

UConn Health Protected Environment (PHI Compliant) FAQs

1. Why am I required to use a Protected Environment (PHI Compliant)?

The UConn and UConn Health (UCH) users are required to use a Protected Environment when:

1. Analyzing data that requires HIPAA compliance.
2. Analyzing data that requires NIST SP 800-171 rev.2 compliance. *
3. Analyzing data from other data sources that require a Data Usage Agreement (DUA) or have data access requirements such as
 - a. Must be analyzed in a secure computing environment
 - b. No local download permitted
 - c. Access limited to approved users
 - d. Must comply with NIH GDS policy

* Typically, NIH and U.S. Federal Controlled-Access databases such as dbGaP, NIMH Data Archive (NDA), AnVIL and research data derived from PHI require NIST SP 800-171 rev.2 compliance. There are some overlapping requirements under HIPAA and NIST SP 800-171 rev. 2 standards. In general, NIST SP 800-171 rev. 2 requirements are stricter.

2. I already have access to some UCH HPC resources for my other research projects. Can I just use them for storing and analyzing HIPAA data or other protected data temporarily while I wait for my Protected Environment request to be fulfilled?

Unfortunately, no. The baseline UCH HPC configuration is an open research environment rather than a protected environment, and certain datasets (including those requiring HIPAA or NIST SP 800-181 rev. 2 or 3 compliance) require restricted access. UConn and UCH researchers can request such a protected environment (a Virtual Machine/VM, commonly referred to as a “HIPAA Island” VM) hosted at the UCH HPC facility.

Regulated datasets may only be stored and processed within an approved, HIPAA or NIST SP 800-171-compliant environment (such as a dedicated HIPAA Island or an equivalent secure enclave). Having access to UCH HPC resources or a pending HIPAA Island request does **not** authorize interim use of non-compliant systems, such as the baseline HPC environment. You will need to wait to access your dedicated HIPAA Island to start downloading or working with data requiring a protected environment.

General shared HPC resources, including Xanadu and Mantis, are not approved for storage or processing of regulated or controlled human subjects data, even if they reside within the broader UCH HPC ecosystem.

For any clarifications regarding these requirements, please contact Research Security at researchsecurity@uconn.edu

3. What are the components and restrictions in this environment?

For UConn and UCH users, a protected environment, also commonly known as a HIPAA island, is implemented as a Virtual Machine (VM) hosted in a secure network environment hosted at UConn Health HPC. The environment contains:

- Secure computation resources as dedicated virtual servers
- Data import/download: enabled upon request and within the DUA (details in Q7)
- Secure storage
- Identity & Access Control: named users
- Network Security: Isolated from Internet and the rest of the UCH network
- Data governance & compliance controls
- Analysis tools: All software packages requested by the user must be approved by IT Security. Restricted configurations may be applied based on the approval conditions.
- Output & export controls: enabled upon request and within the DUA. See details in Q8.
- Auditing and monitoring
- Governance & Oversight

4. What can I do in this environment?

In this environment, you can:

1. Download and store controlled-access or PHI data into this environment
2. analyze the data with software that you requested to be installed
3. export data/data egress per approval (see answer to Q7)

5. How can I submit a request for such an environment?

All such requests must be submitted to UConn Health HPC via a HPC ticket: [Submit a Ticket | High Performance Computing Facility](#). For auditing purposes, HPC will not accept any request via email or other channels.

1. Request Type: select “Protected Environment (PHI Compliant)
2. Name: your name as the one completing the form
3. Status: if you are not a UConn Health employee, select “UCHC Affiliate/Collaborator” *
4. Email Address: Please use your primary work email address. If you are a UConn Storrs/Regional campus employee, use your uconn.edu address
5. Campus and Department: Select your own campus and department.
6. PI: The Principal Investigator’s Name
7. Data Steward – The person who is responsible for data access safeguards and adding/removing authorization to access the data for project users and collaborators. Often this is the project PI/named person on IRB and DUA etc., and usually it is a faculty or staff member; students or postdocs can sometime have this role, but only if the project is sponsored by a fellowship/grant in their name.
8. Project Name – no longer than 10 characters. The first 3-4 characters should be the department name abbreviation followed by a 6–7-character project short name, for example, PSYCXXXXXX.
9. Servers, Operating Systems, Cores, Memory & Local Drive: estimate as best as you can. Other than the number of servers and operating systems, the rest of the configurations can be adjusted later to meet your needs.
10. Data source/URL & Port Number: Please provide the data source IP/URL and the data download protocol permitted by the Data Usage Agreement (DUA)
11. Software Required: please provide software name. The software will be assessed for approval for the protected environment. By default, the latest stable version of the software will be installed unless you specify a different version number.
12. User List: Additional users who need access to the VM. Please provide their UCH user account names.

* The protected environment/VM will be set up in the UConn Health network. Users can only access the environment with a UConn Health network account (@uchc.edu). Please see the answer to Q10 for more details.

6. How can I determine what configuration I should request for this environment? Can that be adjusted later?

The standard configurations for each VM are:

OS: Windows 11

Cores: 4

Memory: 32 GB

Local Drive: 150 GB

Network storage: 5TB

OS: Ubuntu

Cores: 4

Memory: 16 GB

Local Drive: 100 GB
Network storage: 5TB

The user can request other Windows or Linux OS or higher configurations and will be asked to provide justifications for very high configurations. Please estimate as best as you can. Other than the number of servers and operating systems, the rest of the configurations can be adjusted later.

7. Can I have some software installed in this environment? When should I request the software needed?

Please list the software name and version information in the “Additional Information” section in the HPC “Protected Environment (PHI Compliant)” request ([Submit a Ticket | High Performance Computing Facility](#)). HPC will forward the software list to IT Security for approval and provide the approval status updates. HPC will installed the approved software for you.

8. How can I download or save data into this environment?

Because internet access is disabled in the protected environment, HPC provides a separate airlock staging VM for you to download data. You’ll save the data into a dedicated folder on this VM. HPC will then move the data into your HIPAA Island VM for you. Detailed instructions will be sent to you once the HIPAA VM is set up and the data download can begin.

9. Will I be able to export data or save data out of this environment (data egress/export)? What do I need to provide to have data export enabled?

Because of the sensitivity of transmitting PHI and CUI, data egress/export is disabled by default and may only be enabled when permitted by applicable regulations, contract terms, and data use agreements. Any export of PHI must be vetted on an individual case-by-case basis.

Data egress of de-identified research results, which does not constitute PHI, will be permitted upon request and verification. To permit data export of properly de-identified research results, Pls will be asked to affirm the following:

- Data leaving the HIPAA Island has been fully de-identified; and
- Export of the data does not violate the terms of the controlling Data Use Agreement.

For data subject to NIST SP 800-171 Rev. 2 requirements (e.g., NIH and U.S. Federal Controlled-Access databases and Controlled Unclassified Information), export outside the protected environment is generally prohibited unless the receiving system has been formally reviewed and determined to provide equivalent 800-171 controls.

For data subject to HIPAA (but not 800-171), data egress/export may be permitted if:

- The Data Use Agreement (DUA) allows external storage or transfer;
- The destination system has been approved by the UConn Health IT Security as suitable for receiving HIPAA-regulated data and is assigned a static IP Address; and a formal IT service request is submitted and approved.

All data egress requests will be logged and may be audited.

10. How can additional users access this environment?

Please enter the additional users' UConn Health account names (@uchc.edu) in the "Addition Information" section in the "Protected Environment (PHI Compliant)" ticket. To add additional users after the initial ticket for the environment build is closed, you can submit a separate "Permission Request" ticket.

11. Can users use the UConn account to access this environment?

No. The users will need to have a UConn Health account to access this environment.

- If you are the PI and have a UConn Health account, you can submit an IT UAR request ([Welcome to the User Access Request Application](#)) to request UConn Health "Affiliate" accounts for additional users who do not have a @uchc.edu account.
- If you are the PI and don't already have a UConn Health account, please reach out to Lesley Salafia in Research Security at lesley.salafia@uconn.edu for her office to sponsor and request the UConn Health affiliate accounts for you and additional users who need access to this environment.
- Note that if you are requesting access to a dataset that requires HIPAA compliance, you will also need to complete HIPAA compliance training prior to being approved to access the HIPAA Island. Lesley Salafia in Research Security will provide you with the link to the current HIPAA compliance training as part of setting up your affiliate account access.

12. How can I access this environment after it's set up?

To access the HIPAA VM,

Step 1: log into the UConn Health network.

Last updated 06.06.2026 Q Cheng

- If you are using a UCH IT managed device, you can connect to the UCH network through the UCH Cisco AnyConnect VPN if your device is not already on the UCH network.
- If you do not use a UCH IT managed device, you can
 1. Connect to the UCH network through UCH Citrix gateway (<https://remote.uchc.edu>; **NOT UConn Citrix**). You'll need to use your UCH account name and password to log into Citrix. DUO authentication is required for Citrix log in.
 2. Connect to the UCH network through the CAM VPN if you already have it set up previously, or

*Please note that you do NOT need to request CAM VPN for HIPAA VM access.

Step 2: log into the HIPAA VM with your UCH account name and password

To access a Windows HIPAA VM,

- If you have connected to UCH network through UCH Citrix, open the “Remote Desktop Connection” available in “Apps” and log in.
- If you have connected to the UCH network through either UCH Cisco AnyConnect VPN or CAM VPN, open the “Remote Desktop” application for Windows users, or “Microsoft Remote Desktop” for Mac users from your desktop and log in.

To access a Linux HIPAA VM,

- If you have connected to UCH network through UCH Citrix, you can use one of the Windows desktops available in “Desktops” in Citrix to SSH into the VM.
- If you have connected to the UCH network through either UCH Cisco AnyConnect VPN or CAM VPN, you can SSH into the VM.

Step 3: Map the network storage

When you log into the VM the first time, a command prompt window will pop-up for you to map the network storage drive. Enter your UCH user name and password. If you need to re-attempt this step, you can find the shortcut to the link on the desktop.