# Information Privacy and Security Essentials 2020

OHSU postponed its annual information privacy and security training earlier this year to allow the OHSU community to focus its time and energy on the COVID-19 response. Due to ongoing Modified Operations, the Information Privacy and Security Office has prepared this shortened training document to serve as your annual training. It provides key reminders of your role in protecting information at OHSU.

## About the Information Privacy and Security Office

The Information Privacy and Security Office is here to support you. Contact the Office at oips@ohsu.edu:

- To ask specific questions about this document or about information privacy and security in general
- To report information privacy- or security-related incidents
- To access additional training resources

The Office also maintains OHSU's information privacy policies and information security policies, which are based on HIPAA and other federal and state regulations. These policies help you understand how to protect certain types of information that you use in your role at OHSU.

## Guidelines for protecting PHI while teleworking

Many OHSU members are teleworking now due to Modified Operations. Remember, OHSU's information privacy and security policies apply no matter where you are working — on campus, at home or at another offsite location. Please read the policies carefully and contact your manager if you have any questions.

Follow these tips to help keep OHSU information safe and secure while teleworking:

- Ensure you have a private space to do your work, so that your family members, roommates or friends will not inadvertently view any PHI or overhear any conversations about patients.
- If you need to use identifiers in a conversation, keep them to a minimum and use identifiers like initials or MRNs that are less likely to re-identify a patient if accidentally overheard.
- Keep any paper documents with PHI in a secure, locked location that your family members, roommates or friends cannot access.
- Do not dispose of paper PHI at home. Paper PHI must be confidentially shredded, so keep it secure while at home and bring it back to OHSU for disposal in one of the locked shredding bins available around campus when you can.
- Do not print or scan PHI using personally owned printers or scanners at home. These devices have "memory" and can maintain a copy of the item you are printing or scanning. Speak with your manager if you have questions about your workflows.
- Use Box.com, which is the only OHSU-approved cloud storage vendor for restricted information.
- Do not use your personal email or calendar accounts (such as Gmail, etc.) for OHSU business.
- Do not forward your OHSU email to your personal email account (such as Gmail, etc.).

## Recent phishing trends

Phishing is a kind of fraud designed to trick you into sharing valuable information, such as your credit card number or your network username and password. Phishing takes many forms, including emails, websites, telephone calls and text messages.

In recent months, cybersecurity firms have reported a wave of phishing attempts specifically related to COVID-19. These have been reported at OHSU, as have fraudulent emails that appear to come from fellow OHSU members. This practice is known as “spoofing.” Often the "From" field shows the name of an OHSU manager or department chair, along with an unfamiliar email address. The idea is to make it look like someone at OHSU is asking you to complete a work-related task or help with a personal favor.

To learn more about phishing, visit the Phish Bowl on O2.

## Access PHI for work responsibilities only

Your role at OHSU may require that you access and use PHI. You are responsible for limiting your access and use to only the PHI that is required for your role. Epic and other patient-care tools are monitored for inappropriate activity. For example, you may not use Epic, axiUm or other patient-care tools to access your family members’ (including children) health records, even if you have authorization from those family members. You may view your own health information using these tools, but you may not modify, amend, correct or delete any part of your own record, including your contact information. OHSU strongly encourages you to use patient-facing tools like MyChart to manage your own health information.

To learn more about acceptable access, use or disclosure of PHI, visit the Information Privacy and Security page on O2.

## Care relationships

It’s natural to feel a strong connection with your patients as you help them navigate through some of their most difficult and vulnerable moments with dignity and respect. It’s important to balance the compassion that you feel for them with the good judgment to know when you may, and may not, access their information. For example, curiosity — wanting to know how someone is doing after leaving your care — is never an appropriate reason to access a patient’s information. If you are unsure whether you may access a record as part of your role, speak with your manager first.

## Incident reporting and non-retaliation policy

If you see something, it is your duty to say something — even if you aren’t sure whether it is really an information privacy and security incident. Self-reporting is also expected and encouraged.

Information privacy and security incidents include, but are not limited to the following: misdirected faxes or emails, lost/misplaced paper PHI, inappropriate access to health records and lost/stolen electronic devices, such as pagers, USB drives, cell phones and laptops.

Report every potential incident promptly, but **no later than 24 hours** of learning about it. The sooner you notify the Information Privacy and Security Office, the sooner it can take steps to limit the impact of an incident. Report incidents to the Information Privacy and Security Office at 503-494-0219 or oips@ohsu.edu. To report anonymously, call 1-877-733-8313 or visit www.ohsu.edu/hotline.

**Important:** OHSU policy prohibits retaliation for reporting information privacy and security incidents (see IPP-07 Refraining from Intimidation or Retaliation). If you feel you have experienced retaliation for reporting an incident, contact the Information Privacy and Security Office at 503-494-0219 or oips@ohsu.edu.