Chapter 9
The Nationwide Health Information Network:
A Biometric Approach to Prevent Medical Identity Theft

Omotunde Adeyemo
TEKsystems, USA

ABSTRACT

The Nationwide Health Information Network (NHIN) promises many benefits, but may be prone to a new phenomenon in healthcare fraud now rapidly drawing attention and commonly referred to as medical identity theft. As the medical industry continues down the path towards overall infrastructure digitization, it is anticipated that associated electronic records will become more portable hence facilitating efficient exchange. Problem however is, the enhanced transferability may also open a new vista of advantages to fraudsters. To address this risk, the NHIN implementers must implement stringent access control measures. One such solution is using a biometric cryptosystem-based solution. For defense-in-depth, a security strategy suggesting successive layers of controls, the PKI cryptographic scheme is recommended to intrinsically protect medical records when in use, storage or even in the event they are successfully stolen.

INTRODUCTION

In 2004, former US president George Bush, signed an executive order to implement an interoperable Health Information Technology (HIT) framework. The directive, expected to be fulfilled within ten years of the order, birthed the design and continued implementation of the Nationwide Health Information Network (NHIN) (Lafferty, 2007, p.15). NHIN, a "network of networks"

DOI: 10.4018/978-1-60960-174-4.ch009

(Rishel, Riehl and Blanton, 2007, p.7) is planned to interconnect major healthcare establishments designated as Electronic Health Records (EHR). There is however one impending problem with this initiative: it may present new opportunities to cyber criminals perpetrating medical identity theft. The medical industry has experienced a traumatic rise of cases in recent times, of this new trend in healthcare fraud. This chapter discusses the planned healthcare information highway, NHIN and the potential dangers medical identity theft poses to the project. A strong authentication mechanism that leverages cryptography and biometrics is prescribed for the problem.

Medical records are largely characterized by personal health information held at healthcare institutions. The act of stealing or the misuse of an individual's medical record in any manner including illicit submission for claims is a derivative of healthcare fraud (Lafferty, 2007) but now more commonly referred to as medical identity theft.

BACKGROUND

Healthcare fraud continues to be a huge expense for the United States (US) government. According to Hoffman and Podgurski (2007), it has been projected that total health expenditures in the United States (US) will rise to over $4 trillion by 2015, and fraud will account for about 10 percent of that expenditure (p. 12). The statistic accentuates the gravity of the problem and suggests an area government can turn for huge savings.

The problem is observed to be taking an upward trend and it appears economic gains is a leading motivator and attraction for perpetrators. Conn (2006), citing the executive director of the World Privacy Forum (WPF), Pam Dixon, claims medical data is currently being peddled at $50 a record in the black market. To the fraudster, it seems truer now than ever, healthcare is now "where the money is" (Conn, 2006, p.27; Lafferty, 2007, p. 12).

The returns promise to be huge and an enticing incentive for criminals to make larger gains perhaps even easier since more records can potentially be handled in electronic formats given the advent of newer technologies. It is now possible to store relatively larger amounts of data on increasingly smaller and cheaper devices which require very minimal technical expertise.

Central to the problem therefore is, as medical data become more accessible in electronic format across the NHIN, so will it become more portable. This ease of portability, according to Lafferty (2007), is on the one hand, for the good of the initiative, but on the other hand, a risk since it may potentially grant criminals similar ease of access to individuals' records. McGraw, Dempsey, Harris and Goldman (2009) share the same view. They expressed concerns about the privacy issues and potential implications of any single breach of electronically held medical records.

Medical identity theft, as is later shown always involves unauthorized or wrongful access to the victims' personal health records. Those accesses are made either at the point of initial record theft, to falsely obtain medical services, or later when updates are being made to the victim's records by unsuspecting medical officials. While specific laws targeting the crime as a separate issue than the classic financially-driven identity theft are still awaited, other measures must be taken to mitigate the problem. Strong security and privacy strategies with access control measures, rising to the severity of the risk, must be planned. A strong multifactor authentication method is later discussed in later sections as one such compensating control, to address the problem. It is further suggested that all electronic personal records on the NHIN must be encrypted at all times, whether at rest or in transit.

The Nationwide Health Information Network

According to the U.S. Department of Health & Human Services (HHS), in a News Release