CHAPTER 16
PRIVACY REPORT PROCESS

I. INTRODUCTION

The purpose of this Chapter 16 is to establish a framework for the reporting, investigation, and resolution of allegations of violations of DMH privacy policies and procedures. A further purpose of this Chapter 16 is to protect individual privacy rights, comply with DMH privacy policy and procedures, and improve training and development of Workforce Members. Resolution of violations includes mitigation of harm, education of Workforce Members, and prevention of future violations, as applicable.

A Privacy Report[1] may be filed by any person. All Workforce Members have a duty to make Privacy Reports. (See Section III. A. Duty to Report Violation of Privacy Policies or Procedures.)

Further, HIPAA mandates that DMH have a process for individuals (i.e., Affected Persons) to file complaints about DMH's privacy policies and procedures and its compliance with those policies and procedures or the requirements of subparts D and E of HIPAA. All such complaints will be addressed and resolved through the Privacy Report Process.

In addition, or as an alternative, to filing a report of an alleged violation with DMH, any person may file a complaint with the U.S. Secretary of Health and Human Services. DMH must cooperate in any investigation by the Secretary and the Secretary may review such PHI that is maintained by DMH as they determine is necessary. The procedures for filing a complaint with the U.S. Secretary of Health and Human Services and a copy of the U.S. Department of Health and Human Services complaint form can be found at Filing a HIPAA Complaint | HHS.gov.

II. DEFINITIONS

For purposes of this Chapter 16, the following terms shall have the following meanings:

Affected Person: An individual who is alleged to have been the subject of a Violation of Privacy.

Breach: A reportable breach under a HIPAA (HIPAA Breach) and/or a M.G.L. c. 93H (93H Breach) risk assessment. (See Section VIII.) **Note**: All 93H Breaches are HIPAA Breaches but not all HIPAA Breaches are 93H Breaches.

[1] See Section II for defined terms as used in this Chapter 16 of this Handbook. For other capitalized terms see the Glossary to this Handbook for definitions.

Human Rights Officer (HRO): The person designated as the Human Rights Officer for a program or facility.

Legally Authorized Representative (LAR): For purposes of this Chapter 16, LAR means:

(a) a person or entity with authority to make health care decisions on behalf of an individual (e.g., guardian granted such authority, health care agent under a properly invoked health care proxy, custodial parent);
(b) a person authorized, in writing, by an Affected Person or an Affected Person's LAR to act on behalf of the Affected Person in relation to an identified complaint. Such written authorization shall include allowance for release of PHI to such person (consistent the provisions of HIPAA), allowance for release of the Privacy Case File (see Section XV.B.) to such person, and authorization for such person to request an appeal of any decision; and
(c) in the event of an Affected Person's death, the duly appointed personal representative of the decedent's estate or other person with legal authority to access the Privacy Case File and to act on behalf of the decedent.

Next of Kin: The closest living relative in the following order: current spouse, child (or guardian of any minor child), parent, sibling.

Office of Investigations: The office within DMH responsible for conducting certain investigations under 104 CMR 32.00.

Party means:

(a) the Affected Person;
(b) any Person Complained Of or found to be responsible for any incident or condition subject to review under this Chapter 16; provided, however, a recipient of a service from DMH shall not be deemed a Party by virtue of being complained of; and
(c) the LAR of the Affected Person, as defined above.

Person in Charge: The person having the day-to-day responsibility for the management and operation of the applicable DMH operated program, facility or office. The person with responsibility for issuing a decision letter and, if applicable, a Breach notice on a Privacy Report. The person with responsibility to decide Sanctions.

Person Complained Of (PCO): Person(s) alleged to have committed a Violation of Privacy.

Personal Information: Personal Information is a subset of PHI and includes an Affected Person's first name and last name or first initial and last name in

combination with any one or more of the following data elements that relate to such Affected Person:
(a) Social Security number;
(b) driver's license number or state-issued identification card number; or
(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

Privacy Complaint: A Privacy Report of an incident or condition alleged to be a Violation of Privacy filed with DMH by or at the request of an Affected Person or their LAR.

Privacy Report (Report): A report to DMH of an incident or condition alleged to be a Violation of Privacy. Privacy Reports come from one of two sources: Privacy Complaints and Self-Reports.

Reporter: Any person who files a Privacy Report.

Safety Learning System (SLS): The DMH software utilized for tracking Privacy Reports.

Sanction: An action taken in response to a finding that a Workforce Member is responsible for a Violation.

Self-Report: A Privacy Report filed by a Workforce Member reporting an allegation of a Violation that the Workforce Member committed or that another Workforce Member(s) committed that the reporting Workforce Member became aware of or observed.

Violation of Privacy (Violation): The use or disclosure of PHI by Workforce Member(s) in violation of applicable privacy law and/or DMH privacy policy or procedures and/or DMH's failure to comply with those laws, policies and procedures.

III. GENERAL REQUIREMENTS

A. Duty to Report Violation of Privacy Policies or Procedures. A Workforce Member who believes they or another Workforce Member has violated a DMH policy or procedure relating to PHI and/or otherwise violated the privacy of an individual whose PHI is maintained by DMH must immediately file a Self-Report or report such violation to the Person in Charge or to the DMH Privacy Officer or to a Workforce Member with responsibility to file Privacy Reports in SLS.

B. Duty to Cooperate. All Workforce Members must cooperate in the review of a Privacy Report and respond to a request for information in a complete and timely manner, subject to applicable collective bargaining rights.

IV. COMPLAINT SPECIFIC REQUIREMENTS

A. Notice of Right to File a Complaint. DMH must inform an individual whose PHI is created and/or maintained by DMH, or their LAR, if any, of the right to file a Privacy Complaint with DMH and/or a complaint with the U.S. Secretary of Health and Human Services and how they may exercise these rights. This information must be included in DMH's Notice of Privacy Practices.

B. Right to File a Complaint. An individual whose PHI is created and/or maintained by DMH, or their LAR, may file a Privacy Complaint at any time concerning:

1. DMH's response to their request:

   i. to access PHI (Chapter 11).

   ii. to receive an accounting of the disclosures of PHI made by DMH (Chapter 12).

   iii. to amend PHI (Chapter 13).

   iv. for confidential communications (Chapter 14).

   v. for restrictions on the use and/or disclosure of PHI (Chapter 15).

2. DMH's PHI privacy policies and procedures.

3. DMH's compliance with its PHI privacy policies and procedures and applicable laws, including, but not limited to, concerns about the maintenance and unauthorized uses and disclosures of PHI.

V. DMH PROCEDURES FOR PROCESSING A PRIVACY REPORT

The following procedures will be followed for reviewing Privacy Reports.

A. Notice of Privacy Report Process and Availability of Forms.

1. **Privacy Complaints**. The Notice of Complaint Process and Availability of Complaint Forms set forth in DMH regulation 104 CMR 32.02 will serve as the notice of the process and the availability of forms for Privacy Complaints. 104 CMR 32.02 can be found here: 104 CMR 32 (mass.gov). Privacy Complaints must be made in writing. A complaint form or other separate writing must be uploaded into SLS.

2. **Self-Reports**. Self-Reports may be filed directly in SLS or may be filed using a complaint form or other separate writing submitted to the Person in Charge or to the DMH Privacy Officer or to a Workforce Member with responsibility to file Privacy Reports in SLS.

B. Filing a Privacy Report. Any person may file a Privacy Report.

1. **Privacy Complaints**. Any Workforce Member who is notified or who becomes aware that an Affected Person or their LAR wants to file a Privacy Complaint will provide such person with a form, will offer such person assistance in completing and filing the form, and will provide such assistance, if requested. All Privacy Complaints must be made in writing.

2. **Self-Reports**. A Workforce Member who is responsible for a Violation of Privacy or becomes aware of a Violation will immediately file a Self-Report in SLS or notify, verbally or in writing, the Person in Charge who will be responsible for filing the Privacy Report in SLS. Failure to report a Violation of Privacy of which the Workforce Member has knowledge may result in disciplinary action.

3. Any Workforce Member who receives a Privacy Report will immediately forward such Privacy Report to the Person in Charge, who, if necessary, will document it on a form and/or enter it in SLS, as applicable.

C. Privacy Review. For each Privacy Report the Person in Charge, or their designee, will complete or have completed a privacy review in the form attached to this Chapter 16. The form will include a statement of the facts determined through the Privacy Report factual review, the conclusion, and, if applicable, the identity of the DMH policy or procedure or applicable law at issue, a risk assessment, a determination of whether a Breach occurred, actual or possible actions/mitigations, and what notifications, if any, need to be sent. The applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator will complete the risk assessment.

D. Consultation with the DMH Privacy Officer. At the completion of the privacy review (whether or not a Violation is found), the Person in Charge, or designee, or the applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator shall consult with the DMH Privacy Officer, or designee, as to whether a Violation occurred and if so, the appropriate actions and/or mitigations to be taken.

E. SLS Filing. The SLS system will be used for filing and monitoring Privacy Reports. Privacy Reports will be filed separately in SLS from any other

allegations that may arise from or relate to the same incident. For example, a single incident may involve an allegation of verbal abuse and an allegation of a Violation. A Privacy Report is filed separately in SLS as an Administrative Issue type and ADM/Privacy Violation category. All Privacy Reports will be filed as complaints in SLS. All Privacy Reports, privacy analyses, any Breach notices, decision letters, requests for appeal, and decisions on requests for appeal will be uploaded to SLS. SLS records will be maintained so that information about Privacy Reports filed in the immediately preceding six (6) years is readily retrievable.

VI. PRIVACY REPORT FACTUAL REVIEW

A. Determination of Review Process. Upon receipt of a Privacy Report the Person in Charge, or designee, will determine if:

1. Administrative Review. The Report meets one of the following conditions, it may be resolved administratively in accordance with Section VI.B:

i. makes allegations that are objectively impossible;

ii. repeats allegations of fact that have previously been investigated and resolved in accordance with this Chapter 16; or

iii. there is a reasonable basis to believe there will be no disagreements concerning the facts underlying the allegations in the Report.

3. Fact Finding. There is a reasonable basis to believe there will be disagreements concerning the facts underlying the allegations in the Report, it may be resolved through fact finding in accordance with Section VI.C.

4. Referred to the Office of Investigations. There is a reasonable basis to believe the facts underlying the allegations are uniquely complicated and require referral to the Office of Investigations, it will be reviewed in consultation with the Director of Investigations and the Privacy Officer to determine if it should be referred to the Office of Investigations.

B. Privacy Report Administrative Review.

1. Unless a Privacy Report is resolved pursuant to Fact Finding Review under Section VI.C. or is referred to the Office of Investigations pursuant to Section VI.D., the Person in Charge will undertake or, within two business days of receipt of the Privacy Report, assign the

matter for administrative review in accordance with this Section VI.B. In either case the administrative review will be completed within ten business days of receipt of the Privacy Report. The Person in Charge may authorize an extension of up to ten business days if the Privacy Report is sufficiently complicated or if the applicable persons cannot be interviewed within the initial ten-day period. The Person in Charge will document in the Privacy Report file the reasons for any extension.

2. In the case of a:

i. Privacy Complaint, the Person in Charge, or designee, will interview the Affected Person and Reporter, if different. All reasonable efforts must be made to interview each of these persons, as applicable.

ii. Self-Report, no interviews are required, unless needed to clarify facts.

3. Affected Persons and Reporters who are to be interviewed will be permitted to have a designated representative or a Human Rights Officer present.

4. Workforce Members will, subject to applicable collective bargaining rights, cooperate with the review, and will be permitted to have a designated representative present.

5. Unless a person declines to meet or cannot be located, these meetings will take place within five business days of receipt of the Privacy Report.

6. The purpose of the interview will be to:

i. review the specific allegations in the Privacy Report; and

ii. determine whether there are or will be disagreements concerning the facts underlying the allegations that require further review.

7. The Person in Charge, or designee, will review all records related to the Privacy Report. Review of medical record should not be necessary for administrative resolution.

8. If there is no disagreement concerning the facts underlying the allegations of the Privacy Report, the Person in Charge, or designee, will provide a written report of all undisputed facts and the matter will proceed to the Conclusion set forth in Section VII. The written report

need not duplicate undisputed facts contained in the Privacy Report or ancillary documents uploaded into SLS. If there are disputed facts the Privacy Report will be further processed through fact finding as set forth in Section VI.C.

C. Privacy Report Fact Finding Review.

1. Unless a Privacy Report is resolved pursuant to Administrative Review under Section VI.B. or is referred to the Office of Investigations pursuant to Section VI.D., the Person in Charge, or designee, will undertake or, within two business days of receipt of the Privacy Report, assign the matter for fact finding in accordance with this Section VI.C. In either case the fact finding review will be completed within ten business days of receipt of the Privacy Report. The Person in Charge may authorize an extension of up to ten business days if the Privacy Report is sufficiently complicated or if applicable persons or essential witnesses cannot be interviewed within the initial ten-day period. The Person in Charge will document in the Privacy Report file the reasons for any extension.

2. In the case of a:

i. Privacy Complaint, the Person in Charge, or designee, will interview the Affected Person and Reporter, if different, and each PCO. All reasonable efforts must be made to interview each of these persons, as applicable.

ii. Self-Report, the Person in Charge, or designee, will interview the Reporter and each PCO, if different.

3. Affected Persons who are to be interviewed will be permitted to have a designated representative or a Human Rights Officer present.

4. Workforce Members will, subject to applicable collective bargaining rights, cooperate with the review, and will be permitted to have a designated representative present.

5. Unless a person declines to meet or cannot be located, these meetings will take place within five business days of receipt of the Privacy Report.

6. The Person in Charge, or designee, will interview witnesses and other individuals, including family members, who may have information related to a Privacy Report necessary for determination of essential facts; provided, however, authorization to disclose PHI must be obtained from the Affected Person prior to interviewing any

person who is not a Workforce Member or LAR. A good faith effort to interview each witness and other individuals who may have such information will satisfy this requirement.

7. To the extent practicable, and without unreasonably delaying the fact finding process, the Reporter should be interviewed before any other interviews take place.

8. The Person in Charge, or designee, will review all records related to the Privacy Report including, but not limited to, the Affected Person's medical record, if applicable. Records that are part of a peer review process under M.G.L. c. 111, § 204 are exempt from this review.

9. The Person in Charge, or designee, will provide a written report of findings of fact and the matter will proceed to the Conclusion set forth in Section VII.

D. Privacy Reports Referred to the Office of Investigations for Review.

1. The Director of Investigations may consult with the Privacy Officer to determine the appropriate process for resolution of any Privacy Report that has been referred to the Office of Investigations.

2. To the greatest extent possible, all processes and timelines, including extensions thereof, set forth in 104 CMR 32.00 applicable to complaints referred to the Office of Investigations will apply to Privacy Reports that are referred to the Office of Investigations; provided, however, all Privacy Reports must be concluded and HIPAA Breach notices must be issued within sixty (60) calendar days of the discovery of the Breach.

E. Interview of Affected Persons. In all cases where a Privacy Report is a Self-Report and the Affected Person and/or their LAR, if any, is interviewed, they will be asked if they want a copy of any decision letter that may be issued and if they want a copy one will be provided. In all cases where a Breach is found, DMH is required to provide Affected Persons or their LAR, if any, notice of such Breach.

VII. CONCLUSION

At the conclusion of the factual review, the Person in Charge, or designee, will determine if there was:

A. No use or disclosure of PHI, in which case no risk assessment is necessary and the Person in Charge may issue a decision letter. (See Section XI.C.2.i.b. or ii.)

B. A use or disclosure of PHI; however, such use or disclosure was permitted by DMH policy or procedure or applicable law, in which case no risk assessment is necessary and the Person in Charge may issue a decision letter. (See Section XI.C.2.i.b. or ii.) The Person in Charge, or designee, will state with specificity the DMH policy or procedure or applicable law that permitted the use or disclosure.

C. A Violation of Privacy, in which case a risk assessment is necessary to determine whether the incident constitutes a Breach. (See Section VIII.) The Person in Charge, or designee, will state with specificity the DMH policy or procedure or applicable law that was violated.

The Person in Charge, or designee, may consult with the applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator when making this determination.

VIII. RISK ASSESSMENT

Following the conclusion of any privacy factual review (administrative, fact finding or Office of Investigations) finding there was a Violation of Privacy, the applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator, will complete a risk assessment. The risk assessment will be completed within five business days of the conclusion of any privacy factual review. The risk assessment may be extended from five business days up to ten business days if the factual review is sufficiently complicated or if the applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator determines additional factual review is required. The applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator will document in the Privacy Report file the reasons for any extension.

Further, the applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator, will make determinations regarding whether any mitigations should be sought. Such mitigations may include but are not limited to seeking assurances from an unintended recipient that PHI will not be retained, further disclosed or used inappropriately.

Under certain circumstance, the law requires notification to government entities and/or Affected Persons in the event of a breach of confidential information. Two of the most significant are HIPAA and M.G.L. c. 93H.

A. **HIPAA Risk Assessment.** A use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule is presumed to be a Breach under HIPAA unless DMH demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment that includes at least the following four factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
ii. The unauthorized person who used the PHI or to whom the disclosure was made;
iii. Whether the PHI was actually acquired or viewed; and
iv. The extent to which the risk to the PHI has been mitigated.

DMH may also consider other factors as appropriate. The conclusions drawn from the risk assessment must be reasonable, and the risk assessment must be conducted in good faith.

1. **The nature and extent of the PHI involved**. The first factor includes an evaluation of the types of identifiers involved and the likelihood of re-identification. It also includes an evaluation of the type of PHI involved, such as whether the disclosure involved information that is of a more sensitive nature. With respect to clinical information, this may involve considering not only the nature of services or other information disclosed but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, or test results). Evaluating this information will help to determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the Affected Person or otherwise used to further the unauthorized recipient's own interests.

2. **The unauthorized person who used the PHI or to whom the disclosure was made**. DMH must consider the identity of the unauthorized person who used the PHI or to whom the disclosure was made. Under this factor, DMH should consider whether the unauthorized person who received the information (if any) has obligations to protect the privacy and security of the information.

3. **Whether the PHI was actually acquired or viewed**. DMH must investigate whether the PHI at issue was actually acquired or viewed, or, alternatively, if only the opportunity existed for the information to be acquired or viewed. For example: if a laptop that is stolen and later recovered and a forensic analysis shows that data on the laptop was never accessed, there was an opportunity for an unauthorized disclosure but the PHI was not disclosed. For contrast, if PHI is sent to an incorrect recipient and DMH knows the information was actually received by the recipient it will be presumed that PHI was acquired or viewed, unless DMH can determine the PHI was not viewed and has been destroyed or deleted.

4. **The extent to which the risk to the PHI has been mitigated**. DMH must determine the extent to which the risk to the PHI has been

mitigated. Potential mitigation steps include obtaining satisfactory assurances from the recipient of the PHI that the PHI will not be further used or disclosed. DMH should also consider the efficacy of any potential mitigation.

At the conclusion of the HIPAA risk assessment the applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator will determine if the overall risk assessment weighs for or against finding that the incident constitutes a Breach under HIPAA.

B. M.G.L. c. 93H Risk Assessment. M.G.L. c. 93H is the Massachusetts data breach notification statute and is designed to protect against identity theft. It requires notification in the event of a Breach of Personal Information.

M.G.L. c. 93H requires notification to Affected Persons and to the Massachusetts Attorney General and Office of Consumer Affairs and Business Regulation ("OCABR") when a data holder "(1) knows or has reason to know of a breach of security," or "(2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose…." M.G.L. c. 93H § 3. Additionally, state agencies, such as DMH, are required to notify the Massachusetts state information technology division and the Massachusetts division of public records. *Id.*

"Breach of security" is defined as "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth." M.G.L. c. 93H § 1.

In the event of a Breach under M.G.L. c. 93H, the applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator will state with specificity what Personal Information was acquired/used and by whom. The applicable OIM Director of Health Information, or designee, or Area Privacy Coordinator will immediately report such Breach to the Person in Charge and the Privacy Officer. The Person in Charge will assign staff, as necessary, to comply with the reporting and any other applicable requirements of M.G.L. c. 93H.

IX. ACTIONS/MITIGATION

Following the conclusion of the risk assessment, whether or not a there is a finding of a Breach, the Person in Charge will make determinations (or, in the case of a designee, recommendations) regarding appropriate actions and/or

mitigations to be taken in response to the finding of a Violation. Such actions and/or mitigations may include but are not limited to training or retraining, recommendations for new or modified trainings, recommendations for new or modified policies or procedures.

Where a PCO has been found to have violated an established DMH privacy policy or procedure such action will include, at a minimum, retraining the PCO regarding the violated DMH privacy policy(s) or procedure(s). If the Workforce Member has been removed from the workforce, such retraining must be completed and documented in SLS before the Workforce Member resumes the Workforce Member's duties. Retraining is intended to protect client rights, comply with DMH policy, promote health and safety of staff and clients, and improve training and development of staff. Retraining is not meant to constitute or be construed as disciplinary action and does not preclude disciplinary action per usual processes. Except where a Workforce Member has been removed from the workforce, as set forth above, documentation of completion of retraining will be entered in SLS no later than ten business days from the date of issuance of the decision letter.

The results of the Privacy Report review process may be referred to Human Resources and/or Labor Relations and Management for further review and possible disciplinary action. (See Section XVI.)

X. REPORTS AND NOTICES

The Person in Charge will determine (or, in the case of a designee, recommend) what reports and notices are required, such as:

A. Report to the U.S. Secretary of Health and Human Services in the event of a HIPAA Breach (See Section XIX.);

B. Notice to Massachusetts Attorney General, Office of Consumer Affairs and Business Regulation, Massachusetts state information technology division, and the Massachusetts division of public records in the event of a M.G.L. c. 93H Breach. (See Section VIII.B.); and

C. Breach notices/decision letters to applicable Parties or others. (See Section XI.C.)

XI. BREACH NOTICES/DECISION LETTERS

A. **Special Rules**. HIPAA regulations regarding providing notices differ in certain circumstances. Immediately contact the Privacy Officer for additional guidance in the event of a HIPAA Breach involving five hundred (500) or more Affected Persons or a law enforcement delay.

B. **Timing**. Within five business days following the completion of any Privacy Report factual review and risk assessment, the Person in Charge will provide a written decision letter or a Breach notice, as applicable. All HIPAA Breach notices must be issued within sixty (60) calendar days of discovering the Breach. All 93H Breach notices must be issued as soon as practicable and without unreasonable delay.

C. **Persons to Receive Breach Notice/Decision Letter**.

1. Breach. In the event of a Breach, the Affected Person or LAR, if applicable, will be provided a HIPAA Breach notice or 93H Breach notice, as applicable, and the applicable HRO will be provided a copy. If the LAR is provided the Breach notice, the Affected Person will be provided a copy. The PCO will receive a decision letter.

2. Violation but No Breach or No Violation.

i. Complaints/Requested. Except in the case of a Breach, in the event of Privacy Complaint (i.e., a Privacy Report filed by or at the request of an Affected Person or their LAR) or the Affected Person or their LAR was interviewed and has requested a copy of the decision letter:

a. Violation but No Breach. Where there is a finding of a Violation but no Breach, the Affected Person or LAR, if applicable, will be provided a decision letter reflecting that a Violation was found and the applicable HRO will be provided a copy. If the LAR is provided the decision letter, the Affected Person will be provided a copy. The PCO will receive a separate decision letter; or

b. No Violation. Where there is a finding of no Violation (no use or disclosure of PHI or there was a use or disclosure of PHI; however, such use or disclosure was permitted by DMH policy or procedure or applicable law) all Parties and the applicable HRO will be provided the same decision letter.

ii. Self-Reports/Not Requested. Except in the case of a Breach, where there is a Self-Report and the Affected Person or their LAR has not requested a copy of the decision letter, a decision letter will be provided only to the PCO. In such cases, DMH will not advise the alleged Affected Person of a Report that did not compromise their PHI.

Note: See the Quick Reference Guide to Breach Notices and Decision Letters at the end of this Chapter. Also see the form Breach notices and decision letters attached to

this Chapter 16.

D. Content of Notices/Decision Letters

1. **HIPAA Breach Notice**. In the event of a HIPAA Breach, notices must contain, to the extent possible:

   i. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

   ii. A description of the types of PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

   iii. Any steps Affected Persons should take to protect themselves from potential harm resulting from the Breach;

   iv. A brief description of what DMH is doing to investigate the Breach, to mitigate harm to Affected Persons, and to protect against any further Breaches; and

   v. Contact procedures for individuals to ask questions or learn additional information, which will include a toll-free telephone number, an email address, website, or postal address. (See Form HIPAA Breach Notices attached to this Chapter 16.)

2. **93H Breach Notice**: In the event of a 93H Breach, notices must contain all of the information contained in a HIPAA Breach notice and must include:

   i. The Affected Person's right to obtain a police report;

   ii. How an Affected Person may request a security freeze and the necessary information to be provided when requesting the security freeze;

   iii. That there will be no charge for a security freeze; and

   iv. Information necessary for the Affected Persons to enroll in credit monitoring services.

   The 93H notice cannot include the number of Affected Persons by the Breach. (See Form 93H Breach Notices attached to this Chapter 16.)

3. **Decision Letters.** In all cases where a decision letter is to be provided (see Section XI.C.) there will be a written decision containing factual findings, decision of the Person in Charge, actions to be taken, if any, and notification that the Party receiving the decision letter may appeal the finding to the Privacy Officer and/or file a complaint with the U.S. Secretary of Health and Human Services. (See Form Decision Letters attached to this Chapter 16.)

E. Breach Notice: Method of Delivery to Affected Persons

1. **Written Notice.**

   i. Written notification of Breach will be sent by first-class mail to the Affected Person and their LAR, if any, at their last known address.

   ii. If DMH knows the Affected Person is deceased and DMH is issuing a Breach notice, written notification of Breach will be sent by first-class mail to the Affected Person's LAR at their last known address or, if there is no LAR, to the Next of Kin of the Affected Person if DMH has the address of the Next of Kin. Decision letters may NOT be sent to Next of Kin.

2. **Substitute Notice**. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the Affected Person under Section XI.E.1., a substitute form of notice reasonably calculated to reach the Affected Person will be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the LAR or Next of Kin of the Affected Person under Section XI.E.1.

   i. In the case in which there is insufficient or out-of-date contact information for fewer than ten (10) Affected Persons, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

   ii. In the case in which there is insufficient or out-of-date contact information for ten (10) or more Affected Persons, then such substitute notice will:

      a. Be in the form of either a conspicuous posting for a period of ninety (90) calendar days on the home page of the DMH public web site, or conspicuous notice in major print or broadcast media in geographic areas where the Affected Persons likely reside; and

b. Include a toll-free phone number that remains active for at least ninety (90) calendar days where an Affected Person can learn whether the Affected Person's PHI may be included in the Breach.

All forms of substitute notice utilized will be noted in SLS.

3. Additional Notice in Urgent Situations. In any case deemed by the Person in Charge or the Privacy Officer to require urgency because of possible imminent misuse of PHI, DMH may provide information to Affected Persons by telephone or other means, as appropriate, in addition to notice provided under Section XI.E.1. or E.2. Any such notice will be noted in SLS.

F. Decision Letter: Method of Delivery

1. Written Notice.

i. Written notification of decisions will be sent to the applicable persons, as set forth in Section XI.C., at their last known address by first-class mail or in-hand.

ii. If DMH knows the Affected Person is deceased, decision letters may NOT be sent to the Next of Kin or the LAR, unless the LAR is the duly appointed personal representative of the decedent's estate or other person with legal authority to access the Privacy Case File and to act on behalf of the decedent.

2. No Substitute Notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the Affected Person under Section XI.F.1., no substitute form of notice will be required.

G. Reporter. Subject to the redaction of all protected information, as set forth in in Section XII, a Reporter who is not otherwise a Party, may receive an acknowledgment letter containing a summary of the factual review process and decision of the Person in Charge or, if applicable, a copy of the Breach notice.

XII. RELEASE OF BREACH NOTICE/DECISION LETTER

Any Breach notice or decision letter issued pursuant to this Chapter 16 that is to be released to a Party or any other person in accordance with this Chapter 16 or as otherwise required by law will be subject to redaction of PHI or any other information that the recipient is not legally authorized to receive consistent with the requirements of federal and state privacy laws, including but not limited to,

the provisions of HIPAA, Fair Information Practices Act (FIPA), M.G.L. c. 66A, M.G.L. c. 123, § 36, and applicable exemptions under M.G.L. c. 4, § 7(26).

XIII. CLOSING THE PRIVACY REPORT IN SLS

Following the issuance of the Breach notice or decision letter, the Privacy Report will be closed in SLS in one of three ways[2]:

A. Breach. In the event the Person in Charge determines there was a Breach, the Privacy Report will be closed as Substantiated in SLS.

B. Violation But No Breach. In the event the Person in Charge determines there was a Violation; however, there was no Breach, the Privacy Report will be closed as Substantiated in Part in SLS.

C. No Violation. In the event the Person in Charge determines there was no Violation (no use or disclosure of PHI or there was a use or disclosure of PHI; however, such use or disclosure was permitted by DMH policy or procedure or applicable law), the Privacy Report will be closed in SLS as Unsubstantiated.

XIV. APPEAL TO THE PRIVACY OFFICER

A. Filing an Appeal.

1. Applicable Parties.

i. Breach. In the case of any Breach, the PCO will be advised they may appeal the finding of Breach to the Privacy Officer.

ii. Violation But No Breach or No Violation.

a. Privacy Complaints/By Request. In the case of any Privacy Complaint (i.e., filed by or at the request of an Affected Person or their LAR) or the Affected Person or their LAR has requested a copy of the decision letter with a finding of a Violation but no Breach or no Violation, all Parties will be advised they may appeal such finding to the Privacy Officer.

b. Self-Reports/Not Requested. In the case of any Self-Report and the Affected Person or their LAR has not requested a copy of the decision letter with a finding of a Violation but no Breach or no Violation, the PCO will be

[2] The SLS designations of Substantiated, Substantiated in Part, and Unsubstantiated are used for internal record keeping purposes only.

advised they may appeal such finding to the Privacy Officer.

2. General Provisions.

i. An appeal must be submitted in writing to the Privacy Officer within ten business days of receipt of the decision letter, which time period may be waived by the Privacy Officer, upon request and for good cause shown. The Privacy Officer will provide notice of the appeal to the Person in Charge and to any non-appealing Party that received a decision letter, and, to the applicable HRO who received a copy of a decision letter, if any. (See Section XI.C.)

ii. An appeal must be based on one or more of the following factors, which will be set forth with specificity in the request:

a. The fact finder failed to interview an essential witness or to consider an important fact or factor.

b. The decision is not reasonably supported by the facts.

c. The decision is based on an erroneous interpretation of applicable law or policy.

B. Response to Request for Privacy Officer Review.

1. Unless the Privacy Officer determines that additional factual review is required, they will within ten business days from receipt of the appeal affirm or amend the initial decision and issue a final decision letter.

2. If the Privacy Officer determines additional factual review is required, they will conduct or refer the matter for such factual review, which will be completed within ten business days of receipt of the request for additional factual review but which time period may be extended by the Privacy Officer for good cause.

3. Within ten business days of receipt of the results of any additional factual review, the Privacy Officer will issue a final decision letter affirming or amending the initial decision letter.

4. The Privacy Officer's decision letter will be in writing, distributed to all applicable persons.

5. The decision of the Privacy Officer will be final.

XV. PRIVACY REPORT RECORDS

A. **Privacy Report Files**. Files of all reviews conducted pursuant to this Chapter 16 will be maintained by the Person in Charge or Office of Investigations who conducted the factual review. All such files will be maintained for six (6) years from the date of the final disposition of the Privacy Report.

B. **Privacy Case File**.

1. A file, known as the Privacy Case File, shall be kept for each Privacy Report and appeal received by DMH. The Privacy Case File shall consist of the Privacy Report, privacy review, any Breach notice, decision letter, requests for appeal, and decisions on requests for appeal.

2. Release of any portion of the Privacy Case File shall be subject to redaction as set forth in Section XII.

3. Subject to redaction as set forth in Section XII, following the issuance of the Breach notice and/or decision letter(s), upon written request:

i. Any person who is mentioned in the Privacy Case File will have access to a copy of that portion of the Privacy Case File in which they are mentioned.

ii. Any Party, as defined in this Chapter 16, may receive a copy of the Privacy Case File.

iii. In the case of a Privacy Complaint, the Affected Person's attorney may receive a copy of the Privacy Case File, which, pursuant to M.G.L. c. 123, § 36, may contain such Affected Person's PHI.

C. **Public Log**. The provisions set forth in DMH's investigation regulations (104 CMR 32.00) regarding the Public Log, apply to Privacy Reports.

XVI. SANCTIONS

DMH must have in place, apply, and document application of appropriate Sanctions against Workforce Members who fail to comply with DMH policies and procedures relating to PHI.

A. **General.** Workforce Members who violate DMH policies and procedures will be subject to appropriate Sanctions, which may include disciplinary action, up to and including termination of employment. Violations related

to unauthorized use and disclosure of PHI may subject the Workforce Member and DMH to civil and criminal penalties.

B. **Documentation.** Except in the event of retraining, which is documented in SLS and also placed in an employee's personnel record by the Person in Charge, if any Workforce Member becomes subject to disciplinary action for the wrongful use or disclosure of PHI or for violating any other DMH policy or procedure relating to PHI, any disciplinary action imposed will be recorded in their personnel record. Upon request, the applicable Human Resources Office, in conjunction with Labor Relations, where applicable, will be able to provide the DMH Privacy Officer with a report of all disciplinary actions relating to the infraction of DMH privacy policies and procedures that have been imposed during the six-year period immediately preceding the request.

C. **Exceptions.** Sanctions will not be applied to disclosures of PHI by Workforce Members who are whistleblowers or crime victims if the conditions set forth in Chapter 6, Section V.A.12. are met.

D. **Sanctions Against Workforce Members Committing Violations of DMH's Privacy Policy or Procedures**. DMH is strongly committed to ensuring that Workforce Members perform their duties in a professional manner that protects the confidentiality of information. Nothing in this Handbook; however, should be construed to contain binding terms and conditions of employment or be construed as a contract between DMH and its Workforce Members or to conflict with the terms of applicable collective bargaining agreements.

Sanctions against Workforce Members committing a violation of DMH's privacy policy or procedures will be handled in accordance with applicable laws and regulations, collective bargaining agreements, and DMH procedures and/or contractual agreements relating to third-party workforce depending on the classification of Workforce Member being Sanctioned. The Person in Charge is responsible to consult with Human Resources (in the event the employee is a Management employee) and/or Labor Relations (if the employee is a member of a bargaining unit) to determine appropriate Sanctions, including but not limited to disciplinary action.

XVII. REFRAINING FROM INTIMIDATION OR RETALIATORY ACTS

A. No DMH office, program, facility or Workforce Member will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any:

i. Affected Person, or their LAR, if any, for exercising of their privacy rights;

i. person, including a Workforce Member for filing in good faith a Privacy Report with DMH or a complaint with the U.S. Department of Health and Human Services, or for participating in a privacy related investigation, compliance review, proceeding or hearing;

ii. Workforce Member for helping Affected Person or their LAR, if any, to exercise their privacy rights or to file a Privacy Complaint or participate in a privacy related investigation; or

iii. person opposing any act or practice alleged to be unlawful under state or federal law; provided the person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI.

B. Any Workforce Member who becomes aware of retaliatory actions must take immediate steps to ensure that they are stopped and corrected.

C. Workforce Members may report suspected or actual actions of retaliation to Human Resources and/or their union representative, if applicable.

D. Reporting a Violation of Privacy in bad faith or for malicious reasons are grounds for disciplinary action.

XVIII. DMH WORKFORCE TRAINING/ASSISTANCE

All Workforce Members who provide direct care to individuals will be trained on how to receive a Privacy Complaint. Such Workforce Members will provide assistance to Affected Persons and to LARs who need help in filing a Privacy Complaint. (See Section V.)

XIX. MONITORING AND REPORTING RESPONSIBILITIES

The Privacy Officer, and such other persons as the Commissioner of DMH may appoint, will review the Privacy Reports filed in the Safety Learning System periodically to determine if any systemic problem(s) may exist with regard to privacy and if so, to develop plans to address such problem(s).

The Privacy Officer will review, on a regular basis, DMH's activities under this Chapter 16 and provide notices to the U.S. Secretary of Health and Human Services consistent with 45 CFR 164.408, as applicable.

XX. LEGAL REFERENCES, ATTACHMENTS, AND QUICK GUIDE

A. Legal References.

M.G.L. c. 66A, § 2(b)
M.G.L. c. 93H
HIPAA 45 CFR § 160.306
45 CFR § 164.400 et. seq.
45 CFR § 164.402
45 CFR § 164.404
45 CFR § 164.408
45 CFR § 164.520(b)
45 CFR § 164.530(d)
45 C.F.R. § 164.530(e)
Omnibus Rule, Office for Civil Rights, Department of Health and Human Services, 78 Fed. Reg. 5565, 5642 (Jan. 25, 2013).

B. Attachments.

Form Privacy Review

Form Decision Letters:
No Violation
Complaint Violation No Breach
PCO Violation No Breach
PCO Breach

Form Breach Notices:
HIPAA Notice to Affected Person
HIPAA Notice to LAR
93H Notice to Affected Person
93H Notice to LAR

C. Quick Reference Guide to Breach Notices and Decision Letters.

Person in Charge Decision	**Complaint Notice/Letter**	**Self-Report Notice/Letter**
No Violation	No Violation Letter to all Parties and HRO	No Violation Letter to PCO Only

Person in Charge Decision	**Complaint Notice/Letter**	**Self-Report Notice/Letter**
Violation but No Breach	Complaint Violation No Breach Letter to Affected Person/LAR and HRO AND PCO Violation No Breach Letter to PCO Only	PCO Violation No Breach Letter to PCO Only
HIPAA Breach: Notify DMH Privacy Officer Immediately if 500 or more Affected Persons Involved	Notice to Affected Person/LAR and HRO In case of Notice to LAR copy to Affected Person AND PCO Breach Letter to PCO Only	
93H Breach: Notify Person in Charge and DMH Privacy Officer Immediately; Additional Breach Notices are Necessary	Notice to Affected Person/LAR and HRO In case of Notice to LAR copy to Affected Person AND PCO Breach Letter to PCO Only	