What is the Intent?

The seriousness of the fraud is determined by the intent behind the fraud.

- Was the mistake an unintentional error? Or was it the result of intentional fraudulent behavior?
- If the mistake was an unintentional error, could it have been prevented with environmental controls (e.g., better policies directing documentation, better delineation of duties to ensure appropriate decision making, more active monitoring and testing critical processes)?

FWA Laws

The federal and state governments have a long history of regulating health care practices to prevent fraud, waste and abuse. These include:

- False Claims Act
- Anti-Kickback Statute
- Physician Self-Referral Statute (Stark)
- Exclusion Statute
- Civil Monetary Penalties Law

You do not need to know all the details of these laws in order to do your part in preventing FWA. However, by the end of this training, you will have a general understanding of how these laws impact your role at NMH.

False Claims Act

False Claims Act: This law makes it illegal for any person to knowingly make a fraudulent claim for payment to the federal or state government.

- You do not have to intend to defraud the government to violate this law. You can be liable for violating this law if you act with deliberate ignorance or reckless disregard of the law.
- The False Claims Act generally applies to any type of government claim for payment, but the federal government aggressively pursues False Claims Act enforcement within the health care industry.

False Claims Act violations can be fined up to three times the amount of the false claim, plus $23,607 per claim. Fines can add up quickly because each separate claim submitted to the government can be separate grounds for liability.

Anti-Kickback Statute

The Anti-Kickback Statute makes it a crime to knowingly and willfully offer, pay, solicit, or receive, directly or indirectly, anything of value to induce or reward referrals of items or services reimbursable by a government health care program (such as Medicare or Medicaid).

- Remember that both the "giver" and the "receiver" of an inappropriate inducement or reward are liable under the Anti-kickback statute. This is why all NMH business must be conducted in a fair and transparent manner.

Anti-kickback violations can result in prison sentences and fines and penalties of up to $100,000 per kickback plus three times the amount of the underlying transaction.

Stark Law

The Self-Referral Prohibition Statute is also commonly known as the Stark Law.

- This law prohibits physicians from referring Medicare or Medicaid patients to an entity with which the physician or a physician's immediate family member has a financial relationship — unless an exception applies.
- This is a complex law with severe penalties for non-compliance, so every contractual arrangement between NMH and a physician must be reviewed by Provider Services and Compliance/Legal. All relationships must be appropriately documented.

Penalties for physicians who violate the Stark Law may include fines for each service performed in violation of the law, repayment of claims, and potential exclusion from all Federal Health Care Programs.

Exclusion Statute

Under the Exclusion Statue, the federal Health and Human Services Office of the Inspector General must exclude providers and suppliers convicted of any of fraud, waste or abuse from participation in federal health care programs (such as Medicare and Medicaid).

- As a Medicare/Medicaid provider, NMH must not employ, contract, or otherwise do business with any excluded individual or entity.
- The federal government maintains exclusion lists, and NMH is obligated to routinely screen these lists to ensure it does not do business with any excluded individual or entity.

Civil Monetary Penalties Law

The Civil Monetary Penalties Law authorizes penalties for a variety of health care fraud violations. Violations that may justify penalties include:

- Presenting a claim that you know, or should know, is for an item or service not provided as claimed or that is false or fraudulent.
- Presenting a claim you know, or should know, is for an item or service that Medicare will not pay.
- Violating the Anti-kickback Statute.

Penalties may be assessed up to three times the amount claimed for each item or service, or up to three times the amount of payment offered, paid, solicited or received.

FWA Committed by Customers

In addition to the types of errors or intentional bad acts that may constitute FWA committed by health care providers, Medicare/Medicaid beneficiaries may also commit FWA. If you see any of these situations occur, report the activity to the compliance department.

- Drug diversion occurs when someone uses drugs, medications, and other pharmacy supplies for reasons other than their original or intended purpose.
- Member fraud occurs when a member carries out a fraudulent activity by falsifying member enrollment data or identity theft.
- Identity fraud occurs when someone pretends to be someone else by assuming that person's identity; often, this is done to access resources, obtain credit, or obtain other benefits in that person's name.

Which of the following laws makes it a crime to knowingly and willfully offer, pay, solicit, or receive anything of value to induce or reward the referral of services reimbursed by Medicare or Medicaid?

- ○ The Exclusion Statute
- ◉ The Anti-Kickback Statute
- ○ The Affordable Care Act
- ○ The Stark Law

What are your FWA Prevention Responsibilities?

You play a vital part in preventing, detecting, and reporting potential FWA, as well as Medicare/Medicaid non-compliance.

- You must comply with all applicable regulatory requirements, including participating in compliance program activities.
- You have a duty to the to report any suspected or actual non-compliance that you may know of.
- You have a duty to follow NMH's Code of Conduct. The Code of Conduct can be found on the Compliance intranet webpage and in the policy management tool C360.
- When in doubt, ask questions. The Compliance Department is a resource for all NMH team members.

Reporting Fraud, Waste, and Abuse

- All NMH Team Members are expected to report any known or potential concerns of FWA.
- All reported compliance concerns are investigated by the Compliance Department. Investigations are handled confidentially.
- NMH prohibits any form of retaliation against a team member who reports a FWA concern in good faith.

How to Report a FWA Concern

- You can speak to your supervisor, and your supervisor will report the concern to Compliance.
- You can send an email to Compliance.
- You can call or email any Compliance Department team member.
- You can contact the Compliance Hotline.
  - This number is printed on the back of your employee badge!
  - You may leave an anonymous message on the Hotline.

How can you report a fraud, waste or abuse concern?

- ○ Call the compliance hotline, which is printed on the back of your employee badge.
- ○ Contact the Chief Compliance Officer.
- ○ Contact any compliance department team member.
- ◉ All of the above.

Overview of the NMH Compliance Program

The Compliance Program helps NMH identify compliance concerns and reduce compliance risks.

Compliance Department Staff work with team members to implement changes to correct identified non-compliance and prevent the problem from happening again.

Compliance Contact

Chief Compliance Officer
compliance@northmemorial.com

Done!

You have completed this module.

CLOSE THIS MODULE.

Data Security

As a North Memorial Health (NMH) team member, you are responsible for protecting customer information and business data.

In addition to following Privacy policies you must also do you part to help secure the NMH information systems.

This module helps you understand your responsibilities related to data security and protecting the NMH information systems.

Data Security

Click on each lock to learn more about each role.

Created by Vishal patel from Noun Project

Created by Vishal patel from Noun Project

Data Security

Click on each
more abou

Created by Vishal patel
from Noun Project

NMH IT team members ensure Data Security in the following ways:

- Performs annual audits and risk assessments to identify security risks.
- Completes risk management plans to respond to identified risks.
- Maintains appropriate IT policies, processes, technologies, and workflows to manage and secure the IT systems.
- Responds to Data Security Incidents.

The data security program is managed by the Director of IT Infrastructure.

Back

Data Security

Every NMH Team Members must follow NMH IT and Data Security policies to ensure the privacy and security of customer's protected health information (PHI) and the confidentiality of business data. You must know and understand the "IT – Computer, Network and Internet Usage Policy." This policy is available in Policy Tech.

lock to learn
each role.

Created by Vishal patel
from Noun Project

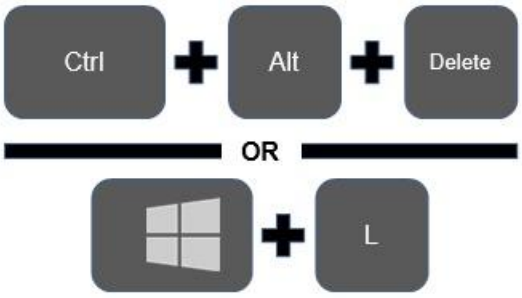
Back

Access to NMH Computer Systems

Your job role will determine the type of access you have to the NMH computer systems.

- All team members need a password to log into the IT systems.
- You must always keep your password private. Do not post or share your password. If you suspect that your password has been used by someone else, change it immediately and contact IT Support Desk at 763-581-2580.

Securing your computer



- If you are using a shared computer, you must always log out when you walk away from the computer. This ensures the privacy of any customer information you were accessing. It also prevents other team members from using the computer under your user account.
- If you have a dedicated work station, you must lock or log out of your computer when you are away from your chair.

You must always secure your computer when you are away from it.

Knowledge Check II

You can save PHI to your local C: drive.

True | False

Knowledge Check II

You can save PHI to your local C: drive.

True | False

Correct!

All NMH data, including any PHI, must be kept on network drives. Never save information to your “local C: drive.”

Next

Knowledge Check III

Data Security policies prohibit using “thumb” or “flash” drives on NMH devices.

True | False

Knowledge Check III

Data Security policies prohibit using “thumb” or “flash” drives on NMH devices.

True | False

Correct!

No PHI or other NMH data may be stored on these devices.

Next

Knowledge Check IV

Contact IT for disposal of equipment (computer, medical device, thumb drive, etc.).

True | False

Knowledge Check IV

Contact IT for disposal of equipment (computer, medical device, thumb drive, etc.).

True | False

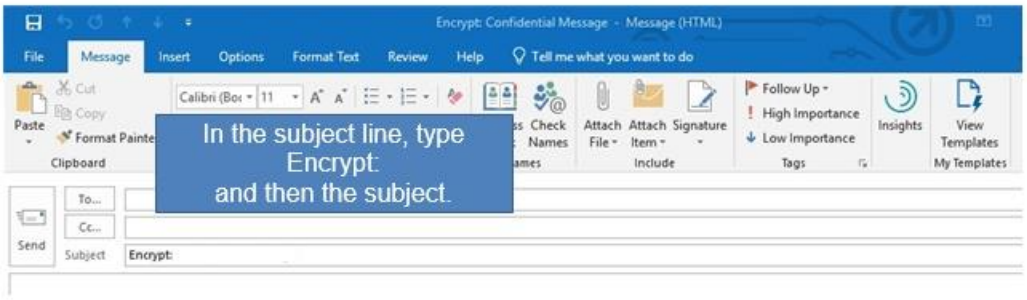
Correct!

This is important because PHI can be retained on equipment, and it must be properly removed before disposal.

Next

Emailing PHI

Ensure you establish minimum but necessary. And encrypt any externally sent email containing PHI or confidential business information.



Phishing Awareness

The scenario at the very beginning of this module is an example of phishing. Data phishing is an attempt to gather sensitive information, such as usernames and passwords, often for malicious reasons, by pretending to be a trustworthy entity.

The most common phishing attempts are email and text message.

Never open emails or attachments if you do not recognize the sender.

NMH Mail from External Sources

CAUTION: This email originated from outside of North Memorial. **DO NOT CLICK** links or open attachments unless you recognize the sender and know the content is safe.
◊ Be sure to look at the email address itself in addition to the sender's name to ensure that it is as expected and not a phishing attempt.
◊ If the email is "pretending" to be from a fellow team member it is likely not valid since it will be coming from an external source.
◊ If the email was not expected or does not look legitimate to you, do not open it or click anything and delete it.
◊ If you have any questions about how to handle a received email, please call the IT Service Desk at X12580 for assistance.

The above banner appears on ANY email originated outside of NMH. When this banner appears, you know it is from outside of NMH.

Only open if you know it's from a safe source and that it is not a spoofed email. Be sure to follow the instructions contained in the caution statement.

Protecting NMH from Malicious Software

Malicious Software (a virus) is often times embedded or disguised to look innocent or non-obtrusive and is a risk to the NMH computer system.

NMH requires that all software be installed by IT. Do not open or "click" on anything that seems suspicious or you do not know what it is. This may be an attempt by a hacker to compromise our computer systems.

If you think something unexpected was installed on your computer, contact IT immediately so that appropriate steps can be taken.

Working From Home

New remote workforce standards have been adopted and deployed to all appropriate NMH depts as per that areas leadership direction. While you are working remotely:

- All policies apply with regards to data security
- Remember to lock your screen if you are away from your computer
- Never copy and paste prohibited content to a personal device or storage device (i.e., USB) or email to your personal email

Click this box to get additional information on how to manage files appropriately in a “cloud/remote” environment efficiently and effectively.

Video Conferencing

Microsoft Teams (MS Teams) is the organizational standard for meeting collaboration. The Zoom app is available upon request, but is primarily used for telehealth needs and providers only.

- In all virtual meetings, any shared info should be minimum but necessary. No PHI should be shared unless approved for an exception from Privacy.

Always Report Concerns

Contact the IT Service Desk when something is not working properly or you notice any suspicious behavior or system malfunctions.

NMH promptly investigates all data security incidents and concerns made by customers, team members, and medical staff members.

Concerns or complaint about data security should be reported to the Data Security Officer.

Created by Xicons.co
from Noun Project

Compliance Contacts

Chief Compliance Officer

Compliance.@northmemorial.com

Privacy Officer

Privacy@northmemorial.com

Data Security Officer

DataSecurity@northmemorial.com

The End

There is no quiz with this module.

CLOSE THIS MODULE.

Compliance Training

Overview of the NMH Compliance Program

The North Memorial Health (NMH) Compliance Program is an organization wide set of activities that:

- Helps team members follow federal and state laws
- Demonstrates NMH's commitment to ethical business practices
- Encourages team members to report compliance concerns
- Facilitates timely response to identified concerns
- Reduces the risk of adverse government/ regulatory actions

Which of the following is a purpose of the NMH Compliance Program?

- ○ To help team members follow federal and state laws.
- ○ To investigate reported compliance concerns and correct any confirmed non-compliance.
- ○ To demonstrate NMH's commitment to ethical business practices.
- ◉ All of the above.

Overview of the NMH Compliance Program

The Compliance Program helps NMH identify compliance concerns and reduce compliance risks.

Compliance Department Staff work with team members to implement changes to correct identified non-compliance and prevent the problem from happening again.

Compliance Program Activities

The compliance program includes:

- Code of Conduct
- Written policies and procedures
- Training and education for team members
- Monitoring and auditing activities that identify areas of non-compliance
- Investigation of reported concerns
- Corrective action plans to correct non-compliance

Reporting Compliance Concerns

- All NMH Team Members are expected to report any known or potential concerns of non-compliance.
- Team members are able to report concerns in several different ways.
- All reported compliance concerns are investigated by the Compliance Department. Investigations are handled confidentially.

How to Report a Compliance Concern

- **You can speak to your supervisor, and your supervisor will report the concern to Compliance.**
- **Email (compliance@northmemorial.com).**
- **Call the Compliance Hotline.**
  - This number is printed on the back of your employee badge!
  - You may leave an anonymous message on the Hotline.

You can may make an anonymous compliance report by calling the compliance hotline, which is printed on the back of your employee badge.

- (●) True
- ( ) False

NMH Prohibits Retaliation

NMH prohibits anyone from retaliating against a team member who asks compliance-related questions or makes a compliance report in goodi faith.

However, if you do not feel comfortable identifying yourself, you may leave an anonymous message on the Compliance Hotline.

Please be aware that anonymous reports do not allow Compliance Staff to gather more details from you to assist with comp'leting a thorough investigation, so you are encouraged to leave contact information when making a report.

Code of Conduct

The NMH Code of Conduct is available on the Comp'liance Department intranet webpage and with our po.licies on C360.

The Code of Conduct is a set of principles that ensure NMH business is conducted in a safe, respectful, and ethical way.

All team members must follow the Code of Conduct when conducting their job duties.

Conflicts of Interest

- A conflict of interest exists when your own personal interests influence or appear to influence your actions while performing NMH duties.
- NMH has a conflict of interest policy that all staff must follow. Any potential conflicts of interest must be reported.
- The next slide explains NMH policies that prevent conflicts of interest.

Conflicts of Interest

Team members must maintain professional relationships with customers. Business relationships may also create conflicts of interests.

Click on the buttons below for tips to avoid conflicts of interests involving customers and violation of NMH policies.

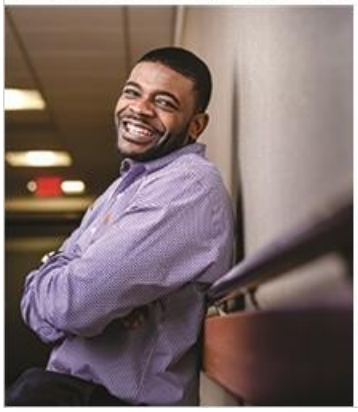
Team Members

Business Relationships

Conflicts of Interest

Go back

Business relationships may create conflicts of interests. To avoid conflicts of interests and violation of NMH policies, remember:



- NMH prohibits team members from accepting gifts or reimbursement from vendors. Please see the Gift policy for more information.
- NMH prohibits team members from conducting personal business when at work, as well as using NMH equipment or property for conducting personal business.
- Medical staff are prohibited from engaging in inappropriate self-referral arrangements.
- No NMH team member may offer gifts or payments of any kind to a physician who refers customers to NMH.

Conflicts of Interest

Go back

Team members must maintain professional relationships with customers. To avoid conflicts of interest involving customers, remember:

- NMH prohibits team members from accepting cash or cash equivalents like gift cards or vouchers from customers. Non-monetary gifts (flowers, candy, cookies, pizza) from a grateful customer may be accepted if the item is reasonable and is shared among team members.
- Team members must not serve as a personal representative for a customer or be named in a customer's will.
- Clinical team members may not provide care to his/her own family members.

NMH prohibits team members from accepting gifts of cash from customers and vendors.

- (●) True
- ( ) False

Policies and Procedures

- All NMH Policies and Procedures are maintained in the Document Management system. Our system is called Compliance 360 or C360.
- All Team Members have access to the Document Management System. It can be accessed through the NMH Portal.
- All new and revised Policies and Procedures must be approved according to NMH policy management process. You can learn more about this process on the NMH Intranet Policies and Procedures webpage.

All team members can access NMH policies and procedures by accessing _____.

- (●) C360
- ( ) Safety First
- ( ) Google
- ( ) Vendormate

Expectations of Compliance

- Compliance is an expectation of your employment.
- Compliance violations are subject to disciplinary action, up to and including termination.
- All disciplinary actions taken for non-compliance are consistent with NMH Human Resources policies.

When in doubt, ask questions and report concerns!

Compliance Contact

Chief Compliance Officer

Compliance@northmemorial.com

Done!

You have completed this module.

CLICK HERE TO CLOSE THIS MODULE.