

# Compliance & Regulatory News

## Drug Diversion Awareness & Prevention Education

Protecting our patients and employees is of the highest importance. To increase our employees' awareness about the warning signs of possible drug diversion (inappropriate prescribing, theft, use or sale of prescription drugs), MHC will assign an education module via McLaren University (HealthStream) on April 1st.

- ◆ MHC's Controlled Substance Oversight Committee has created a new MANDATORY McLaren University course that will be assigned to all employees who work at any subsidiaries that have controlled substances for patient care.

### Who Must Complete the Education?

- ◆ ALL employees, at applicable McLaren subsidiaries, must complete this MANDATORY education.
  - ◆ This is a general overview about drug diversion.
  - ◆ It is for every employee, not only those who have access to medications as part of their job duties.

### What is the Due Date to Complete the Education?

- ◆ The module will be assigned through McLaren University (HealthStream) on **4/1/2021**.
- ◆ You have 60 days to complete the assignment.
- ◆ The module must be completed by **5/31/2021** by all employees.

### What Happens if Not Completed by the Due Date?

- ◆ Failure to complete the education by 5/31/2021 will result in unpaid furlough as outlined in policy HR 0144 "McLaren University Education Records, Student Transcripts and Assignment Completion."
  - ◆ Policy Section 4.6 states: *"Employees who fail to complete mandatory assignments per compliance requirements by the due date will be furloughed and subject to corrective action. If the assignment is not complete within fourteen (14) business days of the effective furlough date, the employee will be deemed to have voluntarily resigned."*

### **How does this relate to McLaren?**

***Each facility that is registered with the U.S. Drug Enforcement Agency (DEA) must follow requirements of the Controlled Substance Act. Educating our workforce about the signs and symptom of potential drug diversion or theft helps achieve this goal.***

***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***

# PHISHING TIP CARD

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computer with viruses or malware, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information like account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access their accounts.

## PHISHING EXAMPLES

The following messages, from the Federal Trade Commission's [OnGuardOnline](http://OnGuardOnline), are examples of what attackers may email or text when phishing for sensitive information:

- ◆ "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- ◆ "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- ◆ "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit [www.irs.gov/uac/report-phishing](http://www.irs.gov/uac/report-phishing).

## SIMPLE TIPS

- ◆ **When in doubt, throw it out:** Links in email and online posts are often the way cybercriminals compromise your computer. If it looks suspicious – even if you know the source – it's best to delete or, if appropriate, mark it as "junk email." Contact the company directly (via phone) to be sure the email is not legitimate.
- ◆ **Think before you act:** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- ◆ **Use stronger authentication:** Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account. For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username. Visit [www.lockdownyourlogin.com](http://www.lockdownyourlogin.com) for more information on stronger authentication.
- ◆ **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- ◆ **Install and update anti-virus software:** Make sure all of your computers are equipped with regularly updated antivirus software, firewalls, email filters, and antispyware.
- ◆ **Be wary of hyperlinks:** Avoid clicking on hyperlinks in emails; type the URL directly into the address bar instead. If you choose to click on a link, ensure it is authentic before clicking on it. You can check a hyperlinked word or URL by hovering the cursor over it to reveal the full address.

### **How does this relate to McLaren?**

***Every person accessing email or the internet on a McLaren network and/or device are vulnerable to a phishing attack. Such attacks could disrupt or corrupt important patient or business information stored within our network and software systems.***

# FAIRWARNING

## PATIENT PRIVACY MATTERS

- ◆ Patients' trust in their healthcare providers has a direct impact on the quality of care provided. When this trust is lost, it is impossible to deliver the best care
- ◆ According to national surveys, privacy considerations impact when, where, and from whom patients seek care, as well as what information is disclosed
- ◆ Protecting privacy gives patients the confidence to share their most sensitive information and seek care early, leading to faster and better outcomes
- ◆ Our patients come first  
Our core beliefs include a duty to protect patients' information

### Worried about your privacy?

If you have concerns about other employees viewing your record, please email us at [Privacy@McLaren.org](mailto:Privacy@McLaren.org) or call the hotline at 1-866-MHCCOMPLY to have a special alert set up, so we can help protect your information.

## FAIRWARNING®

A proactive privacy monitoring solution called *FairWarning*® has been implemented at each McLaren subsidiary as they go live with *OneMcLaren Cerner* to help us ensure compliance with healthcare regulations and internal policies. Use of *FairWarning*® will be more widely used as additional subsidiaries begin using *OneMcLaren Cerner*. By proactively protecting our patients' privacy, we are:

- ◆ Building a reputation for privacy, helping us attract and retain patients
- ◆ Giving our patients confidence in their choice of care provider
- ◆ Assuring patients that they can share sensitive information without fear
- ◆ Positioning our organization for long-term success

By working together to build a culture of privacy, we can reduce the following types of activities:

- ◆ VIP snooping
- ◆ Co-worker snooping
- ◆ Neighbor snooping
- ◆ Identity theft
- ◆ Medical identity theft

## Instagram photos in OR prompt investigation at Spectrum Health

According to an article in Becker's Hospital Review, a now-deactivated Instagram account affiliated 35 Spectrum Health residents that contained insensitive comments and photos of physicians posing with surgically removed tissue and organs has brought on an internal investigation at the Grand Rapids, Mich.-based system.

WOOD-TV, the NBC-affiliate for Grand Rapids, aired a segment about the OB-GYN residents' Instagram account March 12, 2021. The Instagram account was disabled earlier that day, minutes after WOOD-TV sent a direct message to it, seeking answers to questions before airing its report.

The account was not officially affiliated with 14-hospital Spectrum Health, although the residents were employees of the system and photos were taken in Spectrum operating rooms.

WOOD-TV described since-deleted posts, including a photo of a physician holding an organ removed in a cancer operation. "The other game we play in the OR is guess that weight," the poster of the organ picture wrote. "It applies to much more than just babies. As always, 'Price is Right' rules apply so if you go over then you're out!"

A Spectrum Health spokesperson shared the following statement with Becker's:

## *Instagram photos in OR prompt investigation at Spectrum Health, cont'd*

"At Spectrum Health, the trust patients place in us and the confidentiality of their medical information are paramount. Equally important are our values and our core behaviors. We strive to treat everyone with compassion, dignity and respect.

"We were shocked and dismayed when we learned that surgical images were posted on an Instagram account not officially connected to Spectrum Health that was used by a group of medical residents. This unacceptable behavior does not in any way reflect our organization, the outstanding professionalism of our medical staff or our resident physicians-in-training."

In the statement, Spectrum said it is taking steps for corrective action and "actively and comprehensively investigating this unfortunate incident...These posts do not follow our code of excellence, our values or our expectations for team member behavior," the statement reads."

***How does this relate to McLaren?*** Per MHC policy, HR 0169—Social Media, workforce members should never include or disclose any patients' protected health information (PHI) on any social media platform, nor engage in social media activities during active work time (which does not include breaks or lunch).

## *Are You Authorized to Access That?*

As a Hospital employee, provider or volunteer, just because you have access to the electronic medical record, census lists and other patient information does not mean you have the freedom or the authority to access or share that information without permission or for a work-related reason. This also means that when YOU are the patient, you must follow the same authorization process as every other patient. Even though all patients have the right to their information, the medical record, whether in paper or electronic format, is the property of McLaren and may only be released according to established policies.

### **How to Obtain Proper Authorization to Access Records:**

Whether you need a copy of your own (or that of your spouse, child, or for someone for whom you are a legal guardian), the ways to request records are the same:

- ◆ Contact your physician office
- ◆ Use your patient portal
- ◆ Contact the Hospital's Health Information Management department to request a Release of Information and complete an authorization to request copies of records.

### **Important Reminders to Protect Yourself from a Policy Violation:**

- ◆ DO NOT use your work computer to access your own medical record or the medical record of a spouse, child, other family member, co-worker, friend or neighbor unless you have a work-related reason to do so.
- ◆ Intentional disregard of this could result in a violation of not only the "Privacy and Security Violation Corrective Action" policy, but also the "Acceptable Use of Technology Resources" policy.
- ◆ Try not to treat your family members who become patients unless due to staffing, you must do so. When you access that record, your name will show if an access audit is conducted, resulting in questioning as to why you accessed that record.

## Are You Authorized to Access That?, cont'd

- ◆ If you have a family member, friend or neighbor (or even a co-worker) who asks you to access their information “as a favor” – *don’t do it!* Inform them that McLaren policy does not allow you to access any patient information without a work-related reason to do so.
- ◆ Access audits such as a “same name audit” are conducted randomly. As more subsidiaries migrate to OneMcLaren Cerner, the scope and frequency of access audits will increase with “FairWarning”, an automatic access auditing tool. (See page 3 for more about FairWarning).
- ◆ If you overhear or witness someone accessing their own record or “snooping” in other records, you are empowered and obligated to report this to your Supervisor, your Compliance Officer and/or the Compliance Hotline.

### **How does this relate to McLaren?**

***Per MHC policy, CC 1101, Use and Disclosure of Protected Health Information (PHI), work-force members should only access PHI needed to perform the assigned job duties. This means accessing only the “minimum necessary” to do your work.***



# 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@mcclaren.org](mailto:dan.gillett@mcclaren.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@mcclaren.org](mailto:april.rudoni@mcclaren.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@mcclaren.org](mailto:maureen.decker@mcclaren.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@mcclaren.org](mailto:kathy.griffin@mcclaren.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@mcclaren.org](mailto:sivan.clevesis-laufer@mcclaren.org)



**Hope Scruggs**  
Regional Director of Compliance  
**Karmanos Cancer Institute**  
**McLaren Oakland**  
Office: 248-338-5730  
Email: [hope.scruggs1@mcclaren.org](mailto:hope.scruggs1@mcclaren.org)

## Compliance Officers



**Dan Gillett, OTR/L, MBA, CHC**  
Interim Compliance Officer  
**McLaren Healthcare Management Group**  
**McLaren Home Care and Hospice**  
Office: 810-496-8626  
Email: [Dan.Gillett@mcclaren.org](mailto:Dan.Gillett@mcclaren.org)



**Margaret (Peggy) Moran**  
Manager, Patient Safety, Compliance  
and Quality  
**McLaren Medical Laboratory**  
Office: (810) 396-5747  
Email: [Margaret.Moran@mcclaren.org](mailto:Margaret.Moran@mcclaren.org)

# Compliance Officers



**Diab Rizk, J.D., CPC**  
Compliance Officer  
**McLaren Health Plan**  
Office: 810-733-9729  
Fax: 810-213-0406  
Email: [diab.rizk@mcclaren.org](mailto:diab.rizk@mcclaren.org)



**Kim Hamm**  
Director, Quality and Compliance  
**McLaren Physician Partners/  
McLaren ACO**  
Office: 248-484-4930  
Email: [Kim.Hamm@mcclaren.org](mailto:Kim.Hamm@mcclaren.org)



**Michelle Pinter, RN, BSN, JD**  
Director, Medical Group Compliance  
**McLaren Medical Group**  
Office: 810-342-1513  
Fax: 810-342-1076  
Email: [michelle.pinter@mcclaren.org](mailto:michelle.pinter@mcclaren.org)



**James Matthews**  
Compliance Manager/Compliance Officer  
**MDwise**  
Office: 317-308-7354  
Email: [jmatthews@mdwise.org](mailto:jmatthews@mdwise.org)  
  
John Goerges, Security Officer  
Office: 317-822-7454



## Compliance Officers



**Bonnie Kegin**  
Compliance Officer, Hoosier Healthwise Program  
**MDwise**  
Office: 317-983-6094  
Email: [bkegin@mdwise.org](mailto:bkegin@mdwise.org)



**Patricia Ivery**  
Corporate Research Manager and Compliance  
Officer  
**McLaren Health Care**  
Office: 248-484-4955  
Email: [patricia.ivery@mcclaren.org](mailto:patricia.ivery@mcclaren.org)



**April Rudoni, MBA, CHC**  
Interim Compliance Officer  
**McLaren St. Luke's**  
Office: 810-342-1215  
Fax: 810-342-1450  
Email: [april.rudoni@mcclaren.org](mailto:april.rudoni@mcclaren.org)

## Compliance Support Staff

**Vanessa Bauswell**, Compliance Coordinator, MHC  
**Will Dickinson, BSN, RN-BC**, Compliance Program Manager, MNM  
**Chelsea Hebert**, Administrative Assistant, MMG  
**Kim Hector**, Regional Compliance Specialist, MGL, FLT, LAP  
**Renee Lafata**, Compliance Audit Analyst, KCC  
**Cindra Linton**, Auditor/Analyst, MHC  
**Heather McAllister**, Regional Compliance Program Manager, MBR and MCR  
**Kimberly Ross**, Compliance Specialist, MMG  
**Nancy Smith**, Compliance Audit Specialist, MHC