CHAPTER 2
INFORMATION SECURITY INCIDENT
REPORTING AND RESPONSE PROCEDURES

I. OVERVIEW

Chapter 2 sets forth DMH's Information Security Incident reporting and response procedures. The procedures are designed to enable Workforce Members to identify, report, and respond to Information Security Incidents in an effective, timely, and coordinated manner.

DMH follows and complies with the Information Security Incident Management Standard (Standard) set forth in the EOTSS Enterprise Information Security Policies and Standards and the EOHHS Acceptable Use Policy (AUP). All Workforce Members are expected to review and comply with the Standard and the AUP.

II. DEFINITION

Information Security Incident (Incident) has the meaning set forth in the Standard.[1] Other capitalized terms not otherwise defined in this Chapter 2 or in the Glossary to this Security Handbook have the meaning set forth in the Standard.

Some examples of Incidents include, but are not limited to:

- Unauthorized and illegal disclosure, destruction and/or alteration of files, Information Resources and information, including confidential information.
- Unauthorized use of an Information Resource for the transmission, processing or storage of information.
- Changes to system hardware, firmware or software characteristics made without the knowledge or consent of the IT Information Owner.
- Detection of malware or malicious code (viruses, worms, etc.).
- Unauthorized probes, scans or sniffers on an Information Resource.
- Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.
- Harassment and threats conducted via Commonwealth email resources.

[1] It is important to note that the Standard definition of Incident is broader than, but inclusive of, the HIPAA definition.

HIPAA Definition (45 CFR §164.304): Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

EOTSS Standard Definition (as of September, 2023): A security incident is defined as any event which has the potential or has already resulted in the unauthorized acquisition, misappropriation, use or manipulation of information that compromises the confidentiality, integrity or availability of the Commonwealth's Information Assets.

- Web page defacement, unauthorized use of system privileges and attempts (either failed or successful) to gain unauthorized access to a system or its information.
- Legal or regulatory violations involving Information Resources.
- Violation of the Commonwealth's information security policies.
- Cyber-stalking, identity theft or child pornography.
- Unauthorized physical access to a secure area (e.g., data centers).

III. REPORTING AN INFORMATION SECURITY INCIDENT

A. Workforce Members Duty to Report

All Workforce Members are responsible for immediately reporting upon discovery any suspected Incident. Such reports must be made as provided in Section III. C. and D. below.

B. Non-Workforce Members

Any individual who is not a Workforce Member may report a suspected Incident involving a Workforce Member, DMH data and/or an Information Resource to the DMH ISO or any Workforce Member. A Workforce Member who receives such a report shall forward the information to EHS in accordance with the AUP and Section III.C. and D., below. If possible, the Workforce Member should provide the individual making the report with EHS Support Services' telephone number, 617-994-5050**,** so if the individual elects, they can report the Incident directly to EHS.

C. Reporting Procedures

If a Workforce Member detects or suspects that there has been an Incident or is notified of a potential Incident under Section III.B., above, they must notify EHS. The Workforce Member shall also notify their DMH Supervisor and the DMH ISO. All Incidents must be reported immediately whenever possible, or within thirty (30) minutes of discovery. If the suspected Incident involves a Workstation that the Workforce Member is using, they shall not reboot, disconnect, or otherwise alter the Workstation unless directed to do so by EHS Support Services (EOHHS HelpDesk).

EHS Contact Information for reporting a suspected Incident is (all of the following contacts must be notified: EOHHS SCIO, CISO, Security, and EOHHS Support Services (HelpDesk)):

EOHHS SCIO: Mike.Guerin@mass.gov
EOHHS CISO: Anthony.Ristaino@mass.gov
EOHHS Security: EHS-DL-SecurityOperations@mass.gov

EOHHS Support Services (HelpDesk):
Systemssupporthelpdesk@mass.gov or (617)-994-5050

DMH ISO Contact Information for reporting a suspected Incident is:

Telephone: 617-626-8187
Email: DMHSecurityOfficer@Mass.Gov

D. Information Security Incident Log and Reporting

If a Workforce Member detects or suspects that there has been an Incident or is notified of a potential Incident under Section III.B., above, they must file an Incident report in the DMH RL6 Reporting System (RL6) (i.e., the DMH software utilized for tracking Incidents) or report such event to the Person in Charge or to a Workforce Member with responsibility to file Incidents in RL6.

Incidents will be filed separately in RL6 from any other allegations that may arise from or relate to the same events, facts or circumstances. (*See* Section III.F., below.) A single combined Incident and privacy report can be made when an Incident involves PHI. (*See* Section III.E., below.) RL6 records will be maintained so that information about Incidents filed in the immediately preceding six (6) years is readily retrievable.

E. Suspected Information Security Incident Involving PHI

If a suspected Incident could involve a disclosure of PHI (in any form, including EPHI) contrary to the DMH Privacy Handbook and/or the unauthorized access to PHI, the Workforce Member reporting the suspected Incident shall report the potential violation of privacy as set forth in Chapter 16, Privacy Report Process, of the DMH Privacy Handbook.

F. Separate Reporting Under DMH Regulations.

An Incident may also give rise to a Human Rights complaint pursuant to 104 CMR 32.00, in which case a complaint should be filed in accordance with 104 CMR 32.00 and/or reported to the Person in Charge or to a Workforce Member with responsibility to file complaints in RL6. For example, an allegation of using the Commonwealth email resources to harass or threaten a client would be both an alleged Information Security Incident and an alleged condition that is dangerous, illegal or inhumane. Human Rights complaints will be processed in accordance with 104 CMR 32.00.

IV. RESPONSE TO A REPORTED INFORMATION SECURITY INCIDENT

A. Response to Information Security Incident

Upon being notified of the existence of a DMH related Incident, EHS will follow the Standard for investigating and processing of the Incident.

DMH may conduct its own investigation in accordance with the DMH Privacy Handbook of any Incident potentially involving PHI.

B. Review of the Incidents

RL6 is monitored by the DMH ISO to remain apprised of and review Incidents involving DMH.

The DMH ISO shall review Incidents filed in RL6 periodically to determine if any systemic problem(s) may exist with regard to security and if so, to develop plans to address such problem(s).

V. PREVENTION

EOTSS and EHS IT routinely monitor and scan the Network for anomalies and vulnerabilities and has developed protections procedures for the configuration of the Network, including Information Resources.

VI. DUTY TO COOPERATE

All Workforce Members must cooperate with EOTSS and EHS IT, the DMH ISO, the DMH Privacy Officer, the Person(s)-In-Charge, the federal Office for Civil Rights and anyone else designated by DMH or any of these state or federal agencies regarding an investigation of a reported suspected Incident, and all efforts to respond to and correct same. Workforce Members must immediately comply with directives from EOTSS, EHS IT and/or the DMH ISO regarding steps to be taken to control or end an Incident. This may include instructions to disconnect their Workstation from the Network, etc.

VII. PERSONAL DEVICES

Excepted Permitted Use of Personally Owned Devices. If a DMH Manager permits use of a personally owned device to access Information Resources, any personally owned device, such as a computer, smartphone, etc., which is determined to have contributed to an Incident may be subject to seizure and retention by the Commonwealth. Such devices may be held until such time as all matters relating to the Incident have been resolved. By using these devices within the Network, individuals are subject to DMH policies restricting their use. (*See* Chapter 6, Section VII. regarding the use of personally owned devices).

VIII. REVIEW OF INFORMATION SECURITY INCIDENTS, TESTING, AND UPDATING PROCEDURES

The DMH ISO working with the Information Security Coordinators shall, on a periodic basis:

- Review Incident reporting and response practices and procedures to determine if the procedures are being followed.
- Follow up on EHS recommendations or corrective actions.
- Review effectiveness and efficiency of the Incident response procedures.
- Review Incident response and reporting procedures and recommend any improvements to the EHS Security Office.
- Review Incidents that have occurred to evaluate the lessons learned, to make recommendations to DMH Leadership or EHS Security Office, as applicable, based on the results to prevent future occurrences of similar Incidents, and to determine how security can be improved (e.g., hardware, software, and/or policies and procedures).
- Issue alerts or warnings about certain actions that can be taken to reduce vulnerabilities that were exploited during an Incident.

IX. CITATIONS

Regulatory Reference	Security Management Process 45 CFR 164.308(a)(1)(i) Security Incident Procedures 45 CFR 164.308(a)(6)(i) and (ii) M.G.L. c. 6A, sec. 7A and The Acts & Resolves of Massachusetts of 2017 Chapter 64

X. REFERENCES

Enterprise Information Security Policies and Standards
Information Security Incident Management Standard
EHS Acceptable Use Policy