

Securing Work Areas to Prevent Unauthorized Use HIPAA Policy: Privacy 16

Summary: Instructions for keeping both electronic and paper PHI safe from disclosure in work areas.

Affected Individuals: Staff at HIPAA covered entities

1.0 PURPOSE

The University of Mississippi (UM) has a duty to its patients to keep all protected health information (PHI) secure and accessible only to those individuals who need it. Not only does this include securing PHI from visitors and other patients, but it also includes making sure that only the employees who need the information to perform their job duties have access to it. Therefore, the intent of this policy is to guide employees in taking steps to ensure that their work areas are secure.

2.0 SCOPE

The UM Policy on Securing Work Areas to Prevent Unauthorized Use or Disclosure of PHI applies to all UM employees in HIPAA covered entities.

3.0 STANDARDS

Guidelines:

The following guidelines are to be used to safeguard patient information from unintentional uses and disclosures. The procedures are categorized by common work area usage.

- Safeguarding Workstation Peripherals (computers, monitors, printers, fax machines, etc.):

Workstations, especially those located in-patient care areas, should have limited access. The following steps must be taken to ensure that workstations are secure:

- All employees should return to screen saver status when he/she has completed their work and/or plans to leave the computer unattended.
- Monitors should be turned so that the visibility of the screen is reasonably limited to the employee who is actually using the computer.
- Printers, whether located in patient care areas or offices, should be positioned in such a way as to prohibit unauthorized individuals from accessing the information that is printed. For example: because in many patient care areas, lab results are printed on an almost continuous basis, it is essential that all printers be positioned away from the counter where visitors may stand while waiting to speak to a nurse or unit secretary.
- Employees should remove patient information from fax machines, printers, copiers, etc. as soon as he/she has finished using the equipment. For example: an employee who is printing patient

Securing Work Areas to Prevent Unauthorized Use HIPAA Policy: Privacy 16

information on a printer used by others should remove the printed information as soon as possible so that others cannot inadvertently get the information.

- Safeguarding Patient Information on Paper (i.e. the medical record, lab reports, etc.):
 - A patient's medical record should not be left open after use. The medical records should be kept in an area that is not accessible to visitors. Loose papers (i.e. lab reports, ECG readings) that have not been filed into a patient's chart should be placed in a secured area, until they are properly filed.
 - In most clinic areas, charts are placed outside the exam room, either in a holder on the exam room door or on the wall next to the door, for a healthcare provider to easily access. In clinics where this is common practice, the employees must ensure that the chart is positioned so the patient name or other identifying information, which might be on the chart, is not visible to unauthorized individuals. Often times, a clinic encounter form is pre-stamped with the patient name, medical record number, etc. Therefore, if a clinic's routine practice is to clip encounter forms to the front of the chart for the healthcare provider's convenience, then the employee placing the chart outside the exam room, should ensure that the encounter form is turned where it is not visible to unauthorized individuals.
 - No patient information should be thrown into the trash. Patient information that is to be discarded should be shredded, either manually or by a shredder.
- Safeguarding Information Discussed During Phone Calls and While Dictating:
 - Employees should be conscious of the presence of others when using the phone. It is essential that when discussing PHI over the phone, employees make a reasonable effort to minimize the opportunity for the conversation to be overheard. For example: Employees in patient care areas should use the phones located in areas away from counters where patients or visitors might stand, if such a phone is available.
 - Healthcare providers should be conscious of others when dictating. He/she must take reasonable steps to ensure that the chances of being overheard are limited.
- Safeguarding Sign-in Sheets/"White Boards"/Address-o-graph Cards/X-ray Light Boards:
 - All patient sign-in sheets, such as those used in most clinic areas, should contain only the following information:
 - Patient's name;
 - Appointment time; and
 - Sign-in time.

Securing Work Areas to Prevent Unauthorized Use HIPAA Policy: Privacy 16

No diagnostic information, clinic names (i.e. infectious disease clinic, OB/GYN clinic, etc.) or healthcare provider names should be on the sign-in sheet.

- “White Boards” or other such objects, normally used in clinic areas to inform the staff in what rooms their patients are located, can be used, but should be kept in such a manner as to deter those without a need to know, from viewing the information on the board.
- Many patient care areas have X-ray light boards. The employees in these areas must make reasonable efforts to ensure that those without a need to know are prohibited from viewing the radiographs. For example: If an X-ray light board is located in a hallway of a clinic, where visitors and patients normally pass through, employees should ensure that the radiographs are removed from the board once they have finished viewing them.
- **Safeguarding PHI During Equipment Repairs:**
Occasionally, equipment such as copiers, fax machines, etc. must undergo maintenance or repairs. In some work areas, this type of equipment is located where patient information is also maintained or created, such as in a room that houses a department’s medical records. When such instances occur, it is essential that the appropriate personnel ensure that PHI located in the area is secure. The following is a listing of simple steps that, at a minimum, should be taken to ensure that while maintenance or repairs are being performed, patient information not be inappropriately accessed:
 - Take reasonable steps to ensure that patient information located in the areas is not accessible to the visitor. For example: no loose information, such as lab reports, should be left lying out;
 - Have an employee repeatedly visit the area to verify that the visitor is not improperly accessing PHI.
- **Safeguarding PHI on Lab Samples/Drug Carts:**
 - When lab samples are drawn, the samples should be placed in a secure location. For example: employees should not place lab samples at the front counter, where patients and visitors may stand.

Though this policy and its guidelines do not cover every activity that could take place in most work areas, it is important that every employee take reasonable steps to ensure that all PHI remains confidential. Within reason, incidental uses and disclosures must be avoided.

4.0 CONTACT INFORMATION

For questions about the UM Policy on Securing Work Areas to Prevent Unauthorized Use or Disclosure of PHI or for more information, call the Office of General Counsel at 662-915-7014.