US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/28/2025

OPDIV:

NIH

Name:

NICHD General Support System

PIA Unique Identifier:

P-1681432-697426

The subject of this PIA is which of the following?

General Support System (GSS)

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?

Existing

Does the system have Security Authorization (SA)?

No

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 system supplies core infrastructure and networking services but does not house or maintain any minor applications.

Describe the purpose of the system.

The National Institute of Child and Human Development (NICHD) General Support System (GSS) is an interconnected set of information resources managed under the same authority, designed to provide essential information technology (IT) infrastructure and services to NICHD. The NICHD GSS includes hardware, software, and networks that work together to ensure seamless communication, security and operational efficiency. It serves as the backbone for various applications and services, enabling organizations to maintain compliance, protect sensitive information and optimize workflow. The NICHD GSS also contains employee personally identifiable information (PII) data. Additionally, Clinical Trials Database (CTDB), a system component that resides in the GSS, contains patient PII and sensitive PII (SPII) such as medical data.

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

The NICHD GSS collects, maintains (stores), and shares information specific to operation and management and provides a networked infrastructure, associated components, and software for NICHD sites, major applications and minor applications. Number of servers, server capacity, and connection types between servers, are of information that is collected and stored for asset inventory. NICHD-specific data is stored on Isilon Network Attached Storage (NAS), which contains PII and SPII data. The NICHD GSS also contains employee PII data, such as Human Resources information related to employee status, education records, financial account information, leave time, reasonable accommodations, health records, and leave time. Currently CTDB has 400 active protocols collect various medical information from mothers and children, with each protocol collecting different information out of a question bank of approximately 300,000 questions with a different set of processes and procedures. The patient PII and SPII is not de-identified, however it is encrypted at rest and in transit.

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

There are several elements of PII and SPII stored on the NICHD GSS. NICHD staff, both federal and contractor's data is stored on the Isilon network share and databases. Sensitive information related to the network infrastructure, including, routers, firewalls, and Intrusion Detection and Prevention Systems (IDS/IPS) is stored on NICHD GSS components.

Additionally, information related to secure communication channels for internal collaboration and public-facing services is contained on the system. NICHD-specific data is stored on Isilon Network Attached Storage (NAS), which contains PII and SPII data. The NICHD GSS also contains employee PII data, such as Human Resources related information related to employee status, education records, financial account information, leave time, reasonable accommodations and health records. Additional PII residing on the NICHD GSS are users' names, Social Security Numbers, email addresses, phone numbers, medical notes, device and vehicle identifiers.

Currently 400 active protocols collect various medical information from mothers and children. Each protocol varies but retains information according to Institutional Review Board (IRB) requirements. PII and SPII, and sensitive elements stored in the CTDB include patient medical data, such as organ transplant information, mother and child date of birth (DoB), address, research data and institutional records.

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

Yes

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

Social Security Number
Date of Birth
Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Education Records
Device Identifiers
Employment Status
health records
leave time
reasonable accommodation

organ transplant information, research data and institutional records

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

Employees
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

NICHD GSS is utilized as a repository for employee medical data, financial data, HR-related information including SSN, and sensitive information system information. CTDB has Memorandum of Agreements (MOAs) with Service Level Agreements (SLAs) in place with 15 clinical institutes within NIH where a direct link is established to share the data to
Clinical Research Information System (CRIS) and Biomedical Translational Research Information System (BTRIS). Patient data is not deidentified, however is encrypted during
transit and at rest. There are no secondary uses for the data. Each will have a collaborator and associated hospital or lab site.

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

Not applicable (N/A)

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

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.

09-25-0200 Clinical,

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Government Sources
Within the DOC

Identify the OMB information collection approval number and expiration date

N/A

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.

For clinical applications, all participants in research sign an Informed Consent prior to any data collection. All consent is documented within Clinical Research Information System (CRIS). The consent date is documented within CTDB. The consent process is governed by the institute and NIH Institutional Review Board (IRB).

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.

Research participants opt-out by not consenting to the collection of PII.

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

If there was a system change on the NICHD GSS affecting personnel, the ISAO, in coordination with the Information System Security Officer (ISSO) would notify the manager of the individual, who in turn would notify the and obtain consent from the affected person(s). CTDB: Each of the 400 protocols have a different process with the Principal Inspector, Research Team for consent, opting out, disclosure, etc. in accordance with IRB requirements.

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.

If an individual believes their PII has been inappropriately obtained, used, or disclosed on the NICHD GSS, the user is briefed on the situation and provided two (2) years of free credit monitoring. CTDB patient information is re-reviewed on every visit to the facility (hospital or lab) to avoid this, however a manager and principal investigator (PI) would brief the affected individual and move forward according to their protocol and IRB requirements.

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

NICHD GSS has several security measures in place, such as encrypted drives, role-based access, intrusion detection system (IDS), antivirus (AV), endpoint protection, and data leakage protection (DLP). CTDB employs role-based access to patient data. CTDB patient information is not only encrypted at rest but also in transit using Allscripts into the CRIS and Biomedical Transactional Research Information System (BTRIS) repositories. Data is also re-reviewed on every visit or during every procedure. Allscripts helps providers make informed decisions, streamlines processes and automates clinical documentation.

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.

NICHD GSS: Access to PII is by default restricted and only users hired to specific job positions, after passing a background check and undergoing training, are granted access to PII. Account management begins with onboarding through NIH, and then depending on the role, permissions are granted to only applications and information as necessary. CTDB: Permission are approved through managerial and PIs depending on the protocol and information necessary to perform their job functions.

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 is granted based on least privilege and need to know. Access to all resources is role-based depending on job function.

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.

The NICHD inherits and disseminates the annual security and privacy training policies outlined by the NIH Office of the Director (OD), Office of the Chief Information Officer (OCIO),

Information Security and Awareness Office (ISAO), NIH Information Technology (IT) General Rules of Behavior. The NICHD disseminates these the security awareness and training policies, which includes PII training through an online course titled, "NIH Information Security Awareness, Insider Threats and Emergency Preparedness Course." The course is conducted on the NIH Information Security and Information Management Training Portal (https://irtsectraining.nih.gov/), with the completion date recorded for all personnel using the
system. The course must be completed by all NICHD employees, contractors, managers, and program managers (including those with associated awareness training roles and responsibilities) prior to receiving access to NICHD systems. A refresher course must be completed annually to maintain access to NICHD resources. In addition, personnel collecting and using clinical data and PII are required to complete a Clinical Center training regimen (i.e. Patient Confidentiality and Privacy) as well as training via Collaborative Institutional Training Initiative (CITI) (https://irbo.nih.gov/confluence/display/ohsrp/Required+CITI+Training), with annual updates as needed.

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

Administrators and developers are required to complete both Annual and role-based training. Privileged users are issued account administrator (AA) accounts following completion of all mandatory training and eligibility requirements. The following roles get AA accounts: System, Web and Database administrators, along with Application developers.

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.

The NICHD GSS adheres to National Archives and Records Administration (NARA)record retention schedules based on the type of information stored on the network. The CTDB Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1B "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B-361), item 3000-G-3, which allows records to be kept as long as they are useful in scientific research. Collaborative Perinatal Project records are retained in accordance with item 3000-G-4, which does not allow records to be destroyed. Refer to the NIH Manual Chapters for specific conditions on disposal or retention
instructions.

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

PII is secured through a layered approach that leverages administrative, technical, and physical controls.

Administratively, strict access policies are enforced through mandatory security training, regular audits, and role-based access restrictions to ensure that only authorized personnel handle sensitive data.

Technical controls include a collaborative effort between NICHD/NIH IT organizations ensures that PII is protected by access controls, encrypting data both at rest and in transit, and by documenting, monitoring, and implementing robust firewalls, network isolation, encrypted communications, and secure data storage. These technical measures also include least-privileged access controls, continuous environment
monitoring, intrusion detection, incident response procedures, and ongoing system maintenance to promptly resolve vulnerabilities.

The physical controls surrounding PII are fully inherited from the IT organizations that manages the physical data centers, Center for Information Technology (CIT). Servers reside in secure data

centers with restricted access.