HARFORD COUNTY HEALTH DEPARTMENT POLICY

Title of Policy: Health Data Audit Control Policy	
Program Area: Administration	
Approved By: Susan Kelly	Original Effective Date: 5/31/17
Susan Kelly, Health Officer	Revised Dates:

1.0 POLICY

Harford County Health Department shall audit access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI. The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Harford County Health Department shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing which is consistent with available resources.

2.0 PURPOSE

It is the policy of the Harford County Health Department to safeguard the confidentiality, integrity, and availability of patient health information applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, Harford County Health Department shall audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions.
- Breaches in confidentiality and security of patient protected health information.
- Performance problems and flaws in applications.
- Improper alteration or destruction of ePHI.

This policy applies to organizational information applications, systems, networks, and any computing devices, regardless of ownership [e.g., owned, leased, contracted, and/or stand-alone].

3.0 PROCEDURE

3.1 DEFINITIONS

3.1.1 Audit: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing. Audit activities shall also take

into consideration Harford County Health Department's Risk Analysis results.

3.1.2 Audit Controls: Technical mechanisms that track and record computer/system activities.

3.1.3 Audit Logs: Records of activity maintained by the system which provide: 1) date and time of significant activity; 2) origin of significant activity; 3) identification of user performing significant activity; and 4) description of attempted or completed significant activity.

3.1.4 Audit Trail: Means to monitor information operations to determine if a security violation occurred by providing a chronological series of logged computer events (audit logs) that relate to an operating system, an application, or user activities.

3.1.5 Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

3.1.6 Trigger Event: Activities that may be indicative of a security breach that require further investigation (See Appendix).

3.2 GENERAL

3.2.1 Responsibility for auditing information system access and activity is assigned to Harford County Health Department's Information Technology (IT) Supervisor, Security Officer, and Privacy Officer. The responsible individual shall:

a. Assign the task of generating reports for audit activities to the individual responsible for the application, system, or network.
b. Assign the task of reviewing the audit reports to the individual responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task.
c. Organize and provide oversight to a team structure charged with audit compliance activities.

3.2.2 Harford County Health Department's auditing processes shall address access and activity at the following levels:

a. User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and files and resources accessed.
b. Application: Application level audit trails generally monitor and log user activities, including data files opened and closed, specific actions, and printing reports.
c. System: System level audit trails generally monitor and log user activities, applications accessed, and other system-defined specific actions.
d. Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.

3.2.3 Harford County Health Department shall determine the systems or activities that will be tracked or audited by:

a. Focusing efforts on areas of greatest risk and vulnerability as identified in the Harford County Health Department Risk Analysis.
b. Maintaining confidentiality, integrity, and availability of ePHI applications and systems.
c. Assessing the appropriate scope of system audits based on the size and needs of Harford County Health Department by asking:
    1. What information/ePHI is at risk?
    2. What systems, applications or processes are vulnerable to unauthorized or inappropriate access?
    3. What activities should be monitored?
    4. What information should be included in the audit record?
d. Assessing available organizational resources.

3.2.4 Harford County Health Department shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. The "events" may be applied to the entire organization or may be specific to a department, unit, or application. At a minimum, Harford County Health Department shall provide immediate auditing in response to:

a. Patient complaint.
b. Employee complaint.
c. Suspected breach of patient confidentiality.
d. High risk or problem-prone event.

3.2.5 Harford County Health Department shall determine auditing frequency by reviewing past experience, current and projected future needs, and industry trends and events. Harford County Health Department recognizes that failure to address automatically generated audit logs,

trails, and reports through a systematic review process may be more detrimental to the organization than not auditing at all (e.g., state/federal licensing and accrediting agencies).

3.2.6 Harford County Health Department's IT Department, Security Officer or designee is authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Use of such tools is explicitly prohibited by others without the explicit authorization of the Security Officer. These tools may include, but are not limited to:

a. Scanning tools and devices.
b. Password cracking utilities.
c. Network "sniffers".
d. Passive and active intrusion detection systems.

3.2.7 Audit documentation/reporting tools shall address, at a minimum, the following data elements:

a. Application, System, Network, Department, and/or User Audited.
b. Audit Type.
c. Individual/Department Responsible for Audit.
d. Date(s) of Audit.
e. Reporting Responsibility/Structure for Review of Audit Results.
f. Conclusions.
g. Recommendations.
h. Actions.
i. Assignments.
j. Follow-Up.

3.2.8 The process for review of audit logs, trails, and reports shall include:

a. Description of the activity as well as rationale for performing audit.
b. Identification of which workforce members or department/unit will be responsible for review (workforce members shall not review audit logs which pertain to their own system activity).
c. Frequency of the auditing process.
d. Determination of significant events requiring further review and follow-up.
e. Identification of appropriate reporting channels for audit results and required follow-up.

3.2.9 Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), if publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

a. Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services – separation of duties).
b. Testing shall be done on a routine basis (e.g., annually).

3.3 EVALUATION AND REPORTING OF AUDIT FINDINGS

3.3.1 Audit information that is routinely gathered must be reviewed in a timely manner by the individual/department responsible for the activity/process (e.g., weekly, monthly, quarterly, etc.).

3.3.2 The reporting process shall allow for meaningful communication of the audit findings to those divisions/programs sponsoring the activity.

a. Significant findings shall be reported immediately in a written format. Harford County Health Department's security incident response form may be utilized to report a single event.
b. Routine findings shall be reported to the sponsoring leadership structure in a written report format.

3.3.3 Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.

3.3.4 Security audits constitute an internal, confidential monitoring practice that may be included in Harford County Health Department's performance management activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution.

3.3.5 Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible and sponsoring divisions.

3.4 AUDITING BUSINESS ASSOCIATE ACCESS AND ACTIVITY

3.4.1 Periodic monitoring of business associate and vendor information system activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between Harford County Health Department and the external agency.

3.4.2 If it is determined that the business associate or vendor has exceeded the scope of access privileges, Harford County Health Department leadership must reassess the business relationship.

3.4.3 If it is determined that a business associate has violated the terms of the HIPAA business associate agreement, Harford County Health Department must take immediate action to remediate the situation. Continued violations may result in discontinuation of the contract.

3.5 AUDIT LOG SECURITY CONTROLS AND BACKUP

3.5.1 Audit logs shall be protected from unauthorized access or modification, so the information they contain will be available if needed to evaluate a security incident.

3.5.2 Audit logs maintained within an application shall be backed-up as part of the application's regular backup procedure.

3.5.3 Harford County Health Department shall audit internal back-up, storage, and data recovery processes to ensure that the information is readily available in the manner required. Auditing of data back-up processes shall be carried out:

a. At least annually for established practices and procedures.
b. More often for newly developed practices and procedures (e.g., weekly, monthly, or until satisfactory assurance of reliability and integrity has been established).

3.6 WORKFORCE TRAINING, EDUCATION, AWARENESS, AND RESPONSIBILITIES

3.6.1 Harford County Health Department's workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and patient protected health information. Workforce members are made aware of responsibilities with regard to privacy and security of information, as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.

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.

APPENDIX: TRIGGER EVENTS

POTENTIAL TRIGGER EVENTS THAT MAY REQUIRE FURTHER INVESTIGATION/AUDITING

Examples include:

- High risk or problem prone incidents or events.
- Patient/customer complaints.
- High profile patient/event (e.g., accident, homicide, assault, etc.).
- Atypical patterns of activity.
- Failed authentication attempts.
- Users that have the same last name, address, or street name as in the patient file being viewed.
- VIP encounters (board members, celebrities, governmental or community figures, authority figures, physician providers, management staff, or other highly publicized individuals).
- Patient files with isolated activity after no activity for XX days.
- Employees viewing other employee records.
- Diagnosis related (e.g., STD, HIV, pregnancy, AODA, mental health, etc.).
- Remote access use and activity.
- After-hours activity.
- Activity post termination.
- Random audits.
- Department- or unit-specific circumstances – risk areas to be determined by individual departments/business units:
  - Providers viewing files of patients on other units (e.g., medical and surgical nurses viewing files of patients treated only in emergency services or psychiatric services).
  - Transcriptionists viewing files of services or patients for whom they did not transcribe reports.
  - Medicare billers viewing insurance categories they do not process.