Chapter 11
Using Biometrics to Secure Patient Health Information

Dennis Backherms
Capella University, USA

ABSTRACT

The crime of identity theft has proven to be one of the most costly crimes in American history. Identity theft has become so prevalent in our society today that many laws have been passed, and new bills introduced, to try and combat these troublesome issues. However, recently, a new trend in identity theft has been occurring, individuals are now experiencing medical identity theft. One way to help protect a patient's medical information is through biometric authentication for records access. The technology of biometrics, while thought a novelty at first, has proven to be both a reliable and efficient method for securing patient health records. Biometric technology helps to provide a multi-tiered approach to medical record access and also helps create an audit trail for discovery of unauthorized medical record access. Implementing biometric technology in patient health record security will help substantially reduce the likelihood that medical identity theft will occur.

INTRODUCTION

Organizations and individuals concern themselves everyday with identity theft. Some businesses today have even developed seemingly simplistic products to help prevent thieves from ever getting an individual's identity for use in fraudulent activity. Stories of identity theft vary from victims who patronize organizations that lose clientele information to children whose parents use their names to procure credit cards and other forms of credit without that child's knowledge. Employer related risks associated with identity theft have also risen in recent years. The reasons for elevated

DOI: 10.4018/978-1-60960-174-4.ch011

employer risks are because more consumer transactions are occurring online and more employees are in custody of sensitive clientele data.

News stories and print media are notifying consumers how an organization's employees are losing laptops or getting laptops stolen with sensitive clientele data almost all the time. The kinds of sensitive clientele data stored on these lost or stolen laptops include social security numbers, driver's license numbers, and bank account numbers, just to name a few. Identity theft is used, primarily, to defraud businesses and individuals out of billions of dollars annually in the United States alone. Identity theft allows criminals to max out credit cards, open bank accounts or various other financially binding accounts, and grants access to retirement accounts or other long term types of financial nest eggs.

Medical identity theft is equally, if not more, devastating to an individual than identity theft alone. Criminals on the edge of a new frontier, many view medical identity theft as the next step in evolution from identity theft. Medical identity theft has exponential potential to defraud businesses and individuals at levels of financial loss unheard of in years past. Unlike identity theft, medical identity theft has the potential to cause more damage to a victim because of the superfluous information garnered from an individual's medical record. Medical identity theft ranges from opportunists, viewing medical information for personal insight, to people wanting medical attention but do not have their own, or sufficient, medical insurance to cover costs.

The following chapter provides a synopsis on the description of identity theft, actual stories of identity theft, and laws created to help prevent identity theft. The chapter will also describe medical identity theft, actual stories of medical identity theft, and laws created to help prevent medical identity theft. Next, the chapter will focus on biometrics in regards to the history of biometrics, the industry in general, trends in the industry, and how biometrics offers a secure method for authentication. The chapter will also explain how integration of biometric technology into the health industry will provide better security and help to prevent medical identity theft. Finally, the chapter will conclude with ideas for future research directions and how trends in biometric technology will help shape future industry focus.

BACKGROUND

Identity Theft

Criminals, for many years, have been innovating their ways to defraud individuals. Reading studies of criminal activity since the beginning of human times will easily describe criminal mind progression. The progression warrants changes in defrauding tactics used by criminals. One reason criminals change tactics is to overcome newer technological challenges; enter the age of information. The dawn of information has provided individuals with opportunities that may have appeared too futuristic just ten years prior. Organizations can store all types of personal data on wallet-sized cards, some cards are small enough to fit on a key chain, for use in many aspects of everyday life. Digitizing an individual's information, credit cards for example, present an even greater opportunity for the criminal to defraud. Today, identity theft costs the American taxpayers billions of dollars every year and cause problems for an estimated 10 million victims annually (Deybach, 2007).

Identity theft happens more than many people realize and can occur in many different ways. Identity theft is described as a crime in which someone wrongfully obtains someone else's personal data to deceive or commit fraud; typically for economic gain. Identity theft causes hundreds of hours of work to resolve just a single incident and also causes workplace productivity losses because of employees taking the time off needed to resolve issues concerning identity theft. The common story people hear involves someone