# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

04/30/2025

### OPDIV:

NIH

### Name:

Biomedical Translational Research Information System

**PIA Unique Identifier:**

P-7241811-407414

**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.**

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.**

There have been no changes since the last assessment.

**Describe the purpose of the system.**

The Biomedical Translational Research Information System (BTRIS) is an NIH-wide enterprise clinical research system designed to support the NIH clinical research mission of the intramural program. BTRIS assists NIH researchers with many aspects of managing and reporting medical information through the research cycle.

On a daily basis, BTRIS processes and stores patient care and research data, forms and images on patients enrolled in intramural research protocols. This includes medications administered, laboratory tests, patient assessments by physicians, nurses, and other clinical care providers, and other medical information transferred from NIH clinical systems.

BTRIS is the repository for identifiers for data, text, forms and images from multiple NIH clinical care and research systems. This includes:
NIH Clinical Center (CC) clinical information systems at the CC.
Other Institute and Center (IC) information systems and individual laboratories and researchers at NIH on a voluntary basis.
Research compiled by intramural NIH researchers as consistent with NIH policies.

BTRIS production data covers a period from 1976 to the present and encompasses the retired CC Medical Information System (MIS), CRIS, CC data source clinical systems, and CC protocol management. Data are stored in perpetuity in the BTRIS database with the intention of being available to answer secondary research questions in the future. BTRIS has been established by the NIH to serve as the trans-intramural clinical research data repository so that respective Institutes and Centers (ICs) do not bear the long term responsibility and cost for the storage and maintenance of these data sets.

(Intramural research protocols are medical research protocols sponsored by the NIH Intramural Research Program, the NIH's internal research program. Clinical research refers to studies conducted in collaboration with human beings, undertaken to improve human health.)

As the repository for NIH, BTRIS takes data from contributing systems with the express mission of making this data available to users for primary and secondary research. These systems include:
National Cancer Institute (NCI): Cancer Central Clinical Database (C3D) and Labmatrix - research case report forms and biospecimens (human subject sample data);
National Institute on Alcohol Abuse and Alcoholism (NIAAA):
Clinical Research Database;
National Institute of Allergy and Infectious Diseases (NIAID): Cardiovascular Integrated Modelling and Simulation (CRIMSON);
Eunice Kennedy Shriver National Institute of Child Health and Human Development (NICHD):
Clinical Trial Database serving NICHD, National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK), National Institute on Minority Health and Health Disparities (NIMHD) and Clinical Center (CC);
Death data from the Centers for Medicare and Medicaid Services;
Protrak, a CC System for protocol information;
Genomic data sets from specific researchers in National Human Genome Research Institute (NHGRI), NIAAA, National Institute of Arthritis and Musculoskeletal and Skin Diseases (NIAMS) and the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK).

These systems maintain their own unique privacy impact assessment (PIA) with all legal authorities documented.

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

BTRIS collects, maintains and/or stores NIH clinical and research data including diagnostic, therapeutic, imaging, and research testing results. Specifically, information includes name, medical record number (MRN), mother's maiden name, e-mail address, phone numbers, medical notes, date of birth (DOB), mailing address, device identifiers, radiologic images, medical notes (chief complaint, allergies, medical orders), consents, clinical documentation, medications administered and services provided (examples include results of laboratory tests, imaging studies, blood product utilization, clinical documentation such as histories and physicals, signed consent forms, family information, social work encounters, medical & ethical consults, surgery, radiology images and related clinical interactions while a patient is at the CC.

How the data, text and images are presented to the system user depends on their user role and the BTRIS application through which they are accessing the data. Data stored as personally identifiable

information (PII) for presentation as a limited data set is redacted. Discrete data (such as labs) in comment fields and narrative text is redacted using a third party software package (Privacy Analytics) which is then reviewed by BTRIS staff serving as a NIH trusted broker prior to release to a user.

Authorized user credentials are entered by an administrator and stored in BTRIS. Information includes first name and last name, user identification (ID), role, NIH Enterprise Directory (NED) Identity Number, email address, phone number, Institute or Center (IC). This information resides in a table of user roles.

For access to identified subject data, users must be identified as members of the protocol research team. This research team is specified on the protocol, and BTRIS monitors the composition and access of protocol team members through an electronic interface. In addition, the principal investigator may grant access to students or other staff for ministerial functions such as protocol management on a protocol-by-protocol basis. Should a department or Institute wish for an individual to have access to a portfolio of protocols for ministerial functions, such access is granted with written approval of a department head or lab chief.

For access to limited data sets, users must be approved by their supervisor. For database to database access, two individuals per Institute are given permission by their respective Institute Clinical Director.

Staff roles include employees, fellows, students and contractors associated with the research group. All application access must be re-affirmed every sixty days with a log-in. Departing staff or staff that have moved to a new internal NIH group are managed through an electronic interface to the NIH Enterprise Directory (NED). Any role that has been changed or removed from NED is reflected in the BTRIS user tables. Departing users are removed from the user tables. If a user moves to a new NIH group, all roles must be re-established for access for both identified data and limited data sets.

A second instance (separate dedicated server) of REDCap exists in the demilitarized zone (DMZ) (a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks). No personally identifiable information (PII) is collected in this second instance. Users are provided a code that the Primary Investigator would match with answers.

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

BTRIS is an NIH-wide enterprise clinical research system designed to support the NIH clinical research mission of the intramural program.

BTRIS is the repository for identifiers for data, text, forms and images from multiple NIH clinical care and research systems. This includes:
NIH CC clinical information systems;
Other IC information systems, individual laboratories and researchers at NIH on a voluntary basis;
Research compiled by intramural NIH researchers as consistent with NIH policies.

BTRIS production data covers a period from 1976 to the present and encompasses the retired CC MIS, CRIS, CC data source clinical systems, and CC protocol management. Data are stored in perpetuity with the intention of being available to answer secondary research questions in the future. BTRIS has been established by the NIH to serve as the trans-intramural clinical research data repository so that respective ICs do not bear the long-term responsibility and cost for the storage and maintenance of these data sets.

As the repository for NIH, BTRIS takes data from contributing systems, making this data available for primary and secondary research. These include:
NCI: C3D and Labmatrix
NIAAA: Clinical Research Database
NIAID: CRIMSON
Clinical Trial Database serving NICHD, NIDDK, NIMHD and CC
Death data from the Centers for Medicare and Medicaid Services
Protrak,
Genomic data sets from specific researchers in NHGRI, NIAAA, NIAMS and NIDDK.
(These systems maintain their own unique PIA)

BTRIS collects, maintains and/or stores data including diagnostic, therapeutic, imaging, and research testing results. Specifically, information includes name, MRN, mother's maiden name, e-mail address, phone numbers, medical notes, DOB, mailing address, device identifiers, radiologic images, medical notes, consents, clinical documentation, medications administered and services provided (results of laboratory tests, imaging studies, blood product utilization, clinical documentation, signed consent forms, family information, social work encounters, medical & ethical consults, surgery, radiology images and related clinical interactions) while a patient is at the CC.

How the data, text and images are presented to the system user depends on their user role and the BTRIS application through which they are accessing the data. Data stored as personally identifiable information (PII) for presentation as a limited data set is redacted. Discrete data (such as labs) in comment fields and narrative text is redacted using a third party software package (Privacy Analytics) which is then reviewed by BTRIS staff serving as a NIH trusted broker prior to release to a user.

Authorized user credentials are entered by an administrator and stored in BTRIS. Information includes first name and last name, user ID, role, NED Identity Number, email address, phone number and IC. This information resides in a table of user roles.

For access to identified subject data, users must be identified as members of the protocol research team.

For access to limited data sets, users must be approved by their supervisor. For database to database access, two individuals per Institute are given permission by their respective Institute Clinical Director.

A second instance (separate dedicated server) of REDCap exists in the demilitarized zone (DMZ) (a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks). No personally identifiable information (PII) is collected in this second instance. Users are provided a code that the Primary Investigator would match with answers.

**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
Mother's Maiden Name
E-Mail Address
Mailing Address

Phone Numbers
Medical Records Number
Medical Notes
Device Identifiers
Medical orders, consents, User Credentials (first name and last name, user ID, role, NED ID, email address, phone number, IC). Clinical documentation, medications administered, and services provided (social work encounters, medical & ethical consults), surgery and radiology images. Physician names, protocol numbers and titles, unmodified procedure dates, lab results, clinical documentation and user ID, (IC, role, etc), NIH Enterprise Directory Identity Number
Patient family 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 is to support clinical research.

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

There is no secondary use of PII.

**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 Human Subjects Research 45 CFR Part 46; 42 U.S.C. §§ 241, 248, 282 and 284; E.O. 13478, Executive Order 9397 (8 Fed. Reg. 16,094 (Nov. 30, 1943)), as amended by, Executive Order 13478 (73 Fed. Reg. 70,239 (Nov 20, 2008))

**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.**

Government Sources
Within OpDiv
Non-Governmental Sources
Public
Private Sector

**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?**

Yes

**Identify with whom the PII is shared or disclosed and for what purpose.**

**Describe any agreements in place that authorizes the information sharing or disclosure.**

Neither an Information Sharing Agreement (ISA) nor a Memorandum of Understanding (MOU) is required at the CC level for this system.

A data use agreement must be completed for each session and BTRIS automatically sends each data use agreement to the Office of Human Subjects Research, thus recording the activities of each user during each session. Re-use of data is governed by NIH policies for data sharing and re-use.

**Describe the procedures for accounting for disclosures.**

BTRIS maintains a robust auditing system for access to data. For each user log-in there are specific access limitations based on the user role, so for example, only the NIH intramural principal investigator and their designees as per the protocol team may access identified data and run data queries for that active protocol. For data with redacted identifiers, only users with institutional permission may access limited data sets and BTRIS maintains audit logs of each log-in and every data query. Data downloads are also tracked by user and NIH institute affiliation. Employees and direct contractors who maintain the system also have access to data, and audit trails are maintained for various production and development environments. Therefore, should an individual wish to understand who has had access to their record(s), BTRIS would be capable of providing a full audit trail of access events.

**Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.**

BTRIS is a data warehouse that collects data various NIH system. Those systems maintain their own unique PIA and have processes in place to notify individuals that their personal information will be collected. General admission and protocol consent forms are signed by each patient and an information practices notification form is reviewed and acknowledged in writing by each patient at the time of initial admission to the CC.

BTRIS also collects some limited data on system users/administrators (NIH employees) that have been given access rights to the system. Each individual gives personal information upon hiring. Notice of information collection is given at the time of acceptance of employment at the NIH.

**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 collection of all data is voluntary. Every patient must voluntarily execute a protocol consent and data use authorization prior to entry onto 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 certify that they have been so advised.

If system users/administrators do not wish to provide their user credentials in order to gain system access, they will be unable to gain access to the system.

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

As BTRIS is a singular purpose-built data warehouse for medical research that receives data from other systems, major system changes would be communicated to the systems contributing data. There is no relationship between BTRIS and the individuals whose PII is in the system to provide notification of major system changes.

Current system users/administrators are given notice via e-mail when major system changes occur. Former users have been removed from the system.

**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.**

Although a Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed, individuals who are in BTRIS would not have any way of knowing that their PII has been inappropriately disclosed. The Clinical Center's Privacy Office would review a complaint and respond to a concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information System Security officer (ISSO) and CC Privacy Officer.

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

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. All BTRIS systems are audited electronically on a daily basis. System audits are reviewed manually on a weekly basis to ensure proper system functioning of servers, databases, filer servers and terminology coding. The weekly audit review ensures data/database integrity in the system as built. Data availability is monitored and reported on a daily basis to ensure all new data has been processed and loaded into the system and that all user-facing functions are operational.

Regarding data accuracy, BTRIS serves as a data repository and stores all data, text and images in their original format. If a transformation is necessary to enable usability, users are provided with these meta-data, (any transformations required from the original). Data accuracy is also evaluated via system testing. When new data or functionality is added to the system, the BTRIS testing team and/or automated testing scripts ensures that data are added to the database in the correct location without changes.

Data relevancy is addressed through the timely addition of new data on a nightly basis from constituent systems and working with users and stakeholders to ensure BTRIS continues to accrue data of use to the clinical research community.

**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.**

PII data in BTRIS will only be shared with authorized principal investigators for patients enrolled in their active protocols or others authorized by the appropriate Institutional Review Board (IRB) or

Office for Human Subjects Research Protections (OSHRP) such as associate investigators, IC Data Extractors and Administrative Users.

Researchers: access to PII is on a per protocol basis, with access rights determined by the protocol Principal Investigator. Administrative uses of data must be granted by institute leadership. Access to limited data sets is granted on a per researcher basis by Institute leadership.

A BTRIS user must be a member of the NIH intramural researcher community. The user must also have an active NED account (employee, fellow, student or direct contractor), and be a member of an active research team as detailed on the protocol application. Users may also be designated by their IC's leadership (IC Director, Scientific Director or Clinical Director) or their branch chief/department head to use BTRIS for limited data set queries or administrative/ministerial purposes (employee, fellow, student or contractor).

When a protocol is terminated, the investigator may transfer the subjects and their data to a data repository data re-use protocol which has been approved by an appropriate IRB, if they wish to have continued access to subject identifiers and identified data consistent with protocol provisions.

System administrators and database administrators are granted access to all BTRIS servers based on their need to manage the BTRIS infrastructure. Such access is granted on programmatic role and requires additional security training and an elevated security clearance. Special administrative accounts are established for access which are separate and distinct from e-mail and other daily office operation accounts.

Developers, business analysts and testers are given access to PII based on their job functions. These positions require additional security training and an elevated security clearance.

**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.**

Researchers are able to access data in identified form if they are associated with a specific protocol, and granted access by the Principal Investigator. When a protocol is terminated, identified data are no longer available to users. The Limited Data Set application allows researchers access to data from both active and terminated protocols. The custom application also automates the process of exemption from the Intramural Review Board (IRB), allowing the researcher to experience a seamless process of approval and executing a query.

A data use agreement must be completed for each session and BTRIS automatically sends each data use agreement to the Office of Human Subjects Research, thus recording the activities of each user during each session. Re-use of data is governed by NIH policies for data sharing and re-use.

**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. 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.

Users may request and receive individual or group training on how to use BTRIS.

**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.**

NIH Records Schedule 01-001, Records of Intramural Research Projects of Historical Significance
This records schedule is designed to cover all intramural research records, as such, all intramural research records must be evaluated and assigned to one of the following three schedule items, which are listed in order from longest to shortest retention period:
Item 0001 - Records of Intramural Research Projects of Historical Significance. All records originally identified for permanent retention shall be confirmed by the sponsoring IC as supporting a permanent retention value prior to accessioning to NARA.
Item 0002 - Research Records that Support Intellectual Property Rights.
Item 0003 - Records of All Other Intramural Research Projects. At the termination of the project or research program, the Institute or Center (IC) that sponsored the research shall assess the ongoing scientific research and intellectual property value of the project records.
Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference. Transfer to the National Archives in five year blocks when the newest records in the block are 15 years old. DAA-0443-2012-0007-0001

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

The BTRIS system and all data contained therein are protected using administrative, technical and physical security and privacy controls.

Physical: The system is behind locked doors and monitored by closed circuit television (TV). Access to the physical system is limited to authorized staff with Personal Identity Verification (PIV) access cards.

Technical: Only principal investigators or others authorized have access to PII in the application, while all others only have access to de-identified data. Application access is also restricted based on user roles and password authentication. Authentication with NIH PIV cards using SiteMinder will occur for remote application users. Neither the vendor or support staff use remote access.

Administrative: Controls include system security and contingency plan. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices, least privilege through role-based access, and policies for retention and destruction of PII.