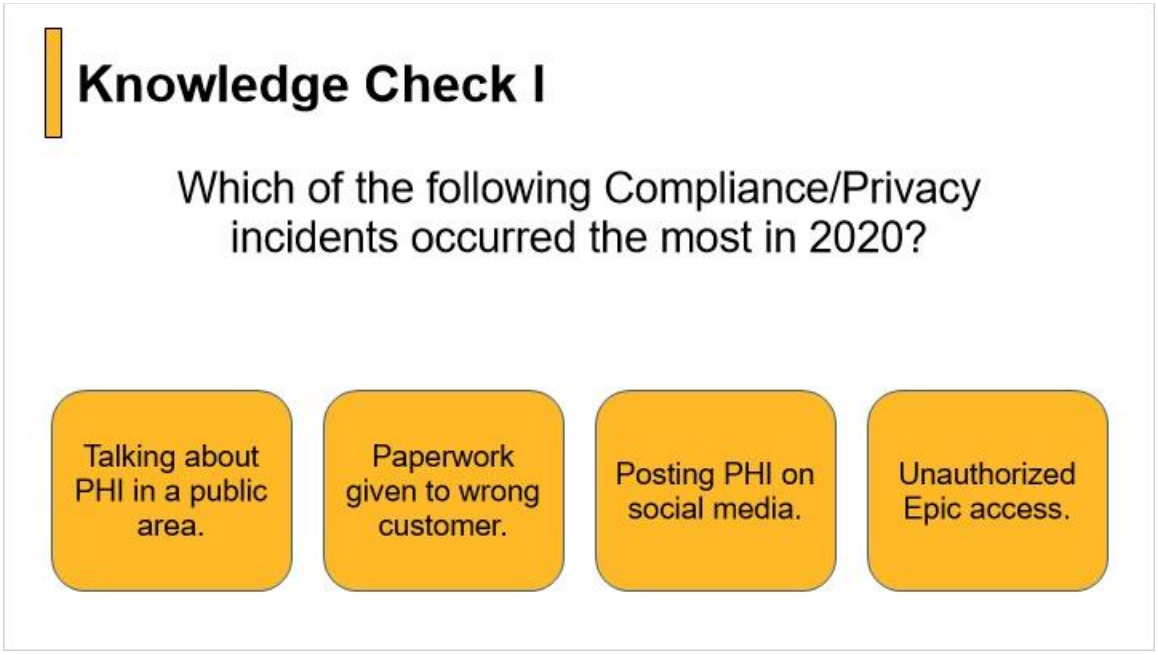
Information Privacy 2020



Knowledge Check I

Which of the following Compliance/Privacy incidents occurred the most in 2020?

Incorrect. Try again.

Talking about PHI in a public area does happen and is a concern.

We must make reasonable attempts to keep PHI private, and should assure that necessary conversations are held in a private area.

However, it was not the incident that occurred the most in 2019.

Back

Knowledge Check I

Which of the following Compliance/Privacy incidents occurred the most in 2020?

Incorrect. Try again.

Paperwork given to wrong customer does happen and is a concern.

Be sure to check customer identifiers on each page to assure that the information pertains to the correct customer.

However, it was not the incident that occurred the most in 2019.

Back

Knowledge Check I

Which of the following Compliance/Privacy incidents occurred the most in 2020?

Incorrect. Try again.

Posting PHI on social media has happened and is a concern.

You are obligated to protect the privacy of our customers and cannot post or share customer names, photos or any information that identifies, or could be used to identify, a customer on social media.

However, it was not the incident that occurred the most in 2019.

Back

Knowledge Check I

Which of the following Compliance/Privacy incidents occurred the most in 2020?

Correct!

Having access to use Epic to do your job does not mean you can look up any customer in Epic that you want to.

Next

The federal Health Insurance Portability and Accountability Act, or HIPAA, other regulations, and some state laws, require us to protect customer privacy.

As a North Memorial Health (NMH) team member, you are responsible for protecting the privacy and security of customer information.

This module helps you understand your responsibilities related to information privacy.

Protected Health Information

NMH must protect each customer's Protected Health Information (PHI). Not only is this a compliance obligation, it is also a requirement for providing unmatched customer service.

PHI is customer information that:

- Identifies or could reasonably be used to identify the customer
- Relates to the customer's health, health services received, or payment for those services

Minimum Necessary

When doing your job, you may only access the minimum amount of PHI necessary for you to accomplish your work. This is know as the “Minimum Necessary Rule.”

- NMH privacy policies prohibit you from viewing any information that is not required for you to complete your job tasks.
- Disclosures of information outside of the organization should be limited to the minimum amount of PHI necessary to fulfill the request.

Knowledge Check II

Which of the following is an example of minimum necessary?

- Including only those team members in a discussion who have a need to know.
- Accessing only the record needed to do your job from a list of customers.
- Not looking through a customer’s old past encounters when responding to a question about a current finding.
- All of the above.

Knowledge Check II

Which of the following is an example of minimum necessary?

Correct!

When sharing protected health information in any manner (including data fields in a report) minimum necessary would be demonstrated by limiting the information to only what is necessary to meet the requirements of the requestors to accomplish their work.

Next

Knowledge Check II

Which of the following is an example of minimum necessary?

Incorrect.

The correct answer is all of the above,

- Including only those team members in a discussion who have a need to know.
- Accessing only the record needed to do your job from a list of customers.
- Not looking through a customer's old past encounters when responding to a question about a current finding.

Next

Disclosure of PHI

Most disclosures that are for purposes other than treatment, payment or health care operations require customer authorization.

- NMH privacy policies explain when disclosures may be made without authorization. Examples include:
  - Reporting child abuse/neglect to child protective services.
  - Responding to inquires from health oversight agencies, such as the Centers for Medicare and Medicaid Services (CMS) or the MN Department of Health.
- When in doubt, do not disclose PHI outside of NMH without consulting the Privacy Department.

Knowledge Check III

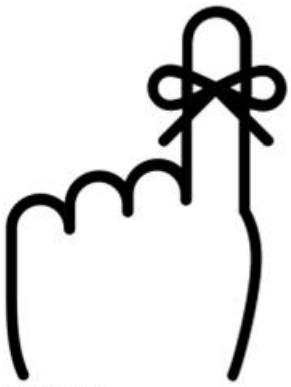
Click on the boxes that are permissible actions to keep PHI private.

Discuss PHI in public areas.	Turn over or cover PHI that is unattended or in plain view.	If visitors present, ask customer if they prefer privacy before discussing PHI.	Leaving PHI in voicemail messages is always OK.
When taking a call, verify identity of caller before providing PHI.	If faxing, use cover sheet to protect PHI.	Always include the customer's name in the subject line of an email.	Lock your computer when you walk away

Right or Wrong? Next

Don't Forget…

- Double check patient identifiers on all paperwork, such as discharge summaries and after visit summaries before handing paper to customers. This will prevent PHI from being given to the wrong customer.
- All paper containing PHI must be disposed of in confidential destruction bins (Shred-It). Keeping discarded PHI in a box near your work station is prohibited.



Created by Álvaro Y. from Noun Project

Cell Phones & Social Media

Cell Phones & Social Media

- Never take customer photos or transmit PHI over personal cell phones/devices.

- Never post North Memorial business or PHI online.

Cell Phones & Social Media

- Never take customer photos or transmit PHI over personal cell phones/devices.

- Never post North Memorial business or PHI online.

HIPAA Privacy & Epic Use

Access to Protected Health Information

Curiosity is NEVER an appropriate reason to look at customer PHI.

- You must have a business purpose for accessing any patient record.
- Only access the minimum necessary PHI needed to complete your work.

Privacy Policies

NMH privacy policies prohibit you from viewing:

- Census reports/customer records from units where you are not assigned.
- Records of family members, friends, co-workers, etc. unless required to do your job.
- Records of customers that you hear about in the news.
- Pages or portions of the Epic record that you do not need to access in order to complete your work.

Privacy Policies

- NMH uses Break the Glass functions in Epic as an added level of information security to certain health records that require additional privacy protections.
- If you get a Break the Glass notice, complete the prompts within Epic to access the record and do your job.
- If you get a Break the Glass notice, and you do not have a job related reason for viewing the record, close the record immediately.
- Privacy Department staff routinely monitor Break the Glass access.

Click anywhere to continue.

Knowledge Check IV

What's the ***best*** way to access your own medical records?

MyChart | HIM | Epic | Insurance Provider

Knowledge Check IV

What's the ***best*** way to access your own medical records?

Correct!

MyChart is the Epic portal designed for use by all customers, including NMH employees who are also customers of NMH.

Next

Knowledge Check IV

Which of the following are permissible when modifying your own Epic record?

- Scheduling Appointment
- Posting Payment
- Updating Diagnosis
- Updating Medication List
- Changing Guarantors
- Correcting Address
- All of the above
- None of the above

Knowledge Check IV

Which of the following are permissible when modifying your own Epic record?

Correct!

Team members are prohibited from documenting in or modifying their own health records in any way.

Next

Knowledge Check IV

Which of the following are permissible when modifying your own Epic record?

Incorrect.

Team members are prohibited from documenting in or modifying their own Epic record in any way.

Try again.

Back

Knowledge Check V

NMH privacy policies prohibit staff from using Epic to view a family member's health record.

True

False

Knowledge Check V

NMH privacy policies prohibit staff from using Epic to view a family member's health record.

Correct!

Team members are prohibited from viewing the Epic records of their children (regardless of age), spouse, or other family members.

Employees who access the Epic records of family members are subject to investigation and disciplinary action.

Next

Knowledge Check V

NMH privacy policies prohibit staff from using Epic to view a family member's health record.

Incorrect

Team members are **prohibited from viewing** the Epic records of their children (regardless of age), spouse, or other family members.

Employees who access the Epic records of family members are subject to investigation and disciplinary action.

Next

Privacy Audits

All team members are subject to random and focused privacy audits.

- If Privacy identifies Epic access that was not for a business purpose or was not limited to the minimum necessary, Privacy will contact the team member's manager and request follow-up.
- Privacy policy violations are subject to disciplinary action in accordance with HR policies.

NMH must report all confirmed privacy breaches to the Office for Civil Rights, which oversees HIPAA enforcement.

Privacy Investigations

- All reports of privacy non-compliance are investigated by the Privacy Department.
- Reports may be made by any team member, customer, or family member.
- Reports may be made to the Privacy Officer.

If you suspect that patient confidentiality may have been compromised, please let us know immediately of the concern so that appropriate action can be taken.

Business Associates

- NMH has contracts with many vendors and business partners that perform functions or activities on behalf of NMH that involve the use or disclosure of PHI.
- These partners are known as Business Associates under HIPAA.
- Prior to disclosing any PHI to a Business Associate, NMH must have a signed contract and a business associate agreement.
- All questions regarding Business Associate Agreements should be referred to the Privacy Officer, privacy@northmemorial.com, or the Chief Compliance Officer.

Customer Privacy Rights

Customers have the right to:

- Access their health records
- Request confidential communications and restrictions on their health records
- Request amendments to their records
- Request a list of certain disclosures of their health records

Release of information requests and other requests related to health records should be directed to the Health Information Management department.

Report Privacy Concerns

If you suspect that patient health information confidentiality may have been compromised, please let us know immediately so appropriate action can be taken. You may notify:

- Your manager
- Privacy Officer
- privacy@northmemorial.com
- Compliance Officer
- Compliance Hotline (on the back of your ID badge)
- compliance@northmemorial.com

Privacy Considerations for Remote Workers

- Requires a private area to be used only for work purposes.
- Do not leave your computer unattended. Do not allow viewing of NMH work or allow others to use your computer while logged-in to iRAS.
- Do not forward NMH emails to your personal email.
- Do not move or save any content to your home computer.
- Do not print unless you have been granted special approval.
- Minimize PHI written on paper.
- Assure two levels of physical safeguards are in place when storing PHI. (Notebook, folder, locked cabinet, safe, closed door)
- Destroy paper PHI in an authorized, secure manner. (cross-cut shredder, Shred-It bin)

Compliance Contacts

Dawn Backlund, *Chief Compliance Officer*

Dawn.Backlund@northmemorial.com

Compliance@northmemorial.com

763-581-4732

Deb Contreras, *Privacy Officer*

Deb.Contreras@northmemorial.com

Privacy@northmemorial.com

763-581-4437

Mike Sweet, *Data Security Officer*

Mike.Sweet@northmemorial.com

DataSecurity@northmemorial.com

763-581-2503

The End

There is no quiz with this module.

CLOSE THIS MODULE.