About Medical Identity Theft and Healthcare Data Breaches – An Overview

March 2010
Nearly 80% of healthcare practitioners who manage personal health information have experienced one or more data breaches involving the loss of patient health information in the last year.³

Introduction

The frequency of medical identity theft is on the rise and medical fraud is estimated to generate financial losses totaling $60 Billion each year.¹

Social security numbers and medical insurance account numbers can easily be stolen as electronic records and paper files move through the healthcare infrastructure. As a result, identity thieves can nefariously use this information to obtain medical treatments, make insurance claims and jeopardize medical benefits of unsuspecting individuals.

Consider for example, a major health insurer who experiences a data breach when a laptop containing personal information, including Social Security numbers, is stolen. As a result, significant medical and financial damages could occur to individuals whose personally identifiable information (PII) and personal health information (PHI) was on that laptop.

These damages may include:

• Receiving the wrong medical treatment
• Finding that health insurance benefits have been exhausted
• Becoming uninsured for both life and health insurance coverage
• Having medical insurance denied because the benefits were used by an imposter

The protection of health records is paramount. A recent Ponemon Institute study, “American’s Opinions about Healthcare Privacy”, sites that over 75% of those surveyed believe that protection of healthcare record privacy is important to very important.

Unfortunately, it has been discovered that 80% of healthcare organizations say they have had one or more data breaches that involve the loss of health information.²

With the recent passing of the Health Information Technology for Economic and Clinical Health (HITECH) Act, companies in the healthcare industry are provided financial incentives to bring healthcare records online. While bringing healthcare data online may contribute to greater quality healthcare in the long term, it also creates opportunities for data thieves, putting customers, clients and employees’ medical data at risk.

As a result, the Act extends the Health Insurance Profitability and Accountability Act’s (HIPAA) rules for privacy and security practices for electronic transmission of medical data. However, it also tightens regulations around enforcement and penalties for not adhering to the data management and breach notification requirements.

Healthcare organizations are now responsible for understanding these new laws and must have infrastructure and safeguards in place to protect medical records and an individual’s PII, and PHI. According to Ponemon Institute research, the average expense incurred for

---

¹ National Healthcare Anti Fraud Association
a company to address a medical data breach is $211 per record. Those companies that do not closely follow the new requirements can incur damages of up to $1.5M.

At every level the enactment of the HITECH Act changes the landscape for how healthcare companies manage and protect data.

**Risks to Individual’s Personal Health Information is Increasing**

As more individual PHI is brought online, the greater the demand is for healthcare organizations to provide necessary protection.

PHI is broadly used across provider networks and the medical ecosystem is vast. Customer access portals (where individuals can access their medical records online) are becoming more commonplace, thereby increasing potential exposure of medical data to savvy identity thieves.

Additionally, increasing numbers of healthcare providers are running on limited budgets and frequently do not invest in the necessary Internet Technology (IT) infrastructure to keep PHI records safe.

**Healthcare Companies at Risk for Data Breaches**

Investing in the infrastructure to keep healthcare records safe is critical in maintaining a healthy business and customer loyalty.

Unfortunately, most companies in the healthcare industry are not making these investments. Over 60% of healthcare industry IT professionals surveyed believe they do not have enough resources to ensure that PHI is kept safe.

Additionally, 70% say that the senior management of their companies does not view privacy and data security as a top priority.

With the necessary safeguards not being implemented, the increased exposure to identity thieves increases. This in turn can put companies at risk for potential data breaches and at risk for loss of business from loyal customers.

Data breaches can result in significantly reduced customer confidence, and therefore will lead to less revenue. As reported in a recent study, 45% of breach victims have less confidence in a business as a result of being victimized by a data breach.

**Legislative Requirements for Healthcare Companies**

Recent legislation has provided the financial motivation to rush bringing medical records online.

How organizations handle the process and develop the required infrastructure is critical to the safety of individual records and to the health of the business.

How an organization handles a breach, should one occur, has significantly changed due to the more stringent notification requirements defined by the HITECH Act. Now more than ever, it is critical that the healthcare industry be aware of the new requirements and standards.

According to the Ponemon Institute up to 94% of healthcare industry companies are not in compliance with the new standards. Companies that do not closely follow the new requirements can incur damages of up to $1.5M.

---


