Chapter 7
Identity Theft in Healthcare

To understand identity theft in healthcare you have to follow the money. And there is a lot of money in healthcare! Growing faster than the overall economy or the rate of inflation, U.S. health care costs are projected to nearly double in the next decade to $4.6 trillion, representing one-fifth of the entire economy by 2020.

Thus far we have examined how data breaches from hacking to phishing to inadvertent disclosure, lead to identity theft. In most cases, lost personal information translates directly into financial losses through fraud and identity theft. The healthcare sector also suffers many data hemorrhages, with a more frightening array of consequences. In some cases, the losses translate into privacy violations and embarrassment. In other cases, criminals exploit the information to commit traditional financial fraud and identity theft. In yet other cases, data losses result in unique crime including medical identity theft.

In this chapter, we consider the threats and vulnerabilities to medical data. We overview the consequences of data hemorrhages, including a look at how criminals exploit medical data—in particular through medical identity theft. We also describe the financial flows and the business models of healthcare criminals.

Data Hemorrhages and Patient Consequences

Data hemorrhages from the healthcare sector are diverse, from lost laptops to exposed servers. Losses include everything from business information and the personally identifiable information (PII) of employees to patient protected health information (PHI). Considering all data losses (Figure 7.1), some are related to business information, like marketing plans or financial documents, and do not involve patient identities. Any loss that identifies a patient results in privacy loss. We focus on these more disturbing releases of individually identifiable information that are pri-

---

vacy violations (including violations of both state privacy laws and federal HIPAA regulation). These losses can also result in more negative patient experiences from fraud and theft to adverse health outcomes.

On one hand, healthcare data can lead to traditional identity theft. This occurs when leaked patient or employee information is used to commit financial fraud. For example, using social security numbers and other identity information to apply for fraudulent loans, take-over bank accounts, or charge purchases to credit cards. We have already covered this crime in detail earlier in the book. In this chapter, we focus on the unique fraud found in healthcare.

**Fraud Models**

Healthcare fraud is often conducted by bad actors within the context of legitimate healthcare organizations. Traditional healthcare fraud models typically involve billing payers (e.g., Medicaid/Medicare or private healthcare insurance) for something more than was provided. Such fraud is referred to as upcoding because it involves exaggerating the severity of the patient’s illness and treatment resulting in larger payments (Figure 7.2). Upcoding is typically invisible to the patient. In a related model, criminals use stolen identities to bill for services never rendered. However, unlike upcoding, this approach requires a more complex ecosystem of identity providers (those who steal identities) and corrupt medical providers. While the corrupt healthcare providers may be purely virtual, providing no real medical services, many have some legitimate business to provide cover for the fraud. In one

![Fig. 7.1 Patient consequences of healthcare data loss.](image)