CHAPTER 8
RISK ASSESSMENT, RISK MANAGEMENT, AND AUDITING

I. OVERVIEW

Chapter 8 sets forth DMH's procedures for risk assessment, risk management and auditing of electronic Information Resources. These activities are crucial for ensuring HIPAA compliance and protecting the confidentiality, integrity, and availability of all electronic information DMH creates, receives, maintains, or transmits. HIPAA requires that DMH's security compliance meets a "reasonable" standard. However, what is "reasonable" will vary with time and changing circumstances, new technologies and emerging threats. As a result, DMH must regularly review its security measures. This includes periodically reviewing the DMH Information Security Handbook and the tools and mechanisms used to implement its procedures to ensure they continue to remain effective in safeguarding its electronic Information Resources.

II. RISK ANALYSIS

The DMH Information Security Handbook calls for ongoing risk analysis to be done on a DMH wide basis. Risk analysis helps identify potential threats and vulnerabilities to DMH's electronic Information Resources.

Risk analysis includes, but is not limited to, the following activities:

- Maintaining current knowledge of applicable and federal and state security laws and accreditation standards and applying them to DMH -- Chapter 1, Section II
- Monitoring advancements in information security technologies to help evaluate if changes should be made to DMH information security policies or procedures -- Chapter 1, Section II
- Identifying environmental and operational changes affecting the security of electronic Information Resources -- Chapter 1, Section II
- Conducting regular Information Security Incident reviews and follow-ups -- Chapter 1, Section II and Chapter 2, Section IV
- Taking prevention measures to prevent Information Security Incidents -- Chapter 2, Section V
- Distributing security alerts and updates to Workforce Members -- Chapter 1, Section V.B
- Having and following a complaint process -- Chapter 1, Section VII
- Periodically conducting system activity reviews -- Chapter 8, Section IV
- Requiring and conducting EPHI System/Database registration and reviews -- Chapter 3, Section II
- Conducting annual reviews of Security Plans for each DMH Location -- Chapter 6, Section II

- Conducting and assessing regular risk management activities -- Chapter 8, Sections III–VIII
- Developing and reviewing business continuity and disaster recovery plans -- Chapter 9.

III. RISK MANAGEMENT - COMPLIANCE WITH THE HANDBOOK

A. Compliance with the DMH Information Security Handbook

Procedures for handling EPHI and other electronic information that is created, received, or maintained by DMH are set forth in the DMH Information Security Handbook. All Workforce Members are required to comply with the procedures set forth in this Handbook.

The Handbook requires all Workforce Members to participate in appropriate information security training. Training ensures that all Workforce Members understand their role and responsibility in protecting Information Resources. The training is tracked, and appropriate action is taken against Workforce Members who fail to attend the required trainings.

B. Reasonable Accommodation

The DMH ISO, to the extent permitted by law, may waive or modify a requirement of this Handbook if it is determined that the modification is necessary to provide a reasonable accommodation for a Workforce Member's disability that will allow the Member to perform the essential functions of their job. Copies of such an accommodation shall be kept in the Workforce Member's personnel record.

IV. RISK MANAGEMENT - MONITORING ACTIVITIES

A. System Activity Reviews

The DMH ISO shall ensure that the system activity reviews and audits required by this Chapter 8 are conducted and that the findings are reported, used and/or acted on as is appropriate. The DMH ISO is to determine if any adjustments need to be made to the DMH Information Security Handbook and/or the training provided to Workforce Members. When appropriate, the DMH ISO will address issues that are discovered in security alerts and updates as set forth in Chapter 1, Section V.

B. Systems and Databases Reviews and Audits

The DMH ISO works with the Application Owners and/or Access Coordinators to conduct periodic reviews of registered EPHI Systems/Databases. EPHI System/Database reviews will be conducted, at a minimum, each time an EPHI System/Database Registration Form is submitted for the EPHI Systems/Databases. These reviews may address one of more of the following items: physical security, operations security, network security, data backup, or business and continuity planning. If issues are identified, the findings and recommendations for improvements and/or corrections will be submitted to the DMH General Counsel for further review as set forth in Section VIII, Other Risk Mitigation Activities, below.

Where appropriate, the DMH ISO will work with the Application Owners and/or Access Coordinators and applicable Workforce Members to develop routine audit procedures and implementation documentation of registered EPHI Systems/Databases. Application Owners and Access Coordinators may not audit their own EPHI System/Database. The audits' findings shall be submitted to the DMH ISO, or designee, and the Application Owner upon completion. If security incidents are identified, the findings shall be reported as an Information Security Incident and the procedure set forth in Chapter 2, Information Security Incident Reporting and Response Procedures, followed. If any other issues are identified, the findings shall be followed by a response by the Application Owner that describes the activities planned and the timeline that will follow to rectify the issues identified by a set date. Such a response must be filed with the DMH ISO within thirty (30) days of the initial findings being reported. Similarly, a report shall be filed by the Application Owner with the DMH ISO by the date specified for improvements and/or corrections to be completed; that provides a status report of such improvements and/or corrections.

C. Complaint and Information Security Incidents Reviews

The DMH ISO must ensure that Information Security Incidents are timely reviewed as set forth in Chapter 2 and Chapter 1, Section II.C. In addition, the DMH ISO shall review and respond to any complaints received concerning DMH Information Security policies and procedures as set forth in Chapter 1, Section VII. At a minimum, the DMH ISO shall provide the DMH General Counsel with a summary of these reviews in January of each year.

D. Documentation Reviews

The DMH ISO, in collaboration with the Area and OIM Information Security Coordinators, shall conduct periodic reviews of information security documentation. Documentation review will be done during security walk-throughs of Locations, as applicable. (*See* Chapter 6, Section II.A.4.) Documentation that is not specific to Locations will be reviewed during the Central Office security walk-through. These reviews will involve reviewing a sampling of documentation in each of the areas set forth in Attachment A, Documentation, to this Chapter 8 to ensure compliance with this Handbook. The DMH ISO shall provide the DMH General Counsel with a summary of these reviews in July of each year.

V. AUDITS OF APPLICATION OWNERS AND ACCESS COORDINATORS

Application Owners and Access Coordinators have system access beyond that of the average Workforce Member and as such require increased systems permissions to perform their assigned job tasks. Application Owners and Access Coordinators may, among other things, create, modify, and terminate Workforce Members' accounts; create, access, modify and/or delete access to electronic resources; grant permissions to shared resources, and monitor Workforce Members' use of systems they oversee.

The DMH ISO shall establish a process whereby Application Owners and Access Coordinators activity is audited and monitored on a regular basis to ensure that these users are not misusing their increased systems capabilities. At a minimum, the process that is developed shall meet the following requirements:

- Assign responsibility for conducting the various audits.
- Require that the person(s) responsible for an audit produce a written report of findings.
- Audits shall be performed over the course of the year and shall be based on a sample of Application Owners and Access Coordinators.
- Reports of all findings of the routine audit process shall be reviewed by the DMH ISO, or designee, and the applicable Application Owner(s) and Access Coordinator(s). If security incidents are identified, the findings shall be reported as an Information Security Incident and the procedure set forth in Chapter 2, Information Security Incident Reporting and Response Procedures, followed. If any other issues are identified, the findings shall be followed by a response by the Application Owner that describes the activities planned and the timeline that will follow to rectify the issues identified by a set date. Such a response must be filed with the DMH ISO within thirty (30) days of the initial findings being reported. Similarly, a report shall be filed by the Application Owner with the DMH ISO by the date specified for improvements and/or corrections to be completed; that provides a status report of such improvements and/or corrections.

- The DMH ISO may perform additional audits if such action is indicated by these audits; or Information Security Incident or Privacy reports.
- Copies of reports of findings of the audit process shall be maintained by the DMH ISO.
- The procedures that are developed shall be documented in writing. A copy of the procedures shall be maintained by the DMH ISO. The procedures shall be reviewed, at a minimum, every three (3) years to determine if they need to be updated. The DMH ISO and the DMH Privacy Officer shall be responsible for such review.

All documentation will be retained for a minimum of six (6) years from last use.

VI. UPDATES TO DMH GENERAL COUNSEL

The DMH ISO shall report quarterly to the DMH General Counsel on DMH's efforts to comply with the HIPAA Security Rule and other similar state and federal laws. This shall include, but not be limited to:

- Raising issues, if any, regarding Workforce Members' compliance with DMH Information Security policies and procedures;
- Discussing risks that have been identified and that need to be addressed;
- Identifying the need to change DMH Information Security policies and procedures; and/or
- Processing changes of technologies that could assist DMH in its compliance.

VII. EVALUATION OF SECURITY SAFEGUARDS

A. The DMH ISO shall conduct evaluations of DMH's compliance with the Security Rule periodically and at a minimum once a year as part of the DMH's annual internal control risk review. In addition to periodic reviews, specific events may trigger additional evaluations of security policies and procedures. Such events include, without limitation:

1. Known security incidents;
2. Identification of new threats or risks to information systems;
3. Changes to organizational or technical infrastructure; and
4. New information security technologies become available to DMH.

B. Evaluation Process:

As part of the evaluation process, the DMH ISO shall gather all relevant input from applicable stakeholders (e.g., Application Owners, Persons in Charge, the EHS IT, etc.). This input will be used to:

- Review the procedures to ensure they continue to appropriately ensure compliance with the Security Rule;
- Conduct an assessment and evaluation of the procedures as reasonable and appropriate protections against the risks that are known; and
- Review DMH's Workforce compliance with the procedures set forth in this Handbook.

The DMH ISO shall timely report their findings and recommendations to the DMH General Counsel and shall adjust the procedures set forth in this Handbook as is determined to be appropriate.

VIII. OTHER RISK MITIGATION ACTIVITIES

The DMH ISO is responsible for recommending strategies, and implementing and maintaining approved strategies to mitigate risks identified in DMH's ongoing risk management activities. This may include any of the following:

- Working with leads of the applicable risk management activities to help evaluate risk.
- Prioritizing risk management strategies based on risk level determination;
- Evaluating and determining process(es) and/or technical solution(s) designed to mitigate identified risks, while balancing the confidentiality, integrity, and availability of PHI. In doing so, the DMH ISO needs to facilitate the determination of a level of reasonability and scalability of possible solutions for DMH senior management consideration based on the size, complexity, organization capabilities, cost, technical capabilities, probable threats, and/or related costs. The DMH ISO, shall work with the DMH General Counsel in determining other stakeholders that need to be involved in this process; including but not limited to the DMH's Office of Administration and Finance, EHS IT, Mental Health Services; Child, Youth and Family Services; other senior management.
- After the process and/or technical solution is identified and appropriately approved, the DMH ISO, working with the ACIO, shall appropriately assign the various related implementation tasks to facilitate a realistic implementation process;
- Ensuring that any and all related policies and procedures be updated, including training materials;
- Ensuring, to the extent that Workforce functions will be affected by a chosen solution, that this is accounted for and addressed with appropriate senior management and that an appropriate implementation plan is approved by key stakeholders and that the Workforce Members are adequately trained on the new policies and/or procedures; and
- Documenting the decisions that are made regarding risk mitigation.

IX. CITATIONS

Regulatory Reference	Risk Analysis 45 CFR 164.308(a)(1)(ii)(A) Risk Management 45 CFR 164.308(a)(1)(ii)(B) System Activity Review 45 CFR 164.308(a)(1)(ii)(D) Audit Controls 45 CFR 164.312(b) Policy Development Risk 45 CFR 164.308(1)(i)

X. ATTACHMENT A

Documentation