HIPAA PRIVACY HANDOUT

Ramiek A. James, Esq.
Privacy Officer and Chief Compliance Officer
MDH-Office of the Inspector General
Ramiek.james@maryland.gov
410-767-5411

1) **What is HIPAA?**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is federal legislation, which applies to covered entities (CE) and their business associates (BA), that provides data and security provisions for safeguarding health information.

2) **What is a Covered Entity (CE)?**

A CE is a health care provider, health plan or health care clearinghouse.

3) **What is a Hybrid Covered Entity?**

A hybrid covered entity is a CE whose business activities include both covered and non-covered functions. A covered function is any function the performance of which makes the performer a health plan, health care provider, health care clearinghouse, or BA. Thus, a covered component of a hybrid covered entity must include any component that would meet the definition of a CE or BA if that component was a separate legal entity. MDH has designated itself as a hybrid covered entity.

4) **What is a Business Associate (BA)?**

A BA is a person or entity that performs certain functions or activities that creates, receives, maintains, or transmits Protected Health Information (PHI) on behalf of, or provide services to, the CE.

5) **What is Health Information?**

Health information is any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

6) **What is Individually Identifiable Health Information (IIHI)?**

IIHI is information that is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a CE;

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;
- Either identifies the individual or could reasonably be used to identify the individual.

7) **What is PHI?**

PHI is IIHI that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium by a CE or BA.

8) **What is a Breach?**

A breach is the "unauthorized acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of the PHI, but there are **3 exceptions:**

- The unintentional acquisition, access, or use of PHI was by a workforce member acting under the authority from the CE or BA. It was in good faith with no further disclosure.
- The inadvertent disclosure of PHI was between two authorized agents of either the CE or BA. It was in good faith with no further disclosure.
- The CE or BA has a good faith belief that the non-authorized person would not retain information that was disclosed.

An unauthorized acquisition, access, use, or disclosure of PHI is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

9) **What is HITECH?**

The Health Information Technology for Economic and Clinical Health Act (2/17/09, as part of ARRA), modified HIPAA in several ways, including BA obligations, definition of breach, breach notifications, increased penalties for non-compliance and provided incentives for meaningful use of electronic health records.

10) **Keep an Eye Out:**

- **Laptops:** Are you working from home? Are they password protected? Encrypted? Don't leave them in cars. Don't leave them unprotected.
- **Flash Drives:** Is there PHI? Are they secured? Encrypted? Password Protected? How are you ensuring they are not accessed by the wrong people?
- **Paper Files:** Are they being kept where unauthorized people can see them? Are the file cabinets locked? Are they secured?

- **Communications:** Are people in the habit of sharing PHI to other people that don't need to know? Are people having communications in a non-private setting?
- **Disposal:** How are CEs destroying PHI? Is it being shredded with a double cross-cut shredder? Is it in an open area before it is being shredded?
- **Cell Phones:** Are they password protected? Don't leave them unprotected. If they are lost, and have PHI on them, notify your HIPAA-Privacy Officer immediately. The same HIPAA rules that apply to other mobile devices apply to cell phones.
- **Fax Machines:** Are they in a secure area with restricted access? Are you using a cover sheet labeled confidential/PHI?
- **PCs:** Never leave your PC unattended-lock it, log-off, or shut your computer down.
- **Emails:** Special precautions must be taken with emails containing PHI that are sent from a Maryland.gov address to a non-Maryland.gov address, such as encrypting and password protecting the information.
- **Disclosures:** Generally, disclosing a patient's PHI requires patient authorization unless it involves treatment, payment, or health care operations (TPO) purposes, unless otherwise permitted or required by law.
- **Mailings:** Ensure proper controls and procedures are in place to minimize the probability of misdirected mailings.
- **Social Media:** Individuals' PHI should never be discussed or disclosed on social media. The same PHI disclosure rules apply.

11) **Top Ten 2019 Privacy Breaches:**

- **Optum 360 LLC**: 11,500,000 people affected; Between Aug 1, 2018 to March 30, 2019; Hackers were able to access PHI for financial gain.
- **Laboratory Corporation of America Holdings DBA LabCorp:** 10,251,784 people affected; Hackers were able to access patient PHI for financial gain.
- **Dominion Dental Services/Dominion National Insurance Company/Dominion Dental Services USA Inc.:** 2,964,778 people affected; During nine-year period, Hackers were able to access patient PHI for financial gain.
- **Clinical Pathology Laboratories, Inc.:** 1,733,836 people affected; Hackers were able to access patient PHI for financial gain.
- **Immediata Health Group Corp.:** 1,565,338 people affected; Due to technical error on the website, hackers could easily access PHI for financial gain.
- **UW Medicine:** 973,024 people affected; During three weeks, technical error on the website allowed hackers to gain access PHI for financial gain.
- **Women's Care Florida LLC:** 528,188 people affected; Hackers installed virus onto the server and encrypted PHI for financial gain.
- **Care Centrix Inc:** 467,621 people affected; Hackers were able to access patient PHI for financial gain.
- **Intramural Practice Plan-Medical Sciences Campus-University of Puerto Rico:** 439,753 people affected; Ransomware attack allowed hackers to access patient PHI for financial gain.
- **BioReference Laboratories Inc:** 425,749 people affected; Between Aug 1 2018 and March 30 2019, Hackers were able to gain access on the web payment page for financial gain.

12) **HIPAA Privacy Rule:**
A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's PHI may be used or disclosed by CEs. The Privacy Rule applies to PHI in any form, written, spoken, or electronic.

13) **HIPAA Security Rule:**
- The Security Rule applies only to electronic PHI (ePHI) and requires that CEs who store information electronic form maintain its confidentiality, integrity, and accessibility.
- The types of information that must be kept secure: 1) data in motion; 2) data at rest; 3) data in use; and 4) data disposed.
- The 3 types of safeguards of the Security Rule: 1) **administrative** (e.g. assigning a security officer and training); 2) **physical** (e.g., equipment specifications and access restrictions); and 3) **technical** (e.g., access control, audit controls, integrity, person or entity authentication; and transmission security).

14) **42 CFR Part 2 (Substance Use Disorder Confidentiality Regulations):**
- Applies to any individual or entity that is federally assisted and holds itself out as providing and provides alcohol and drug abuse services;
- Is generally more stringent than HIPAA; and
- With limited exceptions, requires written patient consent for disclosure of PHI even for the purposes of treatment, payment and health care operations.

15) **Part 2 Disclosures:**
Part 2 generally prohibits treatment programs and certain third-party recipients from disclosing SUD information without patient consent, except in the following circumstances:
- Medical emergencies;
- Child abuse or neglect reports required by state law;
- Reporting a patient's crime on program premises or against program personnel;
- Qualified audit or evaluation of the program;
- Research requests;
- Qualified Service Organization Agreements; and
- Court orders authorizing disclosure and use of the patient records.

HIPAA Civil Penalties

Violation Category	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect-Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect-Not Corrected	$50,000	$1,500,000

HIPAA Criminal Penalties

Violation Category	Each Violation
Knowingly obtain/disclose or with reasonable cause	Up to a 1-year period of incarceration and $50,000 fine
Under false pretenses	Up to a 5-year period of incarceration and $100,000 fine
For personal gain or malicious reasons	Up to a 10-year period of incarceration and $250,000 fine

The Office for Civil Rights (OCR), within HHS, is currently conducting routine audits of CEs and BAs for their compliance with the Security and Privacy Rules. HHS may not impose a civil monetary penalty if 1) HHS concludes that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that he or she violated the provision or 2) Failure to comply with HIPAA was due to reasonable cause, not willful neglect, and the CE corrected the violation within 30 days of when he or she knew or should have known of the violation. **That is why it is important to act quickly to identify how the breach occurred and implement appropriate corrective measures in order to meet the 30-day deadline.**

HIPAA OMNIBUS FINAL RULE

The HIPAA Omnibus Final Rule was published in the Federal Register on January 25, 2013. The effective date of the Final Rule was March 26, 2013 and CEs and BAs had to comply by September 23, 2013. Note below some of the significant modifications to HIPAA included in the Final Rule:

- It extends a-number-of HIPAA requirements to contractors, subcontractors, and other BAs of health care providers and plans, and increase the monetary penalty for noncompliance;
- It requires authorization for the sale of PHI, research using PHI, and future research using PHI;
- It requires CEs and BAs to comply with PHI requirements for deceased individuals for a period of 50 years following the date of death;
- It permits CEs and BAs to disclose a decedent's information to family members and others who were involved in the care or payment of care of the decedent prior to death, unless doing so would be inconsistent with any prior expressed preference of the individual;
- It allows a CE or BA to disclose proof of immunization to a school where state law requires the school to have such information prior to admitting the student;
- It modified the definition of "breach" by removing the significant harm standard and replacing it with a presumptive breach standard;
- It allows patients to ask for a copy of their electronic medical records in an electronic form;

- It gives individuals who pay for their treatment out of pocket the authority to instruct their provider not to share information about their treatment with their health plan; and
- It sets new limits on how information is used and disclosed for marketing and fundraising purposes.

Overview of Permitted Uses and Disclosures of PHI

Covered entities may only use or disclose PHI in the following manner:

- To the individual who is subject of the PHI;
- For treatment, payment or health care operations;
- Incident to a use or disclosure permitted by the Privacy Rule;
- Pursuant to a valid authorization from the individual or his or her personal representative;
- As permitted by an agreement or in situations where HIPAA only requires the covered entity to provide the individual with an opportunity to agree or object;
- For certain fundraising activities permitted by the Privacy Rule;
- In connection with a limited data set;
- For certain underwriting and insurance purposes; and
- As required by law

No Authorization Required:

- Public health activities;
- Victims of abuse, neglect or domestic violence;
- Health oversight purposes;
- Judicial and administrative proceedings;
- Law enforcement purposes;
- Decedents (coroners and medical examiners, funeral directors);
- Cadaveric organ, eye, or tissue donation purposes;
- Research purposes;
- Averting a serious threat to health or safety;
- Specialized government functions;
- Workers' compensation;
- Treatment, payment, and health care operations; and
- As otherwise required by law