CHAPTER 9
CONTINGENCY PLANNING

I. OVERVIEW

Chapter 9 establishes the procedures for responding to an emergency or other occurrences that damage IT Systems or Databases.

The goal is to ensure that a disaster recovery and contingency plan is in place for each EPHI System and Database and other IT Systems or Databases that are identified as supporting an essential service or function of DMH. The plans should help DMH avoid, or at least minimize, the interruption of essential DMH services and functions due to a loss of electricity, fire, network failure, vandalism, natural disaster, or other occurrences that threaten or harm DMH electronic Information Resources or data.

II. EMERGENCY PLANNING

A. DMH must have plans as to how to continue operations when one or more of its systems and/or databases are not available. These plans include down-time procedures.

B Executive Order 490 mandates that all Agencies have a Continuity of Operations Plan (COOP). The COOP for DMH is maintained and managed by the Director of Emergency Management.

C HIPAA requires that Covered Entities, such as DMH, establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI. The existing DMH COOP Plan is posted on the intranet at https://eohhsintranet.ehs.state.ma.us/DMH%20Site/preparedness.asp. The DMH COOP is part of the Executive Office of Health and Human Services' COOP.

III. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

A. Maintenance of the Business Continuity and Disaster Recovery Plan.

The Director of Emergency Management shall oversee the completion, revision, implementation, and testing of a DMH wide Business Continuity and Disaster Recovery Plan.

B Contents of the Business Continuity and Disaster Recovery Plan.

At a minimum**,** the DMH wide Business Continuity and Disaster Recovery Plan must contain the following:

1. Identification of all IT Systems and Databases that support a DMH service or function identified as being essential. (*See* Chapter 3, Section II.D, High Criticality Level.)

2. Identification of the minimum necessary hardware, software, and staff needed to operate each of the IT Systems and Databases. If a system is Software as a Service, the minimum connectivity needed to operate.

3. Identification of key operational resources for each IT System or Database that is outside the control of DMH.

4. The Criticality Level assigned to each IT System or Database. (*See* Chapter 3, Section II.D.)

5. The determination of the order of priority for restoring IT Systems and/or Databases after a disaster or an emergency to ensure that the most critical IT Systems and/or Databases are restored first.

The Plan needs to address how different levels of criticality will be down-time operated and brought back online based on the levels of criticality identified by the Application Owner where multiple levels may apply to a single application.

7. Identification of the initial notification and triage procedures for making the Business Continuity and Disaster Recovery Plan operational (including roles and responsibilities).

8. Identification of recovery time objectives. Determination of how long a loss can be tolerated before implementing a contingency plan.

9. System Specific Business Continuity and Disaster Recovery Plans for each IT System and Database. The System Specific Business Continuity and Disaster Recovery Plans must meet the requirements set forth in Section III.C.

10. Determination of the quantity and type of staff and supplies required for implementing the Plan.

11. Procedures for monitoring, testing, and updating the DMH wide Business Continuity and Disaster Recovery Plan.

12. Determination of the training necessary to implement and maintain the Plan.

C. System Specific Business Continuity and Disaster Recovery Plans

1. Every IT System or Database must have a system specific Business Continuity and Disaster Recovery Plan (a "Specific Plan"). This includes Software as a Service systems.

2. Responsibilities of Application Owners of IT Systems/Databases. Every Application Owner of an IT System or Database that is identified as supporting an essential DMH service or function (*See* Chapter 3, Section II.D, High Criticality Level) is responsible for developing and implementing a Specific Plan for their System or Database.

For an IT System or Database that is owned and/or controlled by the Commonwealth, a Specific Plan must meet the requirements of this Section III.C., System Specific Business Continuity and Disaster Recovery Plans. In addition, each Application Owner is responsible for regularly testing and updating their Specific Plans in accordance with the Plans' testing and update specifications. An Application Owner must work with the DMH ISO and ACIO, or their designees, to develop the Specific Plans.

For an IT System or Database that is not owned and/or controlled by the Commonwealth, such as Software as a Service, the applicable Application Owner shall work with the vendor owner of application and/or EHS IT and/or EOTSS, as applicable, to determine if an appropriate IT System or Database Specific Business Continuity and Disaster Recovery Plan is in place or to develop one, if necessary. If the vendor owner of such IT System or Database does not cooperate, the Application Owner shall develop the Specific Plan to the extent possible and flag to the DMH ISO and ACIO, or their designees, those areas that need further development. The provisions set forth in this Section III.C.2. shall otherwise be followed by the Application Owner in developing a Specific Plan.

Note: A disaster recovery plan is often part of the agreement for contracted services.

a. DMH Person in Charge Responsibilities. To complete a Specific Plan, an Application Owner must work with the Person in Charge of

each DMH Location where the applicable IT System or Database is used to: (a) determine if the Specific Plan, especially the emergency mode of operation (down-time procedures) portion, can be operationalized in a standard manner as specified in the Specific Plan and/or if any modification is necessary for the Location; and (b) determine what a potential loss of the IT System or Database means for each Location and how best to minimize the loss.

b. Contents of a Specific Plan. A Specific Plan shall, at a minimum, contain the following information:

Name of System/Database
Application Owner
Indication if it is on the Network or, if not, where it is maintained and by what entity.
Criticality Level (as determined by the Application Owner in conjunction with the DMH ISO.) *See* Chapter 3, Section II.D.
Primary maintenance staff name/office/contact information
Back-up maintenance staff name/office/contact information
Key users
DMH Locations where the IT System or Database is used
Other systems it is dependent on for operational purposes (e.g., the Network) and their Criticality Levels
Where the system is physically housed Location and room number or off-site location.
Back-up schedule Ensure that the back-up plan developed by EOTSS, EHS IT, or a vendor for the IT System or Database and the Specific Plan are consistent.
Type of back-up media
Where back-up media is located
The back-up retrieval process Description of how one can access the back-up media in an emergency.
Identified potential risks to the IT System or Database – Outline of the emergency levels covered by the Specific Plan. • At a minimum, each risk identified in the DMH wide COOP must be addressed. • The likelihood of each risk must be described.
First response • The initial notification and triage procedures (identify roles and responsibility). • The levels of emergencies covered by the Specific Plan and the general response that is required for each level.

Emergency mode of operations procedures (down-time procedures). The operational procedures must detail how equivalent services are to be provided until the IT System or Database is restored to normal operating mode. The procedures must include:

- Manual procedures that need to be implemented to enable continuation of essential services and functions until the IT System or Database has been restored. (down-time procedures)
- Identification of potential alternate locations (workstations and/or workspace), equipment and off-site storage facilities. (Contact information for accessing such space, workstations, etc.)
- Identification of processing priorities.
- Methods for providing for the back-up and/or replacement of information, equipment, and staff.
- Procedures for assuring the security of EPHI until such time as the IT System or Database has been restored and the data has been entered into the IT System or Database.
- Identification of critical resources and inventories needed to implement the procedures. (e.g., critical forms and supplies are stocked on and off-site)

The procedures must be documented and available as a training resource to all staff members with roles/responsibilities identified within the Specific Plan.

Procedures for recovering lost or damaged data.

- Current system application and documentation need to be located on and off-site in a secure manner. (Specify where such are located.)
- These procedures, at a minimum, must address the following:
  - Back-up plan for obtaining needed hardware and software.
  - Plan for loading the operating systems.
  - Plan for loading data from the most current back-up.
  - Plan for checking systems and data integrity.
  - Plan for performing quality assurance.
  - Plan for communicating that the system or database has been restored and that staff may return to normal operations.
- Identify the staff members responsible for carrying out the recovery.
- If the relocation of staff and/or clients to an appropriate alternate site where system or database is operational is an option, the procedures must specify proposed alternative locations and the staff and/or clients who will need to be relocated.
- The procedures must be documented and available as a training resource to all staff members that have roles/responsibilities identified within the Specific Plan.

Testing of the Specific Plan

A Specific Plan shall specify how frequently it will be reviewed, updated, and tested and who is responsible for such. At a minimum:
• A Specific Plan must be tested at least annually.
• Test results must be reported to the DMH ISO. A report shall include documentation of any modifications made to the Specific Plan due to the test results.
• Key items to be tested:
  ◦ Accuracy and timeliness of data backup files.
  ◦ Ability to restore operations at an alternate location.
  ◦ Correctness of relevant contact information.
  ◦ Verified identification of resources deemed critical in support of the system.

Training/Communication/Coordination • Specifics as to how applicable staff will be trained and otherwise made aware of the Specific Plan. • Specifics as to what coordination must be done with other DMH Divisions or Locations and/or with non-DMH entities to implement the plan and how that coordination will be accomplished.
Date the Specific Plan was developed and approved • Date the Specific Plan last reviewed. • Date the Specific Plan last tested. • Date the Specific Plan last modified.

c. Approval

i. Review and Approval. When developing a Specific Plan, the Plan must be submitted to the DMH ISO for review and feedback. The final Specific Plan must be approved by the ACIO and the DMH ISO, or their designees. All approved Specific Plans will be included in the DMH wide Business Continuity and Disaster Recovery Plan. All amendments to a Specific Plan must also be approved by the ACIO and the DMH ISO, or their designees and will be included and the DMH Statewide Business Continuity and Disaster Recovery Plan. Each application owner is responsible for ensuring that the Specific Plan maintained in the DMH wide Continuity Plan and Disaster Recovery Plan is the most current version of the Specific Plan.

ii. Timing. A Specific Plan must be approved prior to the IT System or Database being operationalized. The DMH ISO and the ACIO, or their designees, may waive this requirement, provided that a specific date is established for the submission and approval of a Specific Plan.

D. Documentation.

Copies of all Specific Plans and the DMH wide Business Continuity and Disaster Recovery Plan shall be kept by the DMH ISO for a period of at least six (6) years from the date such plans were last in effect. Copies shall also be kept by the DMH Director of Emergency Management. The DMH ISO shall ensure that appropriate staff have access to such Plans as is necessary to ensure their proper implementation.

E. Testing and Audits.

The DMH ISO and the ACIO, or their designees, shall periodically test the DMH wide Business Continuity and Disaster Recovery Plan and each of the Specific Plans. In addition, the Director of Emergency Management, in collaboration with the DMH ISO, shall periodically conduct audits of the Specific Plans to ensure they are being timely reviewed and tested and to ensure that staff are aware of them and if they have duties or responsibilities in implementing a Plan that they know what those duties and responsibilities are.

IV. CITATIONS

Regulatory Reference	Data Backup Plan CFR §164.308(a)(7) Disaster Recovery Plan 45 CFR §164.308(a)(7) Emergency Mode of Operational Plan 45 CFR §164.308(a)(7) Testing and Revision Procedures 45 CFR §164.308(a)(7) Applications and Data Critical Analysis 45 CFR §164.308(a)(7) Security Policy Review 45 CFR § 164.308(a)(8) Executive Order 490