NeuroNEXT Network

Standard Operating Procedure (SOP)

System Security Measures and Website Access
Version 2.0
SOP NN CS 704

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 704

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

SOP: NN CS 704	SYSTEM SECURITY MEASURES AND WEBSITE ACCESS	Supercedes
Version No. 2.0		Document: Version 1.0
Effective Date: 21Oct2016		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 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 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 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	Part 11, Electronic Records; Electronic Signatures – Scope and Application, FDA, August 2003
FDA Guidance	Computerized Systems Used in Clinical Investigations, FDA, May 2007
FDA Guidance	Computerized Systems Used in Clinical Trials, April 1999
FDA Guidance	General Principles of Software Validation, FDA, January 2002
FDA	Guidance for Industry: Electronic Source Data in Clinical Investigations, September 2013
NIH	HIPAA Privacy Rule: Information for Researchers <http://privacyruleandresearch.nih.gov/>

5. REFERENCES TO OTHER APPLICABLE SOPS

NN PM 501	Communications
NN CS 701	System Setup/Installation
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
http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

NIST Guide to SSL VPNs, Special Publication 800-113, July 2008
http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf

NIST Guidelines on Securing Public Web Servers, Special Publication 800-44 (Version 2), September 2007
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

NIST Technical Guide to Information Security Testing and Assessment, Special Publication 800-115, September 2008
http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

NIST Information Security Handbook: A Guide for Managers, Special Publication 800-100, October 2006
http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

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.

Physical Security

All servers are protected from unauthorized physical access using biometric and/or electronically controlled door systems. Access is restricted to authorized IT staff 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 eight characters at least two of which must be symbolic or 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 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 current 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 Lead Coordinator 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 reviewed regularly by the DCC to ensure that they are still current and applicable to the activities performed by the users. If during the course of the study the contact information or roles for a user are changed, a new website access request form is submitted to the DCC for review, contact information is updated, and any necessary changes to access rights are implemented. The DCC terminates user access rights for all users who discontinue their association with a study.

Submitting Data to DCC Data Systems

DCC data systems log 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

All DCC data systems maintain audit trails for changes to submitted data. All modifications made to a 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. 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 users be assigned a unique User ID and password for access to DCC internal systems. • University of Iowa HawkIDs are used for access to DCC internal systems. • HawkID passwords must conform to the UI Enterprise Password Policy. • Passwords must contain at least eight (8) characters that include at least two (2) symbolic or numeric characters. • Passwords are to be changed at regular intervals (at least every [6] six months).		
2.	DCC and/or UI CPH IT	Assign system-type roles to the HawkID.		
3.	Users	Acknowledge the following: • 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: • Any electronic signature submitted under this User ID and password is intended to be the legally binding equivalent of a traditional handwritten signature.	21 CFR Part 11	

#	*Who*	*Task*	*Attachment/ Reference*	*Related SOP*
		- The user will be accountable and responsible for any actions initiated the 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

C. Server Electronic Security

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

#	*Who*	*Task*	*Attachment/Reference*	*Related SOP*
4.	DCC IT and/or UI CPH IT	Encrypt all passwords.		
5.	DCC IT and/or UI CPH IT	Establish and maintain system firewalls using 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

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

E. File Access Restrictions

#	*Who*	*Task*	*Attachment/ Reference*	*Related SOP*
1.	DCC IT or UI CPH IT	Restrict the use of the DCC file server to DCC personnel and authorized University of Iowa personnel. Additional material within the DCC file server may be 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 IT Lead	Generate a unique User ID for each new study team member.		

#	***Who***	***Task***	***Attachment/ Reference***	***Related SOP***
3.	DCC Protocol 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. • 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.	DCC	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 indicate approval.		
7.	DCC Lead Coordinator or designee	Retain the signed forms in the study files, and maintain electronic copies 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.		
10.	DCC DM, Protocol Coordination, 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, complete and submit a new website access request form with the appropriate information, and return it to the DCC.		NN PM 501
12.	DCC IT or DM	Ensure that only authorized DCC staff members are permitted to modify user access rights.		
13.	DCC DM or IT	If guest access to the study website is required (e.g. for a study Medical Monitor), perform the steps described above for a new user, and consult with Senior Leadership or an appropriate oversight committee (e.g. Steering Committee) to determine the appropriate user access rights.		

F. 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	
	DCC IT	After the initial submission of an electronic record, track all changes in an audit trail.		
2.	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.		
3.	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	21 CFR Part 11	NN DM 1005

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**
1.0	New	N/A	30Mar2012	29Apr2012
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