UMassMemorial
Health Care

Policy	
Breach of Confidential Information- Reporting, Investigation & Notification of Incidents Requiring Regulatory Reporting	
Developed By: HIPAA Advisory Group	**Effective Date:** 10/31/2019
Policy Owner: Sandra C. Brown, Chief Privacy Officer	**Approved by:** John T. Randolph, Vice President and Chief Compliance Officer, UMMHC **Approved by:** Eric Dickson MD, CEO UMass Memorial HealthCare
Applicability: This policy applies to the Workforce Members of UMass Memorial Health Care	
Keywords: access, audits, Breach, confidential information, discipline, Disclosure, investigation, reporting, security incident, violation	

Policy

UMass Memorial Health Care (UMMHC) addresses the handling of alleged Breaches or security incidents involving confidential information in compliance with the requirements of federal and state data Breach laws and regulations

All Workforce Members have a responsibility to report potential Breaches, inappropriate access, or security incidents within 1 business day of their discovery by reporting incident to the

- UMass Memorial Confidential Reporting System
  - By calling 844-744-9212, or
  - By going to www.umassmemorial.ethicspoint.com, or
- By contacting the applicable UMMHC privacy office.

All reported alleged Breaches or security incidents will be investigated and documented. If a Breach, inappropriate access, or security incident is confirmed, corrective action will be implemented. In the event that the alleged Breach or security incident involves a health care provider who is a Medical Staff member, but not employed by the UMass Memorial Medical Group, the relevant Chief Medical Officer shall be notified, and the occurrence will be investigated, reviewed and resolved in accordance with the UMMHC Member Entity’s Medical Staff by-laws.

Definitions

Breach – the impermissible acquisition, access, use or Disclosure of Protected Health Information which compromises the security or privacy of such information, unless a member of UMMHC or its Business Associate, as applicable, demonstrates that there is a low probability that the Protected Health Information (PHI) has been compromised.

* * If the links in this policy do not work, notify PolicyAdministrator@umassmemorial.org. * *

Business Associate – a person or organization that receives, uses, discloses, creates, or obtains protected health information, or Personal Information, to perform a function or service on behalf of a UMMHC entity or the UMMHC OHCA

Confidential information – data/information (whether oral, written, electronic or any other form) including protected health information, Personal Information, or other information related to the business of UMass Memorial (including finance and administration, human resources, legal, clinical, patient and research data), that is not freely disclosed or is regulated by governmental authorities.

Disclosure – release, transfer, access to or provision of Protected Health Information, Personal Information, or other confidential information to any third party.

Medical Staff – appropriately licensed and credentialed physicians and other providers as defined in the UMMHC Member Entity's Medical Staff Bylaws; it also includes dentists, oral surgeons, podiatrists and psychologists.

Organized Health Care Arrangement (OHCA) – is a clinically integrated care setting in which more than one covered entity participates and in which the participating covered entities need to share protected health information (PHI) for the purposes of treatment, payment or health care operations. The OHCA participants hold themselves out to the public as participating in a joint arrangement. The members of the UMMHC OHCA include the following entities, but not limited to: UMass Memorial Medical Center; UMass Memorial HealthAlliance-Clinton Hospital; HealthAlliance Home Health & Hospice; Community Healthlink; Marlborough Hospital; UMass Memorial Medical Group; private hospital-based physicians; and other private physicians while working at our facilities.

Personal Information – a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements: a) Social Security number; b) driver's license 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.

Protected Health Information (PHI) – information created, transmitted, received or maintained by a member of the UMMHC OHCA, including demographic information, related to the:

- Past, present, or future physical or mental health or condition of an individual;
- Provision of health care to an individual; or
- Past, present, or future payment for the provision of health care to an individual; **together with** any of the identifiers in the list below.

Note: Information for deceased individuals continues to be PHI until the individual has been deceased for more than 50 years.

Names (of patients, relatives, or employers)	Social security numbers	Device identifiers and serial numbers
All geographic subdivisions smaller than a State	Medical record numbers	Web Universal Resource Locators (URLs)
All elements of dates (except year) including birth date, admission date, discharge date, date of death; and all ages over 89	Health plan beneficiary numbers	Internet Protocol (IP) address numbers
Telephone numbers	Account numbers	Biometric identifiers, including finger and voice prints
Fax numbers	Certificate/license numbers	Full face photographic images and any comparable images

Electronic mail addresses	Vehicle identifiers and serial numbers, including license plate numbers	Any other unique identifying number, characteristic, or code

PHI does not include information maintained about an individual by a UMMHC entity for employment purposes, such as employee health records

Qualified Service Organization – an individual or entity that provides services to a Part 2 program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy and has entered into an agreement with a Part 2 program where they agree to be fully bound by 42 CFR Part 2 and that if necessary it will resist in judicial proceedings efforts to obtain this protected information except as permitted under 42 CFR Part 2.

Security Incident – the attempt or successful unauthorized access, use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

Workforce Members – all employees, contractors, volunteers, trainees (including medical students, interns, residents, allied health professional and business students), members of the medical staff including employed and private physicians, nurses in expanded roles, physician assistants, temporary employees, and other persons employed, credentialed or under the control of any member of the UMMHC OHCA whether or not they are paid by a member of the UMMHC OHCA.

Required Criteria for Procedure

Breaches or security incidents occur when a Business Associate or a Workforce Member accesses, uses or discloses confidential information for unauthorized purposes. Examples include but are not limited to: requesting that another individual access his/her medical record; looking up birth dates, addresses or medical records of friends, neighbors, relatives or others; reviewing a public personality’s record, using someone else’s access code or sharing your access code. A Breach or security incident can also include the theft, loss, or destruction of confidential information.

Breaches exclude:

I. any unintentional acquisition, access, or use of PHI by a workforce member, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or Disclosure, (for example: accessing and promptly exiting a medical record that was accessed in error); and,

II. any inadvertent Disclosure by a workforce member who is authorized to access PHI to another workforce member authorized to access PHI within UMMHC or within the UMMHC Organized Health Care Arrangement (OHCA), and the information received as a result of such Disclosure is not further used or disclosed (for example: sending a fax to the wrong UMMHC entity or department).

The responsibility for investigating potential Breaches and security incidents of confidential information rests with the Privacy and/or Information Security Office in conjunction with representatives from any of the following areas: department supervisors/managers where the potential Breach or security incident occurred, Information Security, Human Resources, Health Information Management, Office of the General Counsel, Medical Staff Office, the UMMHC Compliance Office, the member entity’s Compliance Officer, Business Associate if applicable, and other department representatives or administrators as needed.

The following process must be followed when a Workforce Member or Business Associate is potentially indicated in a Breach of PHI or Personal Information, or is involved in a security incident involving PHI, or Personal Information.

A. Reporting Potential Breaches and Security Incidents

1. Workforce Members have an individual responsibility to report potential Breaches or security incidents as noted in the Policy statement above. There shall be no reprisals for *good faith* reporting of actual or possible violations of this policy. Any Business Associate or Workforce Member who deliberately makes a false accusation with the purpose of harming or retaliating against another employee will be subject to discipline. UMMHC will endeavor to keep the identity of anyone reporting a violation confidential to the extent permitted by law, unless doing so prevents UMMHC from fully and effectively investigating or addressing an alleged violation.

2. A Privacy/Information Security investigative report will be initiated by the Privacy Office or the Information Security Office when the complaint is received.

B. Investigation of Suspected Breach or Security Incident

1. The Privacy or Information Security Offices may request additional information to facilitate the investigation. This information includes, but is not limited to: system security audits, medical records, individual electronic mail, other relevant documentation, interview(s) with the individual(s) reporting the suspected Breach, interview(s) with the person accused of the Breach or security incident, and interview(s) with the supervisor/manager or Business Associate. The relevant Chief Medical Officer will be notified of alleged Breaches by members of the Medical Staff and they will be investigated, reviewed and resolved in accordance with the Bylaws of the Medical Staff of the UMMHC Member Entity.

2. Security incident procedures will ensure that:
   - Reasonable actions are taken promptly to minimize the damage of a security incident and prevent further damage; and
   - Only authorized and appropriately trained UMMHC Workforce Members are allowed access to affected information systems in order to respond to or recover from a security incident.

3. The Privacy or Information Security Offices may form an investigative team depending upon the nature and complexity of the reported Breach. Team members may include representatives from the department where the suspected Breach occurred, Information Security, Human Resources, Health Information Management, relevant Chief Medical Officer, Office of the General Counsel, the UMMHC Compliance Office, the member entity's Compliance Officer, University of Massachusetts Medical School, the Business Associate and/or the person who oversees the Business Associate if applicable, and a union representative, if applicable based on union contract.

4. Data Breach Risk Assessment Process

   If the Privacy or Information Security Office determine based on their investigation that a Breach or security incident has occurred, the Privacy or Information Security Office must conduct a risk assessment of the Breach or security incident to determine if there is a requirement to report to the affected individuals and applicable state and federal regulators. Such analysis will be based on applicable state and federal regulations regarding data Breaches. UMMHC Entities will maintain and use a Privacy & Information Security Breach Risk Assessment tool for use in conducting and documenting its risk assessments to determine whether a Breach notification is required.

5. Upon conclusion of the investigation, the Privacy or Information Security Office or investigating team will prepare a written report of findings and recommendations regarding the alleged Breach or security incident. In the event of a potential Breach or security incident all actions taken and UMMHC's investigation must be carefully documented. The Member Entity's Privacy Officer will determine if appropriate to report to senior management.

C. Notification Requirements

The Privacy or Information Security Offices will prepare or coordinate any notifications about the Breach or security incident as required by law. Existing templates will be used and modified as needed for each Breach based on the specific facts of each incident.

UMMHC Entity's Privacy Office, Information Security Office or the Office of the General Counsel will notify outside authorities such as local police, FBI, etc. when circumstances warrant.

1. Internal Notifications:
   Reportable data Breaches and security incidents must be reported to appropriate UMMHC and member entity senior management based on documented Privacy Office internal notification protocols. The UMMHC Entity's Privacy Office will notify, or assure that others have notified, senior management.

2. External Notifications:
   Refer to the table "Comparison of Breach Notification Requirements" for state Security Breach and federal HITECH/Omnibus Breach Notification for Unsecured Protected Health Information for Breaches involving Personal Information (PI) or protected health information (PHI).
   - Annually or at the discretion of the Privacy or Information Security Officer Breaches will be reported to the Audit and Compliance Committee of the UMMHC Board.

3. Business Associate (Vendor or Contractor):
   If a workforce member becomes aware that a Business Associate knows, or has reason to know of a Breach, or that Personal Information was acquired or used by an unauthorized person or used for an unauthorized purpose, the workforce member and Business Associate have a responsibility to report the potential Breach or security incident as noted in the policy statement above.

D. Disciplinary Action

A confirmed Breach of confidential information or security incident may result in disciplinary action, up to and including termination of employment or contracted service or authorization to provide services at the UMMMHC Member Entity, as applicable.

In the case of Medical Staff, corrective action will be in accordance with the relevant contract, Medical Group policy and/or Bylaws of the Medical Staff of the UMMHC member entity.

E. Disciplinary Process

1. The person responsible for implementing the recommended disciplinary action is the person who supervises the workforce member or oversees the Business Associate. Implementation of a disciplinary action against a Medical Staff member is governed by the Bylaws of the Medical Staff of the UMMHC Member Entity. If disciplinary action is recommended, Human Resources will work with the Privacy Officer, the workforce member's immediate supervisor/manager and union representatives, if applicable, to implement the action. In the case of a confirmed Breach or security incident by a Business Associate or Qualified Service Organization, the Privacy or Information Security Office will work with the Office of the General Counsel and the person accountable for the Business Associate/Qualified Services Organization's contract to implement applicable contract remedies.

2. For all Breaches or security incidents, after final resolution, the initial report and all written documentation relating to it shall be filed in a confidential file in the Privacy or Information Security Office. Should a Breach or security incident occur with a Business Associate, it is the responsibility of the Privacy and Information Security Office at the UMMHC Member Entity to inform the Privacy and Information Security Officers at the affected member entities of this incident so that suitable action can be taken, if appropriate.

3. In the case of employees, disciplinary actions will be documented in accordance with UMMHC Member Entity's Human Resources Discipline Policy. Disciplinary actions may be reported to the Massachusetts Board of Registration in Medicine or other professional licensing boards when required by law or as provided in the UMMHC Member Entity's policy.

F. Appeals

The UMMHC Workforce Member may follow the member entity dispute resolution process. Workforce Members covered by a Collective Bargaining Agreement should appeal based on contract procedures.

Clinical/Departmental Procedure

N/A

Supplemental Materials

Privacy & Information Security Breach Risk Assessment tool

Rescission

Supersedes:

- Community Healthlink – 15-19 Breach of Confidential Information - Reporting, Investigation & Notification dated 7/7/2015
- HA-20-09 Breach of Confidential/Protected Information dated 11/16/13
- HAHHH-AD-04 Breach of Confidential/Protected Information dated 8/29/13
- Marlborough Hospital Policy-Breach of Confidentiality dated 5/1/14
- UMMMC policy 1421: Breach of Confidential Information-Reporting, Investigation and Notification dated 10/19/17

References

Uses and Disclosures of Protected Health Information Policy
3000 Information Security Management Policy
4014 Dispute Resolution Policy
4039 Discipline Policy
45 CFR 164.530(d), (e)
HA-60-12 Corrective Action/Performance Improvements