Physical Security of PHI

• Paper PHI
  • Baskets/bins/mailboxes with medical records, patient labels, etc. should not be easily viewable or accessible
  • PHI secure when no one is around (i.e. locking up at night when clinic closes)
  • Transporting PHI (use of approved courier; should not be transporting without prior approval)
  • Shred bins (shred vs. recycle); emptying personal shred bins into locked bins at the end of shift or at the end of the day
  • Thank you cards; Culinary food slips; pt labels on food/drinks in visitor/patient fridge
  • Copy machine, fax printers placed in secure/non-public areas
Physical Security of PHI

• Electronic PHI
  – Locking/suspending computer or Cerner when walking away
  – Do not share passwords/credentials or have them easily accessible or viewable by others
  – Positioning of computers; Privacy screens
  – Unapproved cloud servers; forwarding of emails with PHI; texting PHI

• Other
  – Whiteboards (minimum necessary PHI)
  – Door keypad codes changed routinely