Privacy Awareness

October 2021

Privacy & Security Reports

Faculty, staff, and students are required to report any potential or suspected Privacy or IT Security incident:

privacy@cumc.columbia.edu

security@cumc.columbia.edu

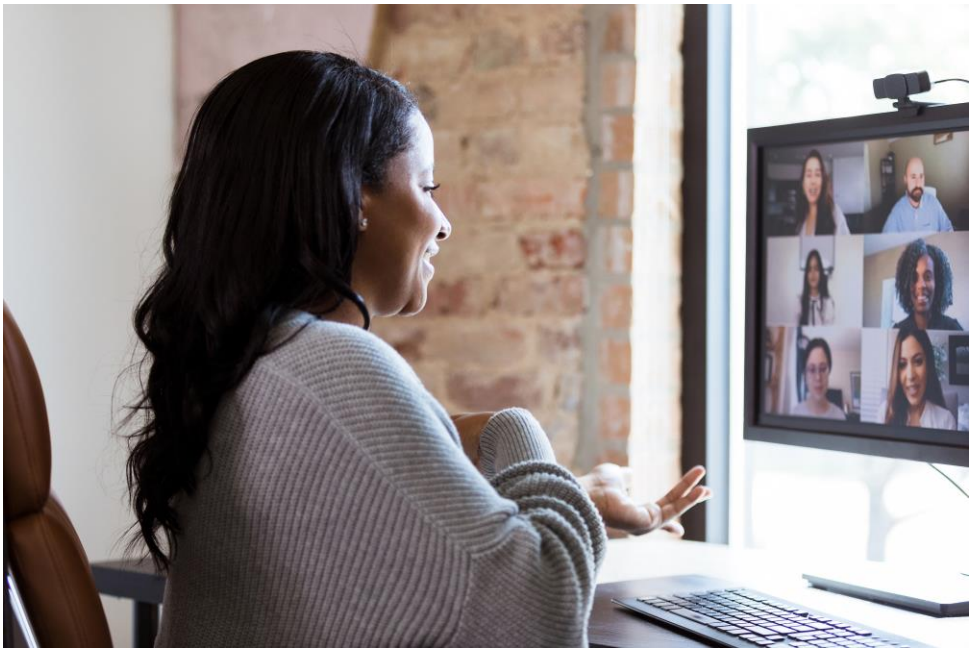
EXAMPLES

- Unauthorized access or disclosure of patient information
- Loss or theft of a device
- Misdirected email or fax
- Patient information in the wrong patient record
- Suspicious computer behavior = Cyberattack

Remote Work

Patient Privacy at Home

A significant number of healthcare workers continue to work remotely. While there are benefits to remote work, there are also significant challenges and risks.



What do I need to think about when working at home?

Multiple electronic devices, paper documents, video & audio privacy

REMOTE WORK PHYSICAL ENVIRONMENT

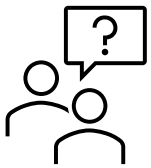
- ✓ Private Space with ear or headphones
- ✓ Lock screen / Log off device when leaving workstation
- ✓ Secure paper documents in a locked drawer/cabinet
- ✓ Do not use unapproved text messaging services to discuss patient or other sensitive information
- ✓ Paper documents must be shredded or securely discarded

Contact Us

Privacy Office
Columbia University
630 West 168th Street
Box 159
New York, NY 10032
(212) 342-0059
privacy@cumc.columbia.edu
https://www.hipaa.cuimc.columbia.edu/

RESOURCES

- **CUIMC Physical Privacy Guidelines**
- **Remote Work - CUIMC IT (service-now.com)**



Q & A

Q. What should I do if I'm notified of a misdirected email or fax with PHI (patient information)?

A. Notify your manager or the Privacy Office. Do **not** reply to the unintended recipient before obtaining further instructions.

Q. Can I send patient information in an unencrypted email?

A. A patient has the right to request to receive unencrypted email. This must be documented in the medical record. When emailing to anyone other than the patient or their designated representative, add **#encrypt** to the Subject line when sending patient information to an external email address (does NOT end in @cumc.columbia.edu, @nyp.org or @med.cornell.edu). **DO NOT** include PHI (e.g., name, MRN, DOB) in the Subject line of an email.

Downloading, exporting and storage of PHI

Q. If I'm using a registered personal device to work remotely, can I save PHI on my device?

A. No, PHI and all CUIMC business documents must be saved on CUIMC IT approved systems, including department network share drives, Microsoft Teams, SharePoint or OneDrive. Contact CUIMC IT for additional information.

Q. What is the policy associated with transporting electronic devices or documents containing PHI?

A. All electronic devices and paper documents used for CUIMC business must always be secured. Electronic devices must be registered and devices with access to PHI must be encrypted. Electronic devices and paper documents cannot be left in locked vehicles (e.g., glove compartment, trunk) or checked in airport luggage. Transporting paper documents containing PHI is prohibited unless required for clinical, regulatory or an approved business need.