This Appendix covers procedures for reasonable safeguards of PHI, which includes information on PHI storage, PHI disposal, email and other safeguards.

Reasonable Safeguards Procedures

The HIPAA regulations permit incidental uses and disclosures of PHI that occur as a by-product of another permissible use or disclosure as long as reasonable safeguards are applied. All UC employees are expected to use professional judgment based on their job on a case by case basis to determine what reasonable safeguards to apply.

1. PHI Storage

   A. Patient charts, records, reports, images, and other documents or media containing PHI must be stored securely. The means for securing such information must be appropriate to the location and risk of unauthorized access. For example, files and charts containing PHI must not be accessible in public areas and should be locked when not in use.
   B. Paper records that are placed outside a patient’s room in clinical areas should be placed with the name facing the wall.
   C. In secure areas, PHI should be put away or locked in the desk or office when not in use. In non-secure areas patient records that are in use with an employee present should be turned face down when not in direct use and filed or disposed of properly when no longer needed.

2. PHI Disposal

   A. Secure methods must be used for disposal of PHI. This applies to all types of PHI including paper, electronic and other forms such as plastic, labels and other materials containing or printed with PHI.
   B. Paper PHI should not be disposed of in the regular trash, recycling bin or hazardous waste bin.
   C. Secure methods for disposing of PHI including shredding of paper PHI or disposal in a locked shred bin provided by a reputable vendor.
   D. If accessible to the public, shred bins must be locked and secured to prevent access.
   E. For disposal of media containing electronic PHI refer to the guidelines of the information security department.

3. Displays of PHI / Computer Screens
A. Computer screens should be positioned so that PHI is not easily viewed by unauthorized persons.
B. Log out of computer when finished using PHI. Computers should not be left unattended when logged in to patient records.
C. Log-in information or passwords should never be shared with anyone else.

4. Conversations

A. Staff should not discuss PHI in elevators, hallways, where other individuals are present and in public areas.
B. When circumstances permit, speaking should be in private.
C. Private areas should be used to discuss patient condition with patients' family and friends.
D. For discussion of PHI with a patient when there is another person present with the patient informs the patient the discussion may disclose PHI and either:
   i. The patient should be asked if they would like the person present during the conversation; or
   ii. The person present with the patient should be asked to leave the room during your discussion with the patient.

5. PHI transfer from location to location

A. PHI carried from location to location between facilities must be secured during transfer. Employees who physically deliver records are responsible to ensure that the PHI is left at the destination in a secure manner. During transfer the PHI should be in a sealed envelope marked “Confidential” and should clearly indicate the name and location of the intended recipient and sender.
B. PHI that is taken out of the institution must be secured and locked up on transfer, for example in the trunk of the car.
C. PHI that is transferred between locations should contain contact information within on what to do if the information is lost or misplaced and someone finds the PHI.

6. Printers

A. Printers should be located in a low traffic area that is not accessible to those not authorized to receive the information.

7. Fax Machines

A. A UC fax cover sheet must be used with all faxes sent that contain PHI. The cover sheet must contain a confidentiality statement and contact information for the recipient in the event the fax is received in error.
B. Fax machines should be located in a low traffic area that is not accessible to those not authorized to receive the information.
C. The fax number of the recipient should be confirmed prior to sending a fax by calling the person or office to which the fax will be sent.
D. When faxes are regularly sent to the same recipients or the numbers are programmed into the machine's memory, the numbers should be checked regularly to verify that the number is still in operation.

8. Sign in lists
   A. A sign in list is permitted as long as there is no PHI displayed on the sheet.
   B. Information on the sign in sheet must not include any information that includes diagnosis or condition.

9. Email
   A. Emails sent to the following partner sites are automatically secured: UCHealth.com, UCPhysicians.com, and CCHMC.com (Cincinnati Children's Hospital Medical Center).
   B. To ensure that emails to other sites over the internet are sent in a secure manner, type the work encrypt as the first word in the subject line.
   C. Place a confidentiality statement on the email and contact information for the recipient in the event an email containing PHI is received in error.

10. Voice Mail and Answering Machines
    A. It is permissible to leave a message with a family member or other person that answers the patient's telephone, on an answering machine or on a voice mail when the patient does not answer the telephone.
    B. The information should be limited to the minimum necessary amount of information.

11. Laptop and Personal Computers
    A. Laptop and personal computers must have an encrypted hard drive if PHI is saved to it.
    B. PHI may only be saved to a flash drive or thumb drive that is encrypted.

12. Mobile devices
    The reasonable safeguards for protection and security of mobile devices include the following:
    A. A password or other user authentication should be used.
    B. Encryption should be installed and enabled to protect PHI stored or sent by mobile devices.
C. Remote wiping and/or remote disabling should be installed and activated to erase data on your mobile device if it is lost or stolen.
D. File sharing applications should not be installed or must be disabled.
E. A firewall should be installed and enabled to block unauthorized access.
F. Security software should be installed and enabled to protect against malicious applications, viruses, spyware and malware-based attacks.
G. Security software should be kept up to date.
H. Mobile applications should be researched before downloading.
I. Physical control of your mobile device should be maintained. User should know where it is at all times to limit the risk of unauthorized use.
J. Users should ensure adequate security to send or receive PHI over public Wi-Fi networks.
K. Users should delete all stored PHI before discarding or reusing the mobile device.

**Business Associate Agreements**

A business associate agreement must identify the uses and disclosures of PHI the business associate is permitted to make and requires the business associate to implement safeguards to protect against a use or disclosure of PHI not permitted by the agreement. UC must take certain actions if a business associate materially violates the Business Associate Agreement.

1. **Business Associate Identification:** Prior to entering into an agreement or contract with an outside entity who will perform a service for or on behalf of University of Cincinnati that will receive or use PHI in order to perform this activity or service, determine if a business associate agreement is required.
   A. Some examples of business associates are: data analysis or aggregation companies, third-party billing companies, collection agencies, outside legal services, actuarial services, accounting services, consulting services, nursing and other professional temporary staffing agencies, temporary office staffing and accreditation services. An example of who is not a business associate is an outside service that is not given PHI in order to perform services for UC. If unsure whether an individual or entity is a business associate, contact the UC Privacy Officer or Office of General Counsel for guidance.
   B. If a Business Associate Agreement is required, use the standard UC Business Associate Agreement form (see Related Links).

2. **Signed Agreement Required:** The Business Associate Agreement must be in writing and contain the signature of the business associate.

3. **Notice of Breach:** On receipt of information that business associate has violated the business associate agreement, the employee receiving the information must notify UC Privacy Officer. The Privacy Officer will investigate the alleged violation and take the necessary actions to cure the breach or end the violation. If the
business associate agreement was materially breached, actions may include termination of the underlying contract. If termination is not feasible, the Privacy Officer may report the violation to the Department of Health and Human Services, Office for Civil Rights.