Guidelines for Protecting PHI

Public viewing

- Create areas for paper charts and other written materials containing PHI that will not be in view or easily accessed by persons who do not need the information. If charts or other documents cannot practicably be kept in a secure area during use (e.g., while being analyzed) then establish a practice of turning documents over to minimize incidental viewing.
- Locate printers, copiers and fax machines in areas that minimize public viewing. Promptly retrieve documents containing PHI to minimize viewing by persons who do not need the information.
- Locate computer screens and monitors in areas or at angles that minimize viewing by persons who do not need the information. Utilize privacy screens and/or screen savers as practicable.
- Locate whiteboards that may be used to display PHI in areas that minimize viewing by persons who do not need the information
- Do not leave materials containing PHI in conference rooms, out on desks, or on counters or other areas where the PHI may be accessible to persons who do not have a need to know the information.
- In areas where PHI is maintained, escort patients, repair and delivery representatives and any other persons not having a need to view the PHI. Before providing a fax or copier repair representative access to a machine, ensure that no PHI has inadvertently been left on the machine

Preventing conversations about PHI from being overheard

- Refrain from discussing PHI beyond that which is the minimum necessary to conduct business.
- Keep voices down when discussing PHI.
- Refrain from discussing PHI in public areas such as elevators and reception areas, unless doing so is necessary to provide treatment to one or more patients.
- Utilize private space (e.g., separate rooms, sound-reducing barriers) when discussing PHI with workforce members, patients or research subjects.
- Do not relay or discuss PHI over the phone unless you confirm the identity of the person to whom you are speaking and their authority to receive the PHI being discussed

Storage and disposal of documents that contain PHI

- Maintain documents containing PHI in locked cabinets or locked rooms when the documents are not in use and/or after working hours.
- Establish physical and/or procedural controls (e.g., key or combination access, access authorization levels) that limit access to only those persons who have a need for the information.
- Control and secure keys to locked files and areas. Do not leave keys in locks or in areas accessible to persons who do not have need for the stored PHI.
- Promptly shred documents containing PHI that are no longer needed. Do not place documents containing PHI in trash bins.
- Master lists and key codes should be secured separate from PHI data.

Safeguarding computer workstations and databases that contain PHI

- Establish controls that limit access to PHI to only those persons who have a need for the information.
- Exit any database containing PHI upon leaving work stations so that PHI is not left on a computer screen where it may be viewed by persons who do not have a need to see the information.

- Do not disclose or release to other persons any item or process which is used to verify authority to create, access or amend PHI, including but not limited to, any badge, password, personal identification number, token or access card, or electronic signature.
- Follow instructions of UTO to update and change passwords and to install security updates.
- Delete or erase PHI from any computer drive as soon as the PHI is no longer needed.

Faxing PHI

- Fax PHI only when other types of communication are not available or practical.
- Limit the PHI contained in the fax to the minimum necessary to accomplish the purpose of the communication.
- When faxing to a patient, do not fax sensitive PHI such as PHI related to alcohol abuse, drug abuse, mental health issues, HIV testing, antigens indicating hepatitis infection, sexually transmitted diseases (STD), or presence of malignancy.
- Do not use faxing as a means to respond to subpoenas, court orders or search warrants.
- Take reasonable precautions to ensure that the intended recipient is either available to receive the fax as it arrives or has exclusive access to the fax machine.
- Pre-program frequently used non-patient fax numbers to minimize potential for misdirected faxes. Confirm pre-programmed numbers at least every six (6) months.
- If there is any reason to question the accuracy of a fax number, contact the recipient to confirm the number prior to faxing PHI.
- When faxing PHI, use fax cover sheets that include the following information:
    - Sender's name, facility, telephone and fax number
    - Date and time of transmission o Number of pages being faxed including cover sheet
    - Intended recipient's name, facility, telephone and fax number
    - Name and number to call to report a transmittal problem or to inform of a misdirected fax
    - If notified of a misdirected fax, instruct the unintended recipient to mail back the information or destroy the information by shredding
    - Confidentiality notice such as the following:
      Confidentiality Notice: The information contained in this facsimile transmission is privileged and confidential intended for the use of the addressee listed on the cover page. The authorized recipient of this information is prohibited from disclosing this information to any other party and is required to destroy the information after its stated need has been fulfilled. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited (Federal Regulation 42 CFR, Part 2, and 45 CFR, Part 160). If you have received this fax in error, please notify the sender immediately by calling the phone number above to arrange for return of these documents.
- Do not include any PHI on the fax cover sheet.

E-Mailing PHI

- E-mail should not be used for sensitive or urgent matters. Topics appropriate for e-mail include appointment scheduling and routine follow-up questions.
- Under state law, e-mail cannot be used to convey the results of tests related to HIV status, sexually transmitted diseases, presence of a malignancy, presence of a hepatitis infection, or abusing the use of drugs.

- If possible, do not transmit PHI via e-mail unless using an IT-approved secure encryption procedure. If a secure e-mail server is not used, do not e-mail lab results.
- Limit the PHI contained in the e-mail to the minimum necessary to accomplish the purpose of the communication.
- E-mail PHI only to a known party (e.g., patient, research subject, health care provider).
- Prior to e-mailing PHI to an individual:
    - Obtain the individual's consent prior to communicating PHI with him or her even if the individual initiated the correspondence; and
    - Clearly communicate to the individual the risks and limitations associated with using e-mail for communications of PHI.
- When e-mailing to a non-health care provider third party, always obtain the consent of the individual who is the subject of the PHI.
- Do not e-mail PHI to a group distribution list unless individuals have consented to such method of communication (e.g., group therapy communications).
- Send PHI as a password protected/encrypted attachment when possible.
- In the subject heading, do not use patient names, identifiers or other specifics; consider the use of a confidentiality banner such as "This is a confidential medical communication".
- If PHI is received in an e-mail, include a copy of the e-mail in the patient's medical record, if applicable.
- Include in e-mail stationary a confidentiality statement such as the following:
  Confidentiality Notice: *This e-mail transmission, and any documents, files or previous e-mail messages attached to it, may contain confidential information. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this message is STRICTLY PROHIBITED.* ***If you have received this transmission in error, please immediately notify us by reply e-mail or by telephone at (XXX) XXX-XXXX, and destroy the original transmission and its attachments without reading them or saving them to disk.***

Terminating an employment, contract or position

Upon termination of employment or contract, or upon termination of authorization to access PHI, ensure that workforce members:

- Return any and all copies of PHI in their possession or under their control;
- Return any keys, badges, codes, or other tools used for the purpose of accessing PHI to which they no longer are authorized;
- Are excluded from access to databases or other applications to which they are no longer authorized (e.g., disable access codes, numbers).

Data provided courtesy of Stanford University. See https://med.stanford.edu/ric/resources/hipaa-primer.html