

GENERAL GUIDELINES TO SAFEGUARD PROTECTED HEALTH INFORMATION POLICY

RESPONSIBILITY: Privacy Official or Designee(s), Security Official, all members of the workforce

BACKGROUND:

Most members of the Behavioral Health and Health Facilities (BHHF) workforce use protected health information every day in the completion of their duties. This policy establishes guidelines to help safeguard this information from being seen by those who are not authorized to see it. For the most part these guidelines are not specifically required by federal privacy or security regulations. But they are consistent with the general limitations on the use and disclosure of PHI that permeate the regulations. Modify the guidelines as necessary to fit the needs of your organization.

POLICY:

BHHF will reasonably safeguard protected health information to limit incidental uses or disclosures. An incidental use or disclosure is a secondary use disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. For example: a conversation that is overheard despite attempts by the speakers to avoid being heard.

All members of the BHHF workforce will follow these guidelines in handling protected health information (PHI) to limit incidental uses and disclosures.

GUIDELINES TO SAFEGUARD PROTECTED HEALTH INFORMATION

Bulletin boards:

- Bulletin boards that are located in areas where they may be seen by patients or visitors may not contain any documents with PHI, unless the patient has authorized the display in accordance with the AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION policy. This includes
 - Baby pictures (even without a name or other identifying information)
 - Cards and notes of appreciation

Cleaning personnel:

- Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets, or rooms before cleaning personnel enter an area.
- When it is not reasonably possible to lock up PHI, it must be removed from sight before cleaning personnel enter an area, and a supervisor must be present.
- Cleaning personnel, whether members of the workforce or business associates, will receive training in BHHF's privacy and security policies, and in the penalties for

violating these policies, before they are permitted in areas where PHI is stored or used.

Computer Screens:

- Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed.
- Computer displays will be configured to go blank, or to display a screen saver, when left unattended for more than a brief period of time. The period of time will be determined by the Privacy and Security Officials. Wherever practicable, reverting from the screen saver to the display of data will require a password.
- Computer screens left unattended for longer periods of time will log off the user. The period of time will be determined by the Privacy and Security Officials

Conversations:

- Conversations concerning patient care or other PHI must be conducted in a way that reduces the likelihood of being overheard by others.
- Wherever reasonably possible, barriers will be used to reduce the opportunity for conversations to be overheard.

Copying medical records and other PHI

- When PHI is copied, only the information that is necessary to accomplish the purpose for which the copy is being made, may be copied. This may require that part of a page be masked.

Desks and countertops

- Medical records and other documents must be placed face down on counters, desks, and other places where patients or visitors can see them.
- Wherever it is reasonably possible to do so, medical records and other documents containing PHI will not be left on desks and countertops after business hours. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers, or other means to secure PHI during periods when the area is left unattended.
- In areas where locked storage after hours cannot reasonably be accomplished, PHI must be kept out of sight. A supervisor must be present whenever someone who is not authorized to have access to that data is in the area.

Disposal of paper with PHI:

- Paper documents containing PHI must be shredded when no longer needed. If retained for a commercial shredder, they must be kept in a locked bin.

Home office

- Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures regarding the security and privacy of PHI, including these guidelines.

Key policy

- The Security and Privacy Officials or Designee(s) will develop a list of which personnel, by job title, may have access to which keys. This includes keys to storage cabinets, storage rooms, and buildings.
- All keys must be signed out.
- Keys must be surrendered upon termination of employment.
- The Security Official will act to change locks whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense.

Medical records carried from one building to another:

- When PHI is carried from one building to another, it must be signed out and signed in.
- When a member of the workforce is transporting PHI from one building to another, it may not be left unattended unless it is in a locked vehicle, in an opaque, locked container. Locking the vehicle alone is not sufficient.

Medical Record Storage:

- Areas where medical records and other documents that contain PHI are stored must be secure.
 - Wherever reasonably possible, the PHI will be stored in locking cabinets.
 - Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves, and no unauthorized personnel may be left alone in such areas without supervision.

Personal digital assistants (PDAs)

- BHHF privacy and security policies apply to any PHI that is stored on a PDA.
- Users of PDAs are responsible for assuring that the PHI on their devices is kept secure and private.
- Any loss or theft of a PDA thought to contain PHI must be reported to the Security Official immediately.
- Users of PDAs who store PHI on their devices will receive special training in the risks of this practice, and measures that they can take to reduce the risks (such as use of passwords).

Printers and Fax Machines:

- Printers and fax machines must be located in secure areas, where only authorized members of the workforce can have access to documents being printed. (See also the following policy template: FACSIMILE MACHINES AND PROTECTED HEALTH INFORMATION.)

Schedules:

- Schedules that contain patient names or other PHI must not be posted in plain view.

- Alternatives: place face down on a desk (preferably in an “out guide” to prevent loss); cover with a blank sheet of paper.

Sign-in lists:

- Only the patient’s name is permitted on a sign-in list. Lists that ask for the name of a physician, or for any medical information, must not be used.

Subsidiary databases:

- Any member of the BHHF workforce who maintains a separate database containing PHI must make it known to the Privacy and Security Officials.
- The Privacy Official or Designee(s) must determine whether this database constitutes a “designated record set.”
- The Security Official must assure that the data are secure, in compliance with relevant BHHF policies.
- Any member of the workforce who uses and discloses PHI in a subsidiary database must follow BHHF policies.

Transcription

- Dictation tapes must be numbered, and transcriptionists must account for each tape they receive and return by number.
- Dictation tapes must be completely erased before being reused.
- Tapes and transcribed hard copy will be subject to the same policies that apply to the safeguarding of paper medical records.
- Access to central transcription units will be subject to the same standards as apply to access to electronic medical records, including the use of access profiles and passwords.

Wall pockets:

- Medical records and other documents containing PHI must be placed so that no PHI can be read.
- Whenever possible, opaque wall pockets should be used.

Workforce Vigilance:

- All members of the workforce are responsible to watch for unauthorized use or disclosure of PHI, to act to prevent the action, and to report suspected breaches of privacy and security policies to their supervisor, or to the Privacy or Security Official (example of a breach: patient or visitor looking through a chart left on a counter).
- This responsibility will be included in workforce training.

Visitors:

- Escorts who arrive with patients are the only visitors allowed in patient care areas of BHHF medical offices without supervision.

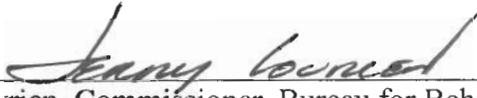
- Visitors to in-patient areas do not need to be escorted. Visitors to other patient care areas, including drug company and vendor representatives, must be accompanied by a member of the BHHF workforce.

REFERENCE: 45 CFR § 164.530(c)

Security Requirements 164.306
164.308 (a)
164.310 (c)
164.312 (a,c)

Effective Date: 4/14/03

Dates Revised:



Jerome E. Lovrien, Commissioner, Bureau for Behavioral Health and Health Facilities