Audits, Investigations, and HIPAA Privacy

The University’s Safeguards Policy covers three main areas of HIPAA compliance. The focus of this summary is Technical Safeguards, specifically email. The University is required to have in place reasonable safeguards to (1) limit access to e-PHI to authorized individuals and (2) protect against unauthorized disclosures of e-PHI. These safeguards include, at a minimum, those below. Each HCC, however, must put in place additional safeguards, based on the clinic or area technology used, operations, types of services provided, and nature or information maintained.

1. An individual with a law enforcement badge is requesting patient records.
   a. Even individuals with badges (police, FBI, FDA) must meet the requirements of HIPAA in order to access PHI. A badge alone is generally not sufficient to entitle someone to access PHI.
   b. University procedure requires that you notify your supervisor, who will contact the University’s Privacy Official or the Office of Legal Counsel to notify them of the request prior to releasing any information.
   c. Make a copy of the individual’s badge and business card, and log any disclosures approved by the Privacy Official or Legal Counsel in the Accounting of Disclosure log for the patient whose records are accessed. (OU Physicians clinics release PHI only through OUP OKC Central Medical Records or OUP-Tulsa Medical Records offices.)

2. One of the University’s external auditors is requesting to review patient records.
   a. Do not release any information to an external auditor until your supervisor tells you it is permissible to do so.
      1. The University’s contracts with its external auditors and with entities that have an audit right (such as OHCA) include Business Associate (BA) or confidentiality language, as appropriate, that enables the auditor to view PHI based on their agreement to maintain the information in confidence.
      2. The auditors should be able to show the clinic supervisor a copy of the contract, or, if they cannot, the Purchasing Department can confirm for the supervisor that the University has an agreement with BA language in it in place.
      3. If a supervisor is not confident that release of PHI is permissible, the supervisor should contact the University’s Privacy Official or the Office of Legal Counsel. (OU Physicians clinics may also contact the appropriate Medical Records office.)
   b. Do not give external auditors your password or log on for them. The clinic supervisor and IT will develop a means of access for the auditors.

3. Another University employee is requesting access to patient records for a University business purpose.
a. All University employees are NOT entitled to access patient records. Employees must be employees of a Health Care Component within the University (see list on NPP) and must have a legitimate right under HIPAA to access the PHI.
   i. If you are not certain that an OU employee is entitled to have access to the PHI requested, check with your supervisor, the University’s Privacy Official, or the Office of Legal Counsel.
   ii. Keep in mind that if you provide access to PHI to individuals who are not authorized to have the PHI, you are individually responsible for any resulting breach. If you are not sure, please ask!!

4. I’ve received a subpoena or other legal request for patient records.
   a. Be aware that an Authorization may still be required, even though a subpoena has been issued.
   b. Send the subpoena or court order to the Office of Legal Counsel as soon as you receive it. (OU Physicians clinics may send the subpoena or order to OUP Medical Records.)
   c. Do not release any PHI until you are asked to do so by the Office of Legal Counsel or OUP Medical Records, as appropriate.