NMH HIPAA Privacy Training

2017 Version

NORTH
MEMORIAL HEALTH

Training Objectives

To gain a better understanding of:

- The Notice of Privacy Practices
- Access Monitoring
- Keeping Customer Information Private
- Minimum Necessary Requirements
- Customer's (customer's) Privacy Rights
- Protected Health Information Uses and Disclosures
- Covered Entities and Business Associates
- Accounting of Disclosures
- Release of Information

HIPAA?

- Health Insurance Portability and Accountability Act (HIPAA)
- Passed in 1996
- Primary goal was to make it easier for people to keep health insurance; protect the confidentiality and security of healthcare information.
- Protected Health Information (PHI) Defined:
  - Any patient (customer) information that relates to a person's health or conditions, the provision of health care to that person, or payment related to that person's health care, if the information identifies the patient or could reasonably be used to identify the patient.

HIM?

Health Information Management (Medical Records)

- Functions
  - Release of Patient Information
  - Scanning Paper-Based Records
  - Data Integrity
  - Chart Completion
  - Document Services - Medical Transcription
  - Records Storage and Retrieval
  - Privacy Audits

Notice of Privacy Practices (NPP)

- The Notice of Privacy Practices (NPP) is a statement provided to customers explaining to them how PHI is protected, and what rights they have.
- It must be available to all customers.
- Customers must acknowledge that they have received the NNP and this acknowledgement is included in the signature on the
- Consent for Services.
  - The NPP is not a consent or an authorization form—it is only an explanation.

Customer's Privacy Rights

Access

– Customers have a right to access their PHI in paper or electronic format. The customer must complete a request form and the request must be fulfilled by following the Health Information Access and Disclosure Policy. The Health Information Management (HIM) Department is a resource to fulfill these requests.

Request Confidential Communication

– Customers have a right to request NMHC communicate with them in a specific manner, time and place. For example, telephone, cell phone, email, mail, etc. The customer must give permission to accomplish this.

Request Amendments

– Customers have a right to request an amendment to their medical record but requests may not result in a change to the medical record. Customer must complete a request form following the Amendment to customer Medical Record policy. The Health Information Management Department is a resource.

Request for Restricted Use

– Customers have a right to request that their PHI is restricted for certain types of situations. We may deny the request if we have defensible grounds for the denial. This is often associated with customers who pay cash for their services.

Treatment, Payment or Healthcare Operations (TPO) Use & Disclosure

- HIPAA allows NMHC and it's Business Associates to use and/or disclose PHI for the purposes of providing treatment, payment or conducting healthcare operations without specific authorization.
- What does this mean? Here is an example of each:
  - Doctors and/or hospitals can share PHI freely and without customer consent to provide treatment to the customer.
  - Our business office can release information to the customer's insurance company in order to receive payment for provided services.
  - Healthcare operations include a number of business activities such as quality assessment, licensing, team member review.
- A Business Associate Agreement is not required when sharing information between care givers for treatment purposes.
- **MN Statute (Health Records Act) requires customer consent to share information for Treatment, Payment or Healthcare Operations (TPO).**

Minimum Necessary

- The HIPAA law requires us to:
  - Limit the use of PHI to only what is necessary…
  - Limit the amount of PHI disclosed to only what is necessary…
  - Limit requests of PHI to only what is necessary…. …..to accomplish the business purpose.
- But “minimum necessary” does not apply to treatment disclosures of information!

Non-TPO Use & Disclosure of PHI

- A customer's authorization is required for most non-TPO use and disclosure. An authorization specifies
  - An expiration date
  - States how the information will be used or disclosed
  - Indicates what PHI will be used or disclosed
  - Indicates to whom the PHI will be disclosed
  - Includes HIPAA-required statements about re-disclosure and other issues

Use & Disclosure of PHI Required by Law

- There are situations that require NMHC to use and/or disclose PHI **without** the customer's authorization.
- The most common reasons are:
  - Reporting vulnerable adult abuse
  - Instances of child abuse or neglect
  - A court order signed by a judge
  - Threats to public health
  - Disaster relief purposes
  - Reporting vital statistics

Release of Information Process

- Please refer to the Policy and Procedure *Health Information Access and Disclosure.*
- Most customer release of information (ROI) request will be fulfilled by the Health Information Management Department.
- Direct customer care sites should respond to customer request for PHI at the point of care, when the customer is present. This includes, discharge instructions, after visit summaries, etc.

Parent Access to Minor Children's Records

- Please refer to the Policy and Procedure *Health Information Access and Disclosure.*
- If the customer is a minor, the parents may access records unless the minor is emancipated, or has consented to his or her own care as permitted by law.
- In the case of treatment given a minor based upon a minor's consent (for conditions such as sexually transmitted infections/diseases (STIs STDs), pregnancy, alcohol/drug abuse), refrain from releasing that portion of the record relevant to this episode of care when responding to a request for information for which the signed authorization is that of the parent or guardian. An authorization by the minor is required in this instance.

Accounting of Disclosures

- Customers have a right to request a list of certain disclosures of their medical information.
- This list does not include disclosures made for treatment, payment or healthcare operations; disclosures that the customer has authorized; disclosures for facility directories; national security or intelligence purposes; disclosures to correctional institutions or law enforcement with custody of customer.
- Request must state the time period and can go back no more than six years
- All requests need to be referred to the HIM Department.
- There is an *Accounting of Disclosures* Policy in Policy Tech

Fax PHI & Emailing PHI

FAX

- If you send PHI using a fax machine, be careful to correctly enter the fax number and use a fax cover sheet. The cover sheet should include a phone number and a standard disclaimer.
- Make sure PHI is not left on fax machines.

Email

- PHI can be sent internally via email within our corporate Outlook system. No customer information should be in the subject line of the email.
- PHI sent EXTERNALLY via email MUST be sent secure and encrypted.
- Limit the use of identifiers to the minimum necessary (without compromising customer safety).
- Any electronic file including PHI should be password protected. The password for the file should be sent to the intended recipient in a separate email.

Phone Verification Process

- When taking a phone call, it is essential to verify the identity of the caller before providing any information.
- If the caller is a customer, have the customer verify their identity by asking them answers to at least 3 identifiers, such as date of birth, last 4 digits of social security number, home address, phone number, etc.
- If the caller is a family member, before providing any information to the caller you must validate the customer has authorized
- NMH to share information with the family member. The amount of information provided to the family member should be limited.

Phone Messages

- If voicemail or an answering machine is reached when calling a customer, no PHI should be left in the message. You may leave a message indicating the name of the doctor/clinic, phone number and request a return call.
- Never leave test results, reason for an appointment or instructions about the appointment in a phone message unless the customer has given permission to do so.
- Test information can be left with a family member if the customer specifically requests for another person to leave the information with someone other than the customer.

Destruction of PHI

- Papers with PHI
  - Put papers with identifiable health information in the confidential destruction bins (Shred-It).
  - Never throw any paper, label, or anything with customer information on it within a regular garbage can or a sharps container. Black out identifiers on medical waste, or remove label prior to disposal.
- Electronic file with PHI
  - All electronic files with PHI must be disposed of using the appropriate software. If you have electronic files with PHI, please contact Information Technology for assistance.
  - Computers or hard drives with PHI will be disposed of by Information Technology.
  - There are specific legal requirements for destruction of PHI in electronic format.

Covered Entities and Business Associates

- Covered Entity is:
  - Health plan, health care clearinghouse, or health care provider that electronically transmits health information.
  - North Memorial is considered a “covered entity”
- Business Associate is:
  - A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
  - A member of the covered entity’s workforce is not a business associate.

Access Monitoring

- Epic Break-The-Glass Audits: Weekly-Capturing 100% of BTG Incidents
- Random Epic Access Audits: Monthly
- Focused Epic Access Audits: As Needed/Appropriate, Upon Request
- Other Non-Epic Applications/Environments Access Audits: Quarterly
- Epic Care Everywhere Consent Audits: Monthly

Access Monitoring – HIM Procedure

- All individuals with access to electronic medical records are subject to random and focused audits.
- Random audits of accesses to electronic medical records are completed
- Focused audits are conducted:
  – high profile customers
  – privacy or security complaints
  – to review specific or individual user access activity.
- Confirm user as a member of the customer care team involved with a particular encounter
- If cannot confirm access was required, contact user's manager and request that follow-up take place with the user to provide the business reason for accessing the specific customer's EMR.
- Continue contacts/follow-up as needed.

Your Responsibilities

- Lock file cabinets
- Turn over unattended charts and any customer paperwork
- If you see PHI unattended, return it to it's proper place
- Turn computer screens away from unauthorized view or use privacy screens
- Use passwords on computers that contain PHI
- Place fax machines, printers and copy machines in secure areas
- If others (visitors) are present, ask the customer if he/she would prefer privacy before conversations are held regarding his/her care.
- Log out of applications or lock your workstation when you leave your workstation
- Double check identifiers when sharing customer information to assure that the right information is being disclosed to the right customer

Your Responsibilities

- Do not discuss customer information in public areas (elevators, cafeteria, hallways, etc.)
- Speak quietly when using PHI in a conversation
- Only access information needed to perform your job duties.
  DO NOT LOOK AT, SHARE or DISCUSS:
  - Health information of a customer if it is not required for your job
  - Census reports/customer records from units where you are not assigned
  - Records of family members, friends, neighbors, co-workers, etc. unless required to do your job
  - Records of customers that you hear about in the news
- Never take customer photos or transmit customer information over personal phones/hand held devices.
- Be careful not to mix-up customer paperwork such as prescriptions, after visit summaries, discharge instructions.
- Assign the correct guarantor during registration.
- Ask questions.

Privacy Concerns/Complaints

- The Office of Civil Rights has the responsibility for investigating official privacy complaints received by their office.
- NMH also has the responsibility for investigating all privacy complaints/concerns made by customers, team members, members of the medical staff, etc.
- Investigations are performed internally by the Privacy Officer.
- Concerns/complaints should be reported to the Privacy Officer at HIPAA.Inquiries@northmemorial.com or 763.581.4437

NORTH
MEMORIAL HEALTH