US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/28/2025

OPDIV:

AHRQ

Name:

Implementation and Testing of Diagnostic Safety Resources

PIA Unique Identifier:

P-5689672-006224

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.

Contractor

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.

The Implementation and Testing of Diagnostic Safety Resources system collects and stores survey results from individual-level surveys conducted by the RAND Survey Research Group (SRG).These data are securely stored in protected server directories and are utilized to support research on the implementation of diagnostic safety tools.

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

The site will collect information related to the evaluation of three tools to prevent diagnostic errors at outpatient clinics. The project will enlist clinic sites to participate in the evaluation. Each site will have several team members assisting in the evaluation, including a site lead to coordination the activities of the team and serve as the primary contact with the RAND team. This information related to each site and site staff will be collected:

Site demographic and location information, name of the Information on Tool selected, Site Lead name and contact information, Team Members name and contact information; Site characteristics (e.

g., type, profit status, urbanicity, CMS region) and contact information for site and site contacts; Additional site characteristics (e.g., size, patient mix) inventory of site abilities to implement tool, confirmation of tool to be implemented; Qualitative ratings on sustainability capacity of the clinical practice; Aggregate information on diagnostic safety events; Information on site safety culture, including use of diagnostic safety event data, activities to improve the quality of care, and the work environment; Clinicians' subjective reflections on their diagnostic performance for 3-5 cases, with additional metrics around time to complete the review and the number of cases reviewed; Information on practitioner type, years in practice, specialty, subspecialty, and percent of time spent in clinical practice;

This information will be collected from participating patients.
Patient-perceived experience and quality of communication, basic patient demographics (e.g., age, sex, education, race, ethnicity), name and contact information for patients who volunteer to be contacted for an interview; reason for visit, provider communication, and other insights into patient experience.
No patient PHI will be collected.

"User access is available only through the RAND VPN, which requires a PIN and two factor verification of identity. Access to the server requires a password and two factor authentication. "

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

The system is a virtual Windows server running on Hypervisor hardware located in the RAND data center. The virtual server is part of the RAND Survey Research Group subnetwork which is behind internal firewalls to partition it from the RAND Corporate Computing Environment. The information on the server is responses to surveys conducted by the Survey Research Group.

he data collected falls into three categories:
Site descriptive information – These are aggregate measures of the type of site and its organizational and work culture characteristics. These data contain no PII.
Site staff information – This includes contact information for participating site Team Members and clinicians. It also includes self evaluation by clinicians of chosen diagnosis events. There is not job performance information for any Team Members.
Patient information – Patient contact, name, and email address. Also patients' qualitative perception of their clinic experience.

User access is available only through the RAND VPN, which requires a PIN and two factor verification of identity. Access to the server requires a password and two factor authentication.

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
basic demographics (e.g., age, sex, education, race, ethnicity)
Name and contact information for patients who volunteer to be contacted for an interview
User Credentials

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

Public Citizens
Patients

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The PII is used to support research on the implementation of diagnostic safety tools. Individuals are asked about their perceived experience and quality of communication with medical professionals. No health data is collected, only individual opinions about the diagnosis process. The system also collects basic demographics (e.g., age, sex, education, race, ethnicity) as well as name and contact information for patients who volunteer to be contacted for an interview.

System administrators will have access to the system only for technical maintenance.

User access is available only through the RAND VPN, which requires a PIN and two factor verification of identity. Access to the server requires a password and two factor authentication.

User access is available only through the RAND VPN, which requires a PIN and two factor verification of identity. Access to the server requires a password and two factor authentication.

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.

RAND holds a Federalwide Assurance (FWA) for the Protection of Human Subjects (FWA00003425, effective until February 18, 2026). The FWA was granted by HHS under authority of 5 U.S.C. 301; 42 U.S.C. 289(a); 42 U.S.C. 300v-1(b). and serves as assurance of compliance with federal regulations 45 CFR 46.

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
Other
Government Sources
Other
Non-Government Sources
Public

Identify the OMB information collection approval number and expiration date

The OMB Control Number for “Implementation and Testing of Diagnostic Safety Resources” is 0935-0268 and the expiration date is 7/31/2027.

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.

The project provides a consent form to each survey participant. This form describes how the persons information will be used and how it will be protected. The project will not gather information if an individual elects not to participate in the survey.

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.

The consent process offers everyone the option to opt out of any data collection.

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

PII will only be obtained from individuals who give consent. The project will retain e-mail addresses to contact individuals in the event of a data breach. If a breach occurs everyone whose PII was collected will be contacted and informed of the type of personal information involved, the date of the breach, and a general description of the incident (if known at the time of the notification).

The project will not communicate changes to the system to any research participants.

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.

As part of the consent process individuals will be provided contact information for RAND where they express any concerns regarding their PII. Individual will also be notified that they can withdraw from the study for any reason and have their information removed from the system.

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 RAND Human Subject Protection Committee (HSPC, the RAND Institutional Review Board, IRB) conducts an annual review of the project to ensure that data safeguards are still in place. At the time the project will conduct a review of data holdings.

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.

SRG staff are allow access to the data only to collect the data and perform checks to evaluate the correctness and accuracy of the data. System level permissions, role based and least privileged are used to restrict access only to selected staff.

In the normal course of their duties, administrators would not access the data, except to diagnose and correct a technical issue affecting the integrity of the data. If project users report an issue with access to or integrity of the data, the on-duty administrator would be allowed access to the data.

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.

SRG staff require access to all data fields to evaluate the accuracy of the information.

System level permissions, role based and least privileged are used to restrict access to the folders where PII is held. Only individuals approved by SRG project management will be granted access to these folders.

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.

All RAND staff need to complete annual Information Security Awareness Training. Compliance is tracked so the accounts of non-compliant staff are disabled.

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

Project members with access to the data are required to agree to procedures described in the project Data Safeguarding Plan (DSP). In addition to annual Information Security Awareness Training, privileged users at RAND are also required to take “Privileged User Training” that upon completion requires signing a “Privileged User Agreement” document that acknowledges the user understands and accepts the responsibility of a privileged account.

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.

All projects using PII at RAND are subject to review by the RAND Institutional Review Board, the HSPC. Any project will PII is required to submit a Data Safeguarding Plan (DSP) that describes the processes and protections used to handle the data. A technical expert on the HSPC must review and approve the DSP. The DSP must include a description of the PII and the method and timing of destruction of the PII. A subcommittee of the HSPC will review the project annually until the PII are destroyed to confirm that data protections remain in place and require any updates to handling of the data based on changes in the technical environment.

According to the General Records Schedule (GRS), 3.1, General Technology Management Records (section 011). Records and should be destroyed 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

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

All hardware is physically located in the RAND Data center located in the Santa Monica. Access the the RAND campus requires a personal key card. Access to the physical servers is restricted only to system administrators, what have under background checks and who hold government clearances

Data on the server resides on Pure Storage devices and is encrypted at rest. Data are protected at the directory and file level by system permissions that restrict access to the file owner and an authorized group of users. System level permissions such as role base and least privileged is implemented to restrict access.

User access is available only through the RAND VPN, which requires a PIN and two factor verification of identity. Access to the server requires a password and two factor authentication.