The heat is on for medical practices to prevent medical identity theft.
The Heat Is On for Medical Practices to Prevent Medical Identity Theft

By Mark Harris

From computers to smartphones, the modern world is increasingly connected in ways earlier generations may have found unimaginable.

The evolving technological landscape has profoundly altered the ways people live, work, and communicate, such as through the convenience of online banking, navigation systems, online education platforms, electronic health records, and the ability to connect with friends and family through email and social media.

But with technological advances also come concerns. In an increasingly interconnected world, safeguarding the privacy and security of individuals, organizations, and industries has become vital. With the gradual adoption of information technology systems in place of paper records, anxieties over the frequency of electronic data breaches and disclosures of sensitive data have also grown.

Since 2005, over 17,000 data breaches in which unauthorized users accessed confidential data have occurred.1 These threats to privacy and security are also significantly affecting the health care system. From late 2009 through the end of 2023, 5,887 large health care data breaches—725 in 2023 alone—were reported in the United States, according to the U.S. Office for Civil Rights. Even more, in 2023, breaches resulted in the unauthorized exposure of 133 million health care records.2

A Hot Topic

When a data breach occurs, individuals...
Medical identity theft is a crime that can cause great harm to its victims. Yet despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes. It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.⁴

While the terms tend to be used interchangeably, differentiating between medical identity theft and medical identity fraud is crucial.

“There is a lot of confusion with these terms,” says Eva Velasquez, president and CEO of the Identity Theft Resource Center (ITRC). This national nonprofit organization assists individuals, businesses, and organizations affected by identity theft. “As the statutes are written, they all refer to medical identity theft. … But there’s a difference between medical identity theft and medical identity fraud. First, theft involves the taking of someone’s credentials. … Medical identity fraud—the actual misuse of that data [to get] medical care, goods or services, prescriptions, durable medical equipment, and so on—is a different activity, and it is one of the less common types of identity fraud.”

When medical identity theft leads to health care fraud, it can prove difficult to remediate because of the way medical records, services, and the industry work, says Velasquez. “With medical identity fraud, it’s very dependent on how your identity was misused and where,” she explains. “There’s no central repository for medical records like there is for something like our credit. If you’re a victim of financial identity theft, you can go to credit reporting agencies, look at your credit report, and see all the areas of misuse. … You can’t do that with medical records. It [depends on the practice and insurance company], so there are a lot more steps involved for people to recover from it. It’s also a lot harder for people to discover.”

A person might discover they are the victim of medical identity theft inadvertently or indirectly and only after some time has passed, cautions Velasquez. “They might discover a prescription is denied, or there’s some discrepancy in their medical record, such as finding they are in [debt] for medical services they didn’t receive,” she remarks. “Or they might see a drop in their credit score or be denied a loan for reasons that don’t make sense.”

And yet it’s uncommon for identity criminals to seek treatment using your health information, notes James E. Lee, ITRC COO and a data protection and technology specialist.

The chance to impersonate people is what makes health information such an attractive target for misuse. Lee cites examples of how a criminal might misrepresent a person’s medical identity. “The criminals may be trying to apply for a cash benefit through a state or federal benefits program, and they need the information from a health provider to be able to apply,” he explains. “Or they want general information so they can go...
Keep Your Cool

Follow these tips to protect both the medical practice’s and your own data:

- Never give telemarketers or strangers financial or medical information over the phone. Scammers can use it to commit insurance or billing fraud, disclose sensitive health conditions for extortion, or sell.
- Be skeptical of urgent requests, which scammers may fake to pressure you into acting fast and giving them information.
- Check a sender’s address in emails you receive, and avoid clicking on suspicious links.

Don’t Get Burned

In recent years, health care information has become especially coveted as a target for theft. Medical records are reportedly among the more valuable types of stolen identity data, selling on dark web internet sites for 4 times more than Social Security numbers and 20 times more than a credit card.

“For the last six years, health care has been the No. 1 industry targeted by identity criminals,” reports Lee. “Medical organizations are targeted more frequently than any other industry because cybersecurity is not as good, and you have a very large supply chain. There are a lot of different organizations that can access the same information. That means there are a lot of opportunities to find a weak link. If you can get into one organization, you get information [about all the] organizations in that supply chain. … In health care, there are so many different players with access to so much information.”

Industry advisers agree that health care providers should not downplay the threat. Medical identity theft poses to the integrity of their operations and its potential impact on patients.

“In addressing the critical issue of medical identity theft, it’s essential for physician practices and medical [practice] managers to first recognize the profound impact such breaches can have not only on their financial stability but also on patient trust and safety,” says Adrienne Palmer Lloyd, MHA, FACHE, a consultant with Medical Group Management Association. “The most crucial aspect to understand is that medical identity theft extends beyond the theft of financial information—it can lead to incorrect entries in patients’ health records and potentially dangerous medical errors.”

Physician practices can address these threats. “To reduce the risk, physician practices should implement robust security measures, including but not limited to two-factor authentication, regular security audits, and encrypted communication channels,” says Lloyd, who is also CEO and founder of Optimize Healthcare, a management consulting group in Chapel Hill, North Carolina. “Furthermore, educating patients about protecting their health information is key. For those who fall victim to identity theft, practices should have a clear, compassionate protocol that includes guiding patients through the steps of reporting the theft to law enforcement and fraud departments of their insurers, as well as correcting their medical records.”

Physician practices should never assume they are too small to be a target of cybersecurity threats. “I think security begins with acknowledging that somebody wants your data,” observes Lee. “Particularly with smaller practices, it’s common for people to think nobody wants their data. They think, ‘We don’t have that much data, and what we do have is either very well protected or not very interesting.’ But none of that is true. Identity criminals can find a way to make money off any amount or type of data. … Frankly, the smaller the organization, the easier for [thieves] to target because they know [smaller practices] don’t usually have the same level of protection or security resources [as] large organizations. So, that’s the first thing: recognize that everybody wants what you have, no matter how big or small [the organization is].”

Whether the concern is for individuals or medical practices, a few preventive practices can go a long way toward minimizing the risk of medical identity theft. For example, in phishing attacks, cybercriminals attempt to trick users—through email, text messages, and other methods—into revealing or providing access to sensitive data (e.g., usernames, passwords, credit card numbers, and bank account information). An email or text link can download hidden malware onto computers that exploit software vulnerabilities to expose confidential personal or financial information.

The advent of artificial intelligence (AI) technology might also increase phishing threats. Using AI technology, computers and machines simulate human intelligence and problem-solving functions.

As a result, phishing threats are becoming more sophisticated, warn experts. “It’s become important that [practice] managers or anybody [with] access to [organizational] systems know to verify [the] information before you act on it,” warns Lee. “Don’t click on email links that you did not request. If it is an unsolicited email, text, or even a phone call, you have to adopt the same process that we use in cybersecurity, and that’s zero trust. If you have not verified that this is the legitimate sender and someone you have an established relationship with, don’t do anything. Phishing attacks are far and away
the No. 1 cause of data [breaches]. That’s how organizations get duped into paying large invoices that were not real or giving people access to systems they shouldn’t have access to.”

**Blaze a Trail**

Ideally, best practices in privacy and security should become second nature for managers and staff, as they continually work to minimize risk.

“By fostering a culture of security and privacy, practices not only protect themselves but also support their patients through potentially devastating experiences,” says Lloyd. “Creating an effective privacy and security culture within a medical office involves more than just implementing policies; it requires fostering an environment where every staff member understands and is committed to the protection of patient information.”

To do so, Lloyd encourages medical practice managers to take a proactive, next-level approach to their security goals. “As a health care leader with a focus on examining and refining processes, I believe it’s crucial to go beyond basic training,” she says. “Medical practice managers should conduct thorough assessments of their current processes to identify any gaps or vulnerabilities that could lead to breaches of privacy and security. By identifying these areas for improvement, practices can develop standard work protocols specifically designed to tighten security measures. Enhanced training programs tailored to address these identified gaps can then be implemented. This approach elevates the overall culture of privacy and security within the office [and] ensures that staff are more effectively prepared to protect patient information against potential threats. It’s about building a proactive—rather than reactive—stance on privacy and security, empowering every team member to contribute to safeguarding patient data.”

**Fan the Flames**

“Ultimately, building a culture of privacy and security is an ongoing process that evolves with the changing landscape of cyber threats. It’s a critical investment in your practice’s and patients’ safety and trust.”

—Adrienne Palmer Lloyd, MHA, FACHE
In turn, staff education and training must be geared to relatable issues and encourage input. “Training should be ongoing, engaging, and practical,” suggests Lloyd. “It’s not enough to have annual training sessions; staff need regular updates on the latest threats and best practices, delivered in a manner that resonates with their daily responsibilities. [Use] real-life examples of breaches and their consequences to underscore the importance of vigilance. Moreover, encourage a culture of openness where staff feel comfortable reporting potential privacy concerns or breaches without fear of retribution. By valuing and acting on staff input, offices can identify vulnerabilities before they are exploited.”

For Shanda McDaniel, CMA (AAMA), an Arkansas-based medical record audit processor for Datavant, a health information technology company, concerns about patient privacy and security are always in mind. As part of her responsibilities, McDaniel regularly handles the release of information requests for patient medical records from providers, insurers, attorneys, and others.

“When I get a records release request in our fulfillment queue, I always make sure that the authorization request is correct and matches what is in the person’s chart,” reports McDaniel. “This includes [checking] their name, date of birth, and signature and validating that the request meets all HIPAA [Health Insurance Portability and Accountability Act of 1996] rules before we release the information.”

“When I look at a request that doesn’t look right … I might get the patient’s phone number and call them to make sure they’re OK with whoever is requesting records on their behalf,” she says. “I can also take the request to my supervisor and ask them to take a second look at it. If, instead, I just went ahead and released the records, it’s possible medical identity theft might occur.”
Medical identity theft

When you validate a request, it doesn’t hurt to dig a little deeper to make sure everything is correct. If it’s an attorney’s request, for example, you have to be careful to ensure they have an authorization.”

“Working remotely, I am also careful to make sure medical record information is always secure on the computer in my home,” she adds. “In this position, we have to be extremely careful about what we’re doing.”

Getting Fired Up

Today, medical identity theft and related privacy and security issues represent a far-reaching societal and health industry challenge that invariably entails multiple levels of response.

“Under HIPAA, there are requirements around what happens and what to do when health records and health information are exposed,” notes Lee. “Frankly, that is keeping medical identity theft from being worse than it already is. But I believe we still need a national standard for cybersecurity that is enforceable and uniform in the protection required for personal information.”

At the state and federal level, Lee notes that initiatives toward stronger cybersecurity requirements and protections for personal information are ongoing. “We’re up to 15 states now that have adopted some form of comprehensive privacy and security law, but it’s still not a minimum standard. At the federal level, President [Joe] Biden has issued a directive around cybersecurity, but it also doesn’t rise to the level of a national law. I think we need a better framework for what organizations need to do to protect data, how they protect it, and what happens when they fail to protect it.”

This concern is understandable. For example, Change Healthcare, a UnitedHealth Group affiliate that provides revenue cycle management and other financial services, was the target of a major ransomware cyberattack in early 2024. The attack caused a massive payment processing shutdown that affected billing, prescription fulfillment, prior authorization requests, and other transactions. The breach also potentially exposed confidential patient information, putting current and former subscribers of UnitedHealth Group at risk for medical identity theft and fraud.

“The recent cyberattack on Change Healthcare is a stark reminder of the vulnerability of the health care sector to cyber threats,” says Lloyd. “This incident underscores a critical challenge facing the U.S. health care system: maintaining the integrity and security of patient data amidst increasing cyber threats. Cyberattacks can disrupt health care operations, delay patient care, and erode the trust between patients and providers. … To safeguard against these threats, it’s imperative that health care organizations not only adopt advanced cybersecurity measures but also actively participate in health care information sharing and analysis centers. These platforms can provide valuable intelligence on emerging threats and best practices for cybersecurity.”

With other experts, Lloyd recognizes the need for a coordinated national and industry-wide response to these ongoing threats: “Protecting the health care system from cyberattacks requires a collaborative effort that spans beyond individual organizations, involving government agencies, cybersecurity experts, and health care stakeholders to foster a resilient and secure health care ecosystem.”

To prevent medical identity theft, patients and the broader public should also be engaged and educated about these security challenges. “As far as public education, I believe everybody has a role to play,” says Velasquez. “[Each] patient should understand that the misuse of their information is a threat and there are ways they can safeguard it. I would encourage individuals seeking medical care or signing up with a new [physician] to ask a few questions when asked to fill out some of the forms. What data do you need? How do you safeguard my data? If the office can’t answer these basic questions, that should give you pause. In 2024, they should know how to answer these questions.”

Patients can empower themselves by reading their health plan’s explanation of benefits and ensuring they understand communications from their medical providers. “For providers, it’s important to make sure you indicate to your patients how you’re going to communicate or interact with them.”

Hot Tips

When a patient experiences medical identity theft, be prepared with these tips:

- Make sure the patient has a copy of the practice’s notice of privacy practices if your practice is covered by HIPAA.
- Advise patients to take advantage of their rights under the HIPAA Privacy Rule, which allows them to get copies of their records maintained by covered health plans and medical providers.
- Inform patients of their rights:
  - To have their medical and billing records amended or corrected
  - To have an accounting of disclosures from their medical providers and health plans
  - To file a complaint if they believe their privacy rights have been violated
- Encourage patients to notify their health plan if they suspect medical identity theft and file a complaint with the Federal Trade Commission.
- Encourage patients to look for signs of other misuse of their personal information.
A Light that Never Goes Out

“Education is very important to prevent medical identity theft. There are always new kinds of cyberattacks and approaches that could compromise your information. … Education is not just something you do on the first day on the job in orientation. The threats are moving targets, so staff education needs to be ongoing.”

—James E. Lee

says Velasquez. “If you never communicate with your patients via text, tell them that. If they get a text purporting to be from their provider, they will automatically know it is not legitimate because that’s not how their provider communicates with them.”

Like Lloyd, Velasquez also recommends that patients use two-factor authentication to access their provider’s online health portals. This security protocol requires a user to provide two forms of identification to access an online account. In turn, health care providers should enable two-factor authentication on their systems and provide patients with instructions on setting up this added layer of security.

Warm Care

Finally, Velasquez advises health care providers to keep in mind the potentially traumatic impact of medical identity theft on individuals. “We need to have more compassion and empathy for the victims of medical identity theft [and] more understanding about what people are going through,” she says.

A ransomware incident in 2023 involving a Pennsylvania health system underscores this point. In this instance, a foreign cybercriminal group was able to encrypt files after data was exfiltrated from the patients’ health records.⁹ The hacked data included sensitive patient information, including images of patients with breast cancer undergoing radiation oncology treatment. The hospital decided to not pay the ransom, so the group posted patients’ images on the internet.

“These were images of mostly women with pre- and post-op breast cancer treatment,” explains Velasquez. “The patients were going through life-and-death medical care, and now they also had all this embarrassment because pre- and post-op photographs of their breasts had been released online.”

Consequently, a class-action lawsuit was filed against the health system on behalf of plaintiffs whose confidential records were exposed. The suit charged the hospital system with violating cybersecurity and privacy requirements under HIPAA, prioritizing financial considerations over the rights of their patients.⁹ While Velasquez does not judge the hospital’s decision to not pay the ransom, she says health care providers should recognize how distressing these experiences can be. Accordingly, she suggests health care providers consider providing trauma-informed staff training on how to best assist and respond to patients who have experienced privacy violations.

As an expression of the larger privacy and security challenges facing the health care system, the ramifications of medical identity theft are certainly far-ranging and disconcerting. From financial harm to the repercussions of privacy violations on organizations and individuals and even the potential impact on the quality and safety of medical care, a cascade of potential consequences can follow when medical identity theft occurs.

In today’s complex health care environment, health care leaders and organizations increasingly recognize the importance of these ongoing challenges. In doing so, the health care sector has begun to address the need for robust and proactive approaches to protect the privacy and security of their health systems and the patients they serve.

References

5. Caminiti S. Why UnitedHealth, Change Healthcare were targeted by ransomware hackers, and more cybercrime will hit patients, doctors. CNBC. March 15, 2024. Accessed June 15, 2024. https://www.cnbc.com/2024/03/15/why-unitedhealth-change-healthcare-were-targets-of-ransomware-hackers.html