BRICS Eletronic Signature Security Policy

Document Information

Document Owners: Matthew McAuliffe, Yang Fann, and Dominic Nathan

Organizations: NINDS DIR ITBP, CIT OIR ISL BIRSS, CNRM

Approval / Distribution Process

The SOP approval/distribution process is as follows:

1. The SOP author sends the SOP SharePoint link to their peers/subject matter experts (SMEs) for review.
2. After editing, the SOP author decides whether the SOP is ready for approval. If the SOP is ready, the author adds the SOP to the ITBP Manager meeting agenda.
3. At the ITBP Managers meeting or via email, NINDS Management formally approves/disapproves the SOP.
4. The SOP Author sends the SOP link to all people on the Distribution List.

NINDS Approval

This Security Policy (SP) is approved for distribution and implementation as of the Director ITBP approval date listed below. NINDS ITBP management is authorized to conduct periodic audits to ensure compliance with this procedure. Requests for corrections or changes to any part of this procedure must be submitted to the Document Owner to review. Exceptions to any procedure must be approved by the ITBP Management and documented.

Approved By:

Name	Title	Organization	Approval Date
Yang Fann	IT Director	NINDS DIR ITBP	03/28/19
Matthew McAuliffe	BIRSS Chief	CIT OIR ISL BIRSS	03/28/19
Dominic Nathan	Informatics Core Director	CNRM	03/28/19
Mark Edwards	IT Manager	NINDS DIR ITBP	03/28/19

Name	Title	Organization	Approval Date
Willy Calderon	ISSO	NINDS DIR ITBP	03/28/19

Peer Reviewers

This Security Policy was reviewed by the peers (i.e., subject matter experts) listed below. The plan will be reviewed by the peer reviewers at least annually.

Reviewed By:

Name	Title	Organization	Date
Tsega Gabremichael	Team Lead	CIT OIR ISL BIRSS	03/27/19
Leonie Misquitta	Sr Scientific Advisor	CIT OIR ISL BIRSS	03/27/19
Dominic Nathan	Informatics Core Director	CNRM	03/27/19

Distribution List

This Security Policy impacts the individuals on this Distribution List. The SP author should notify everyone on this list about changes to this SP *within one week* of NINDS approval.

Distributed To:

Name / Department / Group / Team
Yang Fann
Matthew McAuliffe
Dominic Nathan
Willy Calderon

1. Introduction

1.1 Overview

The purpose of this security policy defines the components and elements that make up the NINDS DIR ITBP's approved approach to electronic signature. The method of authentication used for digital signatures shall be consistent with the e-authentication risk assessment listed in OMB M-04-04 *E-authentication Guidance for Federal Agencies* and the respective technology safeguards applicable to that level of risk as per NIST SP 800-63 *Digital Identity Guidelines*. This security policy follows guidance contained in SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*. The intended audience for this procedure includes the groups/individuals listed below:

- NINDS DIR Users
- NINDS Clinical Informatics Development Team
- Business stakeholders and partners

NINDS has developed this SP to satisfy the NIST 800-53 security control requirements stated below:

- AC-2, Account Management
- AC-3, Access Enforcement
- AC-5, Separation Of Duties
- IA-5, Authenticator Management
- IA-4, Identifier Management

1.2 Purpose

This Security Policy describes the controls in place or planned for implementation and provides a level of security appropriateness for the information processed as of the date indicated in the approval page. The purpose of this Electronic Signaturey Policy is listed as follows:

- To document the approved set of written instructions for managing the electronic signature controls in the BRICS and its associated systems such as CiSTAR, CASA, and ProFoRMS at NINDS, CIT and CNRM.
- To establish a foundation for technical and human interaction policy and procedure decisions to guide legal and compliant electronic siguature processes.
- To improve siganature legibility, facilitate the use of electronic signatures for clinical records, validate information accuracy and completeness, verify the

identification and appropriateness of electronic record authors, and support nonrepudiation.

1.3 Scope

The IT Security Policy is a living document that will be updated periodically to incorporate new and/or modified secuiryt controls. This policy will be revised as the changes occur to the system, the data or the technical environment in which the the system operates. Electronic signature, attestation, and authorship are referred to in this document as E-Signature. Individuals authorized to affix an electronic signature to medical record documentation shall be limited to individuals with defined privileges to document in the medical record, such as investigators, physicians, clinicians, ancillary staff, and clinical researchers.

1.4 System Name

The Biomedical Research Informatics Computing System (BRICS) supports the collection of research studies and clinical trials, using a set of modular components that cover all stages of the clinical research life cycle. CiSTAR and CASA are built with a set of resuable and scalable BRICS components.

1.5 Security Categorization

The BRICS security design is compliant at the Federal Information Security Modernization Act (FISMA) Moderate level. Confidentiality of research subjects is maintained, but data and study protocols are shared to promote scientific collaboration. Appropriate controls and assurance requirements conform to the Federal Information Processing Standards (FIPS) 200 and NIST SP 800-53 Revision 3, and the Department of Health and Human Services policies for information systems.

The overall information system sensitivity categorization was evaluated against FIPS 199 and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* as shown below.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 1: FIPS 199 Categorization

Confidentiality	Moderate
Integrity	Moderate
Availability	Low
Overall Security categorization	Moderate

Should certain events occur that jeopardize the system and/or information it processes, the potential impact is categorized as Low, Moderate, or High.

Impact	Definition
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.)

The potential impact assigned to this system is indicated below:

Low	☒
Moderate	☐
High	☐

1.6 Roles and Responsibilities

The following personnel are primarily responsible for performing the procedures:

Name	Title	Responsibility
Avindra Nath	CiSTAR System Owner	Primary person for performing the steps in this SP

Name	Title	Responsibility
Clinical Trial Unit	NINDS DIR CTU	NINDS Governance committee for approvals
Steering Committee	Informatics Core	CNRM Governance committee for approvals
Yang Fann	BRICS Co-Director NINDS IT Director	Authorizing Official to operate Approve requirements
Matthew McAuliffe	BRICS Co-Director CIT BIRSS Chief	Authorizing Official to operate Approve requirements
Dominic Nathan	Informatics Core Director	Manage the project
Leonie Misquitta	Sr Scientific Advisor	Provide scientific consulting
Tsega Gebremichael	Sr Software Engineer	Provide technical guidance
Change Control Board	Subject Matter Experts	Manage and approve change requests and system enhancements
Business, Product owner, Instance Program Manager	Key Stakeholders	Review and validate requirements and work products
NINDS/CIT Clinical Informatics Development team	Software Engineer	Provide system development support

1.7 System Operational Status

BRICS/CiSTAR/CASA Clinical Trial Software are currently in the operational (production) phase in accordance with the system development life cycle (SDLC) as defined in the NIST SP 800-18.

1.8 Definitions

The following definitions may assist in understanding this SOP.

- Electronic signature – a generic, technology-neutral term for various ways that an electronic record can be signed, including a digitized image of a signature, a

name typed at the end of an email message by the sender, a secret code or PIN, or a digital signature.

- Biometrics – authenticated by physical characteristics prior to applying his or her signature.
- Click Through or Click Wrap – asked to click a button to demonstrate intent.
- Personal Identification Number (PIN) or Password – asked to enter identifying information.
- Attestation – the act of applying an electronic signature to the content, showing authorship and legal responsibility for a particular unit of information.
- Authentication – the security process of verifying a user's identity with the system that authorizes the individual to access the system. Authentication shows authorship and assigns responsibility for an act, event, opinion or diagnosis.

1.9 Key Words

The following key terms are used in this SP.

- BRICS – Biomedical Research Informatics Computing System
- CiSTAR – Clinical Informatics System for Trials and Research
- CASA – Collection Access Sharing Analytics Platform
- CCB – Change Control Board

2. Electronic Signature Procedures

The Standard Operating Procedure for BRICS and its associated systems such as CiSTAR, CASA, and ProFoRMS at NINDS, CIT and CNRM is as follows.

2.1 E-Signature Implementation

A properly executed electronic process signifying an approval of an entry or document content presented in electronic format may encompass a broad gamut of technologies and methodologies, ranging from an "I Agree" button to a handwritten digitized signature, to a digital signature cryptographically tied to a digital ID or certificate. NINDS DIR ITBP's electronic signature implementation is formally reviewed and approved by the CTU (Clinical Trial Unit) governance committee and CNRM Informatics Core Steering Committee as part of the overall system security plan review and approval process.

2.2 E-Signature Requirements

Funcional capability of ITBP's e-signature has been assessed against the following requirements of the business process to ensure reproducibility, defensibility and non-repudiation:

- Verification of content accuracy and completeness of each entry or document is made by the author prior to attestation.
- Accompanying signature phrases should be fitting to the type of documentation referenced on the screen visual and output hard-copy for user and legal identification, such as "Signed by", "Sealed by", "Approved by", "Verified by", "Confirmed by", etc.
- An e-signature event captures and displays the e-signature, author's full name, credentials, date, and time of application.
- Once an entry has been electrnically signed, the system prevents deletion or alteration of the entry and its related electronic signature for the life of the referenced documentation.
- The acceptable timeliness criteria related to an e-signature application should be addressed in the policy according to NINDS DIR ITBP's definition.
- Any necessary revisions (including amendments, corrections, deletions, retractions) to an electronically signed document must follow the organizational policy and procedure below:
    - ***Addendum:*** new documentation added to original entry. Addendums should be timely and bear the current date and reason for the additional information being added to the record.
    - ***Amendment:*** documentation meant to clarify clinical information within a medical record. An amendment is made after the original documentation has been completed. All amendments should be timely and bear the current date of documentation.
    - ***Correction:*** a change in the information that is meant to clarify inaccuracies after the original documentation has been signed or rendered complete.
    - ***Deletion:*** the act of eliminating information from previously closed documentation without substituting new information.
    - ***Late entry:*** delayed documentation. The entry pertains to the regular course of business for the subject it addresses but is recorded subsequent to the usual documentation timeliness. The delay often creates documentation outside of normal chronological order.

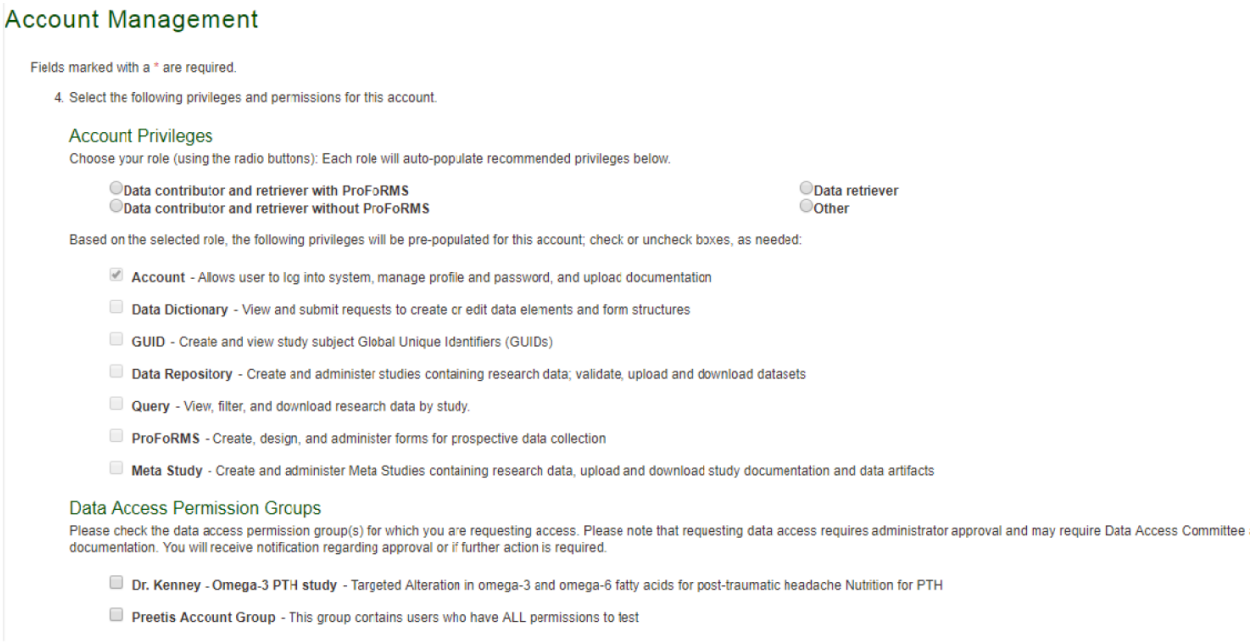
- ***Retraction:*** the act of correcting information that was inaccurate, invalid, or made in error and preventing its display or hiding the entry from further general view.

- Up-to-date policy and procedures are readily accessible by all e-signature users. Staff communication and training include timely updates of policy and procedural changes.
- Periodic software updates and upgrades include testing of design differences or changes impacting a valid, legal approach to e-signature. As technology and software improvements strengthen the e-signature process, policy, procedure, documents will be updated and staff training will be carried out as well.

2.3 Application Funtional Requirements

The implementation of BRICS functional requirements for E-Signature is not only holding the users accountable for their signing actions, but also detering record and signature falsification. Please see Appendix A for the agreement and certification of the E-Signature, which is legally binding equivalent of the signer's handwritten signature.

During the transition to the collection of E-Signature agreements digitally, the E-Signature agreement process will be executed manually using a paper form which after signing will be scanned and appended to the user profile and can be retrieved as needed from the system.



Digital signature place where error message gonna show

The {SYSTEM NAME HERE} use electronic documentation which may require you to provide an electronic signature when you enter, submit, change, access, download, or audit electronic data records.

ELECTRONIC SIGNATURE. This Acknowledgement and Certification of Understanding ("Acknowledgement") is to let you know that by submitting an electronic signature, you are providing an electronic mark that is held to the same standard as a legally binding equivalent of a handwritten signature provided by you. For purposes of the acknowledgement, a digital mark is considered your legally typed First and Last Name (legal name may include middle name, initial or suffix) followed by your password. A date will be recorded with both entries. Any part of the {SYSTEM NAME HERE} requiring an electronic signature may contain a signature acknowledgment statement provided in the same area requiring the electronic signature.

AGREEMENT: By signing this Acknowledgement, I agree that my electronic signature is the legally binding equivalent to my handwritten signature. Whenever I execute an electronic signature, it has the same validity and meaning as my handwritten signature. I will not, at any time in the future, repudiate the meaning of my electronic signature or claim that my electronic signature is not legally binding. I also understand that it is a violation for any individual to sign/e-sign any transactions that occur within {SYSTEM NAME HERE} on behalf of me. Any fraudulent activities related to electronic signatures must be immediately reported to the {SYSTEM NAME HERE} operations team. Violation of these terms could lead to disciplinary action, up to termination, and prosecution under applicable Federal laws.

CERTIFICATION OF UNDERSTANDING: I also understand, acknowledge, agree and certify that:
• I accept my responsibilities in the use of electronic signatures as described on this form.
• My execution of any form of an electronic signature function performed on {SYSTEM NAME HERE} to be the legally binding equivalent of my traditional handwritten signature, and that I am accountable and responsible for actions performed under such an electronic signature.
• I will not share components of my electronic signature such that my signature could be executed by another individual. Such components may include, but are not limited to, passwords.

First Name [ ] **Last Name** [ ] **Password** [ ] **Current Date** [ ]

5. When all entries are complete, click SUBMIT REQUEST.

The Approval Committee will review your request and notify you using the email address in your Contact Information above.
If you have any questions, contact FITBIR-apps@mail.nih.gov.

Submit Request

PRIVILEGE	STATUS	EXPIRATION DATE
Account	Active	No Expiration Date
Admin	Active	No Expiration Date
Data Dictionary	Active	19-Mar-2020
Data Repository	Active	19-Mar-2020
GUID	Active	19-Mar-2020
Meta Study	Active	19-Mar-2020
ProFoRMS	Active	19-Mar-2020
ProFoRMS Admin	Active	No Expiration Date
Query	Active	19-Mar-2020

Showing 1 to 9 of 9 entries First Previous 1 Next Last

Permission Group

Search:

PRIVILEGE	STATUS
BioFIND Sample Catalog	Active
PDBP Biosample Access	Active
PDBP Clinical Coordinators	Active
PDBP Consortium	Active
PDBP Genomics	Active

Showing 1 to 5 of 5 entries First Previous 1 Next Last

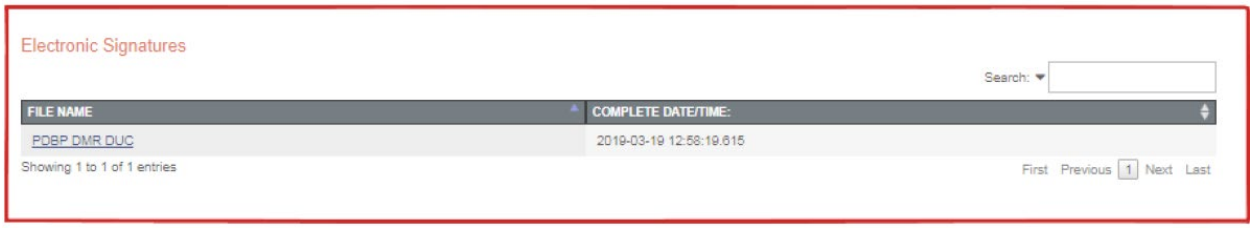
Existing Files

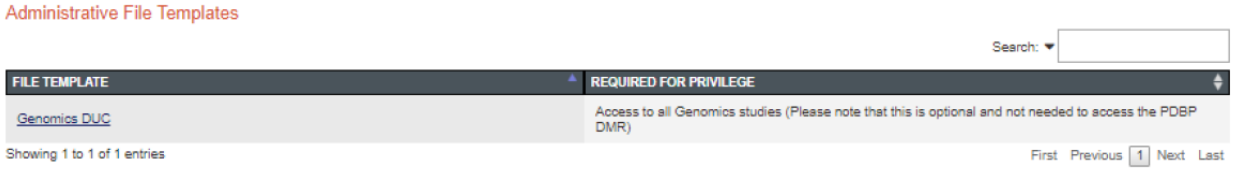
Add Download All

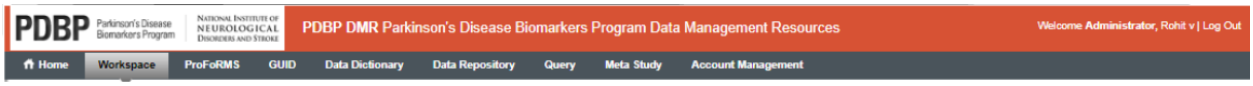
Search:

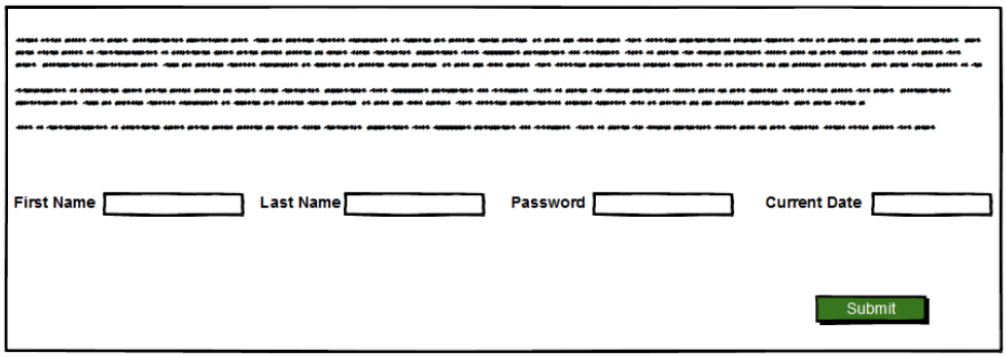
FILE NAME	FILE TYPE	DATE SUBMITTED
No data available in table		

Showing 0 to 0 of 0 entries First Previous Next Last

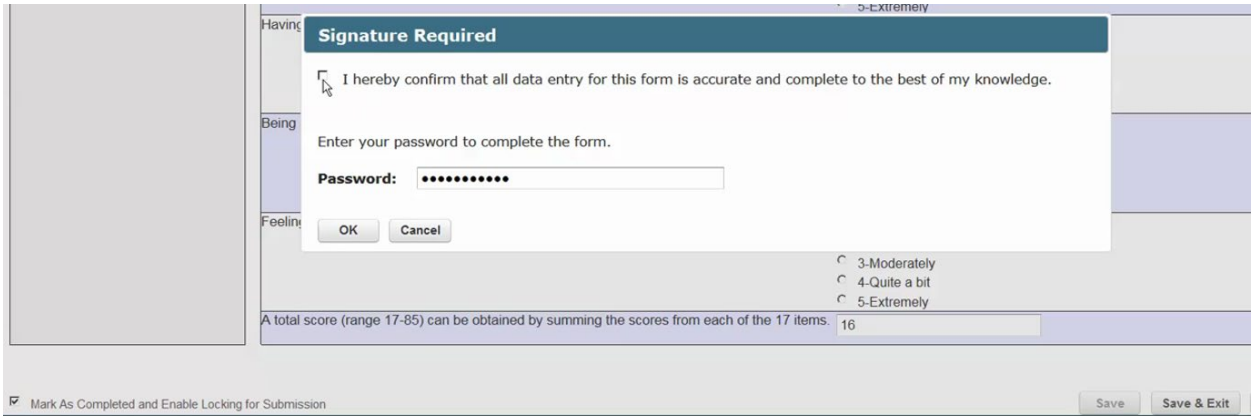

Electronic Signatures
Search:
FILE NAME
COMPLETE DATE/TIME:
PDBP DMR DUC
2019-03-19 12:58:19.615
Showing 1 to 1 of 1 entries
First Previous 1 Next Last


Administrative File Templates
Search:
FILE TEMPLATE
REQUIRED FOR PRIVILEGE
Genomics DUC
Access to all Genomics studies (Please note that this is optional and not needed to access the PDBP DMR)
Showing 1 to 1 of 1 entries
First Previous 1 Next Last


PDBP
Parkinson's Disease Biomarkers Program
National Institute of Neurological Disorders and Stroke
PDBP DMR Parkinson's Disease Biomarkers Program Data Management Resources
Welcome Administrator, Rohit v | Log Out
Home
Workspace
ProFoRMS
GUID
Data Dictionary
Data Repository
Query
Meta Study
Account Management


First Name
Last Name
Password
Current Date
Submit


EULA Agreement
Data Privacy
This system is a collaborative environment with privacy rules that pertain to the collection and display of imaging data. Before accessing and using this system, please ensure you familiarize yourself with our privacy rules available through the Data Access Request and supporting documentation.
Collection of this information is authorized under 42 U.S.C. 241, 242, 248, 281(a)(b)(1)(P) and 44 U.S.C. 3101. The primary use of this information is to facilitate medical research. This information may be disclosed to researchers for research purposes, and to system administrators for evaluation and data normalization.
Rules governing submission of this information are based on the data sharing rules defined in the Notice of Grant Award (NOGA). If you do not have a grant defining data sharing requirements, data submission is voluntary. Data entered into the system will be used solely for scientific and research purposes and is designed to further the understanding of the disease. Modification of information may be addressed by contacting your system administrator at CISTAR-ops@mail.nih.gov. Significant system update information may be posted on the site as required.
Accept
Decline



2.4 Approved E-Signature Types

There are a number of approaches to implementing the use of electronic signatures. The technology approach selected should support the minimum standards outlined in this policy. Examples of technology that support digital signatures that may work for various ITBP related projects. The approved and accepted functional types may include:

- Biometric – use of biological data such as fingerprints, handprints, retinal scans, and pen strokes to authenticate an individual.
- Public/Private or Asymmetric Cryptography (PKI) Digital Signature – using two cryptographic keys (one private and one public to encrypts and decrypts message) that authenticates the user, provides nonrepudiation, and ensures message integrity. It protects the signature by a type of “tamper-proof seal” that breaks if the message content was to be altered.
- Digitized signature – an electronic representation of a handwritten signature. The image of a handwritten signature may be created and saved using various methods.

3. System Environment

Hardware Component	O/S version	Database version	Software version	Supported modules	Location
Dell	Linux	Postgres	BRICS 3.6	CiSTAR/ CASA	Bldg 10 Room 1D41

NINDS ITBP uses a disciplined approach to provide ITSM support. This approach is based on the industry-standard ITIL model for the delivery of IT services. CiSTAR/CASA is a web-based application that written in J2EE with Postgres database and running on Linux with Apache. The application has been tested in current version of Chrome, IE, Firefox and Safari browsers for PC or Mac. It is integrated with NIH Login for Single sign-on (SSO) user federation behind the NIH firewall. VPN access is required for remote users.

4. Accessibility

Incident Response Team (IRT) scans and runs the web application security and section 508 report regularly. Please see section 2.8 in DIR Application Development Best Practices for details.

5. Privacy

NINDS ITBP uses Varonis for discovering sensitive content, finding where it is exposed, and locking it down without interrupting business. Please refer to Privacy Impact Assessment (PIA) for appropriate criteria questions and protection for privacy information. In addition, Appendix B provides a list of examples on PII.

6. Security

To produce secure code and minimize OWASP Top 10 critical risks is the most effective first step for web application security. NINDS automates the detection of vulnerabilities of web applications through some tools, such as IBM Rational AppScan and Tenable security center vulnerability scanner capable of providing a complete infrastructure map of the web applications. Please refer to DIR Vulnerability Scanning SOP for detailed policy and schedule for both server and software components.

NINDS Clinical Informatics Development team follows the DIR Application Development Best Practices. Data and documents are encrypted prior to storage in the database, database files are stored on encrypted volumes. To enforce information security policy, comprehensive testing and evaluation can be found in the NIH Security Authorization

Tool (NSAT) and NINDS DIR GSS System Security Plan with more thorough and complete security controls information.

7. Records Management

All data and/or records generated during this procedure are stored in the NINDS SharePoint-based Document Library.

8. Review/Revision History

Date	Author	Description of Change
03/15/2019	Gladys Wang	Document Creation
03/27/2019	Dominic Nathan	Added Appendix A

Appendix A. E-Signature Functional Requirements

One of the E-Signature features designed to meet the Part 11(2) regulation is displayed below for reference.

This system uses electronic documentation which may require you to provide an electronic signature when you enter, submit, change, access, download, or audit electronic data records.
ELECTRONIC SIGNATURE. This Acknowledgement and Certification of Understanding ("Acknowledgement") is to let you know that by submitting an electronic signature, you are providing an electronic mark that is held to the same standard as a legally binding equivalent of a handwritten signature provided by you. For purposes of the acknowledgement, a digital mark is considered your legally typed First and Last Name (legal name may include middle name, initial or suffix) followed by your password. A date will be recorded with both entries. Any part of this system requiring an electronic signature may contain a signature acknowledgment statement provided in the same area requiring the electronic signature.

AGREEMENT: By signing this Acknowledgement, I agree that my electronic signature is the legally binding equivalent to my handwritten signature. Whenever I execute an electronic signature, it has the same validity and meaning as my handwritten signature. I will not, at any time in the future, repudiate the meaning of my electronic signature or claim that my electronic signature is not legally binding. I also understand that it is a violation for any individual to sign/e-sign any transactions that occur within this system on behalf of me. Any fraudulent activities related to electronic signatures must be immediately reported to the system operations team. Violation of these terms could lead to disciplinary action, up to termination, and prosecution under applicable Federal laws.

CERTIFICATION OF UNDERSTANDING: I also understand, acknowledge, agree and certify that:
• I accept my responsibilities in the use of electronic signatures as described on this form.
• My execution of any form of an electronic signature function performed on this system to be the legally binding equivalent of my traditional handwritten signature, and that I am accountable and responsible for actions performed under such an electronic signature.
• I will not share components of my electronic signature such that my signature could be executed by another individual. Such components may include, but are not limited to, passwords.

E-Signature
Full Name:
Date:

Appendix B. PII

Personal Identifiable Information PII is "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history which can be used to distinguish or trace and individuals identity, such as thier name, SSN(full number and last 4 digits), date and place of birth, mothers maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual". Other examples of PII:

- Name for purposes other than contacting federal employers
- Photographic identifier
- Fingerprint/voiceprint
- Drivers license
- Vehicle identifier
- Personal mailing/phone/email address
- Medical record number
- Medical Notes
- Certificates, legal documents
- Device identifiers, web URL
- IP addressed(when collected with regard to a particular transaction)
- Military status
- Foreign activities
- Identifier that identifies, locates or contacts an individual
- Identifier that reveals activities, characteristics or details about a person
- Bank account numbers

Privacy Act System of Records (SOR)

A Privacy Act System of Records is a group of paper or electronic files that are retrieved by an individuals name, date of birth, SSN(full number and last 4 digits) or other personal identifier, and at least one other element of personal information that actually describes the individual in some way.

A name in and of itself does not constitute a SOR. A single document or a group of records that contains publicly available information is not a "record" under the Privacy Act.

Sensitive Information

Information is considered "sensitive" if the loss of confidentiality, integrity, or availability could be expected to have a serious, severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.