NeuroNEXT Network

Standard Operating Procedure (SOP)
Data Backup, Recovery, and Contingency Plans
Version 4.0
SOP NN CS 705

Originators: NeuroNEXT CCC and DCC Personnel

Reviewed and Approved by:

Signature and Date:	
Christopher S. Coffey Electronically signed by: Christopher S. Coffey Reason: I approve this document Date: Feb 23, 2024 13:36 CST	23-Feb-2024
Name and Title: Christopher S. Coffey, PhD (DCC Principal Investigator)	
Signature and Date: *Merit Cudkowicz* Electronically signed by: Merit Cudkowicz Reason: I approve this document Date: Feb 22, 2024 17:13 CST	22-Feb-2024
Name and Title: Merit E. Cudkowicz, MD MSc (CCC Principal Investigator)	
Signature and Date: *Marianne Chase* Electronically signed by: Marianne Chase Reason: I approve this document Date: Feb 22, 2024 14:38 EST	22-Feb-2024
Name and Title: Marianne Chase, BA (CCC Senior Director of Clinical Trials Operations)	

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR DATA BACKUP, RECOVERY, AND CONTINGENCY PLANS

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	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 17:13 CST*   23-Feb-2024
Name and Title: Dixie J. Ecklund, RN MSN MBA (DCC Associate Director)
Signature and Date: *[signature]* *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 09:03 EDT*   11-Mar-2024
Name and Title: Joan Ohayon, RN, MSN, CRNP, MSCN (NINDS, NeuroNEXT Program Official)

**NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR
DATA BACKUP, RECOVERY, AND CONTINGENCY PLANS**

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	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 and The University of Iowa College of Public Health Office of Information Technology (UI CPH IT) regarding data backup procedures, data recovery measures, and contingency plans in the event of short term server interruptions or extended periods of server failure. This policy is designed to protect the DCC from extended periods of server downtime and data loss resulting from system failures, natural disasters, or malicious attacks.

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 The University of Iowa Information Technology Services and UI CPH IT.

3. ROLES AND RESPONSIBILITIES

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 other DCC and University of Iowa staff members who perform data backup, recovery, and contingency procedures for NeuroNEXT projects.

4. APPLICABLE REGULATIONS AND GUIDELINES

21 CFR Part 11	Electronic Records; Electronic Signatures
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)

5. REFERENCES TO OTHER APPLICABLE SOPS

NN PM 501	Communications
NN CS 701	System Setup/Installation
NN CS 704	System Security Measures and Website Access

6. ATTACHMENTS AND REFERENCES

NN CS 705 – A	Document History

7. TERMS AND ABBREVIATIONS

The following terms and abbreviations are used in this document:

CCC	Clinical Coordinating Center at Massachusetts General Hospital

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR
DATA BACKUP, RECOVERY, AND CONTINGENCY PLANS

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	Supersedes Document Version : 3.0 Effective Date : 08Apr2023

CPH IT	College of Public Health Office of Information Technology
DCC	Data Coordinating Center at The University of Iowa
UI	The University of Iowa
Production	IT environment created for deployment of the final application

8. SPECIFIC PROCEDURES

Data Backup Procedures

. Production data are stored on CTSDMC servers that are managed and backed up by UI CPH IT. A complete backup of these data is performed at least once per week (typically on Friday night). A differential backup is performed on all other nights during the business week. Differential backups capture any changes that have been made to data files since the last backup. The backup system is checked daily to verify that the system is performing correctly. Any errors are reported to the DCC IT Lead for review and corrective action.

Data stored on a DCC SQL Server® are provided with an additional level of backup data security. All SQL Server® databases are scheduled for temporary backup several times during work hours. This backup creates a snapshot of the data in the case that a restore of data items or tables is required.

Data stored on individual workstations are not backed up by the automated system. The system also does not back up files that are installed from setup programs, such as system files and application program files. These files cannot be restored from a backup file, and require a reinstallation of the application.

Data Recovery Measures and Replication Servers

The DCC data backup and recovery system employs restore functions that can restore a complete file from a backup. The current file is restored to a temporary location until the file can be verified as the desired document. The file is then moved to the desired location.

The DCC strives to provide 24-hour-per-day/7-day-per-week coverage by maintaining replication servers that serve a data redundancy function for mission-critical web and database servers. The replication process allows data that are saved to the primary server to be simultaneously written to a secondary server. If a failure or service interruption occurs on the primary server, a rapid failover to the second server allows for application recovery and reduces the time that electronic data capture will not be available to DCC users. The DCC maintains the primary and secondary servers in separate data center locations to protect against extended power outages or natural disasters.

Server Updates, Maintenance and Contingency Plans

The CPH IT performs updates and maintenance for CTSDMC servers and is expected to inform the CTSDMC IT Lead or designee prior to any updates or maintenance (whether scheduled or unscheduled) that may affect server performance or function.

Contingency and communication plans for continuation of DCC IT services during short-term service interruptions and extended periods of server failure are described in Section D. These plans include methods for notifying users, identifying available alternative Information Technology resources within the University system, and transferring backup databases for immediate restoration.

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	Supersedes Document Version : 3.0 Effective Date : 08Apr2023

A. Data Backup

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT or UI CPH IT	Perform weekly full backups of all DCC data stored on file, web, and database servers.		
2.	DCC IT or UI CPH IT	Excepting the day that is scheduled for a full data backup, perform daily differential backups of DCC data stored on file, web, and database servers.		
3.	DCC IT or UI CPH IT	Retain monthly backups for file, web, and database servers for at least one year.		

B. Recovery

#	Who	Task	Attachment/ Reference	Related SOP
1.	Requester	To obtain a backed-up record from a file, web, or database server, submit a request to the DCC IT Lead, and include the following information: file name, the folder location, and the date that the requested record was last saved.		NN PM 501
2.	DCC IT Lead or designee	Evaluate the request. If the file cannot be located, transmit the information to CPH IT and request that the record be restored from the appropriate backup.		
3.	UI CPH IT	Restore the record from the backup to a temporary location, and inform the DCC IT Lead.		NN PM 501
4.	UI CPH IT	Transmit the record to the requester.		NN PM 501
5.	Requester	Verify that the desired record was restored, and move the record to the desired location.		
6.	DCC IT	Retain documentation of the request.		

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	Supersedes Document Version : 3.0 Effective Date : 08Apr2023

C. Sever Updates and Maintenance

	Who	*Task*	*Attachment*	*Related SOP*
1.	CPH IT	Provide a server maintenance plan to the CTSDMC and update as needed.		
2.	CPH IT	Inform the CTSDMC IT Lead or designee as soon as possible when an update to CTSDMC servers is scheduled to occur, and prior to any unscheduled server maintenance that may affect server performance.		
3.	CTSDMC IT Lead or designee	Check performance following server updates and maintenance and inform CPH IT immediately if performance issues or service interruptions are identified (refer also to Section 8.D below).		

D. Short-Term Service Interruptions and Communication Plan

	Who	*Task*	*Attachment*	*Related SOP*
1.	CPH IT	If a CTSDMC website or database server failure occurs, or another issue that affects CTSDMC server performance or function is identified, immediately inform the CTSDMC IT Lead or designee.		
2.	CTSDMC IT Lead or designee	Immediately inform CTSDMC Leadership, Protocol Coordinators, and other applicable personnel of the server issue and provide frequent updates on progress.		
3.	CPH IT and CTSDMC IT Lead or designee	Determine a plan of action, responsible parties, timeline for resolution of the issue, and an escalation plan (if needed).		
4.	CTSDMC IT Lead or designee and CTSDMC Leadership	Actively monitor the situation and inform CTSDMC Protocol Coordinators if it becomes necessary to contact clinical study sites and the CCC (if applicable) to notify them of the server downtime.		
5.	CTSDMC IT Lead or designee and CTSDMC	Continue to communicate with CPH IT during a server interruption until the issue is resolved and report the resolution and any corrective actions to CTSDMC Leadership.		

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	Supersedes Document Version : 3.0 Effective Date : 08Apr2023

	Who	*Task*	*Attachment*	*Related SOP*
	Leadership			
6.	CTSDMC IT Lead or designee and CTSDMC Leadership	Document the issue, resolution, and any corrective actions implemented to prevent future occurrences.		

E.   Replication Failover

	Who	*Task*	*Attachment/ Reference*	*Related SOP*
1.	DCC IT Lead	If an unexpected CTSDMC web or database server failure occurs, work with CPH IT to ensure that replication failover procedures are followed.		
2.	DCC IT	Determine the cause of the failover. Document all steps taken to fix the error and validate the steps used to ensure the problem is fixed.		
3.	DCC Executive Committee	Review the problem and resolution to ensure all issues were resolved.		

F.   Contingency Plans for a Total System Failure

	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT Lead and/or UI CPH IT	In the event of a total DCC system failure, collaborate to identify server hardware and disk space.		
2.	DCC IT and/or UI CPH IT	Retrieve the most recent backup files from the secure offsite storage location.		
3.	DCC IT and UI CPH IT	Restore file server: Designate and create a new file server for DCC Production and user data; restore DCC server data files to the new server; limit access to DCC directories to appropriate users within the DCC; modify the login script to redirect DCC users to the new server.		

**NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR
DATA BACKUP, RECOVERY, AND CONTINGENCY PLANS**

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	Supersedes Document Version : 3.0 Effective Date : 08Apr2023

	Who	Task	Attachment/ Reference	Related SOP
4.	DCC IT and UI CPH IT	Restore database: Designate and create a new database server for DCC Production and user data; install the new DCC Production instance of Microsoft SQL Server® on the new server; restore DCC database files to the new server location; confirm that database login and access is restored correctly; limit access to the DCC database to appropriate users within the DCC.		
5.	DCC IT and UI CPH IT	Restore web server: Designate and create a new web server for DCC Production and user data; restore DCC website applications to the new location on the server; limit access to DCC web server directories to appropriate users within the DCC; redirect database connection strings to the new instances created on SQL Server®; create SSL connections for web services; redirect public domain names for each study to the appropriate location.		
6.	DCC IT	Repair or replace appropriate servers and hardware as quickly as possible.		

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR DATA BACKUP, RECOVERY, AND CONTINGENCY PLANS

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	Supersedes Document Version : 3.0 Effective Date : 08Apr2023

Attachment NN CS 705 - A. Document History

NeuroNEXT Network Standard Operating Procedure (SOP)					
Data Backup, Recovery, and Contingency Plans					
SOP NN CS 705					
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	Updated to reflect increased involvement of The University of Iowa College of Public Health Office of Information Technology (UI CPH IT) in data backup, recovery, and contingency operations for the DCC. Incorporated recent modifications to DCC SOPs, including new specific procedures for data backup, recovery, and replication failover, and clarifications to the contingency plans section.	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	Updates for version 3.0	22Feb2023	08Apr2023	Catherine Gladden

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR DATA BACKUP, RECOVERY, AND CONTINGENCY PLANS

SOP: CS 705 Version No.: 4.0 Issue Date: 01Mar2024 Effective Date: 15Apr2024	Data Backup, Recovery, and Contingency Plans	Supersedes Document Version : 3.0 Effective Date : 08Apr2023

	electronic signatures. Added server updates and maintenance section. Added short-term service interruptions and communication plans section. Additional minor updates throughout.				
4.0	Minor edits for clarity	Periodic review	01Mar2024	15Apr2024	Preeti Paul

NN CS 705 Data Backup, Recovery, and Contingency Plans v4.0 clean

Final Audit Report   2024-03-11

Created:	2024-02-22
By:	Tania Leeder (tleeder@mgb.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAcza0rH4NNkkcyQeyLo9-7kmfk4gHY5Nl
Number of Documents:	1
Document page count:	10
Number of supporting files:	0
Supporting files page count:	0

"NN CS 705 Data Backup, Recovery, and Contingency Plans v4.0 clean" History

Document created by Tania Leeder (tleeder@mgb.org)
2024-02-22 - 7:35:11 PM GMT

Document emailed to christopher-coffey@uiowa.edu for signature
2024-02-22 - 7:37:16 PM GMT

Document emailed to cudkowicz.merit@mgh.harvard.edu for signature
2024-02-22 - 7:37:16 PM GMT

Document emailed to Marianne Chase (mchase@mgh.harvard.edu) for signature
2024-02-22 - 7:37:16 PM GMT

Document emailed to dixie-ecklund@uiowa.edu for signature
2024-02-22 - 7:37:16 PM GMT

Document emailed to Stacey Grabert (SGrabert@mgh.harvard.edu) for signature
2024-02-22 - 7:37:16 PM GMT

Document emailed to ohayonj@ninds.nih.gov for signature
2024-02-22 - 7:37:17 PM GMT

Email viewed by Marianne Chase (mchase@mgh.harvard.edu)
2024-02-22 - 7:37:57 PM GMT

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

Challenge: The user opened the agreement.

2024-02-22 - 7:38:15 PM GMT

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

Signing reason: I approve this document
Signature Date: 2024-02-22 - 7:38:30 PM GMT - Time Source: server

📑 Email viewed by christopher-coffey@uiowa.edu

2024-02-22 - 7:55:48 PM GMT

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

Challenge: The user opened the agreement.

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

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

Signing reason: I approve this document
Signature Date: 2024-02-22 - 8:18:28 PM GMT - Time Source: server

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

2024-02-22 - 11:12:26 PM GMT

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

Challenge: The user opened the agreement.

2024-02-22 - 11:13:19 PM GMT

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

2024-02-22 - 11:13:30 PM GMT

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

Signing reason: I approve this document
Signature Date: 2024-02-22 - 11:13:32 PM GMT - Time Source: server

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

2024-02-23 - 7:12:34 PM GMT

📧 Document emailed to ecklundd@uiowa.edu for signature

2024-02-23 - 7:12:34 PM GMT

🔁 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 - 7:12:45 PM GMT

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

2024-02-23 - 7:12:45 PM GMT

Email viewed by cscoffey@iowa.uiowa.edu

2024-02-23 - 7:35:27 PM GMT

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

Challenge: The user opened the agreement.

2024-02-23 - 7:35:41 PM GMT

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

2024-02-23 - 7:35:59 PM GMT

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

Signing reason: I approve this document
Signature Date: 2024-02-23 - 7:36:01 PM GMT - Time Source: server

Email viewed by ecklundd@uiowa.edu

2024-02-23 - 7:54:20 PM GMT

ecklundd@uiowa.edu authenticated with Adobe Acrobat Sign.

Challenge: The user opened the agreement.

2024-02-23 - 11:13:18 PM GMT

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

2024-02-23 - 11:13:34 PM GMT

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

Signing reason: I approve this document
Signature Date: 2024-02-23 - 11:13:37 PM GMT - Time Source: server

Email viewed by ohayonj@ninds.nih.gov

2024-03-11 - 1:02:31 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 - 1:02:54 PM GMT

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

2024-03-11 - 1:03:14 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 - 1:03:16 PM GMT - Time Source: server- IP address: 72.83.187.43

Agreement completed.

2024-03-11 - 1:03:16 PM GMT