For more information on SMPH Shared Services IT or to request support, please contact us:

Web: https://it.med.wisc.edu/about-us/shared-services
Phone: 608-264-4357 - Option #5 (DoIT VIP Support)
Email: support@med.wisc.edu

UW-Madison is committed to protecting the privacy and security of our patients, research participants, staff, and students. It is your responsibility to know how to adhere to HIPAA policy as an SMPH employee and to be a good steward of our data.

**HIPAA PRIVACY AND SECURITY**

All UW faculty and staff are required to complete annual HIPAA training.

- Complete your HIPAA Training
  go.wisc.edu/hipaatraining
- Report a HIPAA Incident:
  go.wisc.edu/hipaareport
- UW-Madison HIPAA Home
  go.wisc.edu/hipaa
- Contact HIPAA Privacy and Security Coordinators
  go.wisc.edu/hipacontacts

**CYBERSECURITY**

All UW faculty and staff are required to complete annual Information Security Awareness Training as required by the security policies of the University of Wisconsin System. See Security Awareness Training at go.wisc.edu/security-training

How to prevent Cybersecurity incidents at SMPH:
- Complete your Security Awareness Training (go.wisc.edu/security-training)
- Keep all software up-to-date
- Set unique, complex passphrase and change it if you suspect it has been compromised
- Use UW's encrypted password manager software (e.g. LastPass)
- Use Multi-Factor or Two-Step Authentication (e.g. MFA-Duo)
- Lock your workstation when you step away
- Be alert for phishing and other email scams

It is important to report any cybersecurity incident, no matter how large or small, so DoIT and SMPH Cybersecurity can take action to remediate and prevent further issues:
  go.wisc.edu/cybersecurityreport

All UW faculty and staff are required to complete annual HIPAA training.

**CYBERSECURITY CONSULTATION SERVICES**

For Cybersecurity consultation and questions, contact the SMPH Cybersecurity team.

- Risk assessments
- Procurement cybersecurity questions
- Policy and compliance questions
- Vulnerability management questions
- Options for securely transmitting data
- Options for securely transmitting data

SMPH Cybersecurity
Phone: 608-265-6677
Email: security@med.wisc.edu
  go.wisc.edu/smphcybersecurity

UW-Madison Office of Cybersecurity
Email: cybersecurity@cio.wisc.edu
  go.wisc.edu/uwcybersecurity

Securing Your Mobile Device
  go.wisc.edu/securemobiledevice

Safe Computing When Traveling
  go.wisc.edu/safetravelcomputing

LastPass
  go.wisc.edu/lastpass

IT Quick Tips Guides
  go.wisc.edu/itguides

> SMPH Cybersecurity
  go.wisc.edu/smphcybersecurity
> UW-Madison HIPAA Security
  go.wisc.edu/hipaasecurity
> UW-Madison IT Policies
  go.wisc.edu/itpolicies
> UW System Information Security Policies
  go.wisc.edu/systemitpolicies
> UW Health HIPAA Policies
  go.wisc.edu/uwhealthhipaa
> SMPH IT and HIPAA Policies
  go.wisc.edu/smphitpolicies
Contact the SMPH Shared Services IT team when you have advanced computer and IT support needs that DoIT cannot fulfill. Examples of support from Shared Services IT:

- Onsite hardware support
- Purchasing computer hardware or specialty software licenses
- Accessing SMPH network drives
- Content updates on supported departmental websites
- Lab computer set-up for supported labs
- Setting up new or removing departing employees' access

**NETWORK ACCOUNT AND PASSWORD**

Staff supported by SMPH Shared Services IT will have two network login ID options:

- UW NetID (Basic Sciences Departments)
- SMPH Network ID

All faculty, staff, and students are given a UW NetID (e.g., JLast@wisc.edu) when they are hired or enrolled. Use this to access your computer, email, MyUW, and other services contracted or developed by the University.

**MULTI-FACTOR AUTHENTICATION (MFA-Duo)**

UW-Madison requires you to verify your identity with the Duo multi-factor authentication app when logging into campus networks. Install Duo on your smart phone or tablet and set a print of backup login codes in case you lose your mobile device.

**E-MAIL ACCESS**

All UW faculty, staff, and students have an email address that is your NetID@wisc.edu. Your default email address is your NetID@wisc.edu.

**WIRELESS ACCESS**

Campus provides two wireless options. WiscVPN should be accessed when using a wireless network.

**Eduroam (Recommended)**

- Access secure wireless at any participating institution around the world
- Log in securely with UW NetID/password
- Devices can be configured to auto-connect
- More secure than UWNet wireless

**UWNet**

- Available in most UW campus buildings
- Log in securely with NetID/password
- Login only once per semester
- Offers guest registration option for non-University affiliates

**WORKING REMOTELY WITH WiscVPN**

UW-Madison provides tools that allow you secure access while working remotely.

**WiscVPN**

- WiscVPN should be accessed when using remote connections
- Allows you to connect to UW internal networks remotely
- Provides an extra layer of security when using outside and wireless networks

**Work Remotely with Web-Based Tools**

- UW's web-based tools, such as Office 365
- Box, and others, give you flexibility to work where you need
- Download Microsoft Office 365, campus antivirus, and other key software to your personal devices with your NetID

**CLOUD AND RESEARCH DATA STORAGE**

In addition to SMPH Shared Services IT network drives, SMPH strongly encourages storing your data on appropriate systems to ensure security and data longevity. For storing electronic Personal Health Information (PHI), please consult SMPH Cybersecurity.

**Box**

A cloud solution for storing, managing, and sharing files provided by UW-Madison.

**Google Drive**

Part of the UW-Madison G suite of tools that provides a cloud-based solution for storage and collaboration.

**Electronic Lab Notebooks (ELN)**

UW-Madison provides a digital notebook service called LabArchives to qualified users. Electronic Lab Notebooks can be used to record and document the research process and to manage digital research data.

**High Throughput Computing (HTC)**

Scalable computing resources, high-memory, GPU, and services for UW-affiliated researchers and their collaborators provided by the Center for High Throughput Computing (CHTC).