MAGiCARD®

Identity in Healthcare

Table of Contents

The role of ID Card solutions in personal healthcare security..... 2

Introduction..... 2

Challenges in implementing IAM in Healthcare..... 3

Outdated Systems..... 3

Constant Change to Role Based Access..... 3

Large, disparate user populations..... 3

Username and Password is no longer enough..... 4

The role of ID cards in Healthcare..... 4

Using identity to save and protect lives..... 4

Looking for a Smart solution..... 5

Benefits and Opportunities of Implementing Smart Cards..... 6

Health data consistency, availability and management..... 6

Administration and Governance..... 6

Limitations and Challenges of Implementing Smart Cards..... 7

Cost..... 7

Health data management and security..... 7

Successful case studies of smart card implementation in healthcare..... 8

France – SESAM- Vitale..... 8

2017 facts and figures..... 8

Benefits..... 8

Germany - eGK..... 9

Conclusion..... 10

The role of ID Card solutions in personal healthcare security

Introduction

Gartner, one of the world's leading research and analysis specialist firms, defines Identity and Access Management (IAM) as a security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

IAM is therefore a crucial undertaking for any enterprise, but one cannot over-emphasise the importance of IAM in the healthcare sector where a patient's right to privacy is paramount and any inappropriate access to sensitive patient data is a serious abuse of that right.

Unfortunately, in the healthcare industry worldwide, a lack of automation accentuated by the use of old systems combined with a dependence upon manual processes means most medical facilities are highly vulnerable to data breaches. A global '2018 Cost of a Data Breach' study conducted by Ponemon Institute says that for the eighth year running, healthcare organisations had the highest breach-related costs of any industry at $408 per lost or stolen record — nearly three times the cross-industry average of $148.

Notwithstanding the limitations caused by old systems architecture, the trend towards accessing a range of healthcare services online (such as ordering prescriptions, registering with a practice or merely engaging in a support group) has resulted in the rise of a variety of digital identity requirements that demand stringent security standards. According to the McKinsey Digital Patient Survey [1], more than 75% of respondents across countries would like to use digital healthcare services. And, contrary to popular belief, it's not only the young who seek e-health options; the same survey points out that more than 70% of patients over 50 want to use digital healthcare services.

Obviously, with countries facing consumer pressure to digitise healthcare provisioning and make convenient apps and platforms available to citizens for widespread healthcare access, robust ID solutions that ensure patients' privacy requirements become even more important. One example is the National Health Stack that is being proposed for the Indian Healthcare market that will set up an holistic electronic system for consumers, doctors, hospitals, and insurance companies, covering both the private and public sector alike. A key aspect for providing access to the system includes creating a unique system-wide identifier called the Digital Health ID for each user that will preserve privacy when interacting with other users or stakeholders.

[1] McKinsey Digital Patient Survey was conducted in 2014 in Germany, United Kingdom and Singapore with a sample size of more than 1000 respondents.

Challenges in implementing IAM in Healthcare

Outdated Systems

Healthcare organisations retain a large volume of often complex data for each patient or partner organisation that is often saved on outdated systems. These systems can be expensive to update and hard to improve with better protection capabilities. Hence most healthcare organisations abstain from making technical changes which leaves them especially vulnerable to security breaches.

Constant Change to Role Based Access

A daunting challenge for any IAM solution in the healthcare space is to keep up with the ever-changing role-based access to which healthcare providers are entitled. Given the fluid nature of roles that doctors, nurses, physician assistants assume, it is imperative that any technical solution grants access to the right people at the right times and more specifically at the time when they need it most. One essential feature of a robust IAM solution is that access is revoked when roles change and/or healthcare professionals leave a particular team, department or organisation.

Large, disparate user populations

This is especially important in the case of an integrated medical care environment or when a government of a country is trying to create an efficient e-health platform. Managing various stakeholders including patient and family along with the healthcare provider, insurer, employer etc. becomes a herculean task for the most robust of IAM solutions.

Username and Password is no longer enough

Authentication has to look beyond mere username and password. Additional measures such as multifactor authentication and breached password detection facilities are now commonplace. Furthermore users cannot be expected to remember and manually enter a different set of credentials for different services. Not only is manual entry cumbersome and subject to the vagaries of memory but it will also waste precious minutes that users – especially in an emergency – simply cannot spare.

The role of ID cards in Healthcare

Using identity to save and protect lives

For most hospitals, it's now standard practice to require all doctors, nurses, and staff to wear photo ID badges. Prominently displayed photo identification allows patients and visitors to quickly and easily identify hospital staffers. Patients also feel a certain degree of comfort in knowing that the appropriate, qualified individuals are caring for them.

Without an ID programme in place, the threat of random intruders roaming a hospital facility is very real. Basic hospital ID badges include the cardholder's name, photo, department, and title. Colour coding is often used to distinguish departments as well. More sophisticated ID badges might utilise smart card or proximity card technology, allowing for the secure storage of information as well as integration with hospital access control systems. It is also common for hospitals to implement ID badge systems for patients and visitors.

Visitor badges prevent intruders from freely wandering the hospital without authorisation. While visitor badges are typically somewhat basic in design, it is possible to employ a more advanced system that integrates visitor IDs with existing security systems and data tracking software, making use of biometrics and other personal identifiers.

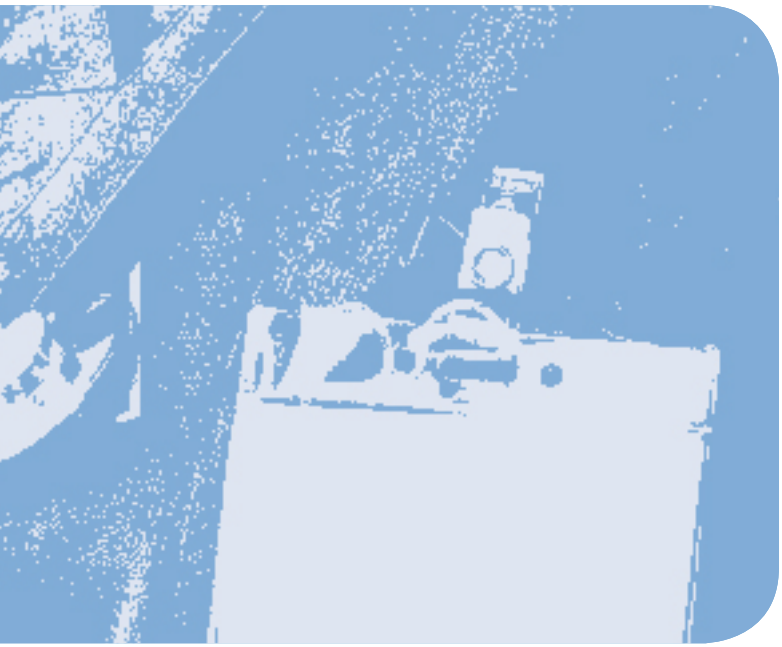
Patient ID cards and badges help to create a more organised and efficient hospital environment. Many use smart card technology allowing patient information to be stored securely on an embedded chip rather than in endless piles of paperwork. Such a system speeds up the patient registration process, facilitates top quality care and also reduces waste. Patient IDs are also used to track surgical itineraries and can contain the cardholder's health records, prescriptions and any allergies of note. This can be read at the bedside or in an emergency situation by a health professional equipped with an appropriate mobile card reader.

Looking for a Smart solution

According to the Secure Technology Alliance, the digital security industry's premier association, issuing a single, secure, multi-purpose credential is the way forward. Such a multi-purpose solution can:

- Support both identity and payment
- Be portable across a variety of form factors ranging from cards to mobile phones
- Provide a secure carrier for portable medical records
- Secure access to emergency medical information
- Enable compliance with government initiatives and mandates

Smart cards should be one of the first options to consider where personal identity, privacy, security, convenience, and mobility are key factors. The biggest benefit of smart cards in the healthcare space is that they can be used as a trusted primary data repository that is constantly in the care of the patient, i.e. the ownership of personal medical information rests with the patient rather than with healthcare providers and insurance companies until such time that a patient gives these entities access to it. Smart cards thus empower patients to be active about the healthcare services they receive. This situation was acknowledged by the US Health Insurance Portability and Accountability Act (HIPAA) legislation in 1996.



Benefits and Opportunities of Implementing Smart Cards

Health data consistency, availability and management

Incomplete or inaccurate patient records are a big problem in effective healthcare delivery. Smart cards enable the storage of a patient's complete medical records in a single, centralised item. Additionally, since the smart card is the patient's property, it is portable and mobile and lends itself to instant availability – an essential requirement in the event of an emergency situation.

Smart cards can improve information flow management, easing up the time, effort and costs involved in manual processes especially at the time of admission. Another important benefit of smart cards (in the hands of healthcare professionals) is the provision of a role-based access framework i.e. data can be accessed only by designated or specifically approved individuals and no one else. This is especially crucial when one considers that more than one-third of healthcare breaches that occur are the direct result of action by insiders within the healthcare system [2].

Administration and Governance

Smart cards enable an efficient e-health ecosystem, laying down an effective platform for a healthcare provider or a government to better administer and govern the delivery of healthcare services. The transparency of the system allows for close monitoring of all stakeholders leading to shorter cycles of measurement and improvement, not to mention timely reports and feedback.

At an academic level, data can be used for disease surveillance and planning, population based data collection and for other research purposes.

> **“Smart cards can improve information flow management...”**

[2] Protenus Breach Barometer

Limitations and Challenges of Implementing Smart Cards

Cost

Cost is often a deterrent in implementing national-level, or indeed any large-scale smart card program. Often however, the cost-benefit of such a system is not accurately calculated or even fully considered, and the overall cost-positive impact of smart-card programmes is therefore understated or ignored completely. The cost aspect is however, impacted and indeed aggravated by the limitations in interoperability of the systems managed by the various healthcare providers and overall issues relating to inconsistent standards of medical record keeping.

Health data management and security

There are numerous questions attached to the subject of where data should be stored and who assumes overall responsibility for the security of patient data. Should a patient's data be stored solely on a smart card or also on online servers? what encryption technique is to be used? Who will have access to what data? And who will ultimately take responsibility for maintaining the data? These are just some of the questions that must be addressed.

Successful case studies of smart card implementation in healthcare

France – SESAM- Vitale

France is an acknowledged pioneer in the large scale use of smart cards in the healthcare sector. The country launched the SESAM-Vitale system – a fully automated system using microprocessor cards called Carte Vitale – as early as 1998.

Initially the Carte Vitale smart cards only included some information about health insurance. The second generation of the system, Carte Vitale 2, was introduced in 2007 with added functionality including the provision of emergency datasets and other medical parameters to authenticated health-care professionals. Carte Vitale 2 is in effect a key to the holder's medical history, which is stored on secure servers.

2017 facts and figures

- **354,387 health professionals are using the system**
- **99,1% of all pharmacists are using the system**
- **Patients are now reimbursed within 5 days**
- **1.245 billion electronic claim forms were processed in 2017; over 90% of all claim forms**
- **98 million card software updates**
- **Administrative productivity and process costs divided by 6 for the e-claims**

Benefits

The SESAM-Vitale program embodies the success of the French universal health care in the eyes of the French people; delivering a simple, fast, computerised system which links patient and healthcare professionals, resulting in improved relationships and an effective modern healthcare system fit for the digital age.

Germany - eGK

The German health card, electronische GesundheitsKarte (eGK), is one of the largest European IT healthcare initiatives which set out to revolutionise the delivery of healthcare services in Germany.

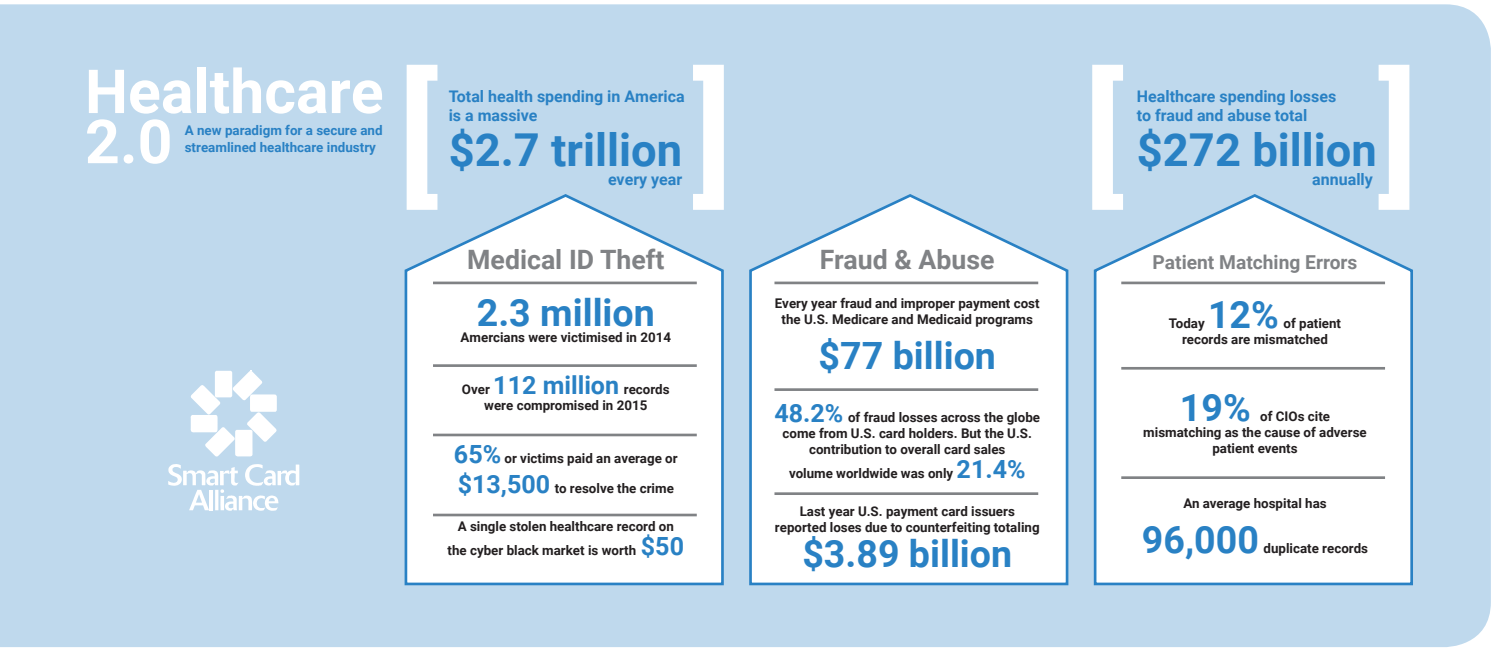
The cards were first issued on October 1, 2011, with the aim of all insured German citizens receiving their card by the end of 2013. Development of the system required infrastructure to connect 76 million insured citizens, 200,000 health professionals, 20,000 pharmacists, 2,000 hospitals and around 145 health insurers in Germany. The Internet forms the network backbone of the system.

Initially, the eGK card just included mandatory patient identification data; however the initial aim was to provide a platform suitable for continual expansion to ultimately include detailed patient histories. To protect privacy, cardholders can choose which information is made available and the smart-cards keep this secure via a PIN code. The eGK cards also include a personal photograph to prevent fraud.

A two-stage security process has been implemented whereby the doctor must also enter their health professional ID card to obtain final access to patient data. Only in an emergency can a doctor gain direct access to patient data, solely with the use of their medical professional ID card.

Conclusion

While one cannot ignore the challenges that wide scale implementation of smart cards pose and the technical limitations that undoubtedly exists, the benefits far outweigh the negatives. According to the Smart Card Alliance, the growth in healthcare-related fraud, patient and record mismatch and payments fraud in the United States of America which can be largely put down to fraudsters targeting the U.S. market as an 'easy target' when compared to countries that have already implemented smart card technology, proves that there is much merit in pursuing smart card implementation [3].



Smart card solutions consistently meet all security standards and help address the various types of fraud occurring in the healthcare industry today. In addition to security, smart card technology provides interoperability, strong authentication and exceeds the standards required to safeguard medical records and payments while also contributing to the best outcome of all, significantly improved patient care.

[3] Healthcare Identity Authentication and Payments Convergence: A Vision for the Healthcare Industry