US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/08/2024

OPDIV:

NIH

Name:

CIT Services and Application SPOK

PIA Unique Identifier:

P-9934042-514599

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

Spok provides the capability to disseminate information for use by doctors, nurses, and patients to stay in contact using secure, mobile communications. This includes an online paging service and an on-call management directory that is used by all NIH Institutes, Centers and Offices (ICOs). Spok also enables the NIH Call Center to dispatch assistance quickly when a time-sensitive response is required.

Spok is a set of products, managed by the NIH Center for Information Technology (CIT).

Spok is a brand name, not an acronym.

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

Spok supports the delivery of the following types of healthcare related data and information:
Health and medical status alerts, including Medical Record Number (MRN), Patient Name, Critical

Values
Health services planning - including MRN, Patient Name
Continuity of care and health services quality, including MRN, Patient Name, Patient demographics
Clinical information - including MRN, Patient Name, Patient Demographics, Diagnosis, Test Results, Exam Results, Progress Note information

The following employee information is pulled from NIH Business Intelligence System (NBIS) which maintains its own unique privacy impact assessment (PIA), with all legal authorities documented: First Name, Middle Name, Last Name, HHS identification (ID), Title, Telephone Number, Department, Building Name, Room Number, Mail Room, Fax Number, and NIH Username. The email address is collected if a staff member requests a Spok Mobile license.

The data is stored on a dedicated Microsoft Structured Query Language (SQL) Server . Information can be accessed using the 102pager.nih.gov website, the Spok Mobile application (app) and Medical Console app.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, with all legal authorities documented. The purpose of the IAM 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 collects unique user credentials and stores them in an encrypted format. The IAM 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.

Spok provides the capability to disseminate information for use by doctors, nurses, and patients to stay in contact using secure, mobile communications. This includes an online paging service and an on-call management directory that is used by all NIH ICOs. Spok also enables NIH call center to dispatch assistance quickly when a time-sensitive response is required.

Spok supports the delivery of the following types of healthcare related data and information:
Health and medical status alerts, including MRN, Patient Name, Critical Values
Health services planning - including MRN, Patient Name
Continuity of care and health services quality, including MRN, Patient Name, Patient demographics
Clinical information, including MRN, Patient Name, Patient Demographics, Diagnosis, Test Results, Exam Results, Progress Note information

The following employee information is pulled from NBIS which maintains its own unique PIA, with all legal authorities documented:
First Name, Middle Name, Last Name, HHS ID, Title, Telephone Number, Department, Building Name, Room Number, Mail Room, Fax Number, and NIH Username. The email address is collected if a staff member requests a Spok Mobile license.

The data is stored on a dedicated Microsoft SQL Server. Information can be accessed using the 102pager.nih.gov website, the Spok Mobile App and Medical Console application.

Those 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.

Spok is a set of products, managed by the NIH CIT.

Spok is a brand name, not an acronym.

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

Yes

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

Name
E-Mail Address
Phone Numbers
Medical Records Number
Medical Notes
Critical Values, Patient Demographics, Diagnosis, Test Results, Exam Results, Progress Notes
HHS ID, Title, Department, Building, Room number, Mail room, Fax number, NIH Username

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?

50,000-99,999

For what primary purpose is the PII used?

Contacting staff for patient care.

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

N/A

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

42 U.S.C. 241, 242, 248, 281, 282, 284, 285a, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285l, 285m, 285n, 285o, 285p, 285q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101.

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
Online
Government Sources
Within the OPDIV
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.

Patients are notified at the time of admission to the NIH CC that their personal information will be shared for clinical/research purposes.

Employees are notified at the time of onboarding that their information will be in NIH Enterprise Directory (NED). NED maintains its own PIA.

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 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 NIH.

Employees may not opt out as it's part of their work processes.

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 is advised at the time of the next admission about major system changes and the Patient 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.

Individuals may contact the NIH Senior Official for Privacy at Privacy@mail.nih.gov.

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

The NIH information technology (IT) Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected 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 awareness training. There are five categories of mandatory 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).

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 NIH 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 03-008 - Clinical Care Administrative Support Records
These administrative records are associated with support activities related to executing work functions unique to a clinical care environment. These files are non-clinical in nature and do not include information that is maintained in patient medical records. The records associated with this schedule item include the following support functions: Patient Support -- food services and patients' travel and transportation records; Oversight and Safety -- occurrence reports, safety program reports, quality assurance records, Food and Drug Administration (FDA) device reports, and FDA drug interaction reports; Nursing Administration -- daily nursing service reports, showing employee absence and tardiness, and personnel reassignment and utilization and nursing unit reports; Pre-admissions -- pre-admission files, relating to referrals, volunteer services records, volunteer payments, and files, reports and
correspondence concerning daily volunteer services operations; and Sponsoring Agency Files -- records relating to private organizations sponsoring clinical patient volunteers, copies of agreements, and related reports and correspondence.
Disposition: Destroy when 3 years old, but longer retention is authorized if needed for business use. DAA-0443-2018-0002-0001

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

Physical Controls: The 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 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.

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.