Stopping Thieves in Their Tracks: What HIM Professionals can do to Mitigate Medical Identity Theft

Save to myBoK

By Lisa A. Eramo, MA

The clues are subtle but critical: Perhaps you get a bill for urgent care services you never received. Or upon reviewing your medical record through a patient portal, you see a diagnosis of back pain and multiple prescriptions for narcotic pain relievers.

Though not definitive, chances are probable that you've been an unfortunate victim of medical identity theft due to a breach of your healthcare data. In the last two years, nearly 90 percent of HIPAA-covered healthcare entities have had a data breach, according to the Ponemon Institute's "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data," published in May 2016.[1] Forty-five percent of healthcare entities had more than five data breaches during the same time period.

Although not every breach leads to medical identity theft, many of them do. Medical identity fraud has nearly doubled since 2010, according to the Medical Identity Fraud Alliance (MIFA). Thirty-eight percent of covered entities said they've experienced at least one case of medical identity theft that affected patients or customers during the past 24 months, according to the 2016 Ponemon study.

Medical Identity Theft on the Rise

Savvy thieves access information using a variety of unsavory techniques—everything from large-scale criminal hacks to smaller-scale phishing schemes, creating fake websites, or even pretending to pose as vendors or IT professionals. All it takes is one exploited vulnerability and a thief has immediate access to protected health information (PHI), financial data, and more. In some cases, the thieves are the victims' close friends and family members. Sometimes the fraud even occurs with the victim's consent. Despite expanded insurance coverage with the Affordable Care Act, many individuals don't qualify for Medicaid, and others have such a high deductible that they can't afford the payment, says Chris Apgar, CISSP, president and CEO of Apgar and Associates. They steal or willingly share information simply to obtain health coverage, he adds.

This frequently occurs in the emergency room (ER), says Barb Beckett, RHIT, CHPS, system privacy officer at Saint Luke's Health System, a 10-hospital system in the Kansas City, MO area. An identity thief uses someone else's information, and when the victim receives a bill, he or she notifies the organization that they never received those services, she says.

Although registration staff are trained to watch for fraud clues, the chaotic nature of the ER environment sometimes makes it difficult to perform a thorough investigation of one's identity prior to treatment, Beckett says. The Emergency Medical Treatment and Active Labor Act (EMTALA) requires providers to treat patients regardless of their ability to show identification or proof of insurance, says Ann Patterson, senior vice president and program director at MIFA. "Since EMTALA dictates healthcare be provided... emergency departments are more easily exploited than other environments, such as banking or retail," she adds.

However, experts say there isn't just one reason why medical identity theft continues to proliferate. Gaps in the Affordable Care Act and exploitation of EMTALA are only the tip of the iceberg.

First, criminals have moved from banking and retail channels into healthcare because of PHI's inherent value. Second, the influx of electronic health record (EHR) systems since the HITECH Act of 2009 has only increased the volume of this data. Add to this the fact that new scamming techniques and strategies change daily—and sometimes even hourly—and you've got a perfect storm of opportunity for a thief.

Unlike the financial industry, healthcare is also incredibly dynamic, says Pam Dixon, executive director at the World Privacy Forum. "The financial services sector can build a gigantic moat, pull up the drawbridge, and lock down the data. Healthcare isn't like that. So many people access this information," she says.

As an industry, healthcare is incredibly vulnerable. "The bad guys are very opportunistic, and they're looking for low-hanging fruit," says Christine Arevalo, vice president of healthcare fraud solutions at ID Experts. "More and more, the amount of healthcare data makes it such an attractive target. With very little work, thieves can secure large amounts of valuable data."

And medical record information is indeed valuable. At $50 per record, stolen PHI is highly monetized compared to financial records, which are valued at only $1, according to MIFA.

Medical records not only include payment and billing information—posing risk to financial identity theft—but they also include sensitive data such as Social Security numbers (SSNs), date of birth, clinical diagnoses, and more.

How Medical Identity Theft Affects Patients

So what happens once medical and financial information have been compromised? Generally speaking, when this data falls into the wrong hands an identity thief could wreak all kinds of havoc. This could include maximizing medical benefits, obtaining prescription drugs to feed an addiction, using credit information to rack up debt, or even blackmailing someone with the threat of posting confidential health information or test results on social media. In particularly egregious cases, a thief can participate in profit schemes to bill thousands or even millions of dollars for services never rendered.

Contamination of the health record with erroneous information (i.e., incorrect blood type, or drug allergies) is one of the most serious risks because it can pose problems with patient safety, such as misdiagnoses, mistreatment, delayed treatment, or adverse reactions.

How CMS is Addressing the Problem

Medicaid and Medicare beneficiaries are particularly at risk for medical identity theft, Dixon says. Retirees residing in southern California, Arizona, Florida, and other areas that are Medicare and Medicaid processing hubs are among those most vulnerable, she adds. "It can take a while before Medicare and Medicaid can catch on," Dixon says. "In a system so big, if you're a really sophisticated criminal you can hide in those numbers and make a lot of money for a while."

Another reason is the ease with which thieves can access someone's SSN. "The SSN has been directly on the card," Dixon says. "When you have the SSN with the legal name, what else do you need?"

The good news is that the new Medicare Access and CHIP Reauthorization Act (MACRA) includes a provision (Section 501) that requires the Department of Health and Human Services (HHS) to work with the Commissioner of Social Security to establish a cost-effective procedure that ensures SSNs are not displayed, coded, or embedded on the Medicare card.

According to a Centers for Medicare and Medicaid Services (CMS) informational bulletin about the Social Security Number Removal Initiative (SSNRI), the agency will remove SSNs and replace them with a randomly-generated Medicare Beneficiary Identifier (MBI) beginning in 2018, at which time approximately 60 million Medicare beneficiaries will receive new Medicare cards. The new MBI must be used in all interactions with the beneficiary, the provider community, and all external partners.

"This step is being taken to minimize the risk of identity theft for Medicare beneficiaries and reduce opportunities for fraud," CMS wrote in the bulletin.

Dixon says this is a symbolic step that will, at a minimum, make it more difficult for thieves to "scan and scram," meaning to simply photocopy the Medicare card, open a fake healthcare business, use the stolen information to bill for services, collect the money, and then close the business shortly thereafter.

Others are less optimistic about whether the SSNRI will actually reduce medical identity theft. Without two-factor authentication, the MBI also becomes simply another data point to steal, adds Patterson. "This reminds me of when we took credit card numbers off of ATM receipts," Arevalo says. "Did all financial identity theft cease to exist? The answer is no."

Many providers may continue to collect patients' SSNs for credit-related reasons even though they won't need this information to bill Medicare, Apgar says. "My advice is don't collect it unless you absolutely need to," he says.

Joanne McNabb, director of privacy education and policy at the California Department of Justice, agrees. "The Social Security number is collected far too often, and it's also breached far too often. It shouldn't only be removed from the card, but it also shouldn't be relied on as an indexing identifier in databases," she says.

Experts say health information management (HIM) professionals should consider these questions as they operationalize the SSNRI:

- Will the organization continue to collect the SSN?
- If so, where will it be stored, and who will have access? The SSN should not be part of a data stream that flows between providers, nor should it appear on demographic forms.
- Will the organization perform a mass conversion of SSNs to MBIs, or will it be done manually on a case-by-case basis?
- If performing a mass conversion, what process will be in place to address any data integrity issues that occur?

Some organizations aren't waiting until 2018 to address the SSN vulnerability. At Parkridge Medical Center in Chattanooga, TN, HIM leaders worked in collaboration with IT to develop software that identifies employees who e-mail or transmit SSNs. The software analyzes text within the e-mail, flags potential SSNs, and then sends a warning to the individual's manager. Lela McFerrin, RHIA, HIM director and privacy officer, says the hospital hasn't yet had any malicious instances of SSN transfers since it began to use the technology in January.

Why Does Medical Identity Theft Occur?

	Covered Entity	**Business Associate**
Unintentional employee action	48%	20%
Intentional non-malicious employee action	15%	33%
Technical system glitches/authentication failure	1%	1%
Criminal attack	9%	8%
Malicious insider	11%	20%
Third-party snafu	11%	14%
Stolen computing device	3%	2%
Unsure	2%	2%

Source: Ponemon Institute. "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data." May 2016.

Seven Tips to Mitigate Medical Identity Theft

HIM professionals are well-equipped to lead conversations about medical identity theft within their organizations. The California Department of Justice has published a medical identity theft guide that can help HIM lead the effort.[2] AHIMA has also published guidance on limiting the use of the SSN, available at http://library.ahima.org/doc?oid=104465. HIM professionals can also consider the following proactive strategies:

1. **Build awareness.** Medical identity theft is a patient safety and quality-of-care issue, and it should be conveyed as such, says John Rogers, CISSP, manager of professional services at Sage Data Security. "Make it a core mission to protect information as well as the infrastructure that supports its use," he says.
2. **Educate registration staff.** These individuals must be able to quickly recognize clues that could indicate medical identity theft, such as:
    - Forged or altered documents

- Critical information that doesn't match the identity of the individual in the master patient index
- A family member calling a patient by a different name than the one he or she used for registration

  Create a script for registration staff to follow when they suspect fraud. Beckett says registrars at Saint Luke's Health System who suspect identity theft ask individuals to repeat their SSN or re-spell their name because they need to make sure the patient's identity is valid. The next step is to call a manager or security officer, which oftentimes prompts patients into providing their real identity, she adds.

3. **Work with IT to educate staff organization-wide.** Rogers says to focus on the following:

   - **Phishing scams.** Reiterate the importance of hovering over any hyperlinks before actually clicking on them. Does the URL actually match the hyperlink's text description? At Saint Luke's Health System, the IT department launched fake phishing alerts to test employees' ability to resist the temptation to click on false links. Beckett says 58 percent of the 300 to 400 people involved in the initial test clicked on a link. After performing staff education, only eight percent clicked on the link during a subsequent round of testing. Beckett says the IT department has also included a tool in Outlook so employees could flag e-mail providing a phishing alert. "Very few get through, and thousands are caught by IT every day," she says.
   - **Suspicious phone calls.** First, offer to call the individual back. Will he or she provide contact information? If a number is provided, Google it first to determine whether it matches the organization's legitimate number. Don't provide any confidential information when you haven't initiated the conversation.
   - **Password applications.** Emphasize the importance of encrypting or locking passwords using applications such as LastPass or RoboForm.
   - **Patch updates.** Apply all security patches for the operating system and third-party applications, especially for Adobe and Java, which are frequently compromised.

4. **Perform comprehensive pre-employment background screenings.** This includes checking individuals against the Office of Inspector General exclusions database at least monthly, depending on the organization's turnover rate, Apgar says. When individuals move into a management role, it's also a good idea to perform another background check, he adds.
5. **Monitor your business associates (BA).** This is particularly true for those BAs that handle large volumes of data on behalf of the organization as well as those that manipulate that data, Apgar says. Ask these questions:

   - What privacy and security policies and procedures does the BA have in place?
   - Has the BA undergone an external validation of compliance?
   - Does the BA have a process in place to mitigate and/or respond to medical identity theft? If so, what are the details of that process, and how does the BA convey incidences of theft to the organization?

6. **Use technical fraud prevention measures.** This could include technology for anomaly detection and data flagging.
7. **Perform proactive audits.** Seventy-four percent of respondents who participated in the 2016 Ponemon study reported that data breaches were discovered by an audit or assessment.

Apgar says although some larger organizations may be able to afford expensive audit log tools and similar technology that can generate detailed reports, many providers must resort to manual methods. Though time-consuming, manual reviews are better than nothing, he says. When performing these reviews, look for the following:

- One SSN associated with multiple names
- One insurance number associated with multiple names
- Access to PHI that's outside of normal business hours

How HIM Professionals Can Educate Patients About Medical Identity Theft

As patient advocates, HIM professionals can and should educate patients about the importance of protecting their medical identity in the same way in which they protect their financial identity.

Remind patients to review the following information regularly:

- Medical record: Obtain a copy in-person or via the patient portal. Consider advertising the patient portal as a tool to help patients monitor PHI in the same way they would monitor their credit reports. Encourage patients to pay close attention to the documented blood type, pre-existing conditions, and allergies. If any of this data is inaccurate, tell them to notify their provider immediately.
- Explanation of benefits: Tell patients to immediately contact their health insurer to report any incorrect items.
- Billing statements: Encourage patients to look for unfamiliar charges related to medical procedures, medical equipment, or pharmaceuticals that may suggest someone has committed fraud. Tell them to notify their provider immediately.

Create an alert form that patients can fill out when they suspect medical identity theft has occurred. Appoint someone in the HIM department who can investigate these reports and work collaboratively with the patient to rectify the problem.

Also refer patients to consumer tips, like those offered by the California Office of the Attorney General, that can help them mitigate medical identity theft.[3]

Developing an Identity Theft Response Program

Once medical identity theft has occurred, organizations need a way to address it immediately so errors don't continue to proliferate throughout the record. Unfortunately, only 19 percent of the covered entities who've had a case of medical identity theft affecting a patient in the past 24 months say they have a process in place to correct errors in the victim's medical record, according to the 2016 Ponemon study.

At Saint Luke's Health System, Beckett says the following departments or individuals are notified immediately when a case of medical identity theft has been confirmed: the privacy officer, health information management, patient accounting, physicians, lab, and radiology. Someone from HIM reviews the record with assistance from the actual patient, if possible, and creates a new "John or Jane Doe" record into which he or she inserts the thief's data.

McFerrin says Parkridge Medical Center follows a similar procedure and also flags both records indefinitely so all providers are aware that the theft occurred. Offer patients who are victims of identity theft a free copy of their medical record in order to review for errors. This should be the entire record that's available in the system—not a document view of the file, Dixon says.

Also consider offering free credit and/or medical ID monitoring to patients. Fifty-six percent of covered entities say victims of data breaches should be protected, and most believe that credit monitoring or medical identity theft protection should be offered for a minimum of three years, according to the 2016 Ponemon study. However, 64 percent of these organizations don't currently offer any protection services for victims whose information has been breached.

Notes

[1] Ponemon Institute. "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data." May 2016.

[2] The California Department of Justice Office of the Attorney General. "Medical Identity Theft: Recommendations for the Age of Electronic Medical Records." October 2013.

[3] The California Department of Justice Office of the Attorney General. "First Aid for Medical Identity Theft: Tips for Consumers." October 2013.

Lisa Eramo (leramo@hotmail.com) is a freelance writer and editor in Cranston, RI who specializes in healthcare regulatory topics, health information management, and medical coding.

Article citation:
Eramo, Lisa A. "Stopping Thieves in Their Tracks: What HIM Professionals can do to Mitigate Medical Identity Theft" *Journal of AHIMA* 87, no.8 (August 2016): 40-43.

Driving the Power of Knowledge