Complete Healthcare Compliance Manual
Patient Privacy and Security: Identity Theft

By Connie Barrera,[1] MBA, CISSP, CISA

What Is Identity Theft in Relation to Patient Privacy and Security?

Despite continued efforts to stop them, we break data breach and identity theft records year after year. The Federal Trade Commission 2019 "Consumer Sentinel Network" report identified a surge of identity theft reports for 2019, totaling 20.3% of all reports.[2] This figure accounts for the largest percentage of any other filing category.[3] Sorting through the data and focusing in on data breaches in healthcare, based on a Protenus 2020 breach barometer report, more than 41 million patient records were affected by data breaches in 2019.[4] The causes of breach of privacy and security incidents are 58% hacking, 19% insiders, 10% loss/theft, and 13% unknown.[5]

Whenever a data theft incident occurs within healthcare, it is a goldmine for thieves because of the extensive nature of the data. Healthcare not only houses basic personally identifiable information (e.g., full names, addresses, and dates of birth), but also Social Security numbers and many aspects of financial data. This full and extensive data set is what attracts adversaries around the globe to target healthcare organizations everywhere. While we focus on the HIPAA regulation within healthcare, because of the extensive nature of the data, many other regulations apply, such as the Gramm-Leach-Bliley Act (aimed to safeguard financial data), Federal Trade Commission Red Flag Rules (meant to help prevent identity theft), and even the Payment Card Industry Data Security (PCI/DSS) Standard (developed to safeguard credit card information).

While there are clear distinctions between the scope of a HIPAA privacy officer and HIPAA security officer, the anatomy of identity theft incidents tightly weaves both functions and requires extensive and continued collaboration. A vast number of risks emerging from medical identity theft affect both HIPAA privacy and security. These risks result in substantial hardships for patients, providers, and health plans. More often, breaches of medical health data result in direct healthcare fraud, even if the data are still being used in tandem for traditional financial gain. Healthcare fraud is also dangerous because it may result in erroneous health data becoming part of a victim's medical record and lead to treatment errors or diminished benefits they are actually entitled to. Not only do patients experience negative credit issues, which are very difficult to correct, but they can also experience legal issues whenever prescription drugs are obtained via medial ID theft (many times later sold on the black market).

Compliance professionals not only need to ensure current controls are functioning as expected, but also need to constantly brainstorm ways to identify how new risks affect the current environment. Although it's not possible to monitor every system, folder, and file throughout the digital environment, ensuring auditing and monitoring capabilities provide sufficient visibility to user actions and behavior is more important than ever. Without knowing the normal thresholds, it is almost impossible to quickly identify security and privacy issues when they occur.

Risk Area Governance

Healthcare providers and payers have a legal and moral obligation to protect patient records at all times. Federal, state, and localized policies have evolved over the years to compel organizations to continually monitor and ensure the privacy and security of patient health data. Key legislation include the following.

HIPAA Regulation (Security and Privacy), 45 C.F.R. §§ 164.102–164.534

The relevant sections from a privacy and security perspective include 45 C.F.R. §§ 164.500, 164.501, 164.514 .[6]

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Pub. L. No. 111-5, § 13,001, 123 Stat. 227, at 13,301, Subtitle B – Incentives for the Use of Health Information Technology

HITECH encourages healthcare organizations to implement electronic healthcare record solutions with an intention to improve privacy and security.[7]

Congressional Statute, 42 U.S.C. § 1320d-5 (Covers Civil Violations)

This is the enforcement provision that allows for the application of civil penalties for relevant violations of the HIPAA regulation.[8]

Congressional Statute, 42 U.S.C. § 1320d-6 (Covers Criminal Violations)

This establishes the enforcement provision, which allows for the application of penalties for criminal violations of the HIPAA regulation.[9]

Wire and Mail Fraud Statutes, 18 U.S.C. §§ 1341, 1343

This regulation would apply to situations of mailing fraudulent bills or claims, or, alternatively, the act of a breach via the internet would be an act of wire fraud.[10]

False Claims Act, 31 U.S.C. §§ 3729–3733

This would apply if an external adversary started to submit false claims with stolen information.[11]

Identity Theft Rules, 16 C.F.R. § 681

These rules require organizations to establish and maintain adequate controls and training to prevent identity theft.[12]

State-Based Identity Theft Protection Laws

Every state has legislation regarding identity theft crimes. Certain states have specific provisions for restitution. A few states have even created programs to help victims from continuing identity theft issues, such as Iowa and Ohio.