Reporting: Drug Diversion & Criminal Acts

What's the Risk?

While there are rules and regulations that govern patient confidentiality, there are also regulations and laws governing the reporting of criminal acts by patients, such as theft. Practitioners who encounter criminal behavior in the practice are faced with navigating between a professional duty to protect patient confidentiality and what may be necessary to report criminal acts.

Confidentiality is a significant part of the foundation upon which the practitioner-patient relationship is built. Any breach of confidentiality may shake and in some cases destroy that foundation. For that reason, any intentional breaching of confidentiality must be done carefully, purposefully and with good cause. The decision of how much information to share with a third party must be based upon federal, state and local laws.

Confidentiality dilemmas sometimes include criminal behavior of patients. A practitioner may be called upon to breach the confidentiality of their patients' protected health information (PHI). For information on when it is appropriate to disclose PHI to law enforcement, see the chapter titled ***HIPAA Privacy***.

In some instances, such as medical identity theft (MIT), breaching confidentiality may not be an issue because the patient may not be the perpetrator, but rather the victim of a crime. Breaching confidentiality also may not be an issue when the perpetrator is a healthcare practitioner and/or employee who works in the practice; for example, drug diversion. Reporting though remains an issue as various organizations need to be aware of the crime.

When Is This Risk an Issue?

This chapter provides an overview of three types of criminal behavior that may occur in the physician practice: drug diversion, MIT and stalking.

Drug Diversion

Drug diversion is "the unauthorized taking or use of any medication, including medication waste" (Coverys, 2013). Drug diversion is one of the most common types of criminal behavior encountered in a physician practice. It is a reportable offense. Some common types of diversion that occur in the physician practice include patients or employees who steal prescription pads or forge prescriptions. Diversion also includes physicians and/or employees who sell prescriptions to drug dealers or abusers and theft of controlled substances maintained by a physician practice.

Updated: February 2016

Drug Diversion vs Drug-Seeking Behavior

On the other hand, drug-seeking behavior raises flags that the patient has the potential to divert medication. It is not a crime; therefore, it is not a reportable offense. Further, practitioners need to be cautious about how drug-seeking behavior is shared with other healthcare professionals. Particularly promising in this respect, according to the Centers for Disease Control and Prevention (2015), are Prescription Drug Monitoring Programs (PDMPs), which are designed to share information between prescribers and pharmacists about a patient's controlled substance prescription history. For more information on PDMPs, see the chapter titled ***Medication: Prescribing Opioids***.

The Drug Enforcement Administration (DEA, 1999) advises physicians to remain alert to drug-seeking behavior and when faced with a patient exhibiting drug-seeking behavior to conduct and document a thorough examination and when prescribing medication, prescribe in limited quantities ("What you should do…" section). For more information on common characteristics of drug-seeking behavior, see the chapter titled Medication: Prescribing Opioids.

Reporting Diversion

According to New (2014), diversion is considered theft and must be reported to several different external agencies, which include the following:

- DEA
- Relevant professional board
- State department of health
- State board of pharmacy
- Local law enforcement (p.9)

State agency reporting requirements vary. For example, some states require practitioners to report any prescription pad theft to local pharmacies, to local law enforcement, and to certain licensing boards. Some states may also require practitioners to report the theft of medications to their particular state public health department.

Reporting a drug diversion incident to the DEA may be accomplished online at https://www.deadiversion.usdoj.gov/rxaor/spring/main?execution=e1s1 , or you may contact an agent directly in one of the DEA's regional offices. Contact information for regional offices is located at http://www.deadiversion.usdoj.gov/Inside.html#contact_us.

Reporting Theft of Controlled Substances

Physician practices that maintain controlled substances are required to report the theft or significant loss of controlled substances to the DEA by completing and submitting DEA Form

106 to the DEA within one business day of discovery. A link to the form as well as instructions for completion can be found at http://www.deadiversion.usdoj.gov/21cfr_reports/theft/index.html.

Medical Identity Theft

According to Ponemon Institute (2015), MIT is a very true and formidable threat to healthcare organizations of all sizes, and the number of MIT victims is on the rise. In 2014, there were approximately 2.32 million MIT victims, a 21.7% increase from the estimated 1.84 million MIT victims in 2013 (p. 8).

Dixon (2006) cites two notable types of MIT:

- When someone uses a person's name and sometimes other parts of his/her identity without the person's knowledge or consent; for example, insurance information.
- When someone uses a person's identity information to make false claims for medical services or goods (p. 5, para. 2).

Harris (2013) states that sometimes healthcare organizations unwittingly increase the risk of identity theft by implementing policies and procedures that require adding unnecessary personal information, such as a driver's license number into the EMR; for example, scanning a government-issued photo ID (p. 6).

In the case of MIT, it may be the patient who alerts the healthcare organization of a possible crime if he/she has discovered a charge for medical services or equipment not obtained. The patient and the healthcare organization may both be involved in reporting the crime. The Department of Health and Human Services (HHS) Office of the Inspector General (OIG) has a helpful consumer brochure available at http://oig.hhs.gov/fraud/medical-id-theft/OIG_Medical_Identity_Theft_Brochure.pdf that identifies when to report and to whom, including the HHS OIG Hotline, Medicare and the Federal Trade Commission.

Stalking

Occasionally a physician contacts Coverys to report a patient stalker. The common thread is that the patient views himself/herself as "special" in the practitioner's life and may bring gifts, send inappropriate letters, or arrange to "run into" the practitioner in the grocery store, at a religious function, or at school events.

Sometimes the physician has unwittingly divulged personal information, such as a home address, and the patient has sent unwanted gifts or letters to the home or even appeared outside the physician's home.

Stalking can be defined as contact (usually two or more times) from someone that makes you feel afraid or harassed.

Examples of stalking include:

- Following or spying on you;
- Sending you unwanted emails or letters;
- Calling you often;
- Showing up at your house, school, or work;
- Leaving you unwanted gifts (Office on Women's Health, 2015, para. 1).

The Stalking Resource Center (2015) points out that the legal definition of stalking varies from one jurisdiction to another. While definitions may vary, there is no doubt that it is a crime in every jurisdiction.

A person who is stalked may experience a number of emotions, including stress, anxiety, depression, confusion, or even isolation because others may not appreciate why the person is afraid (Stalking Resource Center, "Are you being stalked?").

How Can I Reduce Risk?

Report Criminal Acts	
Become familiar with state reporting laws	• Understand that depending on the applicable state law, disclosure of actual or suspected criminal acts committed against the practitioner or practice may be either required or permitted.
Know when to disclose to law enforcement	• Recognize when HIPAA permits disclosure to law enforcement.
Report drug diversion	• Alert authorities and respective agencies (for example, DEA, board of pharmacy, respective professional board) to the theft of medication or prescription pads. • Alert authorities and respective agencies (for example, DEA) to known criminal behavior, for example, the theft and/or selling of controlled substances.
Report MIT	• When a patient is a victim of MIT, alert authorities, respective agencies, and respective insurance companies.

Know When to Disclose Drug-Seeking Behavior

Respect confidentiality	• Recognize that medical information about a patient's chemical dependency or addiction is confidential. Share this information only with covering practitioners, colleagues, or partners who are directly involved in the patient's care. • See the chapter titled ***HIPAA Privacy*** for more information on when disclosure is allowed without the patient's authorization.
Utilize a PDMP	• If a PDMP exists where you practice, use it when prescribing controlled substances. Recognize that PDMP regulations vary greatly by state and that some states require registration and/or training while others do not. For more information on PDMPs, see the chapter titled ***Medication: Prescribing Opioids***.
Know when to breach confidentiality	• Recognize confidentiality may be breached when a criminal act is committed by a patient; for example, theft of a prescription pad or the forging of a practitioner's name on a prescription pad.

Guard Against Medical Identify Theft

Implement safeguards with staff members	• Conduct employee background checks. • Designate a privacy officer who is responsible for developing and implementing privacy policies and procedures. • Assign and monitor IT security access and restrictions. • Monitor staff members' access to patient clinical and financial/business records. • Restrict cellphone use and camera use by staff members (Siders & Amori, 2015).
Implement safeguards with patients	• Require positive identification from patients using at least two pieces of identification, including a photo ID and health insurance card.

Updated: February 2016

Guard Against Medical Identify Theft

- Train employees to check if the photo ID matches the patient.
- Consider including the patient's photo in the EMR as a means to readily identify the patient. Refrain from scanning and using the patient's government-issued ID.
- If there is doubt in non-emergent situations of the patient's identity, validate it by asking the patient which doctor he/she saw last (Harris, 2013, p. 6).
- Consider posting or sharing the Office of Inspector General's (2015) consumer brochure titled Tips to Avoid Medical Identity Theft in your registration area to make patients aware of MIT.
- For more information on guarding against medical identity theft, see ***Insider Medical ID Theft: An Enterprise Nightmare***.

Beware of Stalkers

Maintain professional boundaries

- NEVER share personal information such as a home address with a patient.

Recognize and confront stalking behavior

- Be wary of patients who see themselves as special and give gifts, send inappropriate letters, and/or physically follow you.
- If a patient exhibits stalking behavior, talk to the patient, explain that the relationship is and must remain professional, and discourage the bothersome behavior.
- Report the patient's behavior to the police as stalking if it does not change and/or makes you feel afraid or harassed.
- Contact your personal attorney and/or local authorities if you are unsure what constitutes stalking in your jurisdiction.
- If you feel unsafe, get a restraining order.

Beware of Stalkers

Maintain written information	• When patients send you written letter, file the letter and document your response in the medical record.
Consider terminating the relationship	• If a patient makes you feel afraid or harassed, consider terminating the relationship. Depending on the situation, you may consider immediate termination. For more information on terminating a relationship, see the chapter titled ***Terminating the Provider-Patient Relationship***.
Seek additional information	• For more information on stalking, visit the Stalking Resource Center website at www.victimsofcrime.org/src.
Consider emotional support	• Recognize that you may experience a myriad of emotions if you are stalked. These emotions may impact your ability to provide ongoing care. Take advantage of the emotional support service provided by Coverys. For more information, see the brochure titled ***Emotional Support Program***.

Use Caution If Criminal Behavior Is Uncertain

Consult attorney with questions	• Consider consulting an attorney for guidance and direction if there are questions about either the advisability of intentionally breaching confidentiality or the need to respect and maintain the confidentiality of certain information.

References:

Centers for Disease Control and Prevention. (2015, May 5). *Prescription drug monitoring programs*. Retrieved from http://www.cdc.gov/drugoverdose/pdmp/index.html.

Coverys. (2013, July). Controlled substance access and handling sample policy. Retrieved from https://members.rmpsi.com/MembersOnly/RM_ToolChest_HCF/DrugDiversion/Controlled%20Substance%20Access%20and%20Handling.pdf.

Dixon, P. (2006, May 8). *Medical identity theft: The information crime that can kill you.* The World Privacy Forum, Retrieved from http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf.

Drug Enforcement Administration, Office of Diversion Control. (1999, December). *Don't be scammed by a drug abuser, 1, 1.* Retrieved from http://www.deadiversion.usdoj.gov/pubs/brochures/drugabuser.htm.

Harris, K. (2013, October). *Medical identify theft: Recommendations for the age of electronic medical records.* California Department of Justice. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf.

New, K. (2014, Spring). Identifying drug diversion in the hospital. *Risk Rx.* Coverys. Retrieved from https://members.rmpsi.com/MembersOnly/RM_Newsletters_HCF/2014/RiskRx_HCF_Spring2014.pdf.

Office of Inspector General. (2015, November 25). *Medical identity theft & Medicare fraud.* Retrieved from http://oig.hhs.gov/fraud/medical-id-theft/OIG_Medical_Identity_Theft_Brochure.pdf

Office on Women's Health, U.S. Department of Health and Human Services. (2015, September 30). *Violence against women*. Retrieved from http://www.womenshealth.gov/violence-against-women/types-of-violence/stalking.html.

Ponemon Institute. (2015, February). *Fifth annual study on medical identity theft.* Retrieved from http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

Siders, C. & Amori, G. (2015). *Insider medical ID theft: An enterprise nightmare*. Retrieved from https://members.rmpsi.com/MembersOnly/RM_ToolChest_PHY/ReportingDrugDiversion/InsiderMedicalIDTheft.pdf.

Stalking Resource Center, The National Center for Victims of Crime. *Are you being stalked?* Retrieved from http://www.victimsofcrime.org/docs/src/aybs_english_color.pdf?sfvrsn=4.

Stalking Resource Center, The National Center for Victims of Crime. (2015, January). *Stalking fact sheet.* Retrieved from http://victimsofcrime.org/docs/default-source/src/stalking-fact-sheet-2015_eng.pdf?status=Temp&sfvrsn=0.994206007104367.