NextgenID®

Healthcare
Utilizing Trusted Identity Credentials

NextgenID® - Headquarters
10226 San Pedro Ave, Suite 100
San Antonio, TX 78216
(210) 530-9991

NextgenID® - Washington DC
13454 Sunrise Valley Drive, Suite 430
Herndon, VA 20171
(703) 429-8532

Utilizing Trusted Identity Credentials within Healthcare

Failure to collect complete patient information at registration, redundant information entry, language barriers, common names, misspellings or phonetic spellings can all lead to errors and improper patient identification. A recent report sponsored by the U.S. Department of Health and Human Services, “Medical Identity Theft Report,” stated that little is done to authenticate the identity of individuals throughout healthcare and concluded that medical identity theft is a significant problem and that consumers have the most to lose.

An identity and authentication solution based on smart card technology provides the best foundation for improving healthcare information systems in a secure, privacy sensitive way. 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 healthcare.

A smart card is a plastic identity card with a small computer in it. Unlike magnetic stripe or RFID cards, the smart card's computer provides high levels of security and privacy protection, making the technology ideal for complying with HIPAA and preventing fraud. Smart cards can be readily used online and across networks and deliver very high levels of security over the Internet. Smart cards are also very convenient and easy for people to use.

Requiring strong authentication as a fundamental principle of any identity program will ensure those who access medical records are those who are authorized. Strong authentication will further provide a process by which an audit trail can be established.

Such a system would enable:

- Verification of health care professionals
- Verification of patients
- Processes for gaining access to electronic medical records
- Eliminate fraudulent claims

Ten years ago, very few professionals or consumers knew anything about financial identity theft and fraud; today it is general knowledge. Likewise, today very few professionals or consumers are aware of medical identity theft and fraud and it's potential for harm. Policy decision-makers, organizations that hold protected health information (PHI), law enforcement, regulatory agencies, and consumer advocates now have an opportunity and obligation to bring this serious societal problem to the forefront and work together to protect the public.

The use of another person's PHI to gain medical services, to procure drugs, or to defraud private insurers or government benefit programs, such as Medicare and Medicaid, is pervasive and threatens the health of individuals and the trust in the healthcare system, and also contributes significantly to the rising cost of healthcare. The threats to individuals include contamination of their health records with erroneous information including, among others items, blood type, serious health conditions, and prescription drugs. Fraud losses in the healthcare system are astronomical and in most cases are facilitated by a stolen medical identity of an individual or a provider.

PHI is accessible in many places today, unlike when paper records were the norm. While improving the sharing of information in the healthcare systems, the transformation to electronic health records (EHR) has made patient records more vulnerable to data breaches. The EHRs are found on mobile devices (laptops, smartphones, tablets) throughout the healthcare organization (covered entity), as well as shared with an organization's business associates-- companies that help the covered entity carry out its healthcare functions.

There are a number of contributing factors that, when taken as a whole, demand immediate action by all stakeholders in the healthcare ecosystem. These include the electronic pervasiveness of PHI and the required security measures required to protect it, the changing regulatory landscape, the increased number of individuals with healthcare benefits, more alternative delivery models with care provided outside of facilities, the increased value of PHI to criminal organizations and the rapidly escalating sophistication of domestic and international crime organizations.

Few people think of themselves as having a medical identity and thus the idea of someone stealing their medical identity is not even on their radar screen. For example, if you ask someone what steps they would take to reduce the chance of identity theft if they lost their wallet, they would tell you that they would cancel their credit cards, contact their bank if they have a debit card and apply for a new driver's license. Rarely, would they mention alerting their health insurance company to take measures equivalent to canceling a credit card. What the public does not yet realize is its medical identities have a significant street value and that a nefarious individual can easily gain access to medical services through the use of their stolen medical identity, the result of which can cause them great harm.

The consequences of medical identity fraud can be more complex than that of the greater known financial identity fraud. Financial losses, inability to purchase a house or car, and not being approved for a loan are all consequences that are easily understood if your good credit is comprised by your financial identity being stolen. It is easy to understand why criminals would want to steal an individual's financial identity, as they can profit from using the information in a number of ways.

THE COST OF MEDICAL IDENTITY FRAUD

The following information is based on the Fifth Annual Study on Medical Identity Theft - independently conducted by Ponemon Institute LLC in February 2015.

The FBI reports that healthcare fraud costs the United States at least $80 billion a year and is rising. Given that most healthcare fraud requires a medical identity or a provider identity, any reduction in medical identity theft will have a significant impact on provider fraud and other types of healthcare fraud.

Unlike credit card fraud, victims of medical identity theft can suffer significant financial consequences. Sixty-five percent of medical identity theft victims in our study had to pay an average of $13,500 to resolve the crime. In some cases, they paid the healthcare provider, repaid the insurer for services obtained by the thief, or they engaged an identity service provider or legal counsel to help resolve the incident and prevent future fraud.

Medical identity theft is a complicated crime to resolve.

In the case of medical identity theft, the healthcare provider or insurer seldom informs the victim about the theft. Rather, on average, victims learn about the theft of their credentials more than three months following the crime and 30 percent do not know when they became a victim. Of those respondents (54 percent) who found an error in their Explanation of Benefits (EOB), about half did not know whom to report the claim to.

Resolution of medical identity theft is time consuming to resolve.

Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident. In our research, only 10 percent of respondents report achieving a completely satisfactory conclusion of the incident. Consequently many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis.

Those who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate. Finally, the impacted individual or a third party, such as the insurer or government agency paid the outstanding medical or insurance bills.

Medical identity theft can have a negative impact on reputation.
Forty-five percent of respondents say medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions (89 percent of respondents). Nineteen percent of respondents believe the theft caused them to miss out on career opportunities. Three percent say it resulted in the loss of employment.

Consumers expect healthcare providers to be proactive in preventing and detecting medical identity theft.
Although many respondents are not confident in the security practices of their healthcare provider, 79 percent of respondents say it is important for healthcare providers to ensure the privacy of their health records. Forty-eight percent say they would consider changing healthcare providers if their medical records were lost or stolen. If such a breach occurred, 40 percent say prompt notification by the organization responsible for safeguarding this information is important.

While medical identity theft cannot be completely prevented, there are steps both consumers and healthcare providers can take to slow its growth.
Consumers should be informed about what they can do to prevent medical identity theft, including protecting their credentials from family and friends, monitoring their healthcare records and paying attention to insurance claims for possible signs their identity has been compromised. Twenty-five percent of medical identity theft victims in this study knowingly permitted a family member or friend to use their personal identification to obtain medical services and products and 24 percent say a member of the family took their credentials without their consent.

Healthcare providers and government have a responsibility to ensure the security of the personal information they collect and to prevent unauthorized access to patient records. This is clearly a concern for respondents. Fifty-five percent of respondents say new regulations under the Affordable Care Act increase their chances of becoming a victim of medical identity theft.

SMARTCARD BENEFITS

Healthcare Providers

Machine-readable health identification credentials:

- Increase clinical and administrative staff efficiency,
- Eliminates shared and unknown access to networks and systems,
- Provides a platform for standardized authentication services across the enterprise and systems, and
- Provide a means for paper elimination through electronic document and form data integrity and signatory requirements.

If credentials are extended to patients, identification credentials:

- Eliminate patient and insurance benefit identification errors,
- Reduce costs and aggravation of rejected claims,
- Reduce lengthy admission processes, and
- Contribute to smoother office procedures and patient satisfaction.

Significant reduction in claim errors will enhance provider relations with plans. The costs of traditional photocopying the front and back of cards, manual lookup and key entry of card information, and filing paper copies can be eliminated over time. When integrated with enhanced provider systems, machine-readable identification cards will facilitate immediate automatic transactions such as eligibility inquiries. Even in phone conversations, the simplicity of needing only two identifiers aids both patient and provider to convey insurance benefit information or medical record identification quickly with complete accuracy.

According to the WEDI Health Information Card Workgroup, the industry can realize an estimated $2.2B savings annually - if a machine readable card is used within Healthcare.

Health Plans & Administrators

Patient and insurance benefit identification errors significantly increase processing and service costs for plans; they aggravate providers; and they contribute to member dissatisfaction. Elimination of patient identification errors will benefit health plans to:

- Improve subscriber or member satisfaction
- Improve employer and plan sponsor satisfaction
- Reduce cost to return and subsequently reconcile claims with errors
- Reduce significantly the cost of both provider and member help desks and administrative record searches, and
- Improve plan-provider relations.

In addition, the universal health plan identifier conveyed by the card is one ingredient for improved coordination of benefits. With multiple-benefit cards, administrators and medium sized payers are able more easily to provide a convenient range of benefit plans to meet the needs of employers.

Patients & Consumers

Elimination of patient and insurance identification errors significantly reduces the hassle factor and increases patient and subscriber satisfaction. Consumers' desire simplicity and they want a single card for multiple benefits and functions. This implementation guide, using only two identifiers, enables multiple benefits on a single card. Patients can more easily and accurately read the essential identifiers from a card to a provider over a telephone. It also permits an option to combine an insurance card with a bank card on the same card.

Employers

Employers desire to improve employer-employee satisfaction and reduce costs. Elimination of patient and insurance identification errors increases employee satisfaction with the company's benefit plans and reduces cost of helping employees resolve insurance benefit problems. With a multiple-benefit card, employers are able more competitively to purchase multiple benefits using different administrators while presenting to an employee only a single, simple card.

Clearinghouses

The standard health plan identifier conveyed by the card assists all-plan routing without requiring translation of trading-partner specific identifiers. Reduction of errors will reduce expense and increase client satisfaction. Multi-benefit cards enable clearinghouses to support increased value to providers.

Process Neutrality

The card should meet stakeholders' needs. It should be neutral to the conduct of business. For example, it should permit but not require multi-functional cards. It should permit host and home plan structures, geographical or regional plan structures, provider networks, and any other such arrangement. It should support different types of benefit plans such as medical, dental, drug, vision, supplemental; and it should permit but not require combinations of benefit plans. It should have flexibility to permit new business structures and processes in the future, including potential financial transactions. Its processes should be open, and supporting directories should be publicly accessible to responsible participants in healthcare electronic commerce.