23-Security and Patient Confidentiality (HIPAA)

Prepared by: Yusra Othman /Director/Supervisor-Chem **Date:** May/29/2024
signature/title

Reviewed by: Jordan Dillard /Instructor **Date:** June 24 2024
signature/title

Approved by: Sanford N. Bauch, M.D /Chairman **Date:** July 9 2024
signature/title

ANNUAL REVIEW:

REVIEWED	Sanford N. Bauch, M.D	July-17-2025
	signature/title	Date
REVIEWED		
	signature/title	Date
REVIEWED		
	signature/title	Date
REVIEWED		
	signature/title	Date
REVIEWED		
	signature/title	Date
REVIEWED		
	signature/title	Date

REVISED		
	signature/title	Date/Page/Paragraph
REVISED		
	signature/title	Date/Page/Paragraph
REVISED		
	signature/title	Date/Page/Paragraph
REVISED		
	signature/title	Date/Page/Paragraph
REVISED		
	signature/title	Date/Page/Paragraph

SUPERSEDES: Procedure titled _____

Purpose

A major goal of the HIPAA Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. Laboratory is committed to compliance with HIPAA, safeguarding the security of Protected Health Information, while allowing permissible use of health information to promote high quality health care and protecting the health and well-being of our patients and customers.

Scope

This policy applies to all employees and contractors of Laboratory with access to protected health information.

Definitions & Abbreviation

ARRA - American Recovery and Reinvestment Act

BA – Business Associate

CE – Covered Entity

HHS – U.S. Department of Health and Human Services

HIPAA – Health Insurance Portability and Accountability Act

HITECH - Health Information Technology for Economic and Clinical Health Act ·

OCR – Office of Civil Rights

PHI – Protected Health Information

PHR-protected health Record

Business Associate - In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons

would be incidental, if at all. A covered entity can be the business associate of another covered entity.

Protected Health Information - The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

Individually identified health information - “Individually identifiable health information” is information, including demographic data that relates to:

The individual’s past, present or future physical or mental health or condition, the provision of health care to the individual, or

The past, present, or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

De-Identified Health Information - There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual’s relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

Enforcement of HIPAA Privacy and Security - The enforcement of HIPAA Privacy and Security is managed by the Office for Civil Rights (OCR), a department of Health and Human Services (HHS): http://www.hhs.gov/ocr/

Probability of Compromise – Is the standard for breach analysis mandated by the Omnibus Privacy Final

Rule - This standard contains 4 factors that must be analyzed (at a minimum) to determine whether a privacy Event / HIPAA violation is a reportable breach under Federal regulations.

PHR (Personal Health Record) - an electronic record of identifiable health information (as defined in HITECH section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

Privacy Event - Discovered incidents and occurrences related to the acquisition, access use and disclosure of an individual's PHI that upon further investigation may or may not be deemed HIPAA privacy violations or breaches of unsecured PHI.

Protected Health Information (PHI) - Is defined in 45 CFR 160.103 as any

information whether oral, written, electronic or recorded in any form that is created or received by CE as a healthcare provider and relates to an individual's past, present or future physical or mental condition; healthcare treatment and payment for services. PHI also includes data that identify the individual (e.g. Name, SSN, MRN, account number, address, telephone number, DOB, e-mail address, names of relatives, employer, etc.).

Secured PHI - PHI that is secured through the use of a technology or methodology specified by the HHS Secretary in guidance issued under section 13402(h)(2) of ARRA - Secured PHI applies to data in all of its various states - data in use, motion, at rest, and disposed.

Unsecured PHI - means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in the guidance issued under section 13402(h)(2) of ARRA.

Breach of PHI - The Omnibus Privacy Final Rule added language to the definition of breach to clarify that an impermissible use or disclosure of protected health information is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

Breach Notification – HITECH defines breach notification in Section 13402. In a CE that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured health information (as defined in HITECH Section 13402, subsection (h)(1)) shall, in case of breach of such information that is discovered by the CE, notify each individual whose unsecured

PHI has been or is reasonably believed by the CE to have been accessed, acquired or disclosed as the result of such breach.

Policy:

MMCCCL is dedicated to protecting the privacy of patients, as well as complying with all laws set forth by governing bodies. The Laboratory is a health care provider and covered entity as defined by HIPAA and will maintain compliance with the HIPAA Privacy rule. Laboratory has access to protected health information in the course of providing clinical laboratory testing to its customers. This policy acts to define and limit the circumstances in which an individual's protected health information may be used or disclosed by Laboratory and its business associates. Laboratory will not use or disclose protected health information, except either:

1. as the Privacy Rule permits or requires; or

2. as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

Procedure:

Administrative Requirements

Privacy Policies and Procedures - The laboratory will develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.

Privacy Personnel - The laboratory has designated a Privacy officer responsible for developing and implementing its privacy policies and procedures. This can be delegated to GS, TS. The Privacy officer or delegee is the contact person responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

Workforce Training and Management - Workforce members include employees, volunteers, trainees, and may include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).The laboratory trains all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. Training documentation is archived in the personnel record of the employee. Appropriate

sanctions against workforce members who violate privacy policies and procedures, or the Privacy Rule will be applied.

Mitigation - A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule. Breeches of laboratory PHI are handled by PHI Breech Response.

PHI Breech Response - The laboratory must have policy for determining and addressing HIPAA breech event investigation and determination, risk analysis, and notification are generally outlined by the following steps:

1. Investigation and documentation by CE (or BA) of a privacy event (incident).

2. Final determination of whether a (HIPAA) privacy violation has occurred.

3. Determine if a breach of unsecured PHI has probably occurred;

4. Determine based on the data of the violation / potential breach whether to apply Omnibus Final Rule standards.

5. If unsecured PHI has been breached, perform analysis of the cause then document it.

6. If the breach meets the criteria established by the CE that identifies this violation is technically a breach of unsecured PHI, notify OCR either immediately (if over 500 individuals per event) or annually (if under 500 individuals per event). OCR is notified in the case of either less than 500 individuals per event annually or for greater than 500 individuals immediately (within 60 calendar days under all circumstances) via the following link and the instructions therein

a.
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstr
ucti on.html

b. Notify individual(s) of the breach of their PHI.

Feedback, mitigation, sanctions and corrective actions have been developed and recorded.

45 CFR 164.404(b) requires covered entities to notify individuals of a breach without unreasonable delay but in no case later than 60 calendar days from the discovery of the breach, except in certain circumstances where law enforcement has requested a delay.

Data Safeguards - A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code and limiting access to keys or pass codes.

Complaints - A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. The covered entity must explain those procedures in its privacy practices notice. Among other things, the covered entity must identify to whom individuals can submit complaints to the covered entity and advise that complaints also can be submitted to the Secretary of HHS.

Retaliation and Waiver - A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. A covered entity may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrolment or benefits eligibility.

Documentation and Record Retention - A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

Required Disclosures

Laboratory will disclose protected health information in only two situations:

1. To individuals (or their verified personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health

information; and Personal representatives will be verified by a signed statement from the patient allowing the provider to release information containing PHI to the representative.

2. To HHS when it is undertaking a compliance investigation or review or enforcement action.

Personal Representatives

The Privacy Rule requires a covered entity to treat a "personal representative" the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule. A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

Permitted Uses and Disclosures

The laboratory is permitted, but not required, to use and disclose protected health

information, without an individual's authorization, for the following purposes or situations:

1. To the Individual (unless required for access or accounting of disclosures);

2. Treatment, Payment, and Health Care Operations;

3. Opportunity to Agree or Object;

4. Incident to an otherwise permitted use and disclosure;

5. Public Interest and Benefit Activities; and OCR Privacy Rule Summary

6. Limited Data Set for the purposes of research, public health or health care operations

The laboratory relies on professional ethics and best judgments of the Laboratory

Director in consultation with the Privacy Officer in deciding which of these permissive uses and disclosures to make. Release of protected health information is only done in the above circumstances using approved procedures with authentication of the party requesting the information. Business Associates with access to individually identifiable health information will have a current Business Associate Agreement with Laboratory.

Authorized Uses and Disclosures

The laboratory will obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.

The laboratory will not condition treatment, payment, enrolment, or benefits eligibility on an individual granting an authorization.

Limiting Uses and Disclosures to the Minimum Necessary

The laboratory makes reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. This minimum necessary requirement is not imposed on a disclosure or by a request by a health care provider for treatment or to disclosures to the individual who is the subject of the information or the individual's personal representative.

Notice and Other Individual Rights

The laboratory maintains a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Laboratory will act in accordance with its notice of privacy practices.

References

CLSI. Quality Management System: A Model for Laboratory Services; Approved Guideline — Fourth Edition. CLSI document QMS01-A4. Wayne, PA: Clinical and Laboratory Standards Institute; 2011.

College of American Pathologists Accreditation Program Checklists

The Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA Privacy Rule, 45 CFR Part 160, Part 164 - Subparts A and E