MDX Hawai'i

# HIPAA – Privacy and Security

# Overview of HIPAA – Privacy and Security

- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protections for personal health information held by covered entities and business associates and gives patients an array of rights with respect to that information.
- The Privacy Rule does permit the disclosure of personal health information needed for patient care and other important purposes.
- The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and business associates to use to assure the integrity, confidentiality, and availability of electronic protected health information.

Confidential - Internal Use Only. Do Not Distribute.

MDX Hawai'i

# Privacy

# Privacy Rule Purpose

- To protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
- To protect individuals' medical records and other personal health information and applies to covered entities that conduct certain healthcare transactions electronically.
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections.

Confidential - Internal Use Only. Do Not Distribute.

# Protected Health Information (PHI)

All information that is spoken, written, and/or electronic about a member is confidential and protected.

- Name/Address
- Social Security Number/Health Insurance Claim Number
- Date of Birth
- Enrollment status/application
- Claims
- Satisfaction surveys that may include member data
- Billing information
- Contacts with customer service
- Member appeals/grievances
- Remittance advices that contain member data
- Illness, treatments, medications, notes
- Medical Records

Confidential - Internal Use Only. Do Not Distribute.

# Minimum Necessary

Be prudent and follows this guidance – before looking at or sharing PHI, as yourself:

- Do I need to know this to complete my job function?
- Does the other employee need to know this information to complete his/her job function?


Confidential - Internal Use Only. Do Not Distribute.

# Protection of Health Information

- Always follow these general safeguards:
  - Lock bins, drawers, files, and computers when not in use.
  - Secure work area and desktop when not present.
  - Provide faxes, print-outs, and reports only to an employee who needs to know the information.
  - Keep access doors to office buildings locked.
  - Don't give access to anyone that does not have an access badge.
  - Documents that are no longer needed should be shredded or placed in secure bins.
- Keep electronic data/devices secure at all times.
- Ensure email is secure (encrypted) when transmitting PHI.
- Do not leave PHI on voicemail or leave as a message to an unauthorized individual.
- Take care in public settings when speaking with clients on cell phones. Repeating information back aloud to confirm names, address, to other personal information can cause a privacy issue if overheard.

Confidential - Internal Use Only. Do Not Distribute.

# Privacy and Security –What is their Relationship?

Both rules are closely linked:

- **Privacy** is the "Who, What, and When"
- **Security** is the "How"

Definitions and many administration requirements now aligned with the Privacy regulations.

Privacy covers PHI on paper, in electronic form, and provided orally, while Security covers only e-PHI. 9

Confidential - Internal Use Only. Do Not Distribute.

# Breach Notification Rule

Breach notification regulations require covered entities to provide notification following a breach of unsecured PHI.

- **Breach** – An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.
- **Unsecured PHI** – PHI that has been released to individuals through the use of a technology or some other methodology that does not incorporate an encryption process.

Confidential - Internal Use Only. Do Not Distribute.

# Breach of PHI –What You Need to Know

Steps to take for perceived privacy policy or PHI violations:

- Contact the Chief Compliance Officer immediately.
- Once it determines a breach has occurred, the Chief Compliance Officer will execute the notification requirements for covered entities.

Following a breach of unsecured PHI, covered entities must provide notification of the breach to:

- Affected individuals
- Department of Health and Human Services (DHHS)
- The media, in certain circumstances

Confidential - Internal Use Only. Do Not Distribute.

# Corrective Actions

MDX Hawai'i will undertake appropriate corrective actions in response to potential non-compliance.

- The elements of the corrective action that address non-compliance committed by MDX Hawai'i employee(s) will be documented, include ramifications should the employee(s) fail to satisfactorily implement the corrective action.
- MDX Hawai'i will enforce effective correction through documented disciplinary measures, including employment or contract termination, if warranted.

Confidential - Internal Use Only. Do Not Distribute.

# Penalties for Non-Compliance

There are both civil and criminal penalties for non-compliance with Privacy Standards:

- **Civil Penalties**
  - Monetary penalties based on the type and severity of the violation.
  - Criminal charges against individuals and corporations may also occur.
- **Criminal Penalties**
  - Fine of up to $50,000 and/or 1 year in prison.
  - Fine of up to $100,000 and/or 5 years in prison if the offense is committed under false pretenses.
  - Fine of up to $250,000 and/or 10 years in prison if the offense is committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm.

Confidential - Internal Use Only. Do Not Distribute.

# Non-Compliance Reporting

Employees are required to, and encouraged to, bring forth information on suspected or known issues of non-compliance, FWA, or other violations of patient or company privacy or confidentiality issues.

- MDX Hawai'i's Code of Conduct clearly states this obligation.
- MDX Hawai'i prohibits any form of retaliation or intimidation against employees for reporting a compliance concern in good faith or for good-faith participation in any investigation or other proceeding related to such a report.
- Disciplinary actions that could be imposed for non-compliance or FWA include training, verbal or written warnings, reprimands, suspensions, terminations, and/or financial or criminal penalties.

Confidential - Internal Use Only. Do Not Distribute.

# Non-Retaliation

MDX Hawai'i will not tolerate retaliation or intimidation in any form against an employee who, in good faith, reports a potential issue of non-compliance.

- Any behavior construed as retaliation by any agilon employee or provider may lead to disciplinary action, up to and including termination
- If you feel you are the victim of retaliation, report to your HR Business Partner immediately.

Confidential - Internal Use Only. Do Not Distribute.

# Whistleblower Protections

- A whistleblower is a person who exposes information or activity that is deemed illegal, dishonest, or violates professional or clinical standards
- Protected: Persons who report false claims or bring legal actions to recover money paid on false claims are protected from retaliation
- Rewarded: Persons who bring a successful whistleblower lawsuit receive at least 15 percent, but not more than 30 percent, of the money collected.


Confidential - Internal Use Only. Do Not Distribute.

# Ways to Report Non-Compliance

- Suspected non-compliance or FWA can be reported in the following ways:
- By notifying a supervisor, manager, or director
- Directly to the Compliance Department through the Compliance secured email box (ComplianceAH@agilonhealth.com) or the Compliance hotline (833-668-8638)
- Reports made through Compliance can be made confidentially and/or anonymously.

Confidential - Internal Use Only. Do Not Distribute.