

# Compliance & Regulatory News

## Non-Monetary Compensation (NMC) to Providers... And you thought it was just dinner

Reference: "Compliance Today" magazine

As mid calendar year is upon us, now is a good time for compliance departments to review year-to-date non-monetary compensation (aka – *gifts*) totals to ensure the Centers for Medicare & Medicaid Services (CMS) annual limit has not been reached or exceeded by any provider who refers (or may refer) patients to an MHC subsidiary. According to the federal Stark Law, CMS annually sets the NMC (gifts) and medical staff incidental benefits given to referring providers (and their office staff and/or immediate family members). The annual limit is adjusted prior to the start of each calendar year.

Healthcare providers, like MHC subsidiaries, are required to maintain an ongoing provider gifts log that can be monitored throughout the year to ensure that no provider exceeds the annual federal limit.

- **2021's Non-Monetary Compensation (NMC) limit may not exceed an aggregate of \$429 per provider.**
- NMC given to any provider may not consider the number of referrals or other business generated by a referring provider.
- NMC may not be requested by a provider or their practice.
- NMC may not be cash or cash equivalents (i.e. gift cards, checks, etc.)

### What MUST to be Tracked for NMC? \*Common items include:

- Meals at restaurants or those delivered to a provider's office practice intended to influence/increase referrals to our facility (or as thank you for them)
- Golf greens fees (whether one-on-one or at a charity/facility golf tournament)
- Flowers or other gifts
- Paying for a *non-employed* provider's Continuing Medical Education expenses



### What Does NOT Need to be Tracked for NMC?

- CMS allows hospitals to provide "Incidental Medical Staff Benefits" to all credentialed medical staff members (capped at \$37 for calendar year 2021). Incidental benefits include:
  - ◇ Parking & internet provided at an MHC facility where the provider is completing their work
  - ◇ Doctors' Day activities (food, gifts, etc.) available to all medical staff members
  - ◇ Meals provided at Medical Staff Meetings
  - ◇ Meals incident to a written agreement with a provider to discuss issues related to the contracted services with that provider
  - ◇ Providing items in exchange for Fair Market Value price

***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**

## ***Non-Monetary Compensation (NMC) to Providers... And you thought it was just dinner, cont'd***

### **Actions Required by McLaren Leaders:**

If you have given any of the **\*items listed on the last page** to a provider since January 1, 2021, you must report this information and the associated dollar value of such gifts (by provider) to your Subsidiary Compliance Officer. Compliance Officers track this information throughout the year to ensure that no individual provider exceeds their annual NMC limit.

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

*MHC policy "Non-Monetary Compensation Provided to Potential Referral Sources" (CC 0107) "establishes parameters for providing Non-monetary Compensation or business courtesies to potential Referral Sources, their employees and Immediate Family Members, in accordance with the Non-Monetary Compensation Exception of the Physician Self-Referral "Stark" law."*

## ***Don't Get HOOKED by Phishing! How to Report Suspicious Emails***

In our last newsletter, we focused on tips to avoid "getting phished." That is, being *lured* (see what we did there?!) to click on a link or open an attachment that infects a 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, then attackers can use it to access your work (or personal) accounts or McLaren's IT systems.



### **Don't get HOOKED by a phishing email!**

If you receive a questionable email, **look for the following before you click on any links or attachments:**

- **WHO** – Who sent the email? Do I expect an email from the Sender?
- **WHAT** – Is the Subject a topic you're familiar with or were expecting?
- **WHERE** – What email address is this from? It could look odd or be from someone internal to McLaren whose account was compromised.

## *Don't Get HOOKED by Phishing!* *How to Report Suspicious Emails, cont'd.*

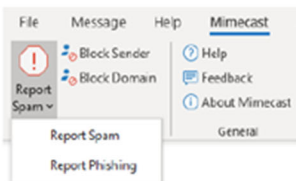
**Below is an example of a phishing email and the items to be cautious of:**



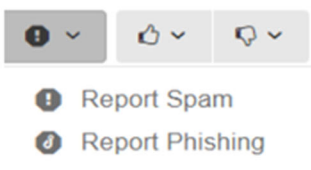
**Depending on the email platform used,  
there are different methods to Report a Phishing Email:**

- 1 **Stop**
  - 2 **Think**
  - 3 **Report**
  - 4 **Delete!**
- A) Send Email to:** [ITservicedesk@mclaren.org](mailto:ITservicedesk@mclaren.org) (This option works regardless of email platform.)

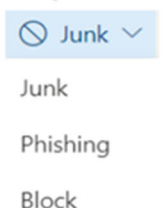
**B) Mimecast for Outlook**



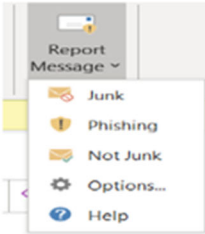
**C) Mimecast Personal Portal**



**E) Microsoft Outlook Web**



**D) Microsoft Outlook App**



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

**EVERY PERSON** who works on McLaren's computers, systems and network must be diligent **EVERY DAY** to review **EVERY EMAIL** to guard against phishing threats.  
**Report any suspicious emails!**

# System Passwords - BE STRONG!

Reference: [www.csoonline.com](http://www.csoonline.com)

Whether at work or at home, we all have system passwords to create. And, most systems have specific minimum requirements for an acceptable password.

According to Information Security experts, there are **three main ways in which passwords can be compromised**:

- 1) **Guessing** (by a human),
- 2) **Cracking** (by algorithmic brute force), and
- 3) **Capturing** (by gaining access to a place a password has been stored, whether that's in a database or on a sticky note).

## Techniques to guard your passwords:

- Avoid passwords containing personal information - they are easier to *Guess*
- Avoid shorter passwords – they are easier to *Crack*.
- Use a sentence and swap out letters for numbers and/or special characters
  - ◊ Alw4y5L4undry2Do% (always laundry to do)
  - ◊ ?Wh4t\$4D1nn3r (what's for dinner)
- Passwords should be created "as a sentence, not a word or words"
  - ◊ Example:
    - \* Password: **0lm@p@lww0**
    - \* Sentence in your mind translate to: **[Zero] I met a puppy as I went walking [Zero]**
    - \* This technique covers password requirements for Upper & lowercase letters; a number, and a special character (@ symbol for the letter "A"), and password length requirement (such as at least 8 characters).

**You have the power to create STRONG PASSWORDS to help keep others from accessing our systems!**



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

*Employees and external users who access McLaren IT systems are required to follow the requirements outlined in the "MHC Acceptable Use and Confidentiality Acknowledgment Form" in which a portion states: "I understand that I am responsible for all activity logged under my password. I understand that I must log off before another user may use the computer."*

## ***CERT Monitoring: One of CMS' Many Payment Programs***

*Reference" "Compliance Today" magazine*

Billing errors can include such things such as unauthorized charges, submitting claims that do not meet medical necessity, improper coding, or charging for services not provided.

To help identify and prevent billing errors that result in improper payments, the Centers for Medicare and Medicaid Services (CMS) developed the Comprehensive Error Rate Testing (CERT) program for the Medicare fee-for-service program.

### **WHAT Does CERT Evaluate?**

- Claims paid when they should have not been, or paid at a different amount
- Both Overpayments and Underpayments are considered "improper payment" errors
- CERT categorizes the most common errors into the following categories:
  - ◊ No documentation
  - ◊ Insufficient supporting documentation
  - ◊ Medical necessity is not established (or not clearly documented)
  - ◊ Incorrect coding



### **HOW does CERT Evaluate Claims?**

1. CMS selects a random sample of claims
2. CMS requests Medical Records from a provider/facility
3. CMS reviewers determine if medical records support the services provided and billed for
4. CMS determine whether the claim was paid properly based on Medicare coverage, coding and billing rules
  - a. Claims that do NOT have sufficient documentation to support the claim payment are counted as a partial or total improper payment.
5. After all errors are identified for a provider/facility, CERT calculates the improper payment rate based on those results.

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

***MHC Standards of Conduct outline our corporate commitment to accurate coding and billing transactions which reflect the patient's diagnosis and services provided. Employees, physicians, and subcontractors are expected to follow applicable laws, policies and procedures to ensure accurate coding, billing, and collection activities to governmental payers, commercial insurances, and patients.  
When in doubt, please contact your Subsidiary Compliance Officer for assistance!***

## DOJ's Health Care Fraud Enforcement Stayed Busy in 2020

Reference: [www.mintz.com](http://www.mintz.com)

The United States Department of Justice's (DOJ) Health Care Fraud (HCF) Unit was busy in 2020, according to a recent DOJ report (click [here](#) to access the full report).

### HCF Unit Purpose:

- Prosecuting complex health care fraud matters and
- Cases involving the illegal prescription, distribution, and diversion of opioid drugs
- Protecting the public from fraud, waste, and abuse of federal healthcare dollars through
  - ◊ Detection, Limitations, and Preventions



### 2020's HCF Unit Focus Areas Included:

#### Telemedicine Fraud:

Since the onset of the COVID-19 pandemic, demand for telemedicine services has surged, and enforcement has followed closely behind.

- HCF's 2020 Takedown, for example, charged 80 defendants involved in telemedicine fraud, resulting in over \$4 billion in false and fraudulent claims.
- Schemes between telemedicine companies and providers to bill for services that were either not medically necessary or did not occur at all.

#### Opioid Drug Enforcement:

Opioid enforcement remains one of the HCF Unit's highest priorities, targeting medical professional involved in unlawful prescribing and distribution of opioids.

- HCF investigated and criminally charges licensed medical professionals typically for alleged conduct far outside the bounds of professional medical care: opioid prescriptions in excessive amounts, dangerous combinations, or in exchange for cash or other services.

### What does 2021 hold for the HCF Unit?

The DOJ's use of data analytics is a key aspect of the HCF Unit's ability to target more complex, higher value fraudulent schemes than in years past. We expect these enforcement trends will continue in 2021.

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

*As providers of care to patients, we are obligated to ensure that we make every effort to submit correct claims for care that is medically necessary, with supporting documentation for the care provided.*

## Introducing MHC Compliance “Lessons Learned”

By Dan Gillett, VP of Compliance



A tremendous benefit of being part of large system like McLaren is the ability to learn from activities occurring at other subsidiaries and working together to standardize processes. The MHC Compliance department is implementing a new standardized approach to communicating “Lessons Learned” from compliance audits which have occurred throughout the McLaren system (particularly CMS, Office for Civil Rights (OCR), Office of Inspector General (OIG) and Payor audits).

By learning from a subsidiary’s experience and results, we can proactively share across the system to allow other subsidiaries to review current processes, make improvements and/or educate providers and staff, as applicable. Local Compliance Officers will collaborate with medical and operational leadership to distribute these lessons learned and implement any applicable monitoring needed. The MHC compliance team will also use the “library” of Lessons Learned to identify potential future internal audits and focus areas.

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

*If you receive a “Lessons Learned” communication, please pause to review and incorporate into your practices to ensure McLaren is Doing What’s Best. Thank you for continued compliance efforts!*



## *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**  
Office: 810-342-1438  
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)



**Jennifer Menker, MHA**  
Compliance Officer  
**McLaren St. Luke's**  
Office: 419-893-7754  
Email: [jennifer.menker@stlukeshospital.com](mailto: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  
**Cindra Linton**, Auditor/Analyst, MHC  
**Heather McAllister**, Regional Compliance Program Manager, MBR and MCR  
**Kimberly Ross**, Regional Compliance Specialist, MMG and FLT  
**Nancy Smith**, HIPAA Coordinator, MHC  
**Brandi Talicerio**, Compliance/Legal Contract Coordinator, MHC