Medical Identity Theft in Healthcare

While identity theft is a global issue that garners much media attention, most do not realize that medical identity theft is a serious and growing threat. Many authorities consider medical identity theft one of the fastest growing crimes in America. With the digital age of healthcare upon us, the risks are expected to increase as electronic medical records become more prevalent and the exchange of this data over expanding networks becomes more pervasive. Heightened concern over personal data security and privacy highlight the importance of having secure electronic medical identities.

According to a recent Ponemon Institute study, nearly 1.5 million Americans have been victims of medical identity theft with an estimated total cost of $28.6 billion – or approximately $20,000 per victim.[1] Further evidence of the significance of the medical fraud problem is the allocation of $1.7 billion for fraud detection in the 2011 U.S. Health and Human Services Department budget.[2] In 2009, 68 reported healthcare data breaches in the U.S. put over 11.3 million patient records at risk of exposure.[3] Two notable instances are the Health Net breach and the Virginia Department of Health Professions breach.

- Health Net (a Connecticut-based health insurance plan) reported the loss of a hard drive containing seven years of personal and medical information on about 1.5 million Health Net customers. They reported the lost drive six months after it disappeared.[4]
- Virginia Department of Health Professions was the victim of a $10 million extortion plot to expose over 8 million patient records and 35 million prescriptions.[5]

Patients whose medical identities are stolen face serious lingering effects. Fraudulent healthcare events can leave erroneous data in medical records. This erroneous information – like information about tests, diagnoses and procedures – can greatly affect future healthcare and insurance coverage and costs. Patients are often unaware of medical identity theft until a curious bill or a surprising line of questioning by a doctor exposes the issue. Then, the burden of proof is often with the patient and it can be difficult to get the patient's legitimate medical records cleaned up. The consequences can also be life threatening and can lead to serious medical errors and fatalities.

The American Recovery and Reinvestment Act (ARRA) and the associated provisions under the Health Information Technology for Economic and Clinical Health (HITECH) Act have highlighted the need to address privacy and security across our healthcare system. In fact, HITECH requires that consumers be notified of healthcare data breaches. Alerting patients when their personal health information has been breached is a necessary response, but it is a reactive measure. It does nothing to *prevent* the breach or address the subsequent issues patients face when they are victims of medical identity theft. The healthcare industry also needs policy that takes a proactive approach – one that implements controls and technology that assure patient information is always protected. It needs to make secure electronic medical identities a priority.

As the ARRA provides incentives for more and more doctors to adopt electronic health records (EHRs), and as health information exchanges (HIEs) becomes more commonplace, consumers are even more at risk of medical identity theft from an intentional or unintentional breach of healthcare records, or the “loss” or theft of a laptop. Right now, healthcare records are likely to be on paper, and secured by the physical safeguards and administrative procedures in the doctor’s office. When these records are digitized and accessible via interconnected EHRs and HIEs, the potential for exposure grows exponentially.

A related issue to identity theft, and a significant problem for the healthcare industry, is the problem of mistaken identity, which can be life threatening. Today most HIEs rely on a record locator service (RLS) to find where patients' data are stored. Many use a “probabilistic match,” which depends on various pieces of information such as the patient’s name, address, Social Security number, date of birth and other personal information. These methods are not 100% accurate and can lead to potentially fatal errors. For example, in an emergency situation, a patient who has been incorrectly identified could be given a transfusion of the wrong blood type. Compounding the issue is the fact that patients must provide this personal information each time they visit a provider so that their records can be located. These verbal and paper-based identification processes are ambiguous and error-prone, as well as ripe for fraud and abuse.

Addressing Medical Identity Theft

The way to stop medical identity theft and identity confusion is to improve patient identification and provide enhanced data protection. Strong authentication and data encryption are methods that can achieve these goals.

Industry experts are already calling for this change. The *Medical Identity Final Report* prepared by Booz Allen Hamilton for HHS stated, “Many stakeholders in medical identity theft have noted that patient authentication can be

one of the simplest yet most effective methods in preventing medical identity theft. Patient authentication consists of ensuring that patients receiving services are the individuals they claim to be. Patients are often asked to provide only verbal assertions of identity and coverage. However, technology solutions such as biometrics, smart cards, or electronic patient records may be able to assist providers in verifying patients' identities based on past histories, demographics or facial photographs."[6]

To address medical identity theft, solutions need to provide higher levels of assurance than today's processes, whether the interactions are in person or remote. Identity management is a crucial foundation for healthcare, and solutions that incorporate smart card technology can be used to address the security and privacy challenges facing the industry. This foundation can be put in place without reinventing the wheel. The federal government has already established a set of best practices, standards and technology solutions for smart card-based identity management and authentication that can be adapted to and leveraged by the healthcare industry.

How Strong Authentication and Data Encryption Prevents Medical Identity Theft

Strong authentication of identity is a critical step in addressing medical identity theft. All personal health record (PHR) providers, health record banks, health insurance and hospital Web portals should provide two-factor authentication mechanisms to their end users to help secure access to personal health information. In two-factor authentication schemes, individuals typically use a card, token or mobile device to access their health information or prove identity when obtaining healthcare services. The safest and most secure two-factor methods are based on smart card technology, where a tamper-resistant chip with security software is embedded into the card, token or mobile device (like a mobile phone). This is the same technology that is used in U.S. electronic passports, and in the U.S. federal government's employee ID cards that are used to access the nation's most secure computer networks and facilities. A smart card allows patients to unambiguously identify themselves to their healthcare provider when accessing patient records or requesting healthcare services.

Data encryption also plays an important role in the protection of personal health information (PHI) and is now mandated as part of the breach notification laws. Encrypting PHI protects against access by intruders; smart cards provide a robust set of encryption-enabling capabilities including key generation, secure key storage, hashing and digital signing. Smart cards also add strong authentication capabilities that ensure only authorized users are able to access PHI. These capabilities can be used by a healthcare system to protect privacy in a number of ways. A doctor can use a smart card to digitally sign orders or prescriptions, protecting the information from subsequently being tampered with and providing assurance that the doctor was the originator of the information. The fact that the signing key originated from a smart card adds credibility and a greater legal stature to the record. The smart card provides two major benefits: one, it securely holds and protects the keys; and two, it is portable, so it stays with the doctor and not in the computer where someone else might be able to fraudulently use it. Smart cards can also put patients in control of their private information. Patients can use their smart card to securely store personal health information, authorize provider access to that information, and secure transmission of data to healthcare systems.

Heath care reform in the U.S. is a major undertaking and it will take time to achieve the levels of identity management and data protection that are required by new electronic health record systems. But the size of the task should not prevent the healthcare industry, both private and public, from beginning the journey towards better securing heath information and increasing the efficiency and quality of the nation's healthcare delivery systems. As the industry moves toward the goal of electronic health records for all patients and with all providers, the need for strong identity management becomes more pressing. Issuing proper identity credentials and authenticating identity are solid steps in modernizing the U.S. healthcare system.

Issuing secure patient and provider identity credentials based on smart card technology will help to reduce medical identity theft, and will also bring numerous efficiencies to existing healthcare administration systems. Identity and authentication solutions based on smart card technology will provide an ideal foundation for improving the security and privacy of health information systems and electronic health records.

---

1 Survey conducted by The Ponemon Institute in February 2010

2 "HHS Budget Makes Smart Investments, Protects the Health and Safety of America's Families," Feb 1,2010, http://www.hhs.gov/news/press/2010pres/02/20100201a.html

3 Identity Theft Resource Center 2009 Data Breach Stats, http://www.idtheftcenter.org/ITRC Breach Stats Report 2009.pdf

4 "Health Net Says 1.5M Medical Records Lost in Data Breach," ComputerWorld, November 19, 2009

5 "Hacker says he stole confidential medical data on 8 million Virginia residents," Healthcare IT News, May 6, 2009

6 Booz Allen Hamilton, *Medical Identity Final* Report, prepared for U.S. Department of Health and Human Services, January 15, 2009, Page 16

About the Smart Card Alliance Healthcare Council

The Smart Card Alliance Healthcare Council brings together payers, providers, and technologists to promote the adoption of smart cards in U.S. healthcare organizations. The Healthcare Council provides a forum where all stakeholders can collaborate to educate the market on the how smart cards can be used and to work on issues inhibiting the industry.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.