Fraud, Waste, and Abuse Program: Medical Identity Theft

(Lead-in music, then standard opening)

Canned: This is a Medicaid program integrity podcast. The Centers for Medicare & Medicaid Services developed and produced these podcasts to keep you informed about Medicaid program integrity topics.

Narrator: Welcome to the "Fraud, Waste and Abuse Program" podcast on Medical Identity Theft. This podcast provides information about Federal guidance for fraud, waste, and abuse programs in a health care setting. Let's join Dr. Williams, the managing partner of a large family practice clinic, and Carolyn, his office manager, as they discuss their practice's plan to prevent identity theft.

(Scene – Dr. Williams' private office:)

Carolyn: Good morning, Dr. Williams. I need to talk to you about our new employee orientation meeting scheduled for tomorrow morning. I see you'll be making the opening remarks and welcoming our new nurse practitioner and the other new employees to our clinic.

Dr. Williams: Yes, I'm looking forward to greeting the new staff. We can certainly use the extra help.

Carolyn: As the clinic's compliance monitor, I'll be presenting our compliance program, and I want to talk about that. In addition to the PowerPoint®, here is a 1-page handout that I've prepared summarizing the key elements of our compliance program.[1] [Hands doctor the paper.] And then after a short break, I'll give them a tutorial on preventing medical identity theft.

Dr. Williams: This handout is a helpful tool. Your plan sounds great. Can you share some of the details on identity theft with me? I guess I've never really thought about it too much.

Carolyn: Well, our primary compliance plan goals are to protect the patients we serve and the integrity of our clinic practice. Medical identity theft can affect providers and patients, so it hits both goals. Medicaid made over $17 billion improper payments in 2014, and some of that was the fraudulent use of patient and provider medical information.[2]

Dr. Williams: That's astonishing. I had no idea it was that much and I've never thought about patients being affected.

Carolyn: Medical identity theft for both patients and providers is a big problem, and I want the new staff to be on alert for it from day one. They need to know the definition of identity theft. It's the "appropriation or misuse of a patient's or [provider]'s unique medical identifying information to obtain or bill public or private payers for fraudulent medical goods or services."[3]

Dr. Williams: That's a mouthful. How're you going to drive the point home?

Carolyn: I'm going to give them real world examples of identity theft, such as the woman who stole prescription pads and Medicaid cards and forged prescriptions for painkillers. She fraudulently billed Medicaid over $200,000.[4] And then there's the guy who stole several physicians' medical identifiers and billed Medicaid for over $4.6 million for prosthetic limbs.[5]

Dr. Williams: Wow! That's a lot of money.

Carolyn: Yes it is. Patient medical identifiers include their Medicaid cards and numbers. I want staff to know how important it is to protect this information. These identifiers may be used to conduct fraudulent billings for services or items not provided, or to enable an ineligible person to receive services by impersonating the beneficiary.

Our compliance plan calls for us to carefully manage patient and enrollment information with payers, monitor billing information with payers, guard medical and personal identifiers, and educate and train our staff. Last, but not least, we need to inform our patients about the risks of medical identity theft.

For example, if we have concerns about a Medicaid patient, we can check with the State Medicaid agency. They have tools to help verify a beneficiary's enrollment and to check if the beneficiary is getting services from another provider or another State or if someone else is using their ID in another State. We should also make sure we don't leave prescription pads or access to patient records or computer systems unsecured.

Dr. Williams: It's good to know the State has resources to help us.

Carolyn: CMS has resources, too, like a 1-page handout on Beneficiary Card Sharing.[6] I'd like staff to start handing it out to our Medicaid patients when they sign our privacy policy. I think it's important for our patients to know that we won't ever share their Medicaid information with anyone outside of the staff who need to know. They should also know how crooks try to get their Medicaid information.

Dr. Williams: It's certainly important information.

Carolyn: Equally important is protecting the medical identifiers for our providers here. Provider medical identifiers include their National Provider Identifiers, Tax Identification Numbers, U.S. Drug Enforcement Administration numbers, and State medical license numbers. If stolen or misused, these identifiers may be used to fill fraudulent prescriptions, refer patients for unnecessary additional services or supplies, or bill for services that were never provided. Some of these numbers are available publicly, so their misuse can be more difficult to guard against—but we need to do what we can.

Dr. Williams: Absolutely. I guess I should consider myself lucky I haven't had to deal with any identity theft issues.

Carolyn: Agreed. There are things providers can do to protect against identity theft like never signing blank authorizations or prescription forms for someone else to complete, and our providers should manage their information whenever it changes, like work or home address, name change for marriage, and banking information. They should also double check all record documentation for the services they're signing off on, making sure they are medically necessary and are appropriately authorized.

I'm planning on giving each new employee a booklet on identity theft that I downloaded from the CMS web site.[7] This will give them additional information on preventing identity theft and help reinforce the importance we place on our clinic's compliance program.

Dr. Williams: I like what you've done! This should certainly help get these new employees off to a good start.

Carolyn: Thank you. This is just a first step in our ongoing compliance staff education and training to prevent fraud, waste, and abuse in our clinic.

Any questions or concerns about my plan for the meeting tomorrow?

Dr. Williams: Nope. I think protecting medical identity information is an important topic and a good introduction to our clinic's compliance program. I'm looking forward to it.

(Standard closing with music)

Canned: More questions? For additional information about fraud, waste, and abuse, contact your State Medicaid agency, Medicaid contractor, or visit www [dot] cms [dot] gov. Click the "Medicare-Medicaid Coordination" tab, and then click the "Program Integrity: Medicaid Integrity Education" link for available toolkits.

Follow us on Twitter #MedicaidIntegrity

(End music)

Disclaimer

September 2015

References

1 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Physician. Retrieved June 3, 2015, from http://oig.hhs.gov/authorities/docs/physician.pdf

2 U.S. Government Accountability Office. (2015, May). Medicaid: Additional Actions Needed to Help Improve Provider and Beneficiary Fraud Controls. Retrieved June 3, 2015, from http://www.gao.gov/assets/680/670208.pdf

3 Agrawal, S. and Budetti, P. (2012 February 1). Physician Medical Identity Theft. Journal of the American Medical Association, 307(5):459-460. doi:10.1001/jama.2012.78 [subscription site]. Retrieved September 4, 2015, from http://jama.jamanetwork.com/article.aspx?articleid=1104942

4 New York State Attorney General Eric T. Schneiderman. (2012, February 16). As Rx Abuse Rises, A.G. Schneiderman Announces Prison Sentence for Woman Who Forged More Than 250 Painkiller Prescriptions. Retrieved September 4, 2015, from http://www.ag.ny.gov/press-release/rx-abuse-rises-ag-schneiderman-announces-prison-sentence-woman-who-forged-more-250

5 Federal Bureau of Investigation. Oklahoma City Division. (2012, June 13). Tecumseh Man Ordered to Serve 51 Months in Prison and Pay Over $4.6 Million in Restitution for Health Care Fraud in Sales of Prosthetics. Retrieved September 4, 2015, from http://www.fbi.gov/oklahomacity/press-releases/2012/tecumseh-man-ordered-to-serve-51-months-in-prison-and-pay-over-4.6-million-in-restitution-for-health-care-fraud-in-sales-of-prosthetics

6 U.S. Department of Health and Human Services. Centers for Medicare & Medicaid Services. (2014, September). Beneficiary Card Sharing. Retrieved September 4, 2015, from https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Beneficiary-Education-Toolkits/Downloads/ben-cardshare-factsheet-082914.pdf

7 U.S. Department of Health and Human Services. Centers for Medicare & Medicaid Services. (2014, March). Partners in Integrity: Understanding and Preventing Provider Medical Identity Theft. Retrieved September 4, 2015, from https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Provider-Education-Toolkits/Downloads/understand-prevent-provider-idtheft.pdf