CHAPTER 3
REGISTRATION OF SYSTEMS AND DATABASES USING EPHI

I. OVERVIEW

Chapter 3 establishes the tracking of EPHI Systems/Databases that contain EPHI. DMH must have a current inventory of all PHI systems that are used and maintained by Workforce Members. In addition, Chapter 3 also provides guidance on the establishment of criticality levels and the acquisition of electronic Information Resources.

II. EPHI SYSTEM/DATABASE REGISTRATION REQUIREMENTS

A. EPHI Systems/Databases Inventory.

The DMH ISO shall maintain or have access to a current inventory of all EPHI Systems/Databases. The inventory shall include, without limitation, the Application Owners, the respective DMH Locations where the Systems/Databases are used, and the Criticality Level. (*See* Section E, below.) The DMH ISO shall review the EPHI Systems/Databases inventory on a yearly basis to ensure that the EPHI Systems/Databases are still in use within DMH.

B. Registration Process and Records.

All EPHI Systems/Databases must be registered so that it is made known to the DMH ISO.

1. The Application Owner of an EPHI System/Database not previously registered with the DMH ISO must register such EPHI System/Database prior to using it for its intended purpose and/or before it is implemented. To register a new EPHI System/Database, the Application Owner must complete an EPHI System/Database Registration Form and send it to the DMH ISO at DMHSecurityOfficer@MassMail.State.MA.US. The link to the Form is provided here and included at the end of this Chapter 3. Prior to using any EPHI in an EPHI System/Database the DMH ISO must accept the initial registration.

2. A new EPHI System/Database Registration Form must be filed if:

   - A major change or enhancement is made to the EPHI System/Database;
   - There is a change in the type of EPHI that is created or maintained by the EPHI System/Database;
   - The is a change in the purpose or in the use of the EPHI System/Database;

- There is a change of Application Owner or Access Coordinator; or
- There is a change in the procedures for access. (See Section II.D.1., below.)

The Application Owner should seek advice from the DMH ISO as to whether a change to the EPHI System/Database warrants the filing of a new EPHI System/Database Registration Form.

3. The DMH ISO shall maintain copies of each EPHI System/Database Registration Form that is filed for as long as the applicable EPHI Systems/Database is used at DMH, and for a minimum of six (6) years from the date the EPHI System/Database ceases to be used.

C. Verification with the DMH Privacy Officer Concerning Designed Record Set.

The DMH ISO shall provide the DMH Privacy Officer with a copy of each new EPHI System/Database Registration Form that is filed. The DMH Privacy Officer will review all newly created EPHI Systems/Databases and each new form to ensure compliance with Chapter 5 Section III.B. of the DMH Privacy Handbook.

D. Establish Criticality Levels

The Application Owner in conjunction with the DMH ISO shall assign a Criticality Level to every EPHI System/Database and any other IT System or Database identified as being a system or database that supports an essential DMH service or function. The Criticality Levels serve as the order in which IT resources should be allocated to recover IT Systems and Databases should a disaster or emergency occur. The Criticality Levels that are assigned shall be reflected in the Specific Business Continuity and Disaster Recovery Plans that are developed pursuant to Chapter 9 of this Handbook and in the EPHI System/Database registry that is established pursuant to this Chapter 3. The Criticality Levels shall be as follows:

High – an IT System or Database that supports an essential service or function that must be available with only a minimum amount of downtime (i.e., forty-eight (48) hours or less) since the lack of availability will have a significant impact on DMH and/or those receiving services from DMH.

Medium – an IT System or Database that supports a time-critical service or function that should be available with only a temporary amount of downtime (i.e., two (2) to seven (7) days) since the lack of availability for a greater period of time will adversely impact DMH and/or those receiving services from DMH.

Low – an IT System or Database that does not support a time-critical service. These Systems/Databases can be suspended for a reasonable period of time (i.e., one (1) or two (2) weeks) resulting in only minimal disruptions to DMH and/or those receiving services from DMH.

E. Person in Charge

Upon request, the DMH ISO shall furnish each DMH Person in Charge with a list of the EPHI Systems/Databases used in their Location.

III. PURCHASE, LEASE OR OTHER ACQUISITION OF AN ELECTRONIC INFORMATION RESOURCE

1. The purchase of any Information Resource by DMH and all peripherals must be approved by the Deputy Commissioner of Management and Budget, or their designee.

2. To purchase an Information Resource check with the ACIO on the current procedure.

3. When purchasing any Information Resource that may use, maintain, disclose, receive, create, transmit or otherwise obtain PHI ensure the HIPAA appropriate language is included in contract.

4. A Risk Assessment for any Information Resource must be completed before the system can go online. (See Chapter 8 of this Handbook.)

IV. CITATIONS

Regulatory   Accountability 45 CFR 164.310(d)(2)(ii)
Reference   Security Management 45 CFR 164.308(a)(1)(i)
              Device and Media Control 45 CFR 164.310(d)
              Protection from Malicious Software 45 CFR 164.308(a)(5)(ii)(c)
              Applications and Data Critical Analysis 45 CFR §164.308(a)(7)

V. ATTACHMENT

EPHI System/Database Registration Form