NeuroNEXT Network

Standard Operating Procedure (SOP)
Data Backup, Recovery, and Contingency Plans
Version 2.0
SOP NN CS 705

Originators: NeuroNEXT CCC and DCC Personnel

Reviewed and Approved by:

Christopher S. Coffey, PhD (DCC Principal Investigator)

Merit E. Cudkowicz, MD MSc (CCC Principal Investigator)

Marianne Kearney Chase, BA (CCC Director of Clinical Operations)

Dixie J. Ecklund, RN MSN MBA (DCC Associate Director)

Katherine B. Gloer, PhD (DCC Quality Management Lead)

Janice Cordell, RN MPH (NINDS, NeuroNEXT Program Official)

September 21, 2016
Issue Date

October 21, 2016
Effective Date (*30 calendar days after the Issue Date*)

NN CS 705

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

SOP: NN CS 705 Version No. 2.0 Effective Date: 21Oct2016	DATA BACKUP, RECOVERY, AND CONTINGENCY PLANS	Supercedes Document: Version 1.0 Effective Date: 29Apr2012

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 extended periods of server failure. This policy is designed to protect the DCC from 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 1996 ICH E6 Consolidated Guidance. 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, FDA, August 2003
FDA	Guidance for Industry: Computerized Systems Used in Clinical Investigations, FDA, 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
Production	IT environment created for deployment of the final application

8. SPECIFIC PROCEDURES

Data Backup Procedures

Data backup operations are performed automatically on a regular basis. 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.

Contingency Plans

Contingency plans have been developed for continuation of DCC IT services during extended periods of server failure. 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 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. 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.		

D. Contingency Plans

	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.		
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.		

	Who	*Task*	*Attachment/ Reference*	*Related SOP*
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.		

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**
1.0	New	N/A	30Mar2012	29Apr2012
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