US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/22/2025

OPDIV:

NIH

Name:

CRSS: ThinkAndor

PIA Unique Identifier:

P-1559761-037843

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.

This validation is intended to refresh content. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The ThinkAndOr is a third party application integrated with NIH Clinical Center (CC) systems to provide critical notifications to CC patients and staff. The primary purpose is to manage communications to patients enrolled in NIH intramural research protocols. ThinkAndOr allows the pushing of communication to both smart-phones and emails on a controlled basis. It is also used to support Telehealth visits between patient and provider.

The application receives patient contact information from the Clinical Research Information System (CRIS) which is stored and used to push communications to both patient smart-phones and email addresses. CRIS has its own approved privacy impact assessment (PIA) on record, with all legal

authorities documented.

The Clinical Center currently utilizes the following ThinkAndOr modules:
Remote Patient Monitoring, used for patient questionnaires
Secure Clinical Communications provides digital contactless screenings and triage with configurable emergency notifications to NIH staff, providers and patients. It also provides educational materials and notifications regarding appointment changes and CC operating hours.
Tele-Sitting allows staff to monitor a patient from a central location via an iPad placed in a patient's room.
Virtual Enterprise Waiting Room allows the creation of a virtual waiting room at which patients can check in. When the clinic is ready for the patient, staff can notify the patient to come in.
Virtual Health is used to configure virtual visits and allow staff videoconferencing.
Virtual Rounding allows for inpatient and outpatient medical rounds with the research team, clinical team, patient, patient family and identified staff.
Pexip Infinity Conferencing Platform, a cloud-hosted, virtualized and distributed multipoint conferencing platform. (It uses Microsoft Azure to provide video/audio components for the ThinkAndor application.)

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

ThinkAndOr collects patient information in order to push notifications to their phone or email address. Patient information includes, name, email address, date of birth (DOB), mailing address, medical records number (MRN), appointment information and patient age and sex. Admission, discharge and transfer messages from CRIS are also captured. Patients do not access the system.

ThinkAndOr collects staff information in order to push notifications and schedule telehealth visits on their calendars. Staff information includes name, role and email address for adding information to their calendar.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (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.

The ThinkAndOr is a third-party application integrated with NIH CC systems to provide critical notifications to CC patients and staff. The primary purpose is to manage communications to patients enrolled in NIH intramural research protocols. ThinkAndOr allows the pushing of communication to both smart-phones and emails on a controlled basis. It is also used to support Telehealth visits between patient and provider.

The application receives patient contact information from CRIS which is stored and used to push communications to both patient smart-phones and email addresses. CRIS has its own approved PIA on record, with all legal authorities documented.

The Clinical Center currently utilizes the following ThinkAndOr modules:
Remote Patient Monitoring
Secure Clinical Communications
Tele-Sitting

Virtual Enterprise Waiting Room
Virtual Health
Virtual Rounding
Pexip Infinity Conferencing Platform

Patient information includes, name, email address, DOB, mailing address, MRN, appointment information and patient age and sex. Admission, discharge and transfer messages from CRIS are also captured. Patients do not access the system.

ThinkAndOr collects staff information in order to push notifications and schedule telehealth visits on their calendars. Staff information includes name, role and email address for adding information to their calendar.

Users log in to this system using the NIH IAM Services which maintains its own unique PIA on record, including 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.

Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Admission, discharge and transfer (ADT) messages
Age, sex and appointment information

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?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of personally identifiable information (PII) is for clinical care.

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

A secondary purpose of PII is for research.

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

The legal authority to operate and maintain this Privacy Act records system is 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,

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

Pub. L. 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 sign a protocol consent and authorization for the collection of PII prior to enrolling in 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 acknowledge 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.

In 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 informed consent documents are 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.

ThinkAndOr does allow patients to opt-out from participation. Patients who do not provide contact information will not be enrolled to receive automated notifications. Once enrolled, patients can reply "STOP" to the text sent to their smartphone if they no longer want to receive messages.

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 and acknowledge the notification in writing. 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.

Modifications to patient PII such as name, MRN, and contact information are sent from CRIS to the ThinkAndOr system to keep the patient PII in synch across the clinical information systems.

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.

Determinations are made based on 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 PII necessary to perform their job.

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.

Access to PII is assigned to personnel based upon current job responsibilities. An IAM account login 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 and privacy awareness training. Training is completed on the http: //irtsectraining.nih.gov site with valid NIH credentials.

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

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

Health Information Management Department (HIMD) system owner and managers will be trained by the vendor initially to configure the system to send messages as necessary.

In order to use the enhanced collaboration features for CC Telehealth virtual visits, the CC HIMD team will provide training through quick reference guides. The training will be reinforced by sending education via email to staff engaged in telehealth appointments.

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

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.