Network Medical Management
HIPAA Training

2022

Network Medical Management

TABLE OF CONTENTS

HIPAA & PRIVACY SECURITY PROGRAM

PURPOSE:

- To support NMM's commitment to comply with the Health Insurance Portability & Accountability Act of 1996 (HIPAA) & all other applicable State & Federal standards.
- To establish a HIPAA Privacy Program to ensure Member's health information is properly protected while allowing the flow of health information needed to provide & promote high quality health care.
- To protect Member's PHI & PII (personal identifiable information) from exposure to any person without authorization or business to know.

SCOPE:

- The HIPAA Privacy Program falls under the auspices of the Compliance Department.
- Federal & State statues & regulations require NMM to investigate potential privacy incidents & report privacy breaches to health plans & appropriate regulatory agencies.

WHAT IS HIPAA?

As someone employed in the healthcare industry, you need to be aware of the HIPAA Privacy and Security regulations and how they apply to you and your work.

The HIPAA (Health Insurance Portability and Accountability Act of 1996) Privacy Rule established standards to protect an individual's private, personal, and health-related information.

PRIVACY RULE

Applies to covered entities such as health plans, health care clearing houses, health care providers, and businesses who do business with healthcare practitioners

- Requires covered entities train all staff members in regards to their responsibilities to ensure that all related policies and procedures are upheld

- Requires appropriate safeguards to protect the privacy and confidential nature of personal health information (PHI)

- Requires set policies and procedures to ensure a patient's privacy and security

-Gives patients' rights in regards to their health information

- Requires a "Notice of Privacy Practices" that explains an organization's policies and procedures relating to privacy and the use and/or distribution of health information

HITECH & OMNIBUS

The Health Information Technology for Economic and Clinical Health (HITECH) Act and the HIPAA Final Omnibus Rule updated the federal HIPAA privacy and security standards.

Collectively, major updates include:

- Breach notification requirements
- Fine and penalty increases for privacy violations
- Patient right to request electronic copies of the electronic health care record
- Patient right to restrict disclosure to health plans for services self paid in full ("self-pay restriction")
- Mandates that Business Associates are directly liable for compliance with HIPAA provisions

NOTICE OF PRIVACY PRACTICES

The Notice of Privacy Practices explains that health information is used for:

-Providing treatment

- Ensuring payment for services

- Operating the facility

- Improving the quality of care

- Maintaining a facility directory

NOTICE OF PRIVACY PRACTICES

The Notice explains that patients may:

- View and receive copies of their medical records

- Restrict who has access to their medical records

- Amend their health information when the information is incomplete or inaccurate

- Request an alternative means or location for receiving protected health information

- Lodge a complaint with covered entities and file complaints with the Department of Health and Human Services

WHAT IS PII?

- **Personally identifiable information (PII)**

PII is information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual. PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII is protected to help prevent identity theft. PII is a person's name, in combination with any of the following information:

- mother's maiden name.
- driver's license number.
- bank account information.
- credit card information.
- relatives' names.
- postal address.
- email address.
- home or cellular telephone number.
- personal characteristics.
- Social Security Number (SSN).
- date or place of birth.

- other information that would make the individual's personal identity easily traceable

WHAT IS PHI?

- **Protected health information (PHI)**

PHI is a subset of PII that relates to health data. PHI is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a healthcare service such as diagnosis or treatment. HIPAA regulations allow researchers to access and use PHI when necessary to conduct research. However, HIPAA applies only to research that uses, creates, or discloses PHI that enters the medical record or is used for healthcare services, such as treatment, payment, or operations. Common identifiers are:

- names.
- all geographical subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code.
- all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
- phone numbers.
- fax numbers.
- electronic mail addresses.
- Social Security Numbers.
- medical record numbers.
- health plan beneficiary numbers.
- account numbers.
- certificate/license numbers.
- vehicle identifiers and serial numbers, including license plate numbers.
- device identifiers and serial numbers.
- Universal Resource Locators (URLs).
- Internet Protocol (IP) address numbers.
- biometric identifiers, including finger and voice prints.
- full face photographic images and any comparable images.
- any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

WHAT ARE PATIENTS RIGHTS?

- Right to Access, Review & Copy
- Right to Amend
- Right to Accounting of any disclosures
- Right to Restrict Use and/or Disclosure
- Right to Request Confidential Communication

WHAT ARE PATIENTS RIGHTS?

Any individual who has entrusted his or her PHI to us has the right to: access, review, and copy that PHI; request amendment of the information; and request an accounting of any disclosures we have made.

Upon receiving a request, we must act on it no later than 30 days after receipt for PHI that is maintained. This time requirement applies regardless of whether the information is maintained on-site or off-site. A single 30-day extension is allowed. If the 30-day extension is needed then the requestor must be informed of the reason.

Covered entities must provide an individual with access to PHI in the electronic form and format requested by the individual if the PHI is maintained electronically in one or more designated record sets. Covered entities may charge for the labor for copying PHI requested by the individual.

PATIENT AUTHORIZATION

A covered entity cannot release PHI without patient authorization

An authorization form is detailed and specific to:

- Permitted uses and disclosure
- Permitted recipient
- Operating the facility
- Personal health information that may be shared

EXCLUSION: Required by law such as subpoenas

HOW CAN WE PROTECT PHI?

- Never leave files/documents open and/or unattended
- Cover, turn, or lock up documents – never dispose in trash cans
- Avoid discussing patients' care in common areas
- Access, use or provide only the minimum amount of PHI necessary
- Lower your voice or move to more private area
- Do not discuss outside of work
- Verify identities/authorization before giving access to data
- Take measures to protect – computers, cell phones, electronic devices
- Questions & violations – report to Supervisor or Compliance Officer

GOOD HIPAA PRACTICES

- Triple check!! When mailing or handing documents to members, slow down and verify that each document belongs to the person

- Check printers, faxes, and copier machines when you are done using them

- Do not leave paper PHI laying on your desk; lock it up at the end of the day

- PHI file are only store behind locked cabinet or rooms for minimum of 6 years unless is business and compliance related for 10 years

-Shred or destroy PHI media (paper or electronic) to unreadable and irreversible fashion

- Security Encryption when emailing

DISCLOSURES PERMITTED BY LAW

- Treatment, payment, and health care operations activities
- Certain communicable diseases to state health agencies
- Cases involving child abuse, elder abuse, suspected neglect and/or domestic violence
- Law enforcement requests certain information to determine if the patient is a suspect in a criminal investigation
- Judicial and administrative proceedings, such as a court order or subpoena
- Reporting of suspicious deaths or certain suspected crime victims, such as cases involving gunshot wounds
- Coroners or medical examiners in the determination and reporting of cause of death
- Funeral directors responsible for the arrangement of funeral services
- Food and Drug Administration (FDA) requires providers to report certain information about medical devices that break or malfunction

SECURITY RULE & SAFEGUARDING PHI

Security Rule requires covered entities to maintain reasonable & appropriate administrative, technical & physical safeguards to protect PHI

Electronic, Printed, Oral, Written or Recorded

- ✓ Report security incidents
- ✓ Ensure computer monitors cannot be viewed by general public
- ✓ Each user must use his/her own unique ID & password
- ✓ Never share your ID & password
- ✓ Do not open suspicious e-mails
- ✓ Do not send PHI through e-mail without proper encryption

POTENTIAL PENALTIES

The Office of Civil Rights (OCR) and the Department of Health & Human Services enforce HIPAA regulations and impose penalties. Penalties include the following:

-Violations without knowledge (where an individual did not know they violated HIPAA regulations) result in a $100 fine for each violation, not to exceed a total of $25,000 per year

- Violations due to reasonable cause, but not willful neglect, result in $1,000 fine for each violation, not to exceed $100,000

- Violations due to willful neglect that the organization corrected will result in a $10,000 fine for each violation, total fines not to exceed $250,000

- Violations due to willful neglect that the organization did not correct result in a $50,000 fine for each violation, fines not to exceed $1,500,000 for the calendar year

- Criminal penalties can not only include large fines but may also include jail time. The more serious the offense, the harsher the penalty

REPORTING OF POTENTIAL HIPAA & SECURITY BREACH

WITHOUT FEAR OF RETALIATION

HIPAA BREACH

NMM Employees:

Call NMM's Compliance Officer:
Jo Espino 626-943-6266

Compliance Hotline: 626-943-6286
24 hours a day/7 days a week
You may report anonymously and confidentially

Email: JEspino@networkmedicalmanagement.com

SECURITY BREACH

What should you do if you suspect potential security breach?

You may do ANY of the following:

a. Tell - your supervisor or security officer
b. Call - IT Security Officer - 626.943.6256
Helpline - 626.943-6172
c. Email - RPagan@networkmedicalmanagement.com or helpdesk@networkmedicalmanagement.com

APPENDIX: Sample Scenario

Question

My supervisor has been out on disability and I'm very concerned about her — we have worked together for over 10 years. Since I am a nurse in medical management and have a job that requires access to and use of medical information, can I check on the status of my supervisor?

Answer

Although you have security clearance to this PHI and PII for purposes of your work, you may not access information and share it outside the scope of your responsibilities, as set forth in our company's HIPAA Privacy Policies and Procedures.

Question

I was visiting my father in the hospital when his doctor came into the room to discuss my father's diagnosis and treatment plan. My coworker told me that under HIPAA it was wrong for the doctor to speak in front of me and should have asked me to leave the room. Is this true?

Answer

The information about your father's medical condition is considered PHI. In this case, however, the doctor had reason to believe that your father accepted you hearing about his medical condition and as such authorization was in effect given. If your father objected in any way, the doctor should have stopped, asked you to leave the room, and then continued the conversation with your father. Adult family relationships do not confer any special rights to another person's PHI.

You've completed the lesson!

You have now learned about HIPAA program.