Last updated: March 2019

Using information technology

You are responsible for the computer and mobile devices you use during your studies at OHSU. If you wish to use a computer to access OHSU resources, please ensure that you are using an up-to-date, vendor-supported operating system. See *Private Wi-Fi (OHSU-Secure)* below for details on the various software required to connect to OHSU's private Wi-Fi network.

In addition, you must abide by OHSU's Acceptable Use of Computing and Telecommuting Resources policy. The following information will help you use your computing resources in line with that policy as well as OHSU's additional information privacy and security policies. For a complete list of policies, visit the Information Privacy and Security site on O2 (intranet) at https://o2.ohsu.edu/oips.

Wireless internet access

There are several ways to connect to wireless internet, whether you are on campus or on the go.

Shared Global Wi-Fi (eduroam)

The eduroam wireless network is a shared global wireless service for participating research and education institutions. Connect to the eduroam wireless network quickly and easily using your OHSU username and password at more than 450 colleges, universities and research facilities in the United States. Visit https://www.eduroam.us for a full list of participating institutions.

Connecting at OHSU is simple:

1. Turn on your device's **Wi-Fi.** (Disable Airplane Mode on smartphones and tablets.)
2. Connect to the **eduroam** wireless network.
3. At the login prompt, enter your complete OHSU email address and password. Connect to the eduroam network.
4. If you see a trust certificate prompt, accept it.
5. After your device connects to the eduroam network, you will have internet access.

Private Wi-Fi (OHSU-Secure)

OHSU-Secure is a secured wireless network that is provided for OHSU employees, students and affiliates. To access internal resources on the secure network, your computer must meet the requirements outlined below. Note that anti-virus software is also required, in addition to the specific software listed below.

BitLocker, FileVault or Symantec Desktop Encryption

Your computer must be encrypted with BitLocker, FileVault or Symantec Desktop Encryption.

- **BitLocker:** Available for Windows 7 Enterprise or Ultimate edition, Windows 8.1 Pro or enterprise edition, Windows 10 Pro, Enterprise or Education. Learn more.
- **FileVault:** Available for OS X 10.8 or newer. Learn more.
- **Symantec Desktop Encryption:** Available for Windows "Home" versions. Learn more.

ForeScout SecureConnector

SecureConnector must be installed and running. SecureConnector checks the encryption status of your computer and ensures it is compliant with security requirements. The ForeScout SecureConnector installers are available to download here.

Dell Data Protection

Dell Data Protection ensures that restricted information (see the *Protecting restricted information* section) cannot be moved from OHSU-Secure to unencrypted removable storage devices, such as USB sticks (thumb drives) and external hard drives. It can also be used to encrypt unencrypted removable storage devices. The Dell Data Protection installers are available to download here.

Public Wi-Fi (OHSU-Guest)

OHSU-Guest is an unsecured wireless network that is provided for OHSU patients, visitors, vendors and others who need internet connectivity. Because OHSU-Guest is outside of the secure network, it is not protected by the firewall. There, it should **not** be used by OHSU employees, students and affiliates.

Mobile device management

If you want to have your OHSU email delivered directly to an app on your smartphone, you must take steps to protect that mobile device: It must be enrolled in OHSU's mobile device management program. If you choose to enroll, you have a choice of two VMware applications:

- **AirWatch Container**, which "contains" your OHSU-related activities to specific apps. When you enroll your smartphone in AirWatch Container, the OHSU App Catalog will be downloaded to your smartphone as well. From there, you can install the Boxer app for access to your OHSU email, calendar and contacts. Other apps, including a secure web browser for access to internal resources, are also available.
- **Intelligent Hub**, which allows you to use your smartphone's built-in apps for OHSU-related activities. For example, if you have an iPhone, you can access your OHSU email, calendar and contacts through its Mail app. You can also use Safari to access other internal resources. In addition, be aware that some OHSU-related applications and technology may only be accessible through Intelligent Hub, rather than AirWatch Container.

Generally, these applications can run on mobile devices built by mainstream manufacturers, such as Apple, Samsung, LG, Motorola, Huawei and HTC, if they have one of the following operating systems: Android 8 or later or iOS 11 or later. Note: These requirements are subject to change over time.

You do **not** need Intelligent Hub or AirWatch Container to check your OHSU email at mail.ohsu.edu from a web browser on your smartphone; however, Duo Mobile may be required, depending on how your smartphone is connecting to the internet (see the *Two-step authentication* section for details).

To learn more, go to the personally owned mobile devices page on O2.

Two-step authentication

Two-step authentication (also called multi-factor authentication) is required to log in to certain OHSU systems from **outside** the OHSU-Secure wireless network — for example, when you log in to mail.ohsu.edu from your home Wi-Fi network or from eduroam. It is also required to remotely log in to applications that use single sign-on, including Banner, Box, Compass and Sakai.

OHSU uses Duo Mobile for two-step authentication. Duo Mobile is a free app that you can download from your smartphone's app store. If your smartphone is enrolled in AirWatch Container or Intelligent Hub as part of mobile device management, the Duo Mobile app is also available from the OHSU App

Catalog. Smartphone apps like Duo Mobile are popular tools for two-step authentication because of their convenience — if you have a smartphone, you probably don't go anywhere without it.

If you cannot or do not want to use the Duo Mobile app, you can request a security token (key fob). Send an email to duo@ohsu.edu, and please include your telephone number and your campus mail code (or your USPS address, if you do not have a campus mail code).

To learn more, go to the Duo Mobile page on O2.

Cloud storage

Box.com is OHSU's approved cloud storage service. You can use it to store your school-related files and share them with others. There is no storage limit, and you can upload files as large as 15 GB. To get started, log in directly at https://ohsu.box.com/ with your OHSU username and password.

Other common cloud storage services, such as Dropbox, Google Docs, OneDrive and iCloud, should **not** be used for OHSU restricted information (see the *Protecting restricted information* section), because these services have not agreed to comply with OHSU's information privacy and security policies.

To learn more, go to the Box.com page on O2.

Removable storage devices (e.g., thumb drives and external hard drives)

Removable storage devices, such as USB sticks (thumb drives) and external hard drives, must be encrypted with Dell Data Protection if they contain restricted information (see the *Protecting restricted information* section).

The Dell Data Protection software is required for computers that need access to internal resources on the secure network. It ensures that restricted information cannot be moved from the secure network to unencrypted removable storage devices. In addition, it can be used to encrypt unencrypted removable storage devices.

To learn more, go to the Dell Data Protection page on O2.

Additional resources

- Help and How To: Help and How To provides solutions for the most common information technology issues at OHSU, as well as FAQ on a variety of topics.
- Phish Bowl: The Phish Bowl is where you can find recent examples of phishing emails reported by others at OHSU. If you receive a suspicious email at your OHSU email address, report it by forwarding it to antispam@ohsu.edu. Also, be aware that OHSU occasionally sends phishing training exercises to help you practice identifying and reporting suspicious emails. Examples of past exercises are also accessible from the Phish Bowl.

Protecting restricted information

You are responsible for protecting all restricted information that you come across at OHSU. Restricted information is anything that is not meant for the public, such as information about patients, employees or students, and research data. Often, it is protected by federal regulations. For example, Protected Health Information (PHI) is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Last updated: March 2019

As a medical student, you may work with PHI and other kinds of restricted information during the course of your studies at OHSU. You can help keep that information safe by following these guidelines.

Text messages

Do **not** use mobile devices, such as smartphones, to text PHI. Mobile devices that are used to receive OHSU pages can and should be encrypted. Follow these instructions to encrypt an iOS or Android device. Note that these steps encrypt the **device** — not the pages it receives. Therefore, the following additional precautions should be taken:

- Limit PHI to the minimum necessary for effective patient care.
- Change your smartphone settings so that the "preview" does not display on the locked screen. If preview is set to "on" then any patient information sent may be viewable without authentication.
- Delete pages containing patient information after reading them.

Photos and videos

- Photos and videos of patients for personal purposes are not permitted.
- If photos are being taken for education purposes, the patient must sign a release prior to being photographed.
- If photos are being taken for treatment purposes, the photos must be incorporated into the patient's chart in Epic.

Additional tips

- Do not include any identifying patient information in written history and physicals (H&Ps) that you complete.
- Never send patient information to personal email accounts (e.g., Gmail, Hotmail).
- Only access the electronic health records of patients for whom you are directly providing care. Do not access the records of your family members or friends.

Be aware that failure to comply with HIPAA regulations may result in serious consequences, up to and including dismissal from medical school.
If you have questions about protecting restricted information, including PHI, contact the Information Privacy and Security Office at 503-49**4-0219** or oips@ohsu.edu.

If you see something, say something

OHSU is responsible for protecting the personal information of thousands of employees, students and patients. If you have a concern about the security or privacy of that information, report it as soon as possible. Even if you aren't sure something is really an incident, go ahead and report it — the privacy experts will take it from there.

What to report

Information privacy and security incidents happen when restricted information is accessed, acquired, used or disclosed without authorization. Some common examples include:

- Sending to the wrong address a fax or email that contains restricted information.
- Sending an unencrypted email that contains restricted information.
- Losing equipment that is used to store or work with restricted information, such as laptops, mobile phones, pagers and removable storage devices (e.g., thumb drives, external hard drives). This also includes cases of theft.
- Sharing OHSU network passwords, which is a violation of OHSU policy.
- Inappropriately accessing records in a patient-care tool, such as Epic.
- Inappropriately sharing PHI. Patients file complaints when they suspect the privacy of their information has been compromised — for example, if it has been verbally disclosed when it shouldn't have been.
- Storing PHI in unapproved cloud-based services. Remember, Box.com is OHSU's approved cloud storage solution.
- Inappropriately disposing of PHI, such as putting an after-visit summary in a recycling bin instead of a locked, confidential shred bin managed by OHSU.

How to report

To report a concern, contact the Information Privacy and Security Office at 503-4**94-0219** or oips@ohsu.edu. Alternatively, you may report a concern anonymously through the Office of Integrity.