Unit Name:

Location:

This document is designed as a checklist that can be used to determine privacy and security risks on a walkthrough of a facility.

To use this checklist it is suggested that you:

1. Print this document and carry on the walkthrough
2. During walkthrough, place checkmarks or x’s in the Yes/No column
3. Get additional information from facility staff member about items that are not visibly apparent or about policies and procedures controlling access to the facility
4. Make any additional notes in the Notes column
5. Provide a copy of this checklist to the HIPAA Privacy Officer at [HIPAA@ucdenver.edu](mailto:HIPAA@ucdenver.edu) along with a plan to address any issues of concern.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Storage** | | Yes | | No |
| Are documents stored in boxes under desks, on window sills or in other unlocked  storage areas? | |  | |  |
| Does it have long-term storage with? | |  | |  |
| Does the unit use an off-site facility for long-term storage? | |  | |  |
| - Can manager retrieve any document from long-term storage within two working  days? | |  | |  |
| Are patient lists, such as schedules, readily visible by patients or visitors? | |  | |  |
| Are documents containing PHI left out on desktops clearly visible to patients or visitors? | |  | |  |
| Are documents stored in locked filing cabinets? | |  | |  |
| Are file cabinets locked each evening at close of business? | |  | |  |
| **Printers** | | | | |
| Does staff print to printers located within the unit area? | |  |  | |
| - If not, are printers shared with or located in another unit? | |  |  | |
| During the walk-through, are there any documents on the printers waiting to be picked up? | |  |  | |
| - If so, how long has the oldest document been left at the printer? Indicate elapsed time: | |  | | |
| Are printers located in a common area or near a corridor through which visitors or staff from other units often pass? | |  |  | |
| **Fax Machines** | | | | |
| Does staff use a fax machine within the unit area? | |  |  | |
| - If not, is the fax machine shared with another unit? | |  |  | |
| Are there any documents on the fax machine waiting to be picked up? | |  |  | |
| - If so, how long has the oldest document been left at the fax machine? Indicate  elapsed time: | |  | | |
| Is the fax machine located in a common area or near a corridor through which visitors or staff from other unit often pass? | |  |  | |
| Does a staff person attend the fax machine on a regular basis throughout the day? | |  |  | |
| Is there evidence that staff uses cover sheets when transmitting faxes? | |  |  | |
| **Document Disposal** | | | | |
| How does the unit dispose of documents containing PHI? Indicate method(s): |  | | | |
| If disposed of by a means other than individual wastebaskets, are special collection bins  provided? | |  |  | |
| - Are collection bins kept locked? | |  |  | |
| - Are collection bins full to overflowing? | |  |  | |
| - Are documents placed next to or on top of collection bins? | |  |  | |
| **General Security** | | | | |
| Are unit staff permitted to take documents or files containing PHI off site or at home? | |  |  | |

|  |  |  |
| --- | --- | --- |
| Does staff deal with PHI on the telephone? Can calls be overheard? |  |  |
| Is confidential information discussed by staff in public areas? |  |  |
| Are all staff wearing name badges? |  |  |
| Do any staff cubicles or workstations open directly onto a common corridor? |  |  |
| Are subject or patient interviews conducted in the unit? |  |  |
| - is there a private interview space available for subject or patient interviews? |  |  |
| Is the Notice of Privacy Practices posted in areas where patient registration is performed? |  |  |
| Are visitors authenticated and escorted or monitored? |  |  |
| Are there physical restrictions to access areas containing PHI? |  |  |
| How: |  |  |
|  |  |  |
| **Information System Security** | | |
| For PCs, are screen savers in use? |  |  |
| - After what period of time do screen savers start? Indicate elapsed time: |  | |
| For PCs and terminals, does each user have a defined ID and password? |  |  |
| Is there evidence of IDs or passwords written down and left at workstations? (e.g., written on paper attached to PCs or terminal screens, kept in drawers, under keyboard, etc.) |  |  |
| Are monitors visible to unauthorized individuals? |  |  |
| Do employees know the emergency plan in the event of an emergency and staff are relocated? |  |  |
| |  | | --- | | **DUA and BAA agreements** | | |  | | --- | |  | | |  | | --- | |  | |
| Who is responsible for any DUAs and BAAs? |  |  |
| How is compliance with the DUA / BAA documented? |  |  |
| Review documentation |  |  |

Additional Comments:

Completed by:

Name:

Signature:

Date

Plan to address any issues of Concern: