UCH Protected Environment (PHI Compliant) FAQs

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

The UConn and UConn Health 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. What are the components and restrictions in this environment?

For UConn and UConn Health users, a protected environment is implemented as a Virtual Machine (VM) hosted in a secure network environment called a “HIPAA Island” in 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 and 2-factor authentication
- Network Security
- Data governance & compliance controls
- Analysis tools: users can request software packages such as R installed
- Output & export controls: enabled upon request and within the DUA. See details in Q8.
- Auditing and monitoring
- Governance & Oversight

3. What can I do in this environment?

In this environment, you can:

1. download 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)

4. 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 emails 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 and Data Location: estimate as best as you can. Other than the number of servers and operating system, the rest of the configurations can be adjusted later to meet your needs.
10. Additional Information: List specific software that you need in this environment. List additional users' UConn Health account names. For users who don't have an uchc.edu account, request UCHC affiliate accounts for them separately*. Additional user access requests can also be submitted later as a "Permissions Request" HPC ticket after the VM is built.

    * 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.

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

Estimate as best as you can. Other than the number of servers and operating system, the rest of the configurations can be adjusted later to meet your needs.

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

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 can help you install any software approved by UConn Health IT security.

7. Will I be able to download data or save data into this environment (data import)? What do I need to provide to have data import enabled?

Yes. Data import is disabled by default. Once you have your DUA approved by Sponsored Program Services, please respond to the HPC ticket email and provide the DUA approval status, data source and data download protocol information.

8. 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?

Data egress/export is disabled by default and may only be enabled when permitted by applicable regulations, contract terms, and data use agreements.

For data subject to NIST SP 800-171 Rev. 2 requirements (e.g., 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 office as suitable for receiving HIPAA-regulated data and is assigned a static IP Address;
- A formal IT service request is submitted and approved.

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

9. How can additional users access this environment?

You can either enter the additional users' UConn Health account names (@uchc.edu) in the "Addition Information" section in the "Protected Environment (PHI Compliant)" ticket, or submit a "Permission Request" ticket after the environment is set up.

10. 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 don't have a @uchc.edu account.
- If you are the PI and don't 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.

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

If you are accessing this environment/VM from a UConn Health IT managed device from within the UConn Health network, you can use the "Remote Desktop Connection" application to log onto the VM.

If you are accessing this environment/VM from outside of UConn Health Network, you can remotely log into the "Citrix Workspace" on your UConn or UConn Health computer, or log into the Citrix web application (Citrix Workspace) with your UConn Health account or UConn Health affiliate account. Please note that if you use a UConn Health managed device to remote into Citrix, you need to log into the UConn Health Cisco AnyConnect VPN first via either connect.uchc.edu or connect.uchc.edu/cam to be able to log into Citrix. Please see the VPN set up instruction: HPC-Cisco-VPN-Instructions.pdf.

If you requested a Windows VM, use the "Remote Desktop" application available in Citrix to log onto the VM.

If you requested a Linux VM, use one of the Windows Desktops in Citrix to SSH into the VM.

Multi-factor authentication via DUO is required for you to log into Citrix and VPN.