HARFORD COUNTY HEALTH DEPARTMENT POLICY

Title of Policy: Health Data Security and Confidentiality Policy	
Program Area: Administration	
Approved By: Susan Kelly	Original Effective Date: March 2012
Susan Kelly, Health Officer	Revised Dates: 11/15/13

1.0 POLICY

The Harford County Health Department (HCHD) Health Data Security and Confidentiality Policy incorporates the Health Insurance Portability and Accountability Act (HIPAA) and COMAR regulations which require strict policy adherence in order to maintain public safety and trust in the Health Department. This policy outlines how protected health information will be obtained, maintained and properly disposed of in order to ensure it is only used for the purposes it is intended.

2.0 PURPOSE

The purpose of this document is to describe the Harford County Health Department's policies regarding the protection and release of protected health information in accordance with HIPAA and COMAR.

3.0 PROCEDURE

3.1 DEFINITIONS

3.1.1 A confidential record is defined as a "record, report, statement, note or other information that … names or otherwise identifies any person."
A confidential record may be either a paper or electronic record containing confidential information.
- Maryland Code Annotated, Health-General Section 4-101

3.1.2 The following information may be considered confidential: names, addresses or small geographic areas; social security numbers; certain dates; facility names and codes; rare conditions; rare causes of death; individual level data with or without identifiers; aggregate data with small cell sizes if the data could permit the deduction of the identity of any person.

3.1.3 Confidential health data are health data that include confidential information.

3.1.3 Qualified personnel are those individuals with sufficient training and experience to carry out the responsibilities connected with collection, maintenance, release, or utilization of specific health data files.

3.2 RELEASE OF DATA

3.2.1 Release of confidential health data requires compliance with Department of Health and Mental Hygiene (DHMH) and Harford

County Health Department (HCHD) program-specific requirements, as well as the approval of the Health Officer and/or Deputy Health Officer.

3.2.2 Health data that include confidential data elements may be released under the following circumstances:

- With written consent of the person (or his/her legal designee) who is the subject of the record being requested.
- To qualified personnel for public health activities mandated by statute or regulation.
- To qualified personnel for the purpose of conducting management audits, financial audits, or program evaluation.
- To qualified personnel for the purposes of health insurance billing and collections.
- To qualified personnel for the purpose of conducting scientific research after the research protocol has been approved by the appropriate Institutional Review Boards (IRBs), in accordance with HCHD policies and protocols.
- By court order pursuant to showing good cause.

3.3 PROGRAM POLICIES AND RESPONSIBILITIES

3.3.1 HCHD Program Managers/Supervisors are responsible for adhering to DHMH and HCHD data security and confidentiality guidelines, as well as developing and maintaining written policies and procedures on data security and confidentiality as it relates to their respective programs.

3.3.2 Written policies and procedures will include review of applicable laws and regulations; description of applicable data; roles and responsibilities of persons with authorized access to the data; applicable confidentiality agreements; controls for data management, security, and access (physical and electronic); will address when use of privacy advice or reminder is appropriate; specified policies applicable to trainees, students, volunteers, visitors, and cleaning and security staff; provisions to prevent indirect release of data; guidance on data sharing.

3.3.3 The number of people with access to identifiable information should be kept to a minimum and de-identified data should be used for routine analyses whenever possible.

3.3.4 Operational security procedures will be devised to minimize number of people with access to confidential data. Written procedures will specify how to obtain authorization for access to both identified and de-identified data.

3.3.5 Breaches of data security protocol that result in unauthorized disclosure of confidential data require immediate notification of the Health Officer and/or Deputy Health Officer.

3.3.6 All new staff members, including volunteers, must sign the HCHD Confidentiality Agreement before being given access to identifiable information (see Attachment A).

3.3.7 All persons who have authorized access to confidential public health data must take responsibility for implementing the program's data security policies and procedures, protecting the security of any device in their possession on which confidential data are stored, and reporting suspected security breaches.

3.3.8 Program Managers/Supervisors should self-certify annually that their programs are in compliance with HCHD's data security and confidentiality policies and procedures or document reasons for non-adherence, with plans for remediation.

3.4 DATA COLLECTION AND USE

3.4.1 HCHD Program Managers/Supervisors are responsible for developing and maintaining written procedures describing the intended public health purposes for collecting data and the scope and limits of the data collection activities when data are shared or used.

3.4.2 Programs will specify minimum data elements and information needed to conduct their specified public health activities.

3.4.3 Programs will collect personally identifiable data only when necessary and use non-identifiable data whenever possible.

3.4.4 Programs will ensure that data collected for public health research are done in compliance with federal and State requirements which includes obtaining institutional review board (IRB) approval when appropriate.

3.5 DATA SHARING AND RELEASE

3.5.1 HCHD Program Managers/Supervisors are responsible for ensuring that sharing of confidential or identifiable information may only be done with a justifiable public health need.

3.5.2 Programs will assess the risks and benefits of sharing identifiable data for other than their originally stated purposes.

3.5.3 Programs will ensure that any public health program with which personally identifiable public health data are shared has data security standards equivalent to the standards in this document.

3.5.4 Programs will ensure that public health information is released only for purposes related to public health, except when required by law.

3.5.5 Programs will establish procedures for determining whether to grant requests for aggregate data not covered by existing data-release policies.

3.5.6 Programs will disseminate non-identifiable summary data to stakeholders in a timely manner after data are collected.

3.5.7 Programs will assess data quality before disseminating data.

3.5.8 Programs will ensure that data release policies define purposes for which the data can be used and provisions to prevent public access to raw data that could contain identifying information.

3.6 PHYSICAL SECURITY

3.6.1 HCHD Program Managers/Supervisors are responsible for ensuring the physical security (such as locked file cabinet or dedicated, secure room) of hard copies of documents containing confidential, identifiable information.

3.6.2 Programs will ensure that documents containing confidential information are shredded before disposal.

3.6.3 Programs will ensure that data-security policies and procedures address the handling and retention of paper copies.

3.6.4 Programs will limit access to secure areas that contain confidential public health data to authorized persons.

3.6.5 Programs will ensure that employees working with documents containing confidential, identifiable data follow security procedures for handling such documents.

3.6.6 Programs will ensure that documents with line lists or supporting notes contain the minimum amount of potentially identifiable information necessary.

3.7 ELECTRONIC DATA SECURITY

3.7.1 HCHD Information Technology staff will ensure that electronic identifiable data are securely stored and password protected.

3.7.2 HCHD Information Technology staff will ensure that any identifiable data that are electronically transmitted from or to sources outside HCHD are done in accordance with the *DHMH Information Technology Security Policy* and other DHMH data security and confidentiality protocols.

3.7.3 HCHD Programs will ensure that data policies include procedures for handling incoming and outgoing facsimile transmissions that protect the confidentiality of records.

Attachment A

CONFIDENTIALITY AGREEMENT

This is to acknowledge that I have reviewed, understand, and agree to follow the guidelines stated in the document entitled, *Harford County Health Department Health Data Security and Confidentiality Policy.*

I recognize that the sharing of confidential information that I have read, seen, or heard in the Harford County Health Department workplace with parties not having a need to know, without the consent of the Health Officer or an authorized representative of the Health Officer, is prohibited. I understand that I am prohibited from discussing any of the patients or clients of the Harford County Health Department without authorization as specified above. Failure to adhere to the *Harford County Health Department Health Data Security and Confidentiality Policy* can result in progressive discipline up to and including termination.

_____

Print Name

_____ _____

Signature Date