



**ALLEGHENY COUNTY
BUREAU OF CORRECTIONS**

APPLICABILITY: All Authorized Personnel

POLICY NUMBER: # 2111

**EFFECTIVE: 1/6/2017
REVISED: 7/25/2017
REVISED: 4/29/2019
REVIEWED: 7/13/2020**

TITLE: Confidentiality of Health Records

**NCCHC: J-A-08
ACA: 4-ADLF-4D-13**

AUTHORIZED BY: ORLANDO L. HARPER

SIGNATURE: *Orlando L. Harper*

AUTHORIZED BY: ASHLEY BRINKMAN, PhD, LPC

SIGNATURE: *Ashley Brinkman PhD, LPC*

AUTHORIZED BY: DONALD STECHSCHULTE Jr., MD

SIGNATURE: *Donald Stechschulte Jr. MD*

POLICY

It is the policy of the Allegheny County Bureau of Corrections Healthcare Services Department to ensure restricted access to, safekeeping, and confidentiality of each permanent health record developed and maintained for patients who receive health care provided by the Allegheny County Health Care Services Department.

PURPOSE

To ensure that the facility has an appropriate system to manage and maintain the confidentiality of all patient health records and protected health information (PHI).

PROCEDURAL GUIDELINES

NCCHC/ACA

1. Health records stored in the facility are maintained under secure conditions separate from correctional records.
2. Access to health records and health information is controlled by the RHA.
3. Evidence exists that health care staff receives instruction in maintaining confidentiality.
4. If records are transported by non-health staff, the records are sealed.
5. When a patient is transferred to another correctional facility:
 - a. a copy of the current health record or a comprehensive health summary accompanies the patient
 - b. the transfer and sharing of health records comply with state and federal law.

PROCEDURAL DETAIL

1. The active health record is maintained electronically and is separate from the correctional record.
2. Health care staff will have access to a patient's health record as needed when acting in the course of their specific duties. Records will be routinely audited to determine if those who have gained access had a business need.
3. The administration/warden of the institution or his designee, internal investigative staff, department or accrediting bodies, or persons authorized by a court order with appropriate jurisdiction may have access to designated information from the health record on a need-to-know basis.
4. A patient may provide authorization to provide health information to an off-site entity by completion of a witnessed Authorization for Release of Health Information pursuant to HIPAA.

5. Health care staff will take precautions to foster private communication when cell-side triage is required or anytime that health care services are being provided, including medication administration.
6. Use of an interpreter should be considered when a health encounter may benefit from language, cultural, and other communication impairments being addressed
7. Health care staff will share with the institutional authority information regarding the patient's health care management necessary to preserve the health and safety of the patient, other patients, volunteers, visitors, or correctional staff.
8. Health care staff may be required to report health information to correctional staff, including the institutional authority if so directed when a patient is identified as;
 - a. suicidal;
 - b. homicidal;
 - c. presenting a reasonably clear danger of injury to self or others;
 - d. presenting a reasonably clear risk of escape or the creation of internal disorder or riot;
 - e. requiring movement to a special unit or cell for observation, evaluation or treatment of acute episodes;
 - f. requiring isolation or precautions due to infectious disease;
 - g. requiring transfer to a treatment facility outside of the institution;
 - h. requiring a new program assignment for health or security reasons.
9. Confidential documentation must not be discarded in trash bins, unsecured recycle bins, or other publicly accessible locations, but must be shredded prior to disposal.

- a. Confidential documentation designated for shredding will be placed in an on-site, specially marked, secure collection bin located in the health care administration office.
- b. Health care staff finding confidential documentation in any other location will immediately remove the documentation and notify the health services administrator.

10. Health care staff are to **REFRAIN** from the following:

- a. Discussing or sharing health information about patients with others who do not have a “need to know” (including co-workers).
 - i) Whenever possible, restrict conversations, regarding patients, to private places and keep anything containing patient information out of the view of others who do not “need to know.”
 - ii) If you must share PHI, only share the “minimum necessary.”
- b. Giving PHI, over the phone, when speaking to unknown callers; call back and verify information first.
- c. Leaving PHI on a voice mail; leave a message requesting a return call leaving only your name and number.
- d. Sharing your computer passwords and log-on with anyone.
- e. Sending patient information via text.
- f. Leaving healthcare records, or anything that contains PHI exposed, open, or unattended in open areas.
- g. Accessing a patient’s health care information other than for providing care or as instructed by your supervisor.
- h. Retaining copies of paperwork that contains PHI after the copies are no longer needed.

- i. Removing anything that contains PHI from the premise without your supervisors' approval for specific purposes.
 - j. Transferring PHI to external drives such as flash or thumb drives without permission from your supervisor.
9. When sending an email that contains PHI, do not include names, DOC, or any other individual identifiers in the subject line of an email.
- i) To secure an email to anyone outside of the ACBOC, make the subject line "secure delivery."; an internal email will not be encrypted.
10. Health care staff are required to:
- a. Lock computer screens when computers are not in use.
 - b. Turn away screens from others when using your computer to ensure that computer screens are not visible to others who are not authorized to view health information.
 - c. Maintain possession of electronic devices, including smartphones, and never leave them unattended.
 - d. Report a potential security breach, theft or loss of laptops, desktops, smartphones, and other devices that contain patient information to your supervisor immediately. Your supervisor will notify the appropriate member of custody and the privacy officer.
 - e. Secure and obscure anything that includes patient health information; before you leave any area, please check to make sure that you are not leaving any patient information behind.
11. When faxing PHI, program fax numbers into speed dial and verify numbers periodically to make sure they have not changed.
12. Always use a cover sheet that includes a confidentiality statement, identifies the recipient, and includes your name and phone number.

13. Failure to adhere to this policy may result in disciplinary action, up to and including discharge.