Standards of Confidentiality and Safeguards to Protect the Privacy and Security of Protected Health Information

Policy A-IC-14

June 29, 2006
Revised Jan 30, 2012

Purpose: To ensure the privacy and security of protected health information and surveillance data.

Policy: Release of information is governed by the TRDHD Policies for Protection of the Privacy and Security of Protected Health Information (PHI) and surveillance data.

Procedure: The official Custodian of Medical Records is the District Director. The day-to-day designee to serve as Custodian of Medical Records is as follows:

1. Home Health Nursing Supervisor or Designee – Home Health Records
2. Clinic Nursing Supervisor – Health Center Records and Disease Surveillance Data as defined by the Reportable Disease Desk Reference, Division of Epidemiology and Health Planning, Department for Public Health, Commonwealth of Kentucky.

Local staff are responsible for the ongoing maintenance of Medical Records in accordance with policies. The HIPAA Compliance Officer or designee must be contacted immediately upon request and prior to release of records for any purpose other than *routine written patient request or as permitted for disease surveillance reporting*. (This includes all subpoenas and court orders.)

I. Medical Records/Protected Health Information (PHI)

A. PHI may come from electronic or paper records or from conversations, and may pertain to medical or financial status, family or social status eligibility, services requested or received, surveillance reporting data and elements, or similar data about any individual regardless of how the data is obtained or stored.

B. PHI is to be available and accessible to authorized personnel only, and only within the context of their job duties.

C. PHI shall be discussed only with authorized personnel and then only within the context of assisting with reporting, record keeping, or a specific health care management problem.

D. During the workday, files containing PHI and surveillance data are to remain in secured file drawers and/or cabinets, except when in use. When in use, a red file divider shall be

placed in the location of the file in the file drawer by the staff utilizing the file/folder, indicating that the file is with that person. At the end of the workday, all files containing PHI and surveillance data shall be returned to the appropriate file drawers.

E. Originals, copies, or excerpts from patient medical records or surveillance data are to be maintained in locked cabinets or locked storage areas when unattended.

F. Support Services Staff at each site are responsible to assure that all medical records and surveillance data are locked at the end of each workday and the key returned to the designated storage area. All staff having responsibility for information containing PHI and/or surveillance data (i.e. A/P, mail, incident reports, etc.) must assure that all file drawers containing PHI shall be locked at any time the office is closed.

G. All electronic or paper medical records, other PHI, or surveillance data are to be accessible only to authorized personnel; indexed, maintained in a secure location; and retained only for the period of time deemed necessary or as required by law. The retention period shall not be permanent unless authorized by Federal or State Law.

H. PHI or individually identifiable surveillance data is never to be included in site visit or other administrative reports. If there is a need to address specific patients, patient records or surveillance data, they should be addressed by code with specific identification provided separately via phone or via a separate supplemental listing which is to be destroyed upon completion of the investigation.

I. Printouts or any other hard copy records with PHI and/or surveillance data are to be covered at any time identifying information could be visible to the public or persons lacking a legitimate need to view the information as it relates to the performance of their jobs.

II. Computer Security – All employees must adhere to the computer use, user access, policies and purging procedures as outlined in TRDHD policies for ensuring of the confidentiality, integrity, and availability of EPHI. All employees must adhere to the information technology requirements in the Administrative Reference for Local Health Departments.

A. All employees must change their computer password on periodic change cycles.

B. Computer screens with PHI and/or surveillance data are not to be visible from hallways, public areas or to persons lacking a legitimate need in order to perform their job duties.

C. All computer screens must be set to activate screen savers after no more than five minutes of inactivity.

D. PHI and/or surveillance data should not be submitted in the form of a message from one site to another on the computer network through the bridge system, except when there is an over-riding immediate need for the information to render care, or as authorized by the patient/guardian.

E. No PHI may be removed from the office on computer disk or other electronic media without the prior approval of the HIPAA Compliance Officer. When the HIPAA Compliance Officer permits removal, the disk/media shall be encrypted and password protected.

F. Electronic media containing PHI is to be erased before disposal.

III. Surveillance Activities, Permitted Disclosure and Uses

A. All information obtained in surveillance activities shall be considered and treated as protected health information as it pertains to individuals and may not be released except as permitted for public health activities, 45 CFR 164.512. For a list of reportable diseases, please see the Reportable Disease Desk Reference from the Division of Epidemiology and Health Planning or the Kentucky Public Health Practice Reference, Reportable Disease Section.

B. Surveillance activities include but are not limited to:

1. Reportable Disease reporting
2. Vital statistics reporting
3. Injury reporting
4. Outbreak investigations medical or food-borne
5. Public health investigations
6. Public health interventions

C. Permitted uses and disclosures:

1. Receipt and use of protected health information in the performance of one's job as it relates to surveillance activities as identified in section III, B, i-vi as identified in this policy, 45 CFR 164.512(b)(2).
2. Disclosure to a public health authority such as another Local Health Department, the Department for Public Health, the Centers for Disease Control, or other governmental agency acting in collaboration with a public health authority, for the purpose of preventing or controlling disease, injury, or disability, and or the reporting of vital events such as birth or death, 45 CFR 164.512(b)(1)(i).
3. Disclosure to an appropriate governmental authority authorized by law to receive reports of child abuse or neglect, 45 CFR 164.512(b)(ii).
4. Disclosure to persons subject to FDA jurisdiction, for public health purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity for which that person has jurisdiction, 45 CFR 164.512(b)(iii).
5. Disclosure to an individual who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, in the course of conducting a public health investigation or implementing a public health intervention, 45 CFR 164.512(b)(iv).

III. Mail

A. Extreme caution is to be taken when mailing PHI to assure that the envelopes or other mailing containers are securely closed, and that the information is mailed to the correct location/addressee.

IV. Fax

A. Facsimile machines must be kept in a location that protects confidentiality of medical records/PHI and must be used in accordance with Policy A-IC-18.

District Director **Date**

Chairperson, Three Rivers District Board of Health **Date**