McLaren HEALTH CARE

September 2021

Compliance Newsletter

Annual Mandatory Education starts October 1st

It's Annual Education time again! Alerts for the 2021-2022 MHC Annual Mandatory Education assignments will be emailed to you on 10/1/2021.

- Your email about the assignment will be sent from: HS-Alerts hs-alerts@healthstream.com
- Please check your Outlook INBOX, CLUTTER, and JUNK folders to be sure you receive it.
- The email will be sent to the address you have listed in the HR system, *so if HR communications go to your personal email address, please look there.*
- If you still have issues locating this email, please contact the IT Service Desk for assistance.

Annual training is MANDATORY. Completion is due by November 30, 2021.

- Please note that the Thanksgiving holiday falls on Thursday, November 25th, and Tuesday November 30th is the last day of the month, so please plan to complete the education prior to the holiday if possible.
- **In accordance with policy, HR-0144, employees not completing the annual education assignments by 11/30/2021 will be furloughed until the assignment is completed.**
    - Employees on furlough who do not complete the assignments within 14 business days will be considered to have voluntarily resigned.
- All new McLaren employees/non-employees hired between 4/1/2021 - 9/30/2021, who *completed* the their new hire assignment are not required to complete the 2021-2022 MHC Annual Mandatory Education assignment (same exemption process as last year).
- Drug Diversion Prevention Education is *not* included in the exemption above. Although employees completed the diversion education module earlier this year, it is now required annually and will be included with the annual mandatory education to align with the annual education process.

*If you experience any technical issues while completing the modules, please **report them to the I.T. Service***

Have a Compliance Concern?
Report compliance concerns to your facility Compliance Officer, your facility Compliance Hotline, or to the McLaren Corporate Compliance Hotline at: 866-MHC-COMPly

McLaren
HEALTH CARE

Government Penalizes Organization for Not Terminating Former Worker's System Access

Reference: HHS.gov

The HHS Office for Civil Rights (OCR) continues to enforce HIPAA regulations, hitting hard on organizations that have experienced breaches and assessing costly fines and penalties. The OCR settled 19 HIPAA violation cases last year, with more financial penalties given than in any previous years. **A total of $13,555,000 was paid by organizations to settle the HIPAA violation cases.**

Violation Example: A Connecticut Health Department reported a data breach of 498 individuals' Protected Health Information (PHI). As a result of the breach, the city of New Haven, CT was fined $202,400.

CAUSE OF BREACH: A former employee returned to the Health Department eight days after being terminated and logged into a work computer and found that their user ID and password were still active.

WHAT WAS ACCESSED? PHI that included patient names, addresses, birth dates, race/ethnicity, gender, and sexually transmitted disease test results were copied onto a USB drive.

How does this relate to McLaren?

This breach article reinforces the need for all management staff to ensure that access rights are terminated when employees, contractors, and other users leave the organization.

MHC's User Access Policy (MHC IS2011) highlights on this topic:

- Management is responsible for communicating status changes for employees to Human Resources.
- Managers are responsible for notifying the Access Control Group (ACG) when there is a change in job responsibilities, transfer of positions, or separation from the organization.
- Notification to terminate access must be communicated to the Access Control Group which is required within 24 hours of the change.
- Access change requests may be submitted prior to an employee/user's termination date; the request must specify the employee's expected last day of work.
- Managers should use the IT Service Portal to request such access changes, which is available online to request access changes.
    - Note that some subsidiaries may use a different access change form.

McLaren
HEALTH CARE

Lessons Learned from a McLaren Privacy/Security Breach

Following a HIPAA privacy/security breach identified at a McLaren subsidiary, the below Lessons Learned are being shared with all workforce members to reinforce HIPAA privacy and security rule requirements:

- Never access applications containing patient Protected Health Information (PHI) from a personal mobile device or personal computer without obtaining supervisor approval first (which may include downloading software on your device to protect the MHC data network).
- Do not create 'links' to applications containing patient PHI.
- Never change an application's settings, including 'permission' settings.
- Don't leave PHI open on shared devices when the PHI could be visible to those passing by.
- All shared computers and devices should require separate logins for each user.
- Report any shared devices without unique login requirements to your IT department or contact your subsidiary Compliance Officer.

HELPFUL HINT: How to Quickly Lock Your Computer

Never Leave Your Computer On and Unattended!

Did you know that pressing the Microsoft flag symbol and the L key *at the same time* on your keyboard will lock your computer?

When you log back in, you'll be right where you left off!

McLaren
HEALTH CARE

Refresher about the HIPAA Notice of Privacy Practices for Protected Health Information

The HIPAA Privacy Rule gives individuals a right to be informed of the privacy practices of their health plans and their health care providers. Individuals also have a right to be informed of their privacy rights with respect to their personal health information.

The Privacy Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information (PHI) about the individual, as well as his or her rights and the covered entity's obligations with respect to that information.

Entities are required to provide notice that describes:

1. How the entity may use/disclose PHI.
2. An individual's right with respect to the information and how the individual may exercise their rights.
3. Covered entity's legal duties with respect to the information, including a statement requiring the privacy of PHI.
4. Who individuals may contact for further information about the privacy policies.

Providing the Notice:

1. Notice must be made available to any person who asks for it.
2. Notice must be posted in the facility and on the facilities web site.
3. Health Plans must:
    a. Provide notice to new enrollees at time of enrollment.
    b. Provide revised notice within 60 days of any revision.
    c. Notify individuals on how to obtain the notice once every three years.
4. Providers must:
    a. Provide notice to individuals no later than the 1st date of service and make an effort to receive acknowledgement of receipt. If unable to obtain receipt, provider must document the effort and the reason why it wasn't obtained.
    b. If service is provided electronically, providers must send notice electronically and make an effort to obtain a return receipt or other transmission from the individual.
    c. For emergency treatment, provide the notice as soon as possible after emergency has ended. For these situations, providers aren't required to make an effort to obtain acknowledgement from individuals.
    d. Post the notice in a prominent location at public facilities.

How does this relate to McLaren?

McLaren policy, ***MHC CC1104 Notice of Privacy Practices****, was created to give adequate notice* to individuals regarding the use and/or disclosure of their PHI. MHC & subsidiaries must make the Notice of Privacy Practices available on request to any individual .

McLaren
HEALTH CARE

"Alexa"-type Devices Not Allowed in Patient Care Areas

The Coronavirus Pandemic continues to pose challenges to our healthcare industry. With ongoing visitor restrictions, travel restrictions and the need to protect both the sick and the healthy, devices like iPads and tablets have assisted patient care providers with communication between our patients and their family members. However, those are usually short interactions, so family members are understandably looking for other options to be in contact with our patients.

We have recently had reports that patients/families are bringing monitoring devices, such as an Alexa device, into patients' hospital rooms to allow family members to watch and listen to hospital interactions with their loved one from home.

MHC policies does not allow the use of these devices without the express permission from our facilities, as these devices have the potential to video-record and audio-record, posing a privacy risk to both employees and other patients.

If you encounter such device in a patient's room, please report this to your supervisor and your local Compliance department.

How does this relate to McLaren?

Two MHC policies do not allow use of such personal monitoring devices.

Per policy, MHC_IS2030 Workstation, End Device and Mobile Device Security (section 4.3.3.1.3):

- *Prohibited Uses.* Mobile Devices such as camera phones, cameras or other devices with recording capabilities may not be used on MHC Property unless the device, the application, and the individual operating it, has been authorized under specific circumstances to promote the educational, treatment, research, scientific, public relations or charitable goals of MHC.

Per policy, MHC_CC1115 Patient and/or Audio/Video Recording by Patients, Visitors or Family:

- Any type of audio or video recording is strictly prohibited without consent by the parties involved.

McLaren HEALTH CARE

Reference: https://www.dhs.gov/be-cyber-smart/common-scams

KNOW HOW TO SPOT A FAKE

Phishing Attacks: *Ever click on a link or open an email attachment, even though you're not quite sure who it's from?*

- Cyber criminals have skillfully figured out how to create emails that look like they're coming from legitimate sources, including banks, government agencies, and other services and businesses. Get savvy in recognizing these frauds since often they not only collect your personal and financial information, but also infect your device with malware and viruses.

Imposter Scams: *You know you're a good person when your first instinct is to help when you receive an email or call from a government official, family member, or friend asking you to wire money.*

- You know you're a smart person when you don't immediately fall for it and verify whether the situation is real or not. Criminals have become experts at impersonating those closest to you by exploiting your personal information available online.

"You've Won" Scams: *Winning isn't always what it's cracked up to be.*

- If you receive an email stating you've won a prize, the lottery, or a sweepstakes, be instantly on your guard if you are asked to pay a fee or tax for the prize, or if there's a request for your credit card or bank account information. Here, you can win by not falling for this scam.

Healthcare Scams: *Keep your stress levels low and be wary of calls, emails, or letters that promise big savings in your health insurance.*

- Cyber criminals will usually request your Medicare or health insurance information, social security number, or financial information. Not falling for these scams will give you a skeptical—but healthy—outlook on cyberspace.

Tech support scams: *If it not's broke, don't fix it.*

- If someone claiming to be with a technology company contacts you and wants to diagnose a computer problem you didn't know you had, or provide tech support you have not requested, STOP! If you receive an unexpected pop-up or spam email about an urgent problem with your computer, stop! Scammers are likely using a nonexistent problem to obtain remote access to your computer or banking information.

Identity Theft: *Here are some signs that you may be a victim of identity theft…*

- Bills for products or services you never purchased
- Unauthorized withdrawals from your bank account; or unauthorized charges on your credit card
- Increase or decrease in the amount of mail/bills you receive

Corporate Compliance Leadership

Dan Gillett, OTR/L, MBA, CHC, CPHRM
VP of Compliance
McLaren Health Care
Office: 810-342-1438
Fax: 810-342-1450
Email: dan.gillett@mclaren.org

MHC HOTLINE: 866-MHC-COMPly

April Rudoni, MBA, CHC
Corporate Director of Compliance Audits
McLaren Health Care
Office: 810-342-1215
Fax: 810-342-1450
Email: april.rudoni@mclaren.org

Janet Bigelow, RN, BSN, JD, CHC
Corporate Director of Compliance Programs
McLaren Health Care
Office: 810-342-1433
Fax: 810-342-1450
Email: janet.bigelow@mclaren.org

Regional Compliance Officers

Maureen Decker, MBA, CHC
Regional Director of Compliance
McLaren Macomb
Office: 586-741-4305
Fax: 586-741-4295
McLaren Port Huron
Office: 810-989-3522
Fax: 810-985-2699
Email: maureen.decker@mclaren.org

Kathy Griffin, BSN, MSN, JD, CHC
Regional Director of Compliance
McLaren Flint
McLaren Greater Lansing
McLaren Lapeer Region
Cell: 714-337-3393
Email: kathy.griffin@mclaren.org

Regional Compliance Officers

Sivan Laufer
Regional Director of Compliance
McLaren Bay Region
McLaren Central Michigan
McLaren Northern Michigan
McLaren Thumb Region
Office: (989) 269-9521 x 4701
Fax: (989) 269-3885
McLaren Caro Region
Office: 989-672-5799
Email: sivan.clevesis-laufer@mclaren.org

Hope Scruggs
Regional Director of Compliance
Karmanos Cancer Institute
McLaren Oakland
Office: 248-338-5730
Email: hope.scruggs1@mclaren.org

Compliance Officers

JANET BIGELOW, RN, JD, CHC
Compliance Director
McLaren Healthcare Management Group Office: 810-496-8626
Email: janet.bigelow@mclaren.org

Diab Rizk, J.D., CPC
Compliance Officer
McLaren Health Plan Office: 810-733-9729
Fax: 810-213-0406
Email: diab.rizk@mclaren.org

Compliance Officers

Dawn Smith
Compliance Officer
McLaren Physician Partners/
McLaren ACO
Office: 248-484-4942
Email: dawn.smith@mclaren.org

Michelle Pinter, RN, BSN, JD
Director, Medical Group Compliance
McLaren Medical Group
Office: 810-342-1513
Fax: 810-342-1076
Email: michelle.pinter@mclaren.org

Erin Krehl, MSM
Compliance Manager/Compliance Officer
MDwise
Office: 317-822-7529
Email: ekrehl@mdwise.org

John Goerges, Security Officer
Office: 317-822-7454

Brigid Murphy
Compliance Officer, Hoosier Healthwise Program
MDwise
Office: 317-822-7271
Email: bmurphy@mdwise.org

Compliance Officers

Patricia Ivery
Corporate Research Manager and Compliance Officer
McLaren Health Care
Office: 248-484-4955
Email: patricia.ivery@mclaren.org

Jennifer Menker, MHA
Compliance Officer
McLaren St. Luke's
Office: 419-893-7754
Email: jennifer.menker@stlukeshospital.com

Compliance Support Staff

Vanessa Bauswell, Compliance/Legal Coordinator, MHC
Will Dickinson, BSN, RN-BC, Compliance Program Manager, MNM
Chelsea Hebert, Administrative Assistant, MMG
Kim Hector, Compliance Coding Auditor, MHC
Renee Lafata, Compliance Audit Analyst, MHC & KCC
Heather McAllister, Regional Compliance Program Manager, MBR and MCR
Kimberly Ross, Regional Compliance Specialist, FLT, MGL, MLR
Nancy Smith, HIPAA Coordinator, MHC
Brandi Talicerio, Compliance/Legal Contract Coordinator, MHC