










# NeuroNEXT Network

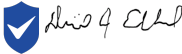
## Standard Operating Procedure (SOP) Data Backup, Recovery, and Contingency Plans Version 3.0 SOP NN CS 705

Originators: NeuroNEXT CCC and DCC Personnel

Reviewed and Approved by:

<b>Signature and Date:</b>  DocuSigned by Christopher Coffey  Christopher Coffey   I approve this document 16-Feb-2023   11:03:37 AM PST 16-Feb-2023  C68AC8DD80334CF982AED1200765F147
<b>Name and Title:</b> Christopher S. Coffey, PhD (DCC Principal Investigator)
<b>Signature and Date:</b>  DocuSigned by Merit Cudkowicz  Merit Cudkowicz   I approve this document 17-Feb-2023   9:33:52 AM EST 17-Feb-2023  9F8FE4180E504C6AB0A67B835E80C644
<b>Name and Title:</b> Merit E. Cudkowicz, MD MSc (CCC Principal Investigator)
<b>Signature and Date:</b>  DocuSigned by Marianne Chase  Marianne Chase   I approve this document 17-Feb-2023   1:40:47 PM EST 17-Feb-2023  58FE690F6BCA4F2390E3DA15BCE3F578
<b>Name and Title:</b> Marianne Chase, BA (CCC Senior Director of Clinical Trials Operations)

**Signature and Date:**

DocuSigned by DIXIE ECKLUND  
 | I approve this document  
17-Feb-2023 | 4:02:34 PM PST  
7006AF622EFC40B6A067A08EC02591B6

17-Feb-2023

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

**Signature and Date:**

DocuSigned by Stacey Grabert  
 | I approve this document  
22-Feb-2023 | 11:15:51 AM EST  
60CC52B0747A44E6B2208D8D880698C0

22-Feb-2023

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

**Signature and Date:**

DocuSigned by Joan Ohayon  
 | I approve this document  
21-Feb-2023 | 6:48:48 AM PST  
72C6AAFD8CC4485582ACA0700072901A

21-Feb-2023

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

## NN CS 705

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

### 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
CPH IT	College of Public Health Office of Information Technology
DCC	Data Coordinating Center at The University of Iowa
UI	The University of Iowa

## 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.

### 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.		

4.	DCC IT or UI CPH IT	Store web, file, and database backups offsite.		
----	------------------------	--	--	--

## 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.		

## C. Server 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**

	<i>Who</i>	<i>Task</i>	<i>Attachment</i>	<i>Related SOP</i>
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.		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.		
6.		Document the issue, resolution, and any corrective actions implemented to prevent future occurrences.		

**E. Replication Failover**

	<i>Who</i>	<i>Task</i>	<i>Attachment/Reference</i>	<i>Related SOP</i>
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

	<i>Who</i>	<i>Task</i>	<i>Attachment/Reference</i>	<i>Related SOP</i>
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	<p><b>Restore file server:</b></p> <ul style="list-style-type: none"> <li>Designate and create a new file server for DCC Production and user data;</li> <li>restore DCC server data files to the new server;</li> <li>limit access to DCC directories to appropriate users within the DCC;</li> <li>modify the login script to redirect DCC users to the new server.</li> </ul>		
4.	DCC IT and UI CPH IT	<p><b>Restore database:</b></p> <ul style="list-style-type: none"> <li>Designate and create a new database server for DCC Production and user data;</li> <li>install the new DCC Production instance of Microsoft SQL Server® on the new server;</li> <li>restore DCC database files to the new server location;</li> <li>confirm that database login and access is restored correctly;</li> <li>limit access to the DCC database to appropriate users within the DCC.</li> </ul>		
5.	DCC IT and UI CPH IT	<p><b>Restore web server:</b></p> <ul style="list-style-type: none"> <li>Designate and create a new web server for DCC Production and user data;</li> <li>restore DCC website applications to the new location on the server;</li> <li>limit access to DCC web server directories to appropriate users within the DCC;</li> <li>redirect database connection strings to the new instances created on SQL Server®;</li> <li>create SSL connections for web services;</li> <li>redirect public domain names for each study to the appropriate location.</li> </ul>		
6.	DCC IT	Repair or replace appropriate servers and hardware as quickly as possible.		

Certificate Of Completion

Envelope Id: 6D2AD6DC532248908AEDB02AB208A277 Status: Completed
Subject: Complete with DocuSign: NN CS 705 Data Backup, Recovery, and Contingency Plans v3.0.docx
Source Envelope:
Document Pages: 7 Signatures: 6 Envelope Originator:
Certificate Pages: 6 Initials: 0 Tania Leeder
AutoNav: Enabled TLEEDER@PARTNERS.ORG
Envelopeld Stamping: Disabled IP Address: 24.62.91.235
Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Record Tracking

Status: Original Holder: Tania Leeder Location: DocuSign
2/16/2023 8:54:55 AM TLEEDER@PARTNERS.ORG

Signer Events

Christopher Coffey Signature Timestamp
christopher-coffey@uiowa.edu Christopher Coffey Sent: 2/16/2023 9:14:58 AM
Security Level: Email, Account Authentication (Required), Login with SSO Viewed: 2/16/2023 2:03:27 PM
Signed: 2/16/2023 2:03:40 PM

Signature Adoption: Pre-selected Style
Signature ID:
C68AC8DD-8033-4CF9-82AE-D1200765F147
Using IP Address: 128.255.113.139

With Signing Authentication via DocuSign password
With Signing Reasons (on each tab):
I approve this document

Electronic Record and Signature Disclosure:
Accepted: 2/16/2023 2:03:27 PM
ID: dbb24f90-1904-434b-9040-3ec13db55221

DIXIE ECKLUND
dixie-ecklund@uiowa.edu
Security Level: Email, Account Authentication (Required), Login with SSO

DocuSigned by DIXIE ECKLUND
I approve this document
17-Feb-2023 | 4:02:34 PM PST
7006AF622EFC40B6A067A08EC02591B6

Sent: 2/16/2023 9:14:59 AM
Viewed: 2/17/2023 7:01:08 PM
Signed: 2/17/2023 7:02:36 PM

Signature Adoption: Drawn on Device
Signature ID:
7006AF62-2EFC-40B6-A067-A08EC02591B6
Using IP Address: 128.255.112.230

With Signing Authentication via DocuSign password
With Signing Reasons (on each tab):
I approve this document

Electronic Record and Signature Disclosure:
Accepted: 2/17/2023 7:01:08 PM
ID: 5ca72af7-54ab-4252-bc98-b4816e8936ee



Signer Events	Signature	Timestamp
---------------	-----------	-----------

Joan Ohayon  
ohayonj@ninds.nih.gov  
Security Level: Email, Account Authentication (Required)

*Joan Ohayon*

Sent: 2/16/2023 9:15:01 AM  
Resent: 2/21/2023 8:26:22 AM  
Viewed: 2/21/2023 9:48:35 AM  
Signed: 2/21/2023 9:48:54 AM

Signature Adoption: Pre-selected Style  
Signature ID:  
72C6AAFD-8CC4-4855-82AC-A0700072901A  
Using IP Address: 156.40.137.188

With Signing Authentication via DocuSign password  
With Signing Reasons (on each tab):  
I approve this document

**Electronic Record and Signature Disclosure:**  
Accepted: 2/13/2023 2:03:22 PM  
ID: 385a0a53-0f0c-4395-88f6-d5700c36e050

Marianne Chase  
MCHASE@mgh.harvard.edu  
Sr Director, Clinical Trial Operations  
Insight OBO The Massachusetts General Hospital  
Security Level: Email, Account Authentication (Required), Logged in

*Marianne Chase*

Sent: 2/16/2023 9:14:59 AM  
Viewed: 2/17/2023 1:40:26 PM  
Signed: 2/17/2023 1:40:51 PM

Signature Adoption: Pre-selected Style  
Signature ID:  
58FE690F-6BCA-4F23-90E3-DA15BCE3F578  
Using IP Address: 73.114.253.109

With Signing Authentication via DocuSign password  
With Signing Reasons (on each tab):  
I approve this document

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Merit Cudkowicz  
cudkowicz.merit@mgh.harvard.edu  
Chief of Neurology  
Security Level: Email, Account Authentication (Required), Logged in

DocuSigned by Merit Cudkowicz  
  
I approve this document  
17-Feb-2023 | 9:33:52 AM EST  
9F8FE4180E504C6AB0A67B835E80C644


Sent: 2/16/2023 9:14:59 AM  
Viewed: 2/17/2023 9:33:43 AM  
Signed: 2/17/2023 9:33:55 AM

Signature Adoption: Pre-selected Style  
Signature ID:  
9F8FE418-0E50-4C6A-B0A6-7B835E80C644  
Using IP Address: 68.239.56.73

With Signing Authentication via DocuSign password  
With Signing Reasons (on each tab):  
I approve this document

**Electronic Record and Signature Disclosure:**  
Accepted: 2/17/2023 9:33:43 AM  
ID: 5658beca-6509-438e-924b-976ac756db4e

Signer Events	Signature	Timestamp
---------------	-----------	-----------

Stacey Grabert sgrabert@mgh.harvard.edu Director QA Stacey Grabert Security Level: Email, Account Authentication (Required)	  Signature Adoption: Pre-selected Style Signature ID: 60CC52B0-747A-44E6-B220-8D8D880698C0 Using IP Address: 132.183.56.49  With Signing Authentication via DocuSign password With Signing Reasons (on each tab): I approve this document	Sent: 2/16/2023 9:15:00 AM Resent: 2/21/2023 8:26:23 AM Viewed: 2/22/2023 11:15:40 AM Signed: 2/22/2023 11:15:54 AM
---	--	--

**Electronic Record and Signature Disclosure:**  
 Accepted: 7/20/2020 8:50:14 AM  
 ID: 5ebadf74-e399-40fd-be82-9c7ca902061b

In Person Signer Events	Signature	Timestamp
-------------------------	-----------	-----------

Editor Delivery Events	Status	Timestamp
------------------------	--------	-----------

Agent Delivery Events	Status	Timestamp
-----------------------	--------	-----------

Intermediary Delivery Events	Status	Timestamp
------------------------------	--------	-----------

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	2/16/2023 9:15:01 AM
Certified Delivered	Security Checked	2/22/2023 11:15:40 AM
Signing Complete	Security Checked	2/22/2023 11:15:54 AM
Completed	Security Checked	2/22/2023 11:15:53 AM

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--

## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, Insight OBO The Massachusetts General Hospital (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

### **How to contact Insight OBO The Massachusetts General Hospital:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [jhenrique@mgh.harvard.edu](mailto:jhenrique@mgh.harvard.edu)

### **To advise Insight OBO The Massachusetts General Hospital of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [jhenrique@mgh.harvard.edu](mailto:jhenrique@mgh.harvard.edu) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

### **To request paper copies from Insight OBO The Massachusetts General Hospital**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [jhenrique@mgh.harvard.edu](mailto:jhenrique@mgh.harvard.edu) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

### **To withdraw your consent with Insight OBO The Massachusetts General Hospital**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to [jhenrique@mgh.harvard.edu](mailto:jhenrique@mgh.harvard.edu) and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Insight OBO The Massachusetts General Hospital as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Insight OBO The Massachusetts General Hospital during the course of your relationship with Insight OBO The Massachusetts General Hospital.