Physical Safeguards Summary

The University's Safeguards Policy covers three main areas of HIPAA compliance. The focus of this week's summary is Physical Safeguards. The University is required to have in place reasonable safeguards to (1) limit physical access to PHI only to authorized individuals and (20 protect against unauthorized disclosures of its PHI. These safeguards include, at a minimum, those below. Each HCC, however, must put in place additional safeguards, based on the clinic or area configuration, operations, types of services provided, and nature of information maintained.

1. **Paper Records that Contain Protected Health Information (PHI)**

    a. Paper records that contain PHI must be stored in a *locked cabinet or room*.
    b. Paper records that contain PHI must not be left in *unattended areas*, such as on a desk or in an unlocked recycling bin in a common area.
    c. Paper records that contain PHI must be placed *face down*, even in attended areas, such as the check-in and check-out areas.
    d. Paper records that contain PHI *may not be removed* from the campus or clinic for the convenience of employees. (All areas should have a check-out procedure to be used when such records must be taken from the campus or clinic for University business purposes.)
    e. Theft or loss or unauthorized disclosures involving paper records that contain PHI *must be reported immediately* to the supervisor and/or Privacy Official. Supervisors (excluding OU Physicians clinic supervisors) will notify the Privacy Official directly; supervisors of OU Physicians clinics will report the incident in the complaint/compliment system on the OU Physicians intranet.

2. **Individuals in Areas Where PHI is Located**
    a. All visitors and patients who will be in areas where PHI is located *must be escorted* at all times.
    b. Pharmaceutical and sales representatives, maintenance staff, and vendors who will be in areas where PHI is located *must be escorted at all times*.

3. **Computers/Work Stations that Contain PHI**
    a. Computer monitors must be positioned so that PHI on the screen *cannot be viewed* by unauthorized individuals. (A privacy screen may also be used.)
    b. Computers that contain PHI must be returned to a *password-protected screen saver or login screen* when they are not attended, even if only for a few minutes.