Commonwealth Medicine

Name of Standard: Reporting
Breach of Personally Identifiable Information

Responsible Department
UMMS Office of Management (OoM)
Contact: PrivacyandCompliance@umassmed.edu or 508-856-TEAM

STANDARD STATEMENT

Commonwealth Medicine (CWM) recognizes its obligation under state and federal law to timely inform its clients of any Breach of PII and to work with clients to determine if consumer notification is required. Workforce members are required to immediately report any actual or suspected Breach or Security Incident to their supervisor, the UMMS Compliance and Privacy Officer or their designee, the UMMS Information Security Officer, and to the UMMS Help Desk or Campus Police, where appropriate.

REASON FOR STANDARD

State and federal laws and regulations, as well as agreements with clients and owners of the PII, obligate CWM to protect the confidentiality and security of PII and to timely report violations. Failure to comply with such obligations may result in financial penalties, costs imposed to notify consumers and reputational harm.

This standard specifies responsibilities of Workforce members, and places them on notice of potential disciplinary actions and sanctions.

ENTITIES AFFECTED BY THIS STANDARD

All Business Units within CWM and all Workforce members.

APPLICABLE LAWS, REGULATIONS AND POLICIES

M.G.L. 93H (or other states’ security Breach and notification laws) – applies when CWM holds data identifying an individual by first and last name, or first initial and last name, in combination with one or more of the following: Social Security Number; driver’s license number; state-issued identification card number; financial account number or credit or debit card number. MGL c. 93H

HITECH Act and 45 CFR 164.400 – applies to CWM as a Business Associate under HIPAA when it: 1) creates, receives, maintains or transmits PHI on behalf of a HIPAA Covered Entity, or 2) discloses PHI to a third party who creates, receives, maintains, or transmits PHI on behalf of CWM. HIPAA presumes a Breach has occurred if there is an impermissible use or disclosure of PHI and requires notice unless a risk assessment establishes that there is a low probability that PHI has been compromised. The Client,
in the event that the Breach involves data owned by a third-party, typically is responsible for this determination.

**UMMS Policies:**

- *UMMS Information Security Incident Response Team Policy (SIRT Team Policy)*

**RELATED DOCUMENTS**

- Non-Retaliation/Whistleblower Standard
- Complaint Reporting and Investigation Standard
- Disclosure Risk Assessment Report

**SCOPE**

This standard applies to all PII, in tangible or electronic form, that CWM Workforce members use, maintain, disclose, receive, create, transmit, or otherwise obtain.

**DEFINITIONS: (See Glossary on Office of Management (OoM) website for additional definitions)**

**Breach:** The acquisition, access, use or disclosure of PII in a manner not permitted under Subpart E of 45 CFR Part 164, or Personal Information not permitted under M.G.L. c. 93H and other applicable states’ security breach statutes, respectively, which compromises the security or privacy of such information.

**Business Owner:** A CWM/UMMS Senior Manager responsible for the confidentiality, availability and integrity of the impacted data.

**Client Owner:** The external party with whom UMMS maintains a contract and who provided the data to or on whose behalf UMMS collects the data.

**Security Incident:** A verified external or internal attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**SIRT:** SIRT shall mean the Security Incident Response Team authorized under the Information Security Incident Response Team Policy.

**PROCEDURE**

The following process must be followed when a member of the UMMS workforce is involved in, suspects or is aware of a Breach or Security Incident (hereinafter referred to as “Breach” or “Security Incident”) involving PII.

Individual roles and responsibilities are set forth in the table that follows this section.
1. All actual and suspected Breaches shall be reported immediately to the workforce member’s supervisor and to OoM at 508-856-TEAM. Anonymous reports are permitted; however, they are more difficult to investigate and verify. All actual and suspected Security Incidents shall also be immediately reported to the UMMS IT HelpDesk by calling 508-856-8643 in addition to those listed above. Any theft of a device that accesses the UMMS network shall be reported immediately to the Campus Police at 508-856-3296. If the HELP Desk is not open, call Campus Police.

2. Any workforce member reporting an actual or suspected Breach or Security Incident shall complete a Disclosure Risk Assessment Report and return it to OoM to facilitate OoM’s ability to investigate and notify the data owner, if such notification is required by the contract.

3. OoM or the SIRT team, depending on the complexity of the actual or suspected Breach or Security Incident, shall investigate the report and take any necessary action along with the Business Unit to mitigate the harm of the disclosure/incident.

4. OoM shall review any contract, business associate or data use agreement related to PII involved with the actual or suspected Breach or Security Incident to identify requirements to report potential Breaches or Security Incidents to the Client or Business Owners.

5. If the investigation concludes that a Breach or Security Incident occurred, OoM and the Information Security Officer/SIRT team, as appropriate, shall:
   a. conduct a risk assessment to determine if there is a low probability that PHI has been compromised, pursuant to guidelines in state and federal regulations for such assessments;
   b. determine appropriate remediation or retraining; and
   c. recommend to or work with HR with respect to appropriate discipline.

6. OoM shall determine, with the input of the relevant Business Owner and the ISO, if relevant, who shall notify the Client Owner of any findings for which notification is required. Notification to the Client Covered Entity shall be made without unreasonable delay and in no case later than 60 calendar days after discovery.

7. OoM shall work with the Client Owner to prepare any notifications if required by state or federal law.

Anyone found in violation of this standard may be subject to disciplinary action up to and including termination.

---

1 References to OoM for this Standard are to the UMMS Compliance and Privacy Officer or their designee.
## RESPONSIBILITIES

<table>
<thead>
<tr>
<th>Reporting to</th>
<th>Workforce Member</th>
<th>Supervisor</th>
<th>OoM</th>
<th>UMMS ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>OoM</td>
<td>Immediately report an actual or suspected Breach or Security Incident to your supervisor or director of your Business Unit and OoM at 508-856-TEAM. Reports may be made anonymously.</td>
<td>Immediately upon becoming aware of an actual or suspected Breach or Security Incident, contact OoM at 508-856-TEAM.</td>
<td>n/a</td>
<td>The ISO shall notify OoM of any actual or suspected Breach or Security Incident involving CWM data and Business Units that are reported directly to the Help Desk or identified by IT.</td>
</tr>
<tr>
<td>Help Desk or Campus Police</td>
<td>Immediately notify the Help Desk of an actual or suspected Breach or Security Incident involving UMMS’ computer systems or network or for Breaches for which immediate mitigation involving the computer systems is required - at 508-856-8643. Also notify your supervisor and OoM. Notify campus police immediately of the theft of any device that accesses the UMMS network. If the Help Desk is not open, notify Campus Police at 508-856-3296.</td>
<td>Immediately upon becoming aware of an actual or suspected Breach or Security Incident involving UMMS’ computer systems or network or a Breach for which immediate mitigation involving the computer systems is required contact the Help Desk - at 508-856-8643. If the Help Desk is not open, notify Campus Police at 508-856-3296. Also notify OoM.</td>
<td>OoM, the Help Desk and Campus Police shall notify the ISO where ISO input is required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Client Owner or consumer</td>
<td>Do not notify the Client Owner or the consumer of the Breach or Security Incident.</td>
<td>Do not notify the Client Owner or the consumer of the Breach or security incident.</td>
<td>OoM shall review contracts, BAAs, or Data Use Agreements covering the data at issue to determine under what circumstances and when notice to the Client Owner is required. OoM shall confer with the ISO with respect to notice required for</td>
<td></td>
</tr>
<tr>
<td>Workforce Member</td>
<td>Supervisor</td>
<td>OoM</td>
<td>UMMS ISO</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-----</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security Incidents. The decision as to who will notify the Client Owner will be made by OoM in conjunction with the relevant Business Owner, with ISO input as needed.</td>
<td></td>
</tr>
<tr>
<td>Disclosure Risk Assessment Checklist</td>
<td>Complete Disclosure Risk Assessment Checklist and submit to OoM as soon as possible</td>
<td>Ensure that workforce member completes and submits the Disclosure Risk Assessment Checklist</td>
<td>OoM shall complete its section of the Disclosure Risk Assessment Checklist</td>
<td></td>
</tr>
<tr>
<td>Mitigation</td>
<td>Cooperate in any mitigation effort.</td>
<td>Cooperate in any mitigation effort.</td>
<td>OoM and the ISO shall work together to define tactics to mitigate any harm resulting from the Breach or Security Incident.</td>
<td></td>
</tr>
<tr>
<td>Investigation</td>
<td>Cooperate in any investigation.</td>
<td>Cooperate in any investigation.</td>
<td>OoM and the ISO shall work together to define tactics to mitigate any harm resulting from the Breach or Security Incident.</td>
<td></td>
</tr>
</tbody>
</table>

The ISO and the SIRT team shall investigate all Security Incidents and certain Breaches and document findings according to the Information Security Response Team Policy (SIRT).
<table>
<thead>
<tr>
<th>Workforce Member</th>
<th>Supervisor</th>
<th>OoM</th>
<th>UMMS ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Endeavor to keep the identity of anyone reporting a violation confidential to the extent permitted by law, unless it prevents OoM from fully and effectively investigating an alleged violation.</td>
</tr>
<tr>
<td>Risk Assessment Form</td>
<td>n/a</td>
<td>n/a</td>
<td>OoM shall complete the Risk Assessment Form for all Breaches and Security Incidents [in consultation with ISO for Security Incidents] to determine if there is a low probability that PHI was compromised and for compliance with any applicable laws and regulations.</td>
</tr>
<tr>
<td>Submit Completed Risk Assessment Checklist and Form to ISO.</td>
<td></td>
<td></td>
<td>ISO will work with OoM to determine if there is a low probability that PHI was compromised.</td>
</tr>
<tr>
<td>Remediation or retraining</td>
<td>Follow all remediation, training or new protocol instructions arising out of any findings related to the Breach or Security Incident.</td>
<td>Ensure that workforce member completes any required training or remediation. Revise or institute any internal control or procedure required to address any identified risks or issues.</td>
<td>Make findings regarding remediation and/or retraining and may make recommendations to HR if discipline is appropriate.</td>
</tr>
<tr>
<td>No Retaliation</td>
<td>Ensure there is no retaliation against workforce for good faith reporting of an actual or suspected</td>
<td>Ensure there is no retaliation against workforce for good faith reporting of an actual or suspected</td>
<td>Ensure there is no retaliation against workforce for good faith reporting of an actual or suspected</td>
</tr>
</tbody>
</table>

Risk Assessment Form
n/a
n/a
OoM shall complete the Risk Assessment Form for all Breaches and Security Incidents [in consultation with ISO for Security Incidents] to determine if there is a low probability that PHI was compromised and for compliance with any applicable laws and regulations.

Submit Completed Risk Assessment Checklist and Form to ISO.

Upon Completion of review or investigation OoM shall submit a completed Risk Assessment Checklist and Form to the ISO.

Maintain documentation related to Security Incident or some Breach investigations,

Remediation or retraining

Follow all remediation, training or new protocol instructions arising out of any findings related to the Breach or Security Incident.

Ensure that workforce member completes any required training or remediation. Revise or institute any internal control or procedure required to address any identified risks or issues.

Make findings regarding remediation and/or retraining and may make recommendations to HR if discipline is appropriate.

The SIRT team findings shall include recommendations for remediation and/or retraining

No Retaliation

Ensure there is no retaliation against workforce for good faith reporting of an actual or suspected

Ensure there is no retaliation against workforce for good faith reporting of an actual or suspected

Ensure there is no retaliation against workforce for good faith reporting of an actual or suspected
<table>
<thead>
<tr>
<th>Workforce Member</th>
<th>Supervisor</th>
<th>OoM</th>
<th>UMMS ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach or security Incident.</td>
<td>suspected Breach or security Incident.</td>
<td>Breach or Security Incident.</td>
<td></td>
</tr>
<tr>
<td><strong>Subcontractors</strong></td>
<td>Report any subcontractor actual or suspected Breach or Security Incident to supervisor and OoM.</td>
<td>Ensure, to the extent that subcontractor’s work involves PII, that the subcontractor signs a BAA and is obligated to notify OoM immediately of any unauthorized disclosure or Security Incident and to take appropriate mitigating actions.</td>
<td></td>
</tr>
</tbody>
</table>

The following are some examples of required reports. This list is not comprehensive. If you are not sure whether something should be reported, call OoM to discuss it. Remember, the ability to mitigate potential damage early is essential.

- Inadvertently faxing PII to the wrong fax number or incorrect provider;
- Any electronic transmission of PII to the wrong recipient;
- Attaching a second individual’s record to a letter sent to a different individual;
- Knowledge of unauthorized external or internal access to PII;
- Disclosing PII to someone known to be without appropriate authorization;
- Forwarding an email with PII, where the PII is not required for the purpose the email is sent. This is a violation of minimum necessary and may also constitute a disclosure of PII to individuals not authorized to access the PII;
- Transmitting real data (identifiable data) as test data (unless mandated by client and proper security protections are enforced);
- Including identifiable data in training materials;
- Unauthorized transmission of photos containing PII;
- Stolen or lost laptop or smartphone that accesses the UMMS network or systems;
- PII sent by mail courier that does not arrive at its intended destination;
- Leaving PII unattended in a public area;
- Looking up the birth dates, addresses, or health information of friends or relatives;
- Reviewing the PII of a public personality;
- Accessing and reviewing PII out of curiosity or concern;
- Using or disclosing PII for commercial advantage or to improve one’s position;
- Using or disclosing PII for harassment or to spread gossip;
- Obtaining PII for a pending personal legal case.
DOCUMENT HISTORY

Effective Date: 10.1.11
Revision Date(s) 2.3.12; 9.23.13; 2.13.15; 8.5.15, 5.5.17
Review Date(s) 12.1.18

APPROVALS

G.J. Campbell
Gerry Campbell
UMMS Senior Privacy Officer
Office of Management