NeuroNEXT Network

Standard Operating Procedure (SOP)
System Setup/Installation
Version 2.0
SOP NN CS 701

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 701

NEURONEXT NETWORK STANDARD OPERATING PROCEDURE FOR SYSTEM SETUP/INSTALLATION

SOP: NN CS 701 Version No. 2.0 Effective Date: 21Oct2016	SYSTEM SETUP/INSTALLATION	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 procedures and security measures related to the setup and installation of new computer systems (e.g., servers, workstations, laptops) for the NeuroNEXT Network.

The DCC only purchases computer systems from vendors approved by The University of Iowa purchasing department. Computerized systems must have a minimum of a three-year on-site maintenance agreement that covers hardware and online downloads, and includes driver support.

Initial setup procedures (e.g. installing firewalls and anti-virus software, managing system services) are performed offline in order to decrease the exposure of new systems to malicious attacks.

Software is installed based on system projected usage and user needs. All software must be approved and installed by UI CPH IT and/or DCC IT to ensure that licensing requirements are met and to decrease the exposure of systems to outside malicious attacks. Software is updated with the latest service packs and patches as they become available.

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 also 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

The University of Iowa DCC IT Team and UI CPH IT are responsible for adhering to the procedures outlined in this SOP, and for ensuring that any DCC or UI CPH IT personnel who perform system setup or installation of DCC computerized systems or servers for NeuroNEXT studies are in compliance with this SOP.

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: General Principles of Software Validation; Final Guidance for Industry and FDA Staff (January 2002)
NIH	HIPAA Privacy Rule: Information for Researchers. <http://privacyruleandresearch.nih.gov/>
University of Iowa	IT Security Best Practices, Information Security and Policy Office <http://cio.uiowa.edu/ITSecurity/bestprac/

5. REFERENCES TO OTHER APPLICABLE SOPS

NN CS 704 System Security Measures and Website Access

NN CS 705 Data Backup, Recovery, and Contingency Plans

6. ATTACHMENTS AND REFERENCES

NN CS 701 – 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
DCC	Data Coordinating Center at The University of Iowa
DCC IT	Information Technology Team at the DCC
GCP	Good Clinical Practice

8. SPECIFIC PROCEDURES

A. University Licensing Agreement

#	*Who*	*Task*	*Attachment/ Reference*	*Related SOP*
1.	DCC IT	Comply with all software licensing agreements.		

B. Initial Setup

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

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT or UI CPH IT	Repartition, format, and install new Microsoft operating system software obtained from UI CPH IT Services on all computer systems (e.g., servers, workstations, laptops).		
2.	DCC IT or UI CPH IT	Assign a strong administrative password to each new computer system.		NN CS 704
3.	DCC IT or UI CPH IT	Name and register the computer system with the IT Security Office, according to UI CPH IT and DCC standards.		
4.	DCC IT or UI CPH IT	If needed, obtain a unique IP number for each computer system from The University of Iowa Information Technology Services.		
5.	DCC IT or UI CPH IT	If applicable, remove or disable all unnecessary services from computer systems.		

C. Security/Anti-Virus Software

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT or UI CPH IT	Install anti-virus software onto applicable computer systems.		NN CS 704
2.	DCC IT or UI CPH IT	If applicable, and prior to connecting to the Internet, set Firewall by setting local security policy (IP Sec), and restricting IP and port access.		
3.	DCC IT or UI CPH IT	Prior to connecting to the Internet, review system services and enable or disable services required for restricted operation.		
4.	DCC IT or UI CPH IT	Establish connection to the Internet, and update anti-virus software to latest definitions.		
5.	DCC IT or UI CPH IT	Update Windows operating system to install the latest security patches.		
6.	DCC IT or UI CPH IT	After any updates to servers, update server log in server binder.		

D. Server Software Installation

#	Who	Task	Attachment/ Reference	Related SOP
1.	UI CPH IT	Add appropriate server roles: Web Server (IIS) for Web Servers File Services for Database and File Servers		NN CS 704
2.	UI CPH IT	Add appropriate server functions: Latest Framework for Web, Database, and File Servers		

#	Who	Task	Attachment/ Reference	Related SOP
3.	UI CPH IT	Enable Remote Desktop Connection: Restrict access to UI CPH IT and/or DCC System Administrators		NN CS 704
4.	UI CPH IT	Update software with the latest service packs and patches.		
5.	UI CPH IT	Using established software, schedule backup for all directories requiring data backup.		NN CS 705
6.	UI CPH IT	On a quarterly basis, run a program to confirm that all new software programs, service packs, and patches have been properly installed, and document the results.		

E. Server Access Restrictions

#	Who	Task	Attachment/ Reference	Related SOP
1.	DCC IT and/or UI CPH IT	Limit physical access to servers to authorized staff.		NN CS 704
2.	DCC IT and/or UI CPH IT	Establish server user accounts and roles for usage rights.		
3.	DCC IT and/or UI CPH IT	Limit server drive access rights to appropriate users.		

F. Workstation Software Installation

#	Who	Task	Attachment	Related SOP
1.	DCC IT or UI CPH IT	Install software based on user needs.		NN CS 704
2.	DCC IT or UI CPH IT	Install software that has been approved by UI CPH IT or DCC IT to ensure that licensing requirements are met and to decrease the exposure of systems to outside malicious attacks.		
3.	UI CPH IT	Run a program to confirm that new installations of, or updates to, SAS® software have been performed correctly, and document the results.		
4.	UI CPH IT	Per UI CPH IT guidelines, track the programs that are installed on computer workstations.		
5.	DCC IT or UI CPH IT	Enable Remote Desktop Connection permissions only for DCC users and/or system administrators.		NN CS 704

Attachment NN CS 701 - A. Document History

NeuroNEXT Network Standard Operating Procedure (SOP) System Setup/Installation SOP NN CS 701				
Version	**Description of Modification**	**Reason or Justification for Modification**	**Issue Date**	**Effective Date**
1.0	New	N/A	30Mar2012	29Apr2012
2.0	Modified to reflect the increased involvement of The University of Iowa College of Public Health Office of Information Technology (UI CPH IT) in the installation and setup of computerized systems at the DCC. Added a provision for a quarterly confirmation that software programs and updates have been properly installed. Added a new section for workstation software installation. Additional minor updates throughout.	Transition of certain responsibilities to UI CPH IT, and updates for version 2.0.	21Sep2016	21Oct2016