New C3PHI Project Guide

Version: Apr 2021

This document provides instructions for principal investigators and data stewards to prepare the IT side of working in a secure, compliant C3PHI environment. This guide draws from, references, and supplements resources from the CRC, OIT, and ND Research.

An electronic copy of this document can be found at:
research.nd.edu/assets/427454

The full HIPAA resource page can be found at:
research.nd.edu/our-services/compliance/human-research/hipaa

Table of Contents

General Guidelines and Reference **1**

Resource Websites 1

Reporting Data Breaches 1

Checklist for New Project Tasks **2**

Guidance for Specific New Project Tasks **3**

Identify a Data Steward 3

Create a Data Security Plan 3

Request NetIDs for Research Affiliates 3

Complete Required Certifications 3

Create a Quick Reference Guide (QRG) for Researchers 4

Request Group(s) and Folder(s) to Manage Data Access 4

Testing the C3PHI Environment 5

Identify and Train Transfer Agents 5

Transfer Files On/Off the System 5

Request Additional Software 5

General Guidelines and Reference

Resource Websites

Resources for specific processes are linked throughout this document. In general:

- Research and compliance resources can be found with ND Research (research.nd.edu)
- Support resources can be found with the CRC (crc.nd.edu)
- Request forms can be found with OIT through ServiceNow (sn.nd.edu)
  Note: Login will be required to view linked articles.

Reporting Data Breaches

The HIPAA Privacy Rule requires that when PHI is inappropriately disclosed or used that the event is reported. There are three ways in which a breach may be identified:

1. An inadvertent disclosure of PHI by workforce (e.g., ND researcher).
2. Unencrypted electronic data that includes PHI is lost, stolen, or accessed by an unauthorized person.
3. Any unauthorized use or disclosure by the workforce of one of ND's business associates, its agents, or subcontractors.

HIPAA requires that Notre Dame make notification without unreasonable delay and within 60 days of discovery of the breach, unless a law enforcement delay has been requested. Some data providers and research partners require notification within 1 hour of the determination of the breach. Once a data breach is discovered, contact the Research HIPAA Privacy Officer (compliance@nd.edu). Notification of a data breach will follow the University's published Incident Response Plan (policy.nd.edu/assets/185245).

Checklist for New Project Tasks

The following tasks relate to the IT technical requirements for establishing a C3PHI secure storage environment for research data.

Item	Task	Responsible
	Identify a Data Steward	Principal Investigator
	Create a Data Security Plan	Principal Investigator
	Request NetIDs for Research Affiliates	Data Steward
	Complete HIPAA Certification	All Researchers
	Complete Human Subjects Research Certification	All Researchers
	Collect, Track, and Store Researcher Certifications	Data Steward
	Create a Quick Reference Guide (QRG) for Researchers	Principal Investigator
	Request Group(s) and Folder(s) to Manage Data Access	Data Steward
	Test the C3PHI Environment	Principal Investigator Data Steward
	Identify and Train Transfer Agents	Data Steward
	Transfer Files On/Off the System	Data Steward Transfer Agents
	Request Additional Software	Data Steward

Guidance for Specific New Project Tasks

Identify a Data Steward

A data steward is an appointed role within a lab or research program. For more information about the role of data steward, please refer to ND Research's HIPAA Policy for Notre Dame Researchers (research.nd.edu/assets/406244).

Once your data steward has been identified, send their name and contact information to both the CRC and the Research HIPAA Privacy Officer (compliance@nd.edu).

Create a Data Security Plan

Each research project is required to have a Data Security Plan in place. This plan outlines the individuals that manage project data as well as how data is both acquired and stored.

Download the Project Data Security Plan template in ServiceNow article KB0022610 from OIT.

Request NetIDs for Research Affiliates

If you have research affiliates on your team that are not part of Notre Dame, they will need a NetID in order to access the data. Two sponsors are required to request an affiliate NetID:

1. Principal Investigator
2. Full-time faculty or staff member

Once the second sponsor is identified, complete the affiliate access request form. For more details as well as the link to the request form, view ServiceNow article KB0010154 from OIT.

When the research affiliate receives their ND credentials, they can then enroll in Okta for Multi-Factor Authentication. This is a requirement for all ND accounts; they will not be able to access the C3PHI environment until completing this step. For step-by-step instructions on how to enroll in Okta, refer the research affiliate to ServiceNow article KB0017218 from OIT.

Complete Required Certifications

Before accessing any PHI data, each researcher must complete two certifications: **HIPAA** and **Human Subjects Research**. The project's data steward is responsible for collecting, storing, and tracking the expiration date of these certifications.

Once a researcher has completed both certifications, the data steward can grant them access to the data by adding them to the project's group(s) in ServiceNow.

Training Materials and Certification:

- HIPAA (research.nd.edu/assets/427459)
- Human Subjects Research (isla.nd.edu/assets/264810)

Create a Quick Reference Guide (QRG) for Researchers

We recommend creating a QRG for your researchers that serves as a one-stop shop for project information. In the QRG template, there are links to instructions for working in the system as well as fillable sections for:

- Project roles and contact information
- Link to the project's data security plan
- Any system specifications for the project's C3PHI environment
- Details about the project's folder structure
- Data steward and transfer agent emails for file transfer requests
- Any stipulations from data usage agreement(s)

Download the Researcher QRG template in ServiceNow article KB0022610 from OIT.

Request Group(s) and Folder(s) to Manage Data Access

Request Institutional/Enterprise Groups through the ServiceNow groups.nd.edu portal. The project's data steward will be the manager of these groups. They are responsible for:

- Managing group membership
- Tracking group member certifications
- Requesting data folders and assigning groups to them

At minimum, each project needs one group that contains all the members of its research team. For projects that require different permission levels on different folders of data, request a group for **each folder that needs permissions**.

Once a group is created, the data steward can request a folder and assign the group to it. With the group assigned, membership to the group grants access to all data in the folder.

To manage data access, see the following ServiceNow articles from OIT:

- KB0022394: Request a New C3PHI Project Data Access Group
- KB0022395: Request a New C3PHI Folder and Assign a Group
- KB0017598: Instructions/FAQ for Managing Group Membership

At minimum, group membership and data access should be audited by the data steward every six months. Any group members whose data access exceeds their needs should have their needs re-aligned with their required access. For a full description of the user account life cycle for C3PHI environments, please refer to ServiceNow article KB0022507 from OIT.

Researchers no longer working on the project should be removed from the group as part of their offboarding.

Testing the C3PHI Environment

Before you begin working in your environment, we recommend completing user acceptance testing (UAT) with your research group. To assist, you can download a UAT template in ServiceNow article KB0022610 from OIT.

Identify and Train Transfer Agents

In addition to the data steward, projects can assign transfer agents to assist with transferring files on and off the system. For more information about transfer agents, please refer to ND Research's HIPAA Policy for Notre Dame Researchers (research.nd.edu/assets/406244).

Once transfer agents are identified, the data steward administers any required system and/or compliance training. Before conducting training, review the Transfer Agent Training Guidelines (research.nd.edu/assets/427458). Once transfer agents have completed training and certifications, the data steward can add them to the appropriate group via the groups.nd.edu portal. This grants the transfer agents the appropriate file transfer permissions. The transfer agent emails can then be added to the Researcher QRG.

Transfer Files On/Off the System

Files are transferred via LiquidFiles. Only the data steward and transfer agents will have permission to transfer files. As such, researchers will submit file transfer requests to two members of each team. Instructions for researchers are linked in the Researcher QRG and can also be found at research.nd.edu/assets/427456.

To transfer files as the data steward or a transfer agent, review your project's file transfer requirements and then follow the step-by-step instructions at research.nd.edu/assets/427455.

Request Additional Software

Initial software requirements were collected during the intake process. However, once your project is underway, you may come across additional software needs.

All software requests must go through the data steward. If there is an additional software application or R/Stata package needed, the data steward can fill out the ServiceNow *AWS: Add Application to Appstream* request form. Note that not all software will necessarily be available in this type of environment.