

POLICIES AND PROCEDURES HARVEY COUNTY HEALTH DEPARTMENT

Page 1 of 3

Title: Confidentiality

<u>New Policy</u>	Date:
<u>X Revised/update</u>	Date: 07/01/09, 09/8/2015
<u>Reviewed</u> (no change made)	Date: 09/11/13

Purpose: Protection of the confidential information imparted to us by our clients is the responsibility of all employees. To ensure that every step is taken to properly safeguard this information, the following policy outlines requirements related to the security of all documents, both electronic and paper, that may contain confidential information. For purposes of this policy, confidential information includes Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA) as well as all other information defined as confidential by federal or state statute.

Procedure:

Access to confidential information

Access to confidential information maintained in any form by the Harvey County Health Department (HCHD) is restricted to those providers and support staff who: 1) have a right to know the information and 2) have a need to know the information. Persons with a right to know include clinic and program managers, audit and review staff as well as system maintenance staff. Need to know includes any person needing access in order to deliver services.

HCHD gives access to confidential information to its employees, including providers and support staff, who are involved in the delivery of service to its clients. Access is further granted to persons who: contract with the agency for delivery of service to clients; enter into agreements with the agency for purposes of obtaining certification as a part of an internship supervised by accredited educational institutions; volunteer and sign a statement acknowledging receipt of and compliance with agency policies; are business associates as defined by HIPAA and documented through business associate agreements otherwise called Memorandum of Agreement (MOA); and are involved the treatment of clients; securing payment for services provided to clients; or the operation of agency business as defined by HIPAA; are involved in the evaluation of services provided either for quality assurance purposes or for the purpose of public health surveillance.

Physical Security

All documents containing confidential client information must be protected at all times and kept from reasonable breaches of security. Confidential client information must be inaccessible to unauthorized persons at all times and must be secured in locked cabinet or passcode computer during non-business hours. All client records are to be returned to the central filing area or other secure area, as designated by HCHD director by the close of each day. In cases where the provider has not yet completed documentation, the records must be stored overnight in a locked

cabinet or passcode computer. Client records and information must not be left unattended in the examination room or other work areas. The provider should remove the record from the room if it is necessary to leave the examination area during the client's visit.

Staff must ensure that other documents, such as appointment logs and sign-in sheets, which may contain confidential information, are kept from view of other clients. Access to such documents is limited to a "need to know" basis. Documents containing confidential information must be shredded or otherwise destroyed when no longer needed. Computer screens must be placed so they are not visible to clients and placed in locked mode when staff is away from screen.

Faxing Records

Documents will be faxed using the county's electronic email/fax method. Faxing documents that contain client information presents a potential risk of an unauthorized disclosure of Protected Health Information. If unforeseen circumstances require faxing of PHI, reasonable and appropriate precautions must be taken to ensure the confidential information reaches the intended receiver.

Prior to faxing confidential information to new or unfamiliar fax telephone numbers; the sending office must contact the receiving office to verify the fax telephone number and to alert the receiving office that confidential information is forthcoming. Using the county fax system the email message serves as the fax cover page; showing the intended recipient's name and the sender's complete telephone number. The cover page must contain a notice informing the recipient that the fax contains confidential information. The notice should also state that the sender must be notified if the fax was received by anyone other than the intended recipient.

Transporting Records

Removing confidential information from the secure environment of the county health department represents one of the most critical opportunities for breach of client confidentiality.

At times it is necessary to transport a record, either in paper form or on a laptop computer that contains individually identifiable patient information. In these instances a locked receptacle must be used to transport the records. This receptacle must contain a label identifying the contents as the property of the health department in the event of a motor vehicle accident. Due care must be taken to ensure that all records transported are returned to their proper location in a timely manner.

Prior to transportation, a list of the records to be transported must be created and placed in a secure file at the site initiating the transport. A comparison with this list is performed once the transported records return to their original location. Any problems must be noted and addressed with the staff involved immediately. This procedure is not required if using the electronic health record system off site.

Public Health Surveillance and Program Quality Assurance health officials involved in the gathering and transporting of Protected Health Information for purposes of public health surveillance or programmatic quality assurance are obligated to use reasonable and appropriate steps to protect all information from damage, loss or unintentional disclosure. This includes all

information containing PHI, whether in paper or electronic format. Any unresolved problems, such as a missing or incomplete file, must be reported to the Privacy Officer.

Electronic Mail

The creation, transmission and storage of electronic mail that contains confidential information represent opportunities to breach the confidentiality of client information. Care must be taken whenever confidential information is attached to or included in the body of an electronic mail. In general, electronic mail sent outside of the HCHD Intranet system for purposes other than treatment, payment or operations of the agency must not contain confidential information.

Confidential information may be included in an electronic mail sent through the HCHD Intranet system under the following circumstances:

- The recipient of the electronic mail is known to the sender; and the recipient is involved with the sender in the treatment of an HCHD client with the sender; or the recipient is involved in assisting the sender with procuring payment for services rendered to the client; or the recipient is involved in assisting the sender in the operation of the Agency's business, such as identifying and correcting duplicate client records in a database.
- The sender is involved in assisting the recipient carry out statutorily required data submissions for the purpose of public health surveillance.
- The sender is providing confidential information to a recipient who has an approved data use agreement on file for research and/or evaluation purposes.
- The sender is providing confidential information to another state or federal agency with an approved data use agreement for the purpose of treatment, payment or operations of the agency.

Reporting Breaches of Confidential Client Information

When a breach of client confidential information has occurred, the breach must be reported within 24 hours of the breach becoming known to any HCHD employee. The report may be made by letter, electronic mail, telephone call, or in person at the following address:

Privacy Officer
Harvey County Health Department
215 S. Pine St., 2nd floor
Newton, KS 67114
(316)283-1637
lredington@harveycounty.com

HARVEY COUNTY HEALTH DEPARTMENT

Receipt of Confidentiality Policy

I have reviewed the Confidentiality Policy, have been provided the opportunity to ask questions concerning its terms, and understand the duties and obligations to me. By signing this form, I am agreeing to the duties and obligations as stated in the Confidentiality Policy.

I understand that in the course of my employment (or student learning experience) at Harvey County Health Department, I may have access to confidential medical information concerning clients. I understand that this information has been obtained and recorded for the purpose of providing client services. I will use this information only for the purpose of my job (or student learning experience).

I understand that violation of this policy may be considered grounds for termination of employment (or student learning experience) at the Harvey County Health Department. The Director of the Health Department may also notify my licensing boards, if applicable. Violations may also result in a finding of professional misconduct, professional malpractice, and legal action against the agency or me.

Note: Students' clinical instructor will be notified of any violation of Harvey County Health Department's Confidentiality policy.

Printed Name: _____

Signature: _____

Date: _____