

HIPAA TIPS Steps to Making Health Information more Secure

Here are some practical tips to help keep protected health information (PHI) private. These tips relate primarily to keeping information from being accidentally disclosed to other staff and clients/patients that do not need to know it. This list is not intended to address all standards and requirements for this area, and the tips are not intended as mandatory items. Privacy protection is about reasonable steps to eliminate the amount of PHI that is accessible. Above all, use good discretion and treat all PHI as if it were sensitive health information about you.

PHI in the Office or on the Desk

- Where practical, limit discussions of PHI in open and/or informal areas
 - Use frequently empty conference rooms, small alcoves, or unused cubicles if available
 - Try not to repeat entire situations or recite already known facts
 - When planning space or moves, and in larger office/areas consider clustering staff with the same roles and/or needs to access PHI together
- When discussing PHI in open areas:
 - Lower voice
 - Small dividers, plants, or clustering chairs, etc. make it easier to talk to certain individuals without everyone overhearing
 - Consider background music or other noise to filter sound
- Public area announcements or broadcast system
 - Decide on what type of information to use and how to use it- this communication is valuable and not prohibited, but should be limited in nature (e.g. just last name, page to a certain location or area, or Mr. Jones to Pharmacy please, instead of: Mr. Jones your <specific drug prescription> is ready or see administration for <specific benefit application>).
- Calling clients/members/patients
 - Decide appropriate locations and whether staff can be in a cubicle or not, facing public areas or other filters in place for routine incoming/outgoing calls
 - Decide what information to leave with others or on answering machine. Again, this communication is valuable and not prohibited (unless restriction is in place), but it should be limited. (Eg. Please have Mr. Jones call <staff name/ number>, or appointment reminder for Tuesday, call <staff name/number> for questions, instead of: Mr. Jones' test results are positive, or application for benefits is denied, or Mr. Jones has an exam for <specific procedure> on Tuesday).
- Decide if a clean desk policy (at end of work shift) is feasible for some or all staff
- Use a cover sheet or protector for telephone notes, files, notebooks, or clipboards that need to be left out or are accessed by multiple staff members
- If working files, papers, and other materials need to be left out or are stacked on a desk, turn them over (or use coversheet)

- Store PHI documents in cabinets or drawers
- Close paper file cabinets, drawers, or file rooms when not in use and lock, if practical (when not in use or at end of work shifts)
- Keep PHI separated from other types of information.
- Depending on amount of access and number of people, use shredders, locking or secure recycle or shred containers, or clearly marked disposal bins for holding confidential materials that are no longer needed
- Securely dispose of confidential materials, including documents, reports, sticky notes, telephone and fax messages: (e.g. use office shredder or secure recycle/shredding service)
- Where physical barriers or safeguards are impractical, talk to staff about what is expected in terms of access.
- Make sure staff understand policies for use, disclosure, storage, and disposal.

PHI On Computer/Electronics

- Faxes or Printers
 - Where shared, consider moving to the least public area available
 - Request staff to regularly check and monitor their own print/fax jobs
 - Use Fax cover sheets with confidentiality notice and request to return/destroy if sent unintentionally
 - Auto-print transmission reports to document where fax was sent
 - For unfamiliar or non-routine (or all) faxes, call to confirm receipt
 - Program auto-dial with frequently used numbers to reduce error in dialing, call ahead and verify non-routine numbers
 - Request senders to call ahead so staff know when to check for faxes
 - Create “in-boxes” and designate responsibility to check and distribute documents regularly, and/or
 - Shred or safely dispose unclaimed items regularly (set time)
- Face monitors away from public/all employee view, or consider
 - strategic location of cubicle partitions, plants or other objects
 - purchasing privacy monitor screens, and/or
 - timed screen-savers and log-outs
- Use timed screen savers
- Close documents or programs with PHI when not in use
- Sign off or log out of computer workstation when leaving it (even for breaks),
 - Consider automatic or timed screen-savers and log-outs
- Use Passwords
 - Individual passwords or role based where necessary
 - Establish password rules related to changing, emergency access, forgotten, etc.
 - Enforce no sharing, no accessible written password

- Work on strong passwords, but be practical
 - If staff need help remembering, have generic or specific reminder questions (not the answers) that can be referenced
- Consider limiting or excluding PHI in e-mail¹
 - If using, consider verification techniques and address books (pre-set addresses) to limit sending to wrong address
 - Consider encryption of external email with PHI
- Regularly Back-up data
 - Set up a schedule
 - If you use CD or other storage media, designate a secure, separate (off-site if possible) place, and label adequately
 - If you use on-line service, contact or review their security and timing
- Label and track equipment
 - Keep a list of all equipment and software purchases (computers, monitors, printers, laptops, faxes, PDAs, peripherals, cell phones, pagers, etc). Should include Name and Manufacturer, purchase date/location, Serial number, in separate, secure place.
 - Label each piece with identifying information (use etching, permanent marker, sticker, etc).
 - Update list regularly, including when equipment is sold or disposed of
- Ensure data is purged or equipment destroyed when disposing of old equipment

PHI On the Go

- Decide if and where it is feasible to limit removal of documents with PHI from the office/facility.
- Where documents are removed, are copies feasible or sufficient instead of originals (in the event of loss or damage the original would still be available).
- Use lock-able carrying cases or file holders
- Set return dates and track removed documents until returned or destroyed
- Decide what information and/or software should be on portable electronics.
- Protect access with passwords (user log-on, and/or program specific, etc).
- Decide what information or software can be accessed remotely (e.g. through internet) and whether encryption or other protection is available when transferring PHI.
- Use same protections, where applicable, as office for PHI in remote locations (e.g. storage and disposal requirements).
- Track usage of portable equipment and return dates, if temporary uses

¹ The security rule, when final may define further requirements for electronic security and sending PHI over networks (internal and external).