HARFORD COUNTY HEALTH DEPARTMENT POLICY

Title of Policy: Health Data Access Control Policy	
Program Area: Administration	
Approved By: Susan Kelly	Original Effective Date: 5/31/13
Susan Kelly, Health Officer	Revised Dates:

1.0 POLICY

Harford County Health Department will implement reasonable and appropriate measures to (i) limit access to ePHI only to those persons or automated processes that have been granted access rights based on their required functions and (ii) prevent those who have not been granted those rights from obtaining access to ePHI.

2.0 PURPOSE

Harford County Health Department is committed to conducting business in compliance with all applicable laws, regulations and HCHD policies. This Policy covers access control management, access rights, the unique user identification and password, emergency access, automatic logoff, and remote and wireless access procedures that will apply to electronic information systems that maintain Electronic Personal Health Information (ePHI) to assure that such systems are accessed only by those persons or software programs that have been granted access rights under the HIPAA Security Policy -- Information Access Management Policy.

3.0 PROCEDURE

3.1 **Authorized Access**. Only workforce members or business associates who have been authorized to have access to specified ePHI, in accordance with the requirements set forth by the Harford County Health Department and Health Insurance Portability and Accountability Act (HIPAA), may access and work with the associated ePHI.

3.2 **Workplace Security**. Persons who are not authorized to access ePHI but who work in or visit locations where ePHI might be accessible, will be supervised, escorted, or otherwise procedurally denied access to such information. Workforce members will safeguard ePHI when persons who are not authorized to access the information are present, in accordance with the HCHD Electronic Information Systems and Computer Software Policy (ADMIN 02-02).

3.3 **Data Backup Plan**. The Harford County Health Department will back up all electronic data, including authorized access documentation, at least weekly in order to protect the integrity of the ePHI stored on agency servers. In the case of data loss, the Security Officer or other designated member of the Information Technology Division will perform data restoration procedures upon request.

3.4 **Access Control Management Responsibilities**. The System Owner of a HCHD information system is responsible for access control management. The Security Officer or designee(s) will serve as:

A. **Access Granting Authority** – the person(s) having managerial authority to approve requests for access rights to the information system.
B. **Access Control Administration** – the person(s) or group (e.g., access control group) responsible for creating, modifying, and terminating a user's ability to access the information system or ePHI based on direction from the Access Granting Authority.

For multi-user systems or databases, if the Security Officer delegates access granting responsibility, the User Account Creation Request Form (1.02.01) and/or Network Access Request Form (1.02.02) will be used to document the designation.
Where appropriate as determined by the Security Officer, including in particular for High Risk systems, Access Granting Authority and Access Control Administration will be separate functions (i.e., will not be the responsibility of the same persons).

3.5 **Access Rights Requirements**. The Access Granting Authority will only grant access rights to those persons (e.g., workforce members, business associates, other legally authorized persons) or automated processes (e.g., an interface between two information systems) that have a legitimate need based on their current responsibilities or function to access the information system. The Access Granting Authority will verify that any necessary requirements have been met to establish that a user is authorized to access ePHI prior to granting access rights.

3.5.1 **User Accounts Management**. A user account will be established and maintained for each user of an information system to control authentication and access rights.

A. **Setup Requirements.** User accounts may only be created and maintained for users whose access requests have been approved by the Access Granting Authority as outlined in Section 3.5 above.

B. **Access Rights**. Each user account will carry with it access rights to the data within the information system. Access rights determine what data sets (e.g., which patients, accounts, records) the user may view, copy, create, update, or delete within the information system.

C. **User Identification and Authentication**. Access to an information system requires the use of a unique user identifier in conjunction with an associated password or other type of authenticator that has been approved by the Harford County Health Department Security Officer or delegate.

1. The Access Control Administration is responsible for:
   - Assigning to each authorized user of the HCHD information system a unique User ID. A user may be assigned the same User ID to access multiple information systems.
   - Providing users a secure mechanism to create a password or other authenticator that will be used to verify that the user seeking access to the information system is the one claimed. Except where not supported by the system, Harford County Health Department two-step authentication must be used.
2. Users are obligated to:
   - Use only their assigned unique User ID and authenticator(s) to access the information system. Use of another user's identifier and/or authentication data to access an information system is strictly prohibited.
   - Change their authenticator (excepting biometric authenticators) on a regular basis. Change prompts will be provided by technical or procedural mechanisms. The Security Officer will determine the frequency for authenticator change prompts based on risks associated with the information system.
   - Change their authenticator whenever there is reason to suspect that the authenticator may have become known to another person or otherwise compromised.

D. **Security of Access Control Data**. HCHD will protect user account and authentication data stored in information systems from unauthorized access or modification.

E. **Modification and Termination**. HCHD division directors or supervisors will promptly notify the appropriate Information Technology Division whenever a user of an information system:

1. Ceases to require access to the information system (e.g., terminates employment, transfers to another department); or
2. Requires modified access rights to perform required functions (e.g., changes roles within a department).

The Information Technology Division will take the required steps to remove ePHI from electronic media that will be transferred to another member of the workforce upon termination or alteration of access rights.

3.6 **Access Control Logs**. The Information Technology Division will maintain for a minimum of six years logs or other documentation of all access request approvals, user account creations, modifications, and deletions.

3.7 **Emergency Access**. The Security Officer will create, document, and maintain procedures for accessing ePHI during an emergency. Procedures for accessing ePHI in an emergency will be documented in the Contingency Plan/COOP for the corresponding information system.

3.8 **Inactivity Logoff/Lockout**. When a computing device is unattended, automated security features and procedures will be employed to deter unauthorized access to ePHI, as follows:

3.8.1 **Automatic Logoff**. If an information system has an automatic logoff capability, then the feature will be enabled to terminate an electronic session after a predetermined time of inactivity. It is the responsibility of the HCHD System Owner to determine the appropriate logoff time, based on a risk determination that considers (i) the nature of the application, (ii) user group information needs, and (iii) the physical location of the computing device used to access the application.

3.8.2 **Automatic Application/Device Lock**. If the information system does not have an automatic logoff capability, then an electronic method will be employed to lock the application or device after a predetermined time of inactivity (e.g., password-enabled screensaver). It is the responsibility of the HCHD System Owner to determine the appropriate lock-out time, based on a risk determination that considers (i) the nature of the application, (ii) user group information needs, and (iii) the physical location of the computing device used to access the application.

If an application or computing device cannot meet either of the requirements defined above (e.g., due to technological limitations or because such security measures would impede necessary operations), then an exception must be obtained from the Harford County Health Department Security Officer or delegate. If an exception is obtained, then users will procedurally logoff or lock the application or device or physically secure the device (e.g., in a locked room or cabinet) as necessary to deter unauthorized access whenever the device is left unattended.

4.0 RELATED POLICIES

4.1 *Information Technology Technical Security Policy, Standards & Requirements Version 4.0.* Maryland Department of Health and Mental Hygiene.

4.2 *Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.* U.S. Department of Health and Human Services.