
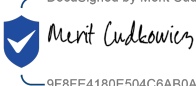



NeuroNEXT Network

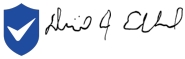
Standard Operating Procedure (SOP) System Security Measures and Website Access Version 3.0 SOP NN CS 704

Originators: NeuroNEXT CCC and DCC Personnel

Reviewed and Approved by

Signature and Date:  I approve this document 16-Feb-2023 11:04:13 AM PST 16-Feb-2023 C68AC8DD80334CF982AED1200765F147
Name and Title: Christopher S. Coffey, PhD (DCC Principal Investigator)
Signature and Date:  I approve this document 17-Feb-2023 9:34:26 AM EST 17-Feb-2023 9F8FE4180E504C6AB0A67B835E80C644
Name and Title: Merit E. Cudkowicz, MD MSc (CCC Principal Investigator)
Signature and Date:  I approve this document 17-Feb-2023 1:19:14 PM EST 17-Feb-2023 58FE690F6BCA4F2390E3DA15BCE3F578
Name and Title: Marianne Chase, BA (CCC Senior Director of Clinical Trials Operations)

Signature and Date:

DocuSigned by DIXIE ECKLUND
 | I approve this document
17-Feb-2023 | 4:00:25 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 | 11:16:23 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 | 6:49:26 AM PST
72C6AAFD8CC4485582ACA0700072901A

21-Feb-2023

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

NN CS 704

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

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 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 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 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)
FDA	Guidance for Industry: General Principles of Software Validation; Final Guidance for Industry and FDA Staff (January 2002)
FDA	Guidance for Industry: Electronic Source Data in Clinical Investigations (September 2013)
NIH	HIPAA Privacy Rule: Information for Researchers

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)

NIST Guide to SSL VPNs, Special Publication 800-113 (July 2008)

NIST Guidelines on Securing Public Web Servers, Special Publication 800-44 (Version 2) (September 2007)

NIST Technical Guide to Information Security Testing and Assessment, Special Publication 800-115 (September 2008)

NIST Information Security Handbook: A Guide for Managers, Special Publication 800-100 (October 2006)

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 personnel 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 nine characters at least two of which must be 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 in real time 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 initial 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 Data Manager 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 updated on an ongoing basis by the DCC to reflect personnel changes and training. If during the course of the study the contact information or roles for a user are changed, the CSS or CCC is responsible for contacting the DCC to update the information. User access rights are terminated for users who discontinue their association with a study.

Submitting Data to DCC Data Systems

DCC data systems log relevant information including, but not limited to, 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

DCC electronic data capture systems maintain audit trails for changes to submitted data. All modifications made to a CRF 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 (when applicable/necessary). 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 authorized users at the DCC be assigned a unique User ID and password for access to DCC internal systems. •		

#	Who	Task	Attachment/Reference	Related SOP
2.	DCC and/or UI CPH IT	Assign system-type roles to the HawkID.		
3.	Users	Acknowledge the following: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Any electronic signature submitted under this User ID and password is intended to be the legally binding equivalent of a traditional handwritten signature. The user will be accountable and responsible for any actions initiated the electronic signature submitted under his/her User ID and password. 	21 CFR Part 11	
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).		
4.	DCC IT and/or UI CPH IT	Encrypt all passwords.		
5.	DCC IT and/or UI CPH IT	Establish and maintain system firewalls including 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 file server to DCC personnel and authorized University of Iowa personnel. Additional material within the file server may be further 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	Generate and maintain a unique User ID for each new study team member.		
3.	DCC Data Manager, Lead 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. <ul style="list-style-type: none"> 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.	CSS Coordinator or Requester	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 acknowledge the review.		
7.	DCC Lead Coordinator or designee	Maintain PDF versions of the signed forms 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		

#	Who	Task	Attachment/Reference	Related SOP
		timeframe. Passwords are to be changed at regular intervals.		
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, inform the CCC and DCC as soon as possible after becoming aware of the need for a change.		NN PM 501

G. 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 (when applicable/necessary).	21 CFR Part 11	NN DM 1005


Certificate Of Completion

Envelope Id: DA83DBCD1E9041CFAE884146D2544283	Status: Completed
Subject: Complete with DocuSign: NN CS 704 System Security Measures and Website Access v3.0.docx	
Source Envelope:	
Document Pages: 9	Signatures: 6
Certificate Pages: 6	Initials: 0
AutoNav: Enabled	Envelope Originator: Tania Leeder
Envelopeld Stamping: Disabled	TLEEDER@PARTNERS.ORG
Time Zone: (UTC-05:00) Eastern Time (US & Canada)	IP Address: 24.62.91.235

Record Tracking

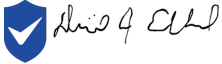
Status: Original 2/16/2023 8:48:57 AM	Holder: Tania Leeder TLEEDER@PARTNERS.ORG	Location: DocuSign
--	--	--------------------

Signer Events

Signer Events	Signature	Timestamp
Christopher Coffey christopher-coffey@uiowa.edu Security Level: Email, Account Authentication (Required), Login with SSO		Sent: 2/16/2023 8:54:40 AM Viewed: 2/16/2023 2:04:04 PM Signed: 2/16/2023 2:04:17 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 2:04:04 PM
ID: 466a4ed8-c05f-45c9-a0fc-520719c862cf

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 | 4:00:25 PM PST
7006AF622EFC40B6A067A08EC02591B6

Sent: 2/16/2023 8:54:41 AM
Viewed: 2/17/2023 6:59:26 PM
Signed: 2/17/2023 7:00:30 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 6:59:26 PM
ID: ef1745ed-5114-4ead-871d-998649a10bb6

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

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

Joan Ohayon

Sent: 2/16/2023 8:54:42 AM
Resent: 2/21/2023 8:26:27 AM
Viewed: 2/21/2023 9:49:13 AM
Signed: 2/21/2023 9:49:29 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 8:54:41 AM
Viewed: 2/17/2023 1:18:56 PM
Signed: 2/17/2023 1:19:18 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 | 9:34:26 AM EST
9F8FE4180E504C6AB0A67B835E80C644

Sent: 2/16/2023 8:54:40 AM
Viewed: 2/17/2023 9:34:17 AM
Signed: 2/17/2023 9:34:28 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 9:34:17 AM
ID: 71bc2b43-8bee-4a58-a9c6-4610006c9b47

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 8:54:42 AM Resent: 2/21/2023 8:26:27 AM Viewed: 2/22/2023 11:16:13 AM Signed: 2/22/2023 11:16:26 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 8:54:42 AM
Certified Delivered	Security Checked	2/22/2023 11:16:13 AM
Signing Complete	Security Checked	2/22/2023 11:16:26 AM
Completed	Security Checked	2/22/2023 11:16:26 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

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 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 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 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.