OMD Administrative Operational Policy
HIPAA

DRAFT for Review and Approval 7/03/2024;
Effective 8/1/2024; Review Before 9/2026

Purpose

The HIPAA Privacy Rule establishes strict authorization and other requirements that must be met before Protected Health Information [PHI]* may be used or disclosed for purposes other than treatment or health care operations. Health care operations will be defined as administrative, legal and quality improvement activities of the Medical Control Board (MCB)/Office of the Medical Director (OMD) as a covered entity that are necessary to conduct business and support the core functions of medical oversight.

Policy

The MCB/OMD participates in the practice of protecting the confidentiality, integrity and security of Protected Health Information [PHI] contained in the designated record set and comply with legal standards governing the use or disclosure of such information. The Chief Medical Officer will appoint and maintain the position of Privacy Liaison within the Office of the Medical Director.

The specific agency who completes and maintains the Electronic Health Record (EHR) will be referred to as the owner of the Protected Health Information (PHI)

Authorization to Use and Disclose PHI

The MCB/OMD will utilize Protected Health Information (PHI) for review of quality measures, protocol development, coordination of efforts between responding agencies and other health care operations. The position of the MCB/OMD is supportive of these individual rights, however the requesting party is to be referred back to the specific agency, whether transport or first response, to formally request a copy of the medical record(s). Any request by another health care professional or third parties for purposes other than health care operations will be referred back to the specific agency(s) that were involved in the patients care for formal request of PHI.

Breach Notification for Protected Health Information

Purpose

The Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) requires HIPAA covered entities to notify affected individuals of certain security breaches concerning their protected health information (PHI). To ensure that the MCB/OMD complies with the breach notification regulation provisions (Breach Rule) of the Privacy Rule, this policy outlines the procedures for investigation and proper notification.

Policy
In the case of a breach of Protected Health Information, the MCB/OMD will notify the specific agency who owns the PHI.

As a covered entity, the MCB/OMD must work to timely and accurately report any breach of unsecured PHI according to ARRA to the agency who owns the PHI. They will continue to work closely with the agency to investigate the breach and all other Federal and State regulations and interpretive guidelines promulgated thereunder. Documentation related to the breach (e.g., notification letters) will be maintained for a minimum of six (6) years.

Definitions
The following definitions apply to all patient privacy and security policies and procedures.

1. **Breach** – Unauthorized acquisition, access, use, or disclosure of unsecured, unencrypted PHI which compromises the security or privacy of such information and poses a significant risk of financial, reputational, or other harm to the individual. To determine if a breach has occurred, a risk assessment must be performed to determine if the security or privacy of the PHI has been compromised. Limited Data Sets (except those that exclude patient zip code and date of birth) are subject to the breach notification reporting requirements. The term 'breach' does not include:

    a. Any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate if:
        i. Such acquisition, access, or use was made in good faith and within the course and scope of authority; and
        ii. Such information is not further used or disclosed in a manner not permitted;
    b. Any inadvertent disclosure by a person who is authorized to access PHI of the covered entity or business associate, or organized health care arrangement in which the covered entity participates;
    and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
    c. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. **Protected Health Information (PHI)** – Any oral, written or electronic individually-identifiable health information collected or stored. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.

3. **Unsecured PHI** – PHI that is not encrypted and rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS).

Additional Definitions – Refer to the HIPAA Privacy Standards, 45 CFR Parts 160.101 and 164.501,

Patient Privacy Compliance

Purpose

The MCB/OMD, through its Privacy Liason, will work with the specific agency(s) who owns the PHI, in order to investigate and resolve complaints that an individual's privacy rights under HIPAA and/or the MCB/OMD's privacy policies and procedures have been violated.

Procedure

1. Any complaint about handling of PHI is to be made in writing on the Patient Privacy Complaint Form to the Privacy Liason.

2. Upon receiving a complaint, the Privacy Liason will:
   a. Document on a Privacy Complaint Investigation Form the patient's run number and/or PCR ID, if applicable, and the date complaint was received and forward the complaint to the specific agency who owns the PHI
   b. Inform the Chief Medical Officer, Chair of the Medical Control Board and the compliance officer for the agency who owns the PHI of the complaint, the investigation and the proposed resolution.
   c. Document the resolution of the complaint on the Privacy Complaint Investigation Form and notify the Chief Medical Officer, Chair of the Medical Control Board and the compliance officer for the agency who owns the PHI of the final resolution.
   d. Provide a summary of the resolution of the complaint to the individual making the complaint.
   e. Document on the Privacy Complaint Investigation Form the communication with the individual making the complaint.
   f. Sign/ date the Privacy Complaint Investigation Form.The form is to be retained for six years.

Creation of De-Identified Information

Purpose

The MCB/OMD is committed to ensuring the privacy and security of Protected Health Information (PHI)*. Federal law allows certain health care organizations to create de-identified information—that is, information that has been stripped of any elements that may identify the patient, such as name, birth date, or social security number. The MCB/OMD will, from time to time, use de-identified date for various purposes such as utilization review, clinical performance review/analysis, or for research. In doing so, we will ensure that the appropriate administrative and technical processes are in place to properly de-identify PHI, as well as to secure any methods of re-identification, as required under 45 CFR §164.514(a) and other applicable federal, state, and/or local laws and regulations.

Policy

1. MCB/OMD through consultation with the specific agency who owns the PHI may create de identified information for the purposes of research.

2. De-identification of information will be performed only under the close supervision of the Privacy Liason or his designee, who shall have appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.

3. De-identified information will not be disclosed if the MCB/OMD employee creating or disclosing the information have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Procedures

1. When it is unclear the Privacy Liason or his designee will consult the specific agency who owns the PHI to determine when specific PHI should be de-identified.

2. The following individually identifying elements will be removed or otherwise concealed from PHI in order to create de-identified information:

(a) names;
(b) all elements of dates (except year) directly related to an individual, including:
- birth date
- transport date
- date of death
- all elements of dates (including year) indicative of age 89, except that such ages and elements may be aggregated into a single category of age 90 or older

(c) telephone numbers;
(d) fax numbers;
(e) electronic mail addresses;
(f) social security numbers;
(g) medical record numbers;
(h) account numbers;
(i) device identifiers and serial numbers;
(j) web Universal Resource Locators (URLs);
(k) Internet Protocol (IP) address numbers;
(l) biometric identifiers, including finger and voice prints;
(m) full face photographic images and any comparable images;
(n) all geographic subdivisions smaller than a state, including
- street address
- city
- county
- precinct
- zip code, and their equivalent geocodes; and

(o) any other unique identifying number, characteristic, or code.

(p) the initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000).

3. If the PHI is to be used for purposes other than Health Care Operations and will include any of the listed identifiers it will only be disclosed when the Privacy Liason or his designee has consulted with the specific agency who owns the PHI. It must be determined that the risk for information to be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information must be very small.

4. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

Discipline/Sanctions of Employees, Agents, and Contractors Violating HIPAA Policies

Purpose

To establish the process for disciplining or sanctioning employees or agents who fail to comply with the MCB/OMD's privacy policies and procedures.

Policy

1. The MCB/OMD will appropriately discipline its employees who fail to comply with the policies and procedures governing HIPAA compliance.
2. The type of discipline applied shall vary depending on the severity of the violation; whether the violation was intentional or unintentional; whether the violation indicates a pattern or practice of improper access, use or disclosure of Protected Health Information [PHI]*; whether the violation was for personal gain or advantage; and other factors. Discipline imposed is within the discretion of the MCB/OMD, and is to be reviewed on a case by case basis.
3. Employees, agents and other contractors should be aware that violations of a severe nature may result in notification of law enforcement officials and regulatory, accreditation and licensing organizations. Under HIPAA, penalties for misuse or misappropriation of PHI include both civil monetary penalties and criminal penalties. Civil penalties range from $100 for each violation to a maximum of $25,000 per year for the same violations. Criminal penalties vary from $50,000 and/or 1 year imprisonment to $250,000 and/or 10 years imprisonment.
4. Not withstanding the policies and procedures contained herein, employees may exercise their right to:
    a. File a complaint with HHS.
    b. Testify, assist or participate in an investigation, compliance review, proceeding or hearing under Part C of Title XI.
    c. Oppose any act made unlawful by the HIPAA Privacy Rule provided the individual or person has a good faith belief that the act opposed is unlawful, and the manner of the opposition is

reasonable and does not involve a disclosure of protected health information in violation of the HIPAA Privacy Rule.

d. Disclose PHI as a whistleblower to a health oversight agency, public health authority, or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity.
e. Report a crime committed against an employee. An employee who is a victim of a crime may disclose PHI to a law enforcement official, provided that the PHI is about a suspected perpetrator of the criminal act, and is limited to only the information necessary to report the crime.

Procedure

1. The following disciplinary actions are a guide to be considered and may be applied for failure to comply with MCB/OMD's HIPAA policies or procedures or with the requirements of HIPAA regulations:

    a. First offense of non-compliance:
        i. Unintentional violation – verbal warning
        ii. Intentional violation – written counseling
    b. Second offense of non-compliance:
        i. Unintentional violation - Written counseling
        ii. Intentional violation – Termination
    c. Third offense of non-compliance:
        i. Unintentional violation – Further disciplinary actions up to and including termination as determined by the Chair of the MCB, the Chief Medical Officer, and the Privacy Liason.
    d. A violation stays on an employee's record for six years. The number of violations on an employee's record at the time of another violation determines the level of discipline to be imposed. For example: An employee had two unintentional violations in October, 2017 and received a written counseling after the 2nd occurrence. In November, 2018, the employee has another unintentional violation. At that time, with the earlier two violations off of the employee's record, the employee would be given a verbal warning.
2. The Chair of the MCB, the Chief Medical Officer, and the Privacy Liason collectively are responsible for determining the severity of the violation and whether such violation merits immediate termination regardless of whether unintentional or intentional.
3. All disciplinary actions against employees will be documented and retained for a period of at least six years from the date discipline was imposed.
4. Agreements or contracts with agents and other non-employee representatives may be terminated for failure to comply with the policies and procedures of the MCB/OMD. In addition, notice of violations may be given to law enforcement and appropriate licensure or regulatory agencies.

DRAFT for Review and Approval 7/03/2024;
Effective 8/1/2024; Review Before 9/2026

Disclosing Protected Health Information For Research Purposes

Purpose

The MCB/OMD may use or disclose protected Patient Health Information (PHI)* for research. The MCB/OMD is committed to ensuring the privacy and security of PHI. To support this commitment, the MCB/OMD will ensure any use or disclosure of PHI for research purposes is in compliance with applicable laws and regulations.

Policy

The MCB/OMD may use or disclose PHI for research purposes, regardless of the source of funding for the research, except as otherwise stated in this policy.The specific agency who owns the PHI shall be provided a list of the patient care records that will be reviewed in the course of research. It is anticipated that appropriate access to the PHI will be provided by the agency once appropriate documentation is provided by the MCB/OMD.

Procedure

1. Documentation will be obtained indicating that an alteration to or waiver, in whole or in part, of the individual authorization required for use or disclosure of PHI has been approved by the Institutional Review Board (IRB).

2. Documentation of approval of an alteration or waiver must include the following information:

   (a) a statement identifying the IRB and the date on which the alteration or waiver of authorization was approved.
   (b) a brief description of the PHI for which use or access has been determined to be necessary by the IRB.
   (d) a statement that the IRB has determined that the alteration or wavier of authorization, in whole or in part, is permissible based on all of the following which must be documented in the minutes of the IRB:

      1) the use or disclosure of PHI involves no more than minimal risk to the individuals because:
         - there is an adequate plan to protect the identifiers from improper use and disclosure;
         - there is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

- there are adequate written assurances that the PHI will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this subpart.

2) The alteration or wavier will not adversely affect the privacy rights and the welfare of the individuals;
3) The research could not practicably be conducted without the alteration or waiver;
4) The research could not practicably be conducted without access to and use of the PHI; and
5) The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals and the importance of the knowledge that may reasonably be expected to result from the research.

3. Documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB.

DRAFT for Review and Approval 7/03/2024;
Effective 8/1/2024; Review Before 9/2026

Employee Training on Use/Disclosure of PHI

Purpose

To ensure the MCB/OMD personnel receive appropriate training regarding privacy practices and the use and disclosure of Protected Health Information (PHI).

Policy

The MCB/OMD will train all current staff in accordance with the HIPAA Privacy Rule prior to it's implementation on January 1, 2018. After January 1, 2018, the MCB/OMD will train employees on its privacy practices upon initial employment. All staff members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time following a material change the MCB/OMD's policies and procedures on privacy practices. All employees will also undergo annual refresher training. Training will be conducted and documented by a Privacy Officer or designee.

Procedure

For new employees:

1. As part of their regular job orientation, new employees will be given clear instruction regarding the MCB/OMD's privacy practices, the use and disclosure of PHI and disciplinary actions that may be taken for violation of policies. Training will be tailored to match the individual's job description and responsibilities.

2. The name and contact information of the MCB/OMD's Privacy Liason. New employees will also be given instruction on where they can find all of the MCB/OMD's privacy policies, procedures and corresponding forms.

3. New employees will sign a form stating they have received instruction on the privacy practices and agree to adhere to MCB/OMD's policies and procedures on privacy practices.

For existing employees:

1. Each year, the MCB/OMD will provide mandatory refresher training to all its employees. Training will include, but not be limited to, instruction on where all privacy policies, procedures and corresponding forms may be found. Potential disciplinary actions that may be taken for violation of policies will also be reviewed.

2. Upon completion of the training, employees will sign a form stating they have received refresher training on the MCB/OMD's privacy practices and agree to adhere to those policies and procedures on privacy practices.