HIPAA Privacy & Security

Training for External (Non-McLaren) Providers and Others

Your Responsibilities Related to Accessing a McLaren Electronic Medical Record (EMR)

- McLaren Health Care requires that computer/EMR users hold all information/data accessed in the strictest confidence.
- Only authorized persons will have access to written and computer data as needed to provide patient care, or for health care operations purposes.
- As stated in HIPAA regulations, computer users must only access the minimum information needed to carry out their professional responsibilities.
- Viewing/accessing patient information for person use is prohibited.

Responsibilities - continued

- Accessing confidential patient information without a business reason is a violation of the federal HIPAA law and McLaren policies. You are prohibited from:
  - Accessing records of your spouse or your child
  - Accessing records of your neighbor or co-worker
  - Accessing records of a public figure, such as athlete or mayor
  - Accessing records of a high-publicity patient, for example, someone in the news related to a murder case, or motor vehicle accident
- You can be subject to HIPAA penalties/fines and your access may be terminated for accessing patient information without a business reason.

Monitoring for Inappropriate Access

- McLaren uses monitoring software to identify inappropriate access of any McLaren record, including patient or business data.
- You will be held responsible for accessing information without a legitimate business purpose.
  - McLaren will notify law enforcement and/or the federal government when inappropriate access of any McLaren system is identified.

HIPAA – Federal Patient Privacy Law

- HIPAA stands for Health Insurance Portability and Accountability Act
- HIPAA requires us to keep patient information private and secure
- Maintaining patient privacy is a duty of all person with access to McLaren computer systems or EMRs, including McLaren workforce members (employees, physicians, residents, and suppliers/vendors) and our community partners/external providers.

Protected Health Information ("P.H.I")

- HIPAA identifies patient information as "Protected Health Information" or "P.H.I."
  - PHI means any patient information, in any form (such as verbal or written) created or received by a health care provider and is related to a patient's medical condition or payment for services.
    - PHI examples include:
      - Patient name, address, email address
      - Medical record number
      - Health insurance numbers, Social Security Number
      - Patient photographs and images
      - Diagnosis, treatment, prognosis, etc.
      - Images such as x-rays

Electronic PHI (ePHI)

- The HIPAA Law also addresses protected health information that is stored, maintained or transmitted electronically. This is called ePHI, or electronic PHI.
- Examples of ePHI include:
  - Patient notes transmitted via mobile device (phone)
  - X-rays or digital images
  - Emailed lab results
  - E-prescriptions
- The same privacy protections for PHI apply to ePHI.

Authorization Required

- Most uses or disclosures of PHI require a signed authorization from a patient.
- An exception exists for using or sharing a patient's PHI for TPO (treatment, payment or operations). Sharing PHI for TPO does not require a signed authorization from a patient.
  - Examples of TPO = Treatment, Payment, Operations Purposes include:
    - Treatment: i.e., doctors, nurses, lab, etc., for treating the patient
    - Payment: for the purposes of obtaining payment for services
    - Operations: for business operations purposes (for quality monitoring, care management, etc.)

Authorization Required

- A signed authorization from a patient would be required in the below examples:
    - Subpoenas from an attorney requesting medical records be sent for the patient's divorce proceeding
    - Husband wishes to obtain a copy of his wife's medical record (or vice versa)

When Can PHI be Used or Shared Without the Patient's Authorization?

- With the patient or the patient's legal representative, i.e., guardian
- For TPO = Treatment, Payment, Operations Purposes without a patient release/authorization
    - With the treatment team, i.e., doctors, nurses, lab, etc., for treating the patient
    - For the purposes of obtaining payment for services
    - For business operations purposes (for quality monitoring, care management, etc.)
- For other purposes as outlined in the HIPAA Law, for example:
    - To a public health department for communicable disease reporting
    - To the police for wound inflicted by means of violence, such as knife or gunshot wound
    - For reporting of abuse to protective services

Minimum Necessary Standard

- The HIPAA Law requires that health care staff disclose only the *minimum necessary* amount of information required under each situation.
  - NOTE: The minimum necessary standard does NOT apply in treatment situations; for example, a physician and nurse may freely discuss all relevant patient information when treating a patient.

- EMR users are NOT permitted to access PHI of patients they do not have a treatment relationship with. Users should only access what is required.

How to Dispose of PHI

- Always dispose of paper PHI in a shred bin. Never dispose of PHI in regular trash receptacles.
  - Remember – all documents containing PHI should be shredded. This includes all lab reports, correspondence, etc.

- USB drives or CDs containing PHI should also be disposed of properly.

How to Protect PHI in Paper Form

- When faxing PHI, use a fax cover sheet with a confidentiality statement at the bottom. Verify the fax number of the recipient prior to sending.
- Store PHI in locked cabinets
- Pull paper off printers and copiers as soon as possible
- Ensure information in records is covered, for example, in a chart folder, and not left unattended on nursing station counters and other high traffic areas.

Strong Passwords are your First Line of Defense Against Hackers

- How to choose a strong password:
  - At least 8 characters long (the longer the better!)
  - Don’t use common dictionary words
  - Don’t use “Password123” as your password
  - Don’t use consecutive keyboard letters, i.e. qwerty
  - Make it complex. Use at least 3 of the following:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Special characters (@, %, #, ?)
- Never share or post your passwords; store them in a secure location such as a file with password protection

Be on the Lookout for Email Phishing

- Ninety-one (91) percent of successful data breaches or ransomware attacks started with an email phishing attack.
    - Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
    - The phishing email typically contains a message requiring the user's immediate response. When the user clicks on the link or attachment, a virus is launched that encrypts the user's data files.

Email Phishing (Continued)

- Example subject lines in phishing emails:
  - Problem with your bank account
  - A friend has sent you an ecard
  - The attached invoice needs your attention

- When the user clicks on the link or attachment, a virus is launched that encrypts the user's data files

Email Phishing (Continued)

- Red flags of possible phishing emails:
  - Misspellings and poor grammar
  - Website addresses (URL's) that use a variation in spelling or different domain
  - Requests for urgent and immediate action

- What to do if you receive a phishing (or ransomware) email:
  - DO NOT CLICK ON ANY LINKS OR ATTACHMENTS
  - Delete the email from your Inbox and from your Deleted Items folder

- If you become a victim of ransomware:
  - Immediately notify the McLaren IT Service Desk: ITServiceDesk@mclaren.org

Social Media (Facebook, Twitter, etc.).)

- Unless expressly authorized by a patient, posting any type of patient information, pictures or records is strictly prohibited.
  - This is true regardless of whether a patient name is used.

Log Out of your Workstation When you Walk Away or Leave

- If you share your workstation, be sure to log out of the application or system when you walk away from your workstation.
- If you are the only user on your workstation, be sure to lock the workstation when you walk away.
- NOTE that if you leave your workstation and someone else accesses a patient's PHI under your password, *you will be held responsible* for the access.

Mobile Device Security – Removable Media

Users are required to label, account for, and control all removable media containing ePHI.

- Store PHI in a locked cabinet or desk drawer
- If you must transport the removable media, use a secure transport method
- Dispose of removable media in a secure manner, such a by shredding.

Mobile Device Security

The HIPAA Security Rule and McLaren policies require that confidential information be protected from inappropriate use, access, and disclosure.

This includes electronic PHI (ePHI) stored on Removable Media or accessed through Mobile Devices.

Breach of PHI

- A Breach is the improper access, use or sharing of PHI which compromises the privacy or security of the PHI.
  - The determination of whether a HIPAA violation rises to the level of a breach is made by the local Compliance Officer.

- The HIPAA law requires the following when a breach occurs:
  - The patient(s) be notified, and
  - The U.S. Department of Health and Human Services be notified
  - The media will be notified, under some circumstances

Examples of Potential HIPAA violations which may Become Breaches

- A fax containing PHI is sent to the wrong recipient
- A bill is mailed to the wrong patient
- Records are given to the wrong patient at discharge
- An employee accesses a patient's (or co-worker's) PHI without a work-related reason
- A laptop containing PHI was stolen (or is missing)
- You suspect someone is using your login and password

HIPAA Penalties

- There are penalties for violating the HIPAA laws.

- Violations can result in the following:
  - Corrective action, suspension, or discharge from employment
  - Civil monetary penalties up to $1.5 million dollars, depending on the nature and extent of the violation
  - Criminal penalties including fines up to $250,000 and up to ten years in prison

Follow the ‘Need to Know’ Rule

- Ask yourself “Do I need to see/access or share this patient’s information to perform my job?
  - If the answer is no, then STOP. Accessing information other than what is needed is a violation of federal law, even if the information isn’t shared with another person.
  - Accessing a medical record for curiosity is a violation of law for which your access can be terminated. This includes accessing records of co-workers, family members, etc.

Reporting Potential or Suspected Violations

- You have an obligation to immediately report any suspected or known cases of:
  - Inappropriate access, use or disclosure of PHI
  - Password and other security violations
  - Security incidents such as phishing, or ransomware – report to the IT Help Desk
  - Privacy violations and/or breaches - report to the McLaren IT Service Desk:
    - ITServiceDesk@mclaren.org


QUESTIONS