

Compliance, Risk & Regulatory News

How HIPAA Allows Providers to Share Information During an Emergency

By John Hyden, Compliance Officer, McLaren Greater Lansing

With opioid abuse dramatically increasing in the United States, the Office for Civil Rights (OCR) of the Department of Health & Human Services has issued a bulletin clarifying its position on what health professionals may share with a patient's family or caregiver in emergency or dangerous situations. **The following is directly excerpted from the OCR Bulletin:**

HIPAA regulations allow health professionals to share health information with a patient's loved ones in emergency or dangerous situations – but misunderstandings to the contrary persist and create obstacles to family support that is crucial to the proper care and treatment of people experiencing a crisis situation, such as an opioid overdose. This document explains how health care providers have broad ability to share health information with patients' family members during certain crisis situations without violating HIPAA privacy regulations.

INCAPACITATED PATIENTS

HIPAA allows health care professionals to disclose some health information without a patient's permission under certain circumstances, including:

- ◇ Sharing health information with family and close friends who are involved in the care of the patient if the provider determines that doing so is in the best interests of an incapacitated or unconscious patient **and** the information shared is directly related to the family or friend's involvement in the patient's health care or payment of care.
- ◇ *For example, a provider may use professional judgment to talk to the parents of someone incapacitated by an opioid overdose about the overdose and related medical information, but generally could not share medical information unrelated to the overdose without permission.*

CONTINUED ON PAGE 5

CMS Issues Memo Regarding Texting

The Centers for Medicare and Medicaid Services (CMS) issued a memorandum on December 28, 2017 in an effort to clarify its position as it relates to texting. CMS indicated that the practice of **texting orders** from a provider to a member of the care team is not in compliance with its Conditions of Participation or the Conditions for Coverage. The memo noted that Computerized Provider Order Entry, or CPOE, is the preferred method of order entry by a

provider. Hand written orders are also acceptable. The memo indicates that while CMS recognized that the use of **texting as a means of communicating** with other members of the health care team has become an essential and valuable tool, providers must utilize **secure and encrypted texting systems** and/or platforms to minimize the risks to patient privacy and confidentiality under HIPAA.

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**



News From the Corporate Risk, Safety and Insurance Department

McLaren Health Care Patient Safety & Risk Vision Statement

The MHC vision for Patient Safety & Risk is to maximize the opportunity to achieve best patient outcomes through providing risk-free, evidence-based, high quality and cost effective care. To achieve these purposes, we will:

- Strive to always promote health in a safe, caring and cost-effective manner
- Promote the MHC commitment to and development of organizational high reliability through the collaboration of Patient Safety & Risk, Clinical Excellence, Academic Affairs and Service
- Facilitate a Just Culture promoting individual accountability and eliminating individual blame
- Build a robust culture of safety encouraging near miss identification and error reduction
- Encourage prompt and reliable proactive risk identification through McLaren Safety First (MSF)
- Develop a reliable model for improvement utilizing the plan-do-study-act cycle ensuring efficient and effective response to error
- Facilitate open and honest communication pathways between, and among, leadership, clinicians, employees, visitors, and patients to share knowledge and learnings

Physician leadership is key in promoting a culture of safety by encouraging every team member to STOP—SPEAK UP—REPORT when things do not go as expected.

Please Report the Following Events in MSF IMMEDIATELY Upon Discovery

- Any unexpected event occurring outside of the routine expected practice/process
- Patient Safety issues jeopardizing the quality of care
- Near Misses that potentially jeopardize the quality of care
- Any unanticipated death, paralysis, coma or psychological injury, including loss of limb or major permanent loss of function associated with, but not limited to:
 - ◊ Medication Error
 - ◊ Patient fall
 - ◊ Any elopement or unauthorized departure from the facility or department
 - ◊ Any intra-partum maternal death related to the birth process
 - ◊ Attempted suicide of a patient
 - ◊ Wrong side, site, patient procedure or near miss
 - ◊ Unintentionally retained foreign object
 - ◊ Fire, flame, or unanticipated smoke, heat, or flashes during patient care
 - ◊ Equipment malfunction or failure during patient care
 - ◊ Post-partum blood loss requiring the administration of 4 units, or more, of blood products and/or transfer to higher level of care

Please contact Corporate Risk, Safety & Insurance with questions/concerns

Main Office: 810.342.3650

Sonja Wilcox-Berriel, Executive Vice President Risk, Safety, Insurance & Senior Legal Counsel

Tami Gipson-Goodnough, Corporate Director Clinical Risk & Patient Safety



Meet MMG Compliance Officer Michelle Pinter

Michelle Pinter is the Director of Compliance for the McLaren Medical Group (MMG) and serves as the Compliance Officer and HIPAA Privacy/Security Officer for the Group. MMG is comprised of approximately 200 provider offices with around 450 providers, including physicians, nurse practitioners and physician assistants. MMG offices are located from Port Huron to Portland (near Lansing), and from Sault St. Marie to Macomb County.

Michelle works in the MMG Compliance Department with Kim Ross, Compliance Specialist, and Valarie Shepard, Administrative Assistant. In fiscal year 2017, Michelle investigated more than 110 compliance, privacy and security related incidents.

McLaren has been a part of Michelle's life since the day she was born at McLaren Flint. She worked there as a candy striper in her teens, worked as an x-ray transporter through her high school co-op program, worked as an RN for many years and served as a nursing instructor for Baker College students at McLaren Flint. After she received her law degree from Cooley Law School, and after working for a law firm for several years, she began working for MMG as a Performance Improvement Specialist and Nurse Educator. She also served as HIPAA Privacy Officer. Several years later she became the Manager of the MMG Quality

and Compliance Department and was recently promoted to her current position.

Michelle's favorite vacation destination is Glacier National Park in Montana, which she plans on returning to this year. Michelle shared a picture from her last trip to the Park, standing next to a goat on one of the mountains. She enjoys gardening and made 44 loaves of zucchini bread one summer with fresh zucchini from her garden. She also enjoys playing board, card and video games with her family and traveling.

Michelle can be reached at (810) 342-1513 or by e-mail at Michelle.Pinter@mclaren.org.



Phishing: Don't Take the Bait

By George Goble, Chief Information Security Officer

McLaren continues to be attacked by Phishing emails. While McLaren IT is constantly monitoring and fine-tuning the filters and procedures in place to prevent unsolicited and malicious e-mail messages, no solution is 100% effective. Each of us are the last line of defense in reducing such messages and the potential damage they can cause.

Every employee needs to be diligent and exercise extreme caution when reviewing unsolicited emails from an unknown sender- especially the content or links within an email if we do happen to open them by mistake. If ever in doubt, delete it.

What is Phishing?

One of the most common types of hacking techniques is called phishing. This is the oldest and most reliable tool out there because it works. Phishing is an attack that uses "email or malicious websites to solicit personal information by posing as a trustworthy organization". Attackers tend to take advantage of current events and certain times of the year such as natural disasters, epidemics and health scares, economic concerns, major political elections, and holidays.

CONTINUED ON NEXT PAGE

How do I Identify Phishing?

- ◇ Most of these phishing emails are poorly written and contain poor spelling and grammar.
- ◇ The sender's email address does not match the name that is included in the body of the email.
- ◇ The message asks for personal information
- ◇ The offer seems too good to be true
- ◇ You didn't initiate the action
- ◇ You're asked to send money to cover expenses
- ◇ The message appears to be from a government agency
- ◇ Something just doesn't look right

What to Do.

Here are some tips to reduce your chances of being hooked and reeled in by hackers:

- ◇ Never share personal information (login and pass-

words, social security numbers, payment card information, etc.) over email.

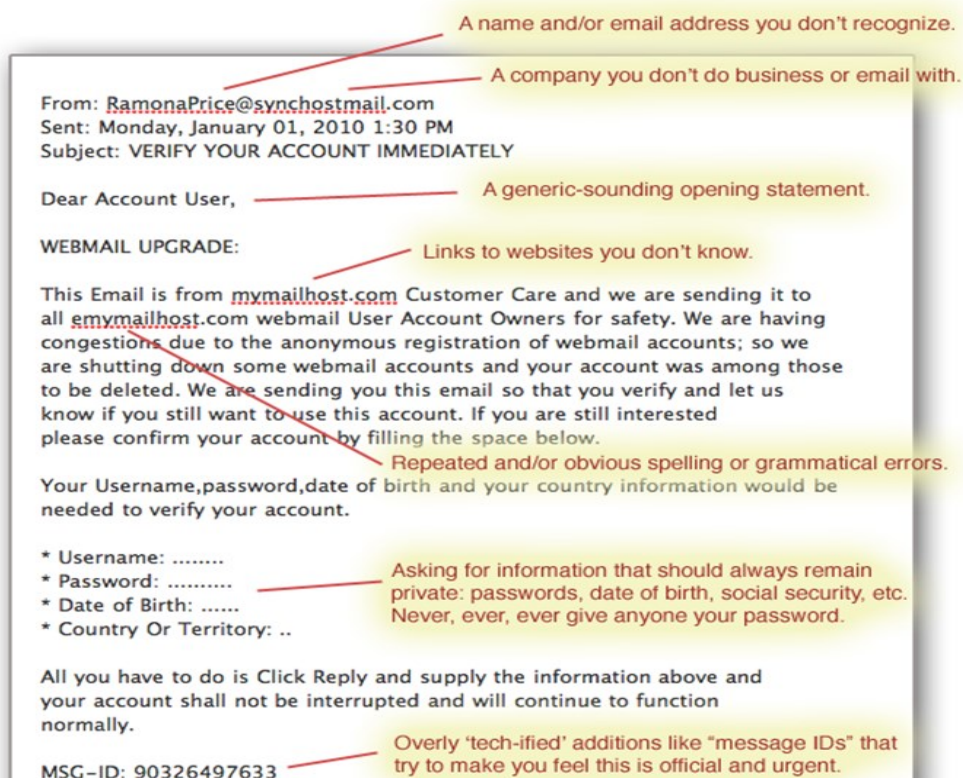
- ◇ Do not download attachments from unknown senders.
- ◇ Always consider context, even for messages from known senders. Does Mike from accounting usually send attachments with no text in the body at 10:30 p.m.?
- ◇ If an executive requests personal information or a money transfer over email, confirm that request in person or via phone.

If you are unsure whether an e-mail is legitimate, or if you believe you have fallen victim to a malicious e-mail, immediately contact the IT Service Desk at 810-424-8400, Toll-Free at 888-622-2036 or via email at ITServiceDesk@mclaren.org.

SPOTTING A PHISHING SCAM/SPAM EMAIL

EXAMPLE #1

A "phishing" email is sent in the hopes that you will divulge back to the scammer details (passwords, personal information, etc.) which they can exploit for their own gain.



From: RamonaPrice@synchostmail.com
Sent: Monday, January 01, 2010 1:30 PM
Subject: VERIFY YOUR ACCOUNT IMMEDIATELY

Dear Account User,

WEBMAIL UPGRADE:

This Email is from mymailhost.com Customer Care and we are sending it to all emymailhost.com webmail User Account Owners for safety. We are having congestions due to the anonymous registration of webmail accounts; so we are shutting down some webmail accounts and your account was among those to be deleted. We are sending you this email so that you verify and let us know if you still want to use this account. If you are still interested please confirm your account by filling the space below.

Your Username,password,date of birth and your country information would be needed to verify your account.

* Username:
 * Password:
 * Date of Birth:
 * Country Or Territory: ..

All you have to do is Click Reply and supply the information above and your account shall not be interrupted and will continue to function normally.

MSG-ID: 90326497633



Information Sharing during an Emergency

(Continued from Page 1)

- ◇ Informing persons in a position to prevent or lessen a serious and imminent threat to a patient's health or safety.

For example, a doctor whose patient has overdosed on opioids is presumed to have complied with HIPAA if the doctor informs family, friends, or caregivers of the opioid abuse after determining, based on the facts and circumstances, that the patient poses a serious and imminent threat to his or her health through continued opioid abuse upon discharge.

CAPACITATED PATIENTS

HIPAA respects individual autonomy by placing certain limitations on sharing health information with family members, friends, and others without the patient's agreement.

- ◇ For patients with decision-making capacity: A health care provider must give a patient the opportunity to agree or object to sharing health information with family, friends, and others involved in the individual's care or payment for care. The provider is not permitted to share health information about patients who currently have the capacity to make their own health care decisions, and object to sharing the information (generally or with respect to specific people), *unless* there is a serious and imminent threat of harm to health as described above.

CHANGE IN PATIENT CAPACITY DURING TREATMENT

HIPAA anticipates that a patient's decision making capacity may change during the course of treatment.

- ◇ Decision-making incapacity may be temporary and situational, and does not have to rise to the level where another decision maker has been or will be appointed by law. If a patient regains the capacity to make health care decisions, the provider must offer the patient the opportunity to agree or object before any additional sharing of health information.

For example, a patient who arrives at an emergency room severely intoxicated or unconscious will be unable to meaningfully agree or object to information-sharing upon admission but may have sufficient capacity several hours later. Nurses and doctors may decide whether sharing information is in the patient's best interest, and how much and what type of health information is appropriate to share with the patient's family or close personal friends, while the patient is incapacitated so long as the information shared is related to the person's involvement with the patient's health care or payment for such care. If a patient's capacity returns and the patient objects to future information sharing, the provider may still share information to prevent or lessen a serious and imminent threat to health or safety as described above.

PERSONAL REPRESENTATIVES

HIPAA recognizes patient's personal representatives according to state law.

- ◇ Generally, HIPAA provides a patient's personal representative the right to request and obtain any information about the patient that the patient could obtain, including a complete medical record. Personal representatives are persons who have health care decision making authority for the patient under state law. This authority may be established through the parental relationship between the parent or guardian of an un-emancipated minor, or through a written directive, health care power of attorney, appointment of a guardian, a determination of incompetency, or other recognition consistent with state laws to act on behalf of the individual in making health care related decisions.

If at any time questions arise regarding disclosure of PHI for the purposes set forth above, please contact your local Compliance Officer. You may also visit <https://www.hhs.gov/hipaa> for more information.



New Michigan Opioid and Controlled Substance Laws

At the end of 2017, Governor Snyder signed new legislation aimed at controlling the opioid epidemic as part of his Task Force on Prescription Drug and Opioid Abuse. Health care professionals will be required to comply with the new requirements as follows:

- ◇ A prescriber must not prescribe more than a seven day supply of an opioid within a seven day period for the treatment of ‘acute pain’, beginning July 1, 2018.
- ◇ Beginning March 27, 2018, a health professional who treats a patient for an opioid-related overdose must provide information to the patient on substance use disorder prevention or treatment services.
- ◇ Beginning June 1, 2018, before an opioid is prescribed to a patient, the prescriber or another health professional must inform the patient: of the danger of opioid addiction; how to properly dispose of expired or unused opioid; that diversion of a controlled substance is a felony; and of the risks to the fetus of exposure to controlled substances. There is an exception to this requirement for inpatients.
- ◇ Beginning June 1, 2018, before prescribing the first opioid prescription in a single course of treatment for a minor (under 18), the prescriber must discuss certain risks, including the risk of addiction and overdose, with the minor and his or her parents or legal representative, and obtain consent of the parent or legal representative on a Start Talking Consent Form, which must be included in the minor’s medical record. In lieu of parental signature, another ‘authorized adult’ may sign the consent; however, the quantity prescribed must be limited to a 72 hour supply. There are exceptions to this requirement, such as when the treatment is related to a medical emergency or surgery; when treatment is rendered in a hospice; or when obtaining consent would be harmful to the minor’s health or safety.
- ◇ Beginning March 31, 2018, a prescriber cannot prescribe a schedule 2-5 controlled substance unless the prescriber is in a ‘bona fide patient treatment or counseling relationship’ with the patient, which means the prescriber has reviewed the patient’s medical records and completed a full assessment of the patient’s history and condition, including a medical evaluation of the patient either in person or via telehealth, and the prescriber has created and maintained records of the patient’s condition. The prescriber must ask the patient about other controlled substances the patient may be using and must record the response in the medical record. The prescriber must also provide follow up care to monitor the effectiveness of the controlled substance. If the prescriber is unable to provide follow up care, he/she must refer the patient to the patient’s primary care physician (PCP) for follow up care, or, if the patient does not have a PCP, the prescriber must refer to another licensed prescriber who is geographically accessible to the patient for follow up care. *Note: There is legislation currently pending which would delay implementation of the bona fide prescriber requirements until March 31, 2019.*
- ◇ Beginning June 1, 2018, before prescribing or dispensing a controlled substance to a patient in a quantity more than a 3-day supply, the prescriber is required to obtain and review a Michigan Automated Prescription System (MAPS) Report on the patient. There are exceptions to this rule if the controlled substance is dispensed to a patient in a hospital or freestanding surgical outpatient facility.

For questions regarding these new laws, please contact your local Compliance Officer.

Compliance Officers



Denise Dach, MBA, RHIA, CHC
Vice President of Compliance
Compliance/Privacy/Security Officer
McLaren Health Care
Office: 810-342-1438
Fax: 810-342-1929
Email: Denise.Dach@mclaren.org

MHC HOTLINE: 866-MHC-COMPLY



Heather Elandt, CHC
Compliance Manager
Compliance/Privacy/Security Officer
McLaren Oakland
Office: 248-338-5697
Fax: 248-338-5667
Email: Heather.Elandt@mclaren.org

HOTLINE: 877-299-3713



Heather McAllister, RHIA, CHC
Director Regulatory Compliance
Compliance/Privacy/Security Officer
McLaren Bay Region
Office: 989-894-3849
Fax: 989-891-0464
Email: heather.mcallister@mclaren.org

HOTLINE: 989-894-3945



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

HOTLINE: 810-342-1044



John Hyden, Esq.
Compliance, Legal Risk and Safety
Officer
McLaren Greater Lansing
Office: 517-975-8954
Fax: 517-975-7610
Email: John.Hyden@mclaren.org

HOTLINE: 517-975-8333



**Janet Bigelow, RN, BSN, JD,
CPHRM**
Compliance Officer (Interim)
McLaren Flint
Office: 810-342-2097
Fax: 810-342-2945
Email: janet.bigelow@mclaren.org

Nancy Smith – Privacy/Security Officer
Office: 810-342-3570

HOTLINE: 810-342-2256

Compliance Officers



Stephen Gerwolds, CHC
Director of Financial Assurance and Compliance
Compliance/Privacy/Security
McLaren Lapeer Region
Office: 810-667-5952
Fax: 810-667-5989
Email: Stephen.Gerwolds@mclaren.org

HOTLINE: 810-667-5787



Maureen Decker, MBA, CHC
Director, Financial Assurance & Compliance
Compliance/Privacy/Security Officer
McLaren Macomb
Office: 586-741-4305
Fax: 586-741-4295
Email: maureen.decker@mclaren.org

HOTLINE: 1-586-741-4300



Sue Bayer
Compliance Officer
McLaren Health Plan
Office: 810-733-9584
Fax: 810-733-5788
Email: Sue.Bayer@mclaren.org

Carol Solomon – Security Officer
Office: 810-733-9705

HOTLINE: 866-866-2135



Dan Gillett, MBA, OTR/L
Director, Integration
Compliance Officer
McLaren Healthcare Management Group
Office: 810-496-8626
Email: Dan.Gillett@mclaren.org

HOTLINE: 810-424-8200, #, ext. 91031



Joyce Schafer
Director, Risk Management & Compliance
Compliance/Privacy/Security Officer
McLaren Central Michigan
Office: 989-772-6896
Fax: 989-772-6842
Email: joyce.schafer@mclaren.org

HOTLINE: 989-772-6816



Kathy Beyer
Director, Quality and Compliance
Compliance/Privacy/Security Officer
McLaren Northern Michigan
Office: 231-487-3069
Fax: 231-487-3139
Email: kbeyer@northernhealth.org

HOTLINE: 888-616-1015

Compliance Officers



Renee Lafata
Compliance Officer
Karmanos Cancer Center
Office: 313-576-8898
Fax: 313-576-9648
Email: rlafata@karmanos.org

HOTLINE: 877-857-6007



Janet Bigelow, RN, BSN, JD, CPHRM
Corporate Compliance Program Manager
McLaren Health Care
Office: 810-342-1430
Fax: 810-342-1450
Email: janet.bigelow@mclaren.org



Maureen Decker, MBA, CHC
Compliance Officer (Interim)
McLaren Port Huron
Office: 810-989-3522
Fax: 810-985-2699
Email: maureen.decker@mclaren.org

HOTLINE: 800-968-0916



Lana Gevorkyan
Corporate Director
McLaren Health Care
Human Research Protections Program
Office: 810 342-3843
Fax: 810 342-1514
Email: Lana.Gevorkyan@mclaren.org

Pic Coming Soon

Margaret (Peggy) Moran,
Manager, Patient Safety,
Compliance and Quality
McLaren Corporate Lab
Office: (810) 396-5747
Email: Margaret.Moran@mclaren.org



Kim Hamm
Director, Quality and Compliance
McLaren Physician Partners/McLaren ACO
Office: 248-484-4930
Email: Kim.Hamm@mclaren.org



Compliance Officers

Pic Coming Soon

LouAnn Detmer, RN, BA
Director, Clinical Records, Business
Services and Referral Center, Quality
& Education, Risk Management
McLaren Homecare and Hospice
Office: (800) 342-7711 x3154
Email: ldetmer@vitalcare.org