

NeuroNEXT Network

Standard Operating Procedure (SOP) System Security Measures and Website Access Version 4.0 SOP NN CS 704

Originators: NeuroNEXT CCC and DCC Personnel

Reviewed and Approved by

Signature and Date: <i>Christopher S. Coffey</i> <small>Electronically signed by: Christopher S. Coffey Reason: I approve this document Date: Feb 23, 2024 13:35 CST</small>	23-Feb-2024
Name and Title: Christopher S. Coffey, PhD (DCC Principal Investigator)	
Signature and Date: <i>Merit Cudkowicz</i> <small>Electronically signed by: Merit Cudkowicz Reason: I approve this document Date: Feb 22, 2024 17:16 CST</small>	22-Feb-2024
Name and Title: Merit E. Cudkowicz, MD MSc (CCC Principal Investigator)	
Signature and Date: <i>Marianne Chase</i> <small>Electronically signed by: Marianne Chase Reason: I approve this document Date: Feb 22, 2024 14:37 EST</small>	22-Feb-2024
Name and Title: Marianne Chase, BA (CCC Senior Director of Clinical Trials Operations)	


NN CS 704

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR
SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

Signature and Date:
Dixie Ecklund Electronically signed by: Dixie Ecklund
Reason: I approve this document
Date: Feb 23, 2024 17:12 CST
23-Feb-2024

Name and Title: Dixie J. Ecklund, RN MSN MBA (DCC Associate Director)

Signature and Date:
 Electronically signed by: Stacey Grabert
Reason: I approve this document
Date: Feb 22, 2024 15:18 EST
22-Feb-2024

Name and Title: Stacey Grabert, Pharm.D, MS, (CCC Director of Quality Assurance)

Signature and Date:
Joan Ohayon Electronically signed by: Joan Ohayon
Reason: I approve this document
Date: Mar 11, 2024 09:02 EDT
11-Mar-2024

Name and Title: Joan Ohayon, RN, MSN, CRNP, MSCN (NINDS, NeuroNEXT Program Official)

**NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR
SYSTEM SECURITY MEASURES AND WEBSITE ACCESS**

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

1. POLICY

The purpose of this SOP is to provide guidelines to the NeuroNEXT Data Coordinating Center (DCC) Information Technology (IT) Team regarding user access and system security measures used by the DCC to protect data systems from unauthorized access or unintended activity. Unintended activity may be categorized as authenticated misuse, malicious attacks, or inadvertent mistakes made by authorized individuals or processes. DCC servers are administered and protected in collaboration with the University of Iowa Information Technology Services (ITS) and the UI College of Public Health Office of Information Technology (UI CPH IT).

2. SCOPE

This SOP has been developed to be in alignment with federal regulations and Good Clinical Practices (GCP) as set forth in the 2016 Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2). The policies and procedures described in this SOP apply to the NeuroNEXT Clinical Coordinating Center (CCC) and DCC within the context of their oversight and advisory roles for the NeuroNEXT Network, and to all NeuroNEXT investigators, staff, subcontractors, or other entities associated with the NeuroNEXT Network who manage, oversee, and conduct research regulated by FDA and/or applicable review committees. This SOP is in alignment with Information Technology policies set forth by Information Technology Services at the University of Iowa and UI CPH IT.

3. ROLES AND RESPONSIBILITIES

These policies and procedures apply to NeuroNEXT DCC and CCC staff and any individuals who are granted access to DCC data systems or databases. This policy conforms to the Information Technology policies set forth by The University of Iowa College of Public Health and Information Technology Services. The NeuroNEXT DCC IT Team is responsible for adhering to the procedures outlined in this SOP, and for ensuring that these procedures are adhered to by individuals requesting data from the NeuroNEXT DCC.

4. APPLICABLE REGULATIONS AND GUIDELINES

21 CFR Part 11	Electronic Records; Electronic Signatures
46 CFR 46	Protection of Human Subjects
FDA	Guidance for Industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application (August 2003)
FDA	Guidance for Industry: Computerized Systems Used in Clinical Investigations (May 2007)
FDA	Guidance for Industry: Computerized Systems Used in Clinical Trials (April 1999)
FDA	Guidance for Industry: General Principles of Software Validation; Final Guidance for Industry and FDA Staff (January 2002)
FDA	Guidance for Industry: Electronic Source Data in Clinical Investigations (September 2013)
NIH	HIPAA Privacy Rule: Information for Researchers

5. REFERENCES TO OTHER APPLICABLE SOPS

NN PM 501	Communications
NN CS 701	System Setup/Installation

NN CS 704

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

NN CS 705	Data Back-up, Recovery, and Contingency Plans
NN CS 706	Retention and Protection of Electronic Records
NN DM 1005	Data Collection and Data Handling

6. ATTACHMENTS AND REFERENCES

NN CS 704 – A	Document History
---------------	------------------

National Institute of Standards and Technology (NIST) Guides:

NIST	Guide to Secure Web Services, Special Publication 800-95 (August 2007)
NIST	Guide to SSL VPNs, Special Publication 800-113 (July 2008)
NIST	Guidelines on Securing Public Web Servers, Special Publication 800-44 (Version 2) (September 2007)
NIST	Technical Guide to Information Security Testing and Assessment, Special Publication 800-115 (September 2008)
NIST	Information Security Handbook: A Guide for Managers, Special Publication 800-100 (October 2006)

7. TERMS AND ABBREVIATIONS

The following terms and abbreviations are used in this document:

CCC	Clinical Coordinating Center at Massachusetts General Hospital
CPH IT	Information Technology at the University of Iowa College of Public Health
CSS	Clinical Study Site
DCC	Data Coordinating Center at the University of Iowa
DM	Data Management Team
User ID	Unique user identification code for secure access to DCC computer systems
HIPAA	Health Insurance Portability and Accountability Act

8. SPECIFIC PROCEDURES

Database security refers to the systems, processes, and procedures that protect a database from unintended activity. The DCC utilizes multiple security measures to ensure the safety of its database systems, including physical security, electronic security, data restrictions, access rights, electronic signatures, and audit trails. Physical access to DCC servers and database hardware is restricted to authorized personnel only. Electronic security measures protect the database from unauthorized access and help to ensure the security of data during transfers to and from the DCC. Data access roles and rights are assigned to all DCC personnel and other authorized users to further control access to the information stored in DCC databases. An audit trail of all changes to DCC databases is also maintained to aid the investigation and tracking of any authorized or unauthorized activity that might occur.

**NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR
SYSTEM SECURITY MEASURES AND WEBSITE ACCESS**

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

Physical Security

All servers are protected from unauthorized physical access using biometric and/or electronically controlled door systems. Access is restricted to authorized personnel and trusted individuals representing the University of Iowa who require access. The electronic lock monitors and logs the access information of individuals who open the door to the server room. All keyboards are automatically locked out after 30 minutes of inactivity to help prevent unauthorized access to the data system through a computer workstation.

Electronic Security

For electronic security purposes, and in compliance with 21 CFR Part 11, access to all DCC computers and data systems requires a unique User ID and password. The system requires strong passwords (at least nine characters at least two of which must be numeric). Passwords must be changed at regular intervals, and at a minimum of every 6 months. Previously used passwords may not be reused. All passwords are encrypted at the DCC to prevent unauthorized usage. All data transferred over the Internet is encrypted using the Secure Sockets Layer (SSL) protocol.

This protocol allows an encrypted link to be established between the DCC web server and the remote computer. DCC systems have a firewall to protect from attacks via the Internet. All systems are protected in real time by University approved antivirus software and are swept daily. The web servers are monitored for any suspicious activity that would indicate an attempt to break into the system.

Protection of Human Subject Data

All data variables to be stored in DCC databases are reviewed to meet IRB and HIPAA requirements. If PHI is collected or stored at the DCC, it is stored as coded subject information.

User Access Roles and Rights

The DCC defines user access roles for each study that limit access to data and data system functionalities. Appropriate roles are assigned to the User ID of personnel who are authorized to perform certain data system or database functions, or who have certain rights to view or modify data in the database.

A website access request form is used to provide the DCC with initial contact information and descriptions of roles and responsibilities for personnel who will be performing study-related activities, and to document the process for requesting data access rights. This form is completed and signed by the user and is submitted to the DCC Data Manager or designee for review. The request is reviewed to ensure that the roles are appropriate, and access rights are then assigned based on the user roles. Depending on the roles assigned to a user, access may be restricted to one or more of the following rights: view only, add data, modify data, or delete data.

When specific data access rights are assigned to a User ID, the user is granted access to the data system and associated functionality as required for the position, and is notified that he/she is accountable for any actions performed under his/her User ID. As a security measure, applications designed at the DCC clearly display the user's name on each web page to indicate the identity of the current user.

Access rights are updated on an ongoing basis by the DCC to reflect personnel changes and training. If during the course of the study the contact information or roles for a user are changed, the CSS or CCC is responsible for contacting the DCC to update the information. User access rights are terminated for users who discontinue their association with a study.

**NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR
SYSTEM SECURITY MEASURES AND WEBSITE ACCESS**

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

Submitting Data to DCC Data Systems

DCC data systems log relevant information including, but not limited to, the system dates and times that records are created (initiated), dates and times that records are submitted, and the User ID of the person submitting the data. The submitting user is taking ownership that the information submitted on the eCRF is complete, valid, and correct.

Audit Trails

DCC electronic data capture systems maintain audit trails for changes to submitted data. All modifications made to a CRF record after submission to the DCC are tracked in the audit trail with the User ID of the person responsible for the change, the item (variable) that is changed, the date and time of the change, the previous value, the new value, and a comment describing why the change was made (when applicable/necessary). The audit trail cannot be modified by the user.

A. Overview

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC and/or UI CPH IT	Require that all authorized users at the DCC be assigned a unique User ID and password for access to DCC internal systems.		
2.	DCC and/or UI CPH IT	Assign system-type roles to the HawkID.		
3.	Users	Acknowledge the following: <ul style="list-style-type: none"> • User will protect his/her unique User ID and password from unauthorized use, and will not share the User ID or password with others. • User understands that his/her unique User ID and password will be used to identify him/her as being responsible for actions associated with the data that are accessed or submitted to the DCC using that User ID. 	21 CFR Part 11	
4.	DCC IT	When an electronic signature is used, require that the user acknowledge understanding of the requirements for electronic signatures: <ul style="list-style-type: none"> • Any electronic signature submitted under this User ID and password is intended to be the legally binding equivalent of a traditional handwritten signature. • The user will be accountable and responsible for any actions initiated the 	21 CFR Part 11	

NN CS 704

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

#	Who	Task	Attachment/ Reference	Related SOP
		electronic signature submitted under his/her User ID and password.		
5.	DCC IT	Require the use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, submit, modify, or delete electronic records.	21 CFR Part 11	
6.	DCC IT	Use authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	21 CFR Part 11	
7.	DCC IT, DM, Protocol Coordination	Ensure that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	21 CFR Part 11	

B. Physical Security

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT and UI CPH IT	Ensure physical security of all data system servers.	21 CFR Part 11	
2.	DCC IT and UI CPH IT	Server rooms are secured through the use of electronic and/or biometric access mechanisms. Limit access to server rooms only to authorized personnel.		
3.	DCC IT and UI CPH IT	Follow all security measures related to system setup and installation of new hardware.		NN CS 701

NN CS 704

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

C. Server Electronic Security

#	<i>Who</i>	<i>Task</i>	<i>Attachment/ Reference</i>	<i>Related SOP</i>
1.	DCC IT and/or CPH IT	Ensure that electronic security systems are in place to protect all data systems and databases.	21 CFR Part 11	
2.	DCC IT and/or UI CPH IT	Follow all security measures related to system setup and installation of new software and anti-virus protection.		NN CS 701
3.	DCC IT and/or UI CPH IT	Assign a unique User ID to each individual who requires access to DCC internal systems (including web, file and database servers).		
4.	DCC IT and/or UI CPH IT	Encrypt all passwords.		
5.	DCC IT and/or UI CPH IT	Establish and maintain system firewalls including Windows Server's Local Security Policy.		
6.	UI CPH IT	Install the currently supported antivirus software on all computers.		
7.	UI CPH IT	Set up automatic virus protection updates to scan new files for viruses in real time, and to scan all directories for viruses daily.		
8.	DCC IT or UI CPH IT	Remove all internal systems access for individuals who are no longer employed at The University of Iowa.		
9.	DCC IT and/or UI CPH IT	Require all web-based data collection to be encrypted via Secure Sockets Layer (SSL).		

D. Data Restrictions

#	<i>Who</i>	<i>Task</i>	<i>Attachment/ Reference</i>	<i>Related SOP</i>
1.	DCC IT	Ensure that data stored in DCC databases conform to HIPAA and IRB requirements for data collection, confidentiality, and storage.		

NN CS 704

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

E. File Access Restrictions

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT or UI CPH IT	Restrict the use of the file server to DCC personnel and authorized University of Iowa personnel. Additional material within the file server may be further restricted to specific users and/or groups.		

F. Study Website and Data System Roles and Access Rights

#	Who	Task	Attachment/ Reference	Related SOP
1.	Clinical Study Site (CSS) or CCC	Inform the DCC of new personnel who will be conducting study-related activities, and the roles that they will be serving on the study.		NN PM 501
2.	DCC	Generate and maintain a unique User ID for each new study team member.		
3.	DCC Data Manager, Lead Coordinator, or designee	Transmit the User ID and a website access request form to the new study team member.		NN PM 501
4.	Study Team Member	Complete and sign the website access request form, and return it to the DCC. <ul style="list-style-type: none"> By signing and returning the form, the user acknowledges that he/she will protect the User ID and password from access by others, and that the User ID and password will be used to identifying him/her as being responsible for data accessed or submitted to the DCC under that User ID. 		NN PM 501
5.	CSS Coordinator or Requester	Ensure that the study activities designated on the form are consistent with the roles of the requester on the study.		
6.	DCC Lead Coordinator	Review the form and the assigned study functions, and sign to acknowledge the review.		

NN CS 704

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

#	Who	Task	Attachment/ Reference	Related SOP
7.	DCC Lead Coordinator or designee	Maintain PDF versions of the signed forms on the internal shared drive.		
8.	DCC Lead Coordinator or designee	Send a default password, instructions for creating a personal password, the login process, and access information for any mandatory training modules to the new study team member.		NN PM 501
9.	Study Team Member	Create a personal password and complete any mandatory training modules within the assigned timeframe. Passwords are to be changed at regular intervals		
10.	DCC DM, Protocol Coordinator, or IT	Assign user access rights to the study website for each study team member according to the roles and responsibilities for the study.		
11.	CSS or CCC	If it is necessary to change contact information or user access rights, or to terminate access rights for study team personnel who are no longer affiliated with a study, inform the CCC and DCC as soon as possible after becoming aware of the need for a change.		NN PM 501

G. Audit Trail

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT	When an electronic record is initiated in the database, ensure that the system stores the date and time that the record was initiated.	21 CFR Part 11	
2.	DCC IT	After the initial submission of an electronic record, track all changes in an audit trail.		
3.	DCC IT	When an electronic record is submitted as finalized, capture in the system the User ID of the user who submitted the record, as well as the date and time the record was submitted.		

NN CS 704

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

#	Who	Task	Attachment/ Reference	Related SOP
4.	DCC IT	Whenever a finalized data record is changed (either through a post-complete change or through a data change request), ensure that they system stores the User ID of the person responsible for the change, the record and item that is changed, the date and time of the change, the previous recorded value(s), the new value(s), and a comment explaining why the change was made (when applicable/necessary).	21 CFR Part 11	NN DM 1005

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SECURITY MEASURES AND WEBSITE ACCESS

SOP: CS 704 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supersedes Document Version : 3.0 Effective Date : 08Apr2023
---	--	---

Attachment NN CS 704 - A. Document History

NeuroNEXT Network Standard Operating Procedure (SOP) System Security Measures and Website Access SOP NN CS 704					
Version	Description of Modification	Reason or Justification for Modification	Issue Date	Effective Date	Reviewer(s)
1.0	New	N/A	30Mar2012	29Apr2012	N/A
2.0	This SOP was extensively modified to align with SOP revisions at the DCC. The new version includes additional policies and procedures for user access rights and roles; revisions to the section on audit trails; an overview of user access and system security; and numerous minor revisions.	Updates for version 2.0	21Sep2016	21Oct2016	N/A
3.0	Updated "1996 ICH E6 Consolidated Guidance" to "2016 Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2)". Updated signature block to accommodate for electronic signatures. Additional minor updates throughout.	Updates for version 3.0	22Feb2023	08Apr2023	Catherine Gladden
4.0	Minor edits for clarity	Periodic review	01Mar2024	15Apr2024	Preeti Paul









NN CS 704 System Security Measures and Website Access v4.0 clean

Final Audit Report

2024-03-11

Created:	2024-02-22
By:	Tania Leeder (tleeder@mgb.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAynt8XTVQAJGP43Q2Gq6DWSqBRqRfbHhN
Number of Documents:	1
Document page count:	12
Number of supporting files:	0
Supporting files page count:	0

"NN CS 704 System Security Measures and Website Access v4.0 clean" History

-  Document created by Tania Leeder (tleeder@mgb.org)
2024-02-22 - 7:30:06 PM GMT
-  Document emailed to christopher-coffey@uiowa.edu for signature
2024-02-22 - 7:34:23 PM GMT
-  Document emailed to cudkowicz.merit@mgh.harvard.edu for signature
2024-02-22 - 7:34:24 PM GMT
-  Document emailed to Marianne Chase (mchase@mgh.harvard.edu) for signature
2024-02-22 - 7:34:24 PM GMT
-  Document emailed to dixie-ecklund@uiowa.edu for signature
2024-02-22 - 7:34:24 PM GMT
-  Document emailed to Stacey Grabert (SGrabert@mgh.harvard.edu) for signature
2024-02-22 - 7:34:24 PM GMT
-  Document emailed to ohayonj@ninds.nih.gov for signature
2024-02-22 - 7:34:24 PM GMT
-  Email viewed by ohayonj@ninds.nih.gov
2024-02-22 - 7:34:52 PM GMT

✓ Marianne Chase (mchase@mgh.harvard.edu) authenticated with Adobe Acrobat Sign.

Challenge: The user opened the agreement.

2024-02-22 - 7:35:48 PM GMT

📄 Document e-signed by Marianne Chase (mchase@mgh.harvard.edu)

Signing reason: I approve this document

Signature Date: 2024-02-22 - 7:37:32 PM GMT - Time Source: server

📧 Email viewed by christopher-coffey@uiowa.edu

2024-02-22 - 7:55:47 PM GMT

✓ Stacey Grabert (SGrabert@mgh.harvard.edu) authenticated with Adobe Acrobat Sign.

Challenge: The user opened the agreement.

2024-02-22 - 8:18:47 PM GMT

📄 Document e-signed by Stacey Grabert (SGrabert@mgh.harvard.edu)

Signing reason: I approve this document

Signature Date: 2024-02-22 - 8:18:58 PM GMT - Time Source: server

📧 Email viewed by cudkowicz.merit@mgh.harvard.edu

2024-02-22 - 11:15:38 PM GMT

✓ cudkowicz.merit@mgh.harvard.edu authenticated with Adobe Acrobat Sign.

Challenge: The user opened the agreement.

2024-02-22 - 11:16:05 PM GMT

📄 Signer cudkowicz.merit@mgh.harvard.edu entered name at signing as Merit Cudkowicz

2024-02-22 - 11:16:19 PM GMT

📄 Document e-signed by Merit Cudkowicz (cudkowicz.merit@mgh.harvard.edu)

Signing reason: I approve this document

Signature Date: 2024-02-22 - 11:16:21 PM GMT - Time Source: server

📧 Tania Leeder (tleeder@mgb.org) added alternate signer cscoffey@iowa.uiowa.edu. The original signer christopher-coffey@uiowa.edu can still sign.

2024-02-23 - 7:13:07 PM GMT

📧 Document emailed to cscoffey@iowa.uiowa.edu for signature

2024-02-23 - 7:13:07 PM GMT

📧 Tania Leeder (tleeder@mgb.org) added alternate signer ecklundd@uiowa.edu. The original signer dixie-ecklund@uiowa.edu can still sign.

2024-02-23 - 7:13:15 PM GMT

📧 Document emailed to ecklundd@uiowa.edu for signature

2024-02-23 - 7:13:15 PM GMT

 Email viewed by cscoffey@iowa.uiowa.edu

2024-02-23 - 7:34:42 PM GMT

 cscoffey@iowa.uiowa.edu authenticated with Adobe Acrobat Sign.

Challenge: The user opened the agreement.

2024-02-23 - 7:34:55 PM GMT


 Signer cscoffey@iowa.uiowa.edu entered name at signing as Christopher S. Coffey

2024-02-23 - 7:35:13 PM GMT

 Document e-signed by Christopher S. Coffey (cscoffey@iowa.uiowa.edu)

Signing reason: I approve this document

Signature Date: 2024-02-23 - 7:35:15 PM GMT - Time Source: server

 Email viewed by ecklundd@uiowa.edu

2024-02-23 - 11:11:41 PM GMT

 ecklundd@uiowa.edu authenticated with Adobe Acrobat Sign.

Challenge: The user opened the agreement.

2024-02-23 - 11:11:55 PM GMT


 Signer ecklundd@uiowa.edu entered name at signing as Dixie Ecklund

2024-02-23 - 11:12:13 PM GMT

 Document e-signed by Dixie Ecklund (ecklundd@uiowa.edu)

Signing reason: I approve this document

Signature Date: 2024-02-23 - 11:12:16 PM GMT - Time Source: server

 Email viewed by ohayonj@ninds.nih.gov

2024-03-11 - 1:01:25 PM GMT- IP address: 104.47.64.254


 ohayonj@ninds.nih.gov authenticated with Adobe Acrobat Sign.

Challenge: The user opened the agreement.

2024-03-11 - 1:01:45 PM GMT

 Signer ohayonj@ninds.nih.gov entered name at signing as Joan Ohayon

2024-03-11 - 1:02:09 PM GMT- IP address: 72.83.187.43

 Document e-signed by Joan Ohayon (ohayonj@ninds.nih.gov)

Signing reason: I approve this document

Signature Date: 2024-03-11 - 1:02:11 PM GMT - Time Source: server- IP address: 72.83.187.43

 Agreement completed.

2024-03-11 - 1:02:11 PM GMT