US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/14/2024

OPDIV:

NIH

Name:

CWA: Pharmacy Wait Time Tracker

PIA Unique Identifier:

P-5444619-765304

The subject of this PIA is which of the following?

Minor Application (child)

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 and update the security authorization date. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The Pharmacy Wait Time Tracker tracks when a NIH Clinical Center (CC) patient's prescription is ready. The tracker application's primary function is to circumvent a pharmacist having to call someone's actual name out to summon them to the window to pick up the prescription.

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

Only the patient's name is collected in order to process the prescription for pickup.

Pharmacists requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is 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 Pharmacy Wait Time Tracker tracks when a CC patient's prescription is ready. The tracker application's primary function is to circumvent a pharmacist having to call someone's actual name out to summon them to the window to pick up the prescription.

When patients come to the Pharmacy, there is a kiosk computer available to them to check in. The patient's name is entered into the computer and the computer dispenses a printed ticket with a number on it as well as the date and time the ticket was printed. The person entering the name could be the patient themselves, or a family member, or a clinician. (Verification of identity occurs when the prescription is picked up.)

The kiosk computer relays the patient's name that was entered to a pharmacist on duty, who fills any and all prescriptions for the patient. The pharmacist then indicates that the prescription is filled in the wait time tracker application, and the application shows the ticket number on a television (TV) monitor in the pharmacy lounge waiting room area. Only the patient's name is collected in order to process the prescription for pickup.

The person then takes their ticket to the pharmacy window. A pharmacy technician verbally asks the patient's name and date of birth to ensure the safety aspect of dispensing the right drug for the right person. Patient information is pulled from the Clinical Research Information System (CRIS), the source system for all patient data. CRIS maintains its own unique PIA on record, with all legal authorities documented. For certain controlled substances such as narcotics, more identifying information may be requested by the pharmacist.

After the prescription is picked up, an indication is made in the wait time tracker software and the data "expires" and is deleted. The next day, the ticket numbers that are dispensed start all over again at the number 1.

Pharmacists requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, 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

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

Public Citizens
Patients

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

For patients to track their prescription's readiness.

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

There are no secondary uses.

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?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

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.

Patients are notified verbally that information is needed from them in order to pick up their prescription(s). Every patient must voluntarily execute a protocol consent and authorization prior to entry onto an intramural research protocol and treatment at the Clinical Center (CC). 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 personally identifiable information (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.

N/A. The data expires and is deleted after pickup.

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.

No process exists. Any identifier (which may be a pseudonym if the patient wishes) that the patient enters is deleted when the prescription is picked up.

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

N/A. NIH may not access the PII.

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 awareness training. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). 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).

N/A

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 Records Retention Schedule.

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.

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 training and awareness classes and refreshers. Personnel accessing these systems use privileged and separate accounts for administrative access to systems.

Technical Controls: The IT hardware and software used to host information is segregated from default commodity public networks to prevent unauthorized or malicious 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.

Physical Controls: The IT hardware used to host 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.