and not publicly accessible. 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.
Note: web address is a hyperlink.