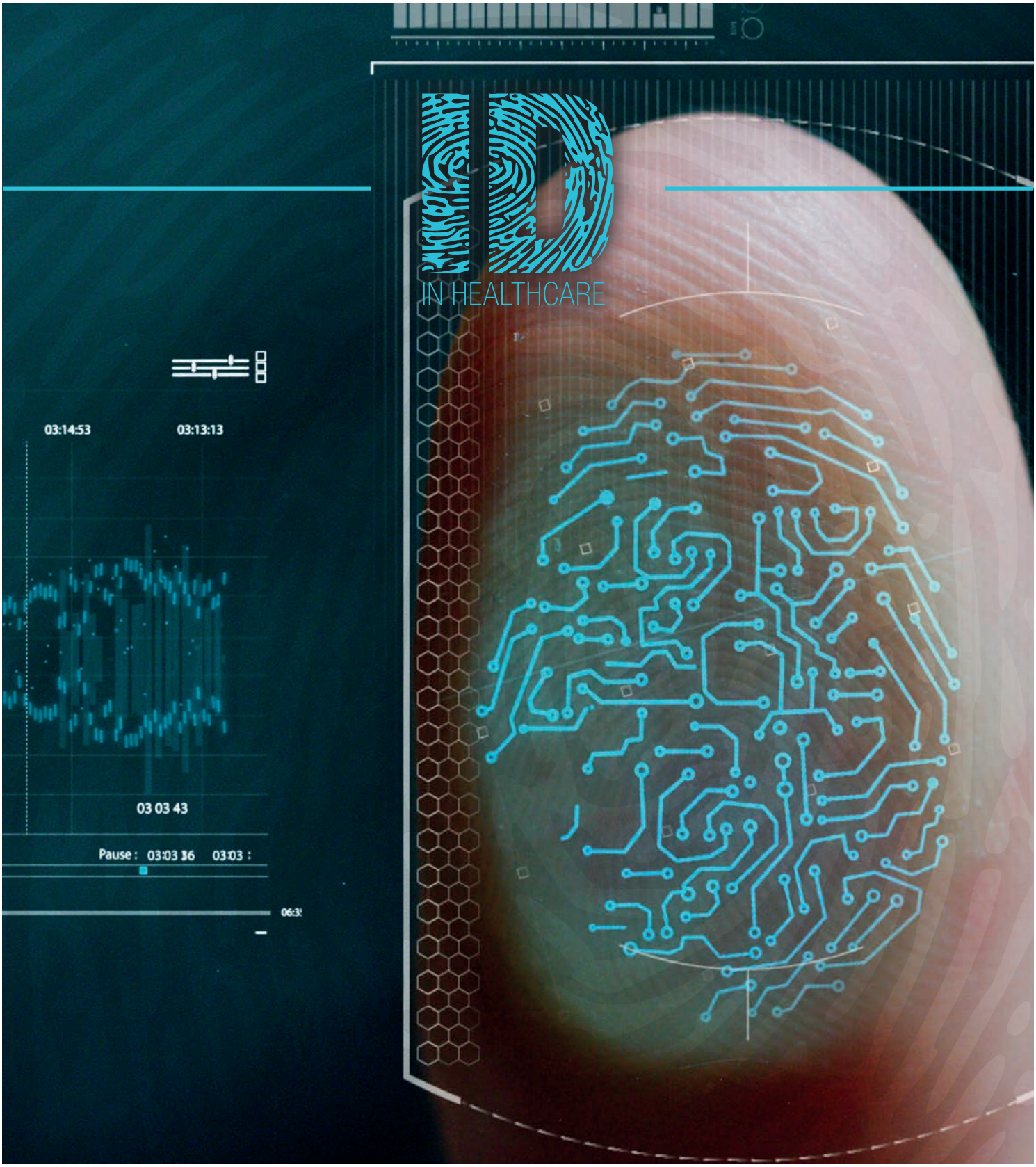


IDENTITY
IN HEALTHCARE

A KEY ENABLER TO INTEGRATED CARE / MAY 2018

COCIR

SECURE IDENTITY ALLIANCE

ID
IN HEALTHCARE

TABLE OF CONTENTS

INTRODUCTION

Healthcare is in need of identity solutions. As the number of patients continues to rise and many healthcare providers embrace electronic medical records (EMRs), the industry is struggling to manage identities properly, ensure patient privacy, and meet the growing demand. Most providers lack efficient solutions to help them control costs, protect privacy, prevent fraud, and ultimately to offer the new gold standard in healthcare: integrated care.

As people live longer and require more chronic illness care, our current models for delivering and funding care are at their limits. Integrated care – which connects all the different medical professionals involved in patient care – has the potential to transform healthcare as we know it. But in this traditionally fragmented industry, bringing everyone together is difficult, even in the digital age. Add to that the increasing threat of identity theft and fraud, and we are left with healthcare systems that face enormous challenges.

Interestingly though, these challenges and the available solutions are actually well known. Providers have long recognised the need to integrate technology in order to transform their model. With better coordination, resource pooling, interoperability strategy, cloud technology and more, the industry has much to gain, not least in the ability to deliver truly integrated care. New technologies such as telehealth, mHealth (mobile health) and the Internet of Things (IoT), are poised to become key tools to expand the power and reach of healthcare.

So, with all these tools at our disposal, why haven't we solved the problem? Besides the necessary change of business models and the major interoperability challenge among others, one key enabler needs to be in place: state-of-the-art identity management. Without the ability to create and manage trusted identities, and without a system that ensures security and protects privacy, healthcare providers will not be able to take advantage of technology to develop integrated care systems and achieve better outcomes. A solid identity management solution is one of the first and key steps on the path toward integrated care.

This paper intends to explain how healthcare providers can leverage trusted identities and robust identity management to tackle these challenges. We address the critical role that trusted identities play in the transformation of healthcare not only to protect security and privacy, but also to reduce costs, drive integration, and foster the use of new technologies. First, we introduce the identities that are vital to the healthcare industry and discuss the interrelationships between these identities. Then we showcase the benefits of efficient identity management that puts patients first and provides the foundation for integrated care.

EXECUTIVE SUMMARY

Healthcare is in need of identity solutions. As many healthcare providers embrace electronic medical records and the number of patients continues to rise, the industry is struggling to manage identities properly, ensure patient privacy, and meet the growing demand. Most providers lack an efficient identity management solution to help them control costs, protect privacy, prevent fraud, and ultimately to offer integrated care. This paper intends to explain how healthcare providers can leverage trusted identities and robust identity management to tackle these challenges.

Identity is a key to unlock many opportunities: integrated care is the first one, closely followed by patient empowerment. Not only can identity be the glue that sticks stakeholders together around the patient's case, it is also the sesame that gives the patient both peace of mind that his data are well protected and the actual key to access his data online. As Europe has put cross border healthcare as a major stake, identity will also prove there to play a pivotal role. Last but not least, robust identity management directly and indirectly contributes to cost control for the benefit of the healthcare system and its sustainability.

While the opportunities are aplenty, let us not forget the challenges to overcome: identity is clearly not central in healthcare yet, there is a need to raise awareness around its usefulness and importance. When identity is checked and verified, the means to do so are currently poorly matched to the stake at hand. Healthcare providers and the ecosystem at large still need to better understand and grasp the implication of identity management on GDPR[1] compliance and more commonly on fraud fighting.

This led us to the following recommendations:

COCIR RECOMMENDATIONS

To reap all the benefits of integrated care, we need to lay solid foundations: efficient, reliable identity management is one of the necessary pillars. Through this paper, we want to raise the level of awareness regarding the importance of identity management in healthcare and would like to recommend the following action items to support its implementation:

STRONGER POLICY REGARDING ID

REVIEW PROCESS OF ID CREATION FOR ALL 3 TYPES OF ID

The process of creation of those identities (Patient ID, Health Insurance ID, Healthcare Provider ID) should follow the same practices as the Citizen ID. For Citizen ID, it is commonly known that the end-to-end process from registration to issuance to document verification needs to be secure. At registration, this means obtaining reliable data from civil registries or national identity systems in order to ensure that newborns are properly linked to parents' health insurance plans for instance. The issued credentials (be they physical documents or digital identities) must be secure enough to prevent forgery or alteration. Identities shall be verified at the point of care with a minimum Authentication Assurance Level.

We recommend all Member States to review their processes to create, manage and verify the 3 types of identities (insurance ID, Patient ID and Healthcare professional ID) in their countries to ensure best practices are applied to adequately support the needs of healthcare in terms of outcome, security, privacy and cost control.

INCENTIVES FOR HEALTHCARE PROFESSIONALS TO VERIFY PATIENT ID

While it makes perfect sense to check the Patient ID at the point of care, this is yet not commonly performed in practice. There is still a need to incentivise this practice until it becomes common place across the board.

We recommend EU and Member States to assess the possibility to adopt a policy enforcing the systematic strong ID verification of patients at the point of care.

1. ***GDPR**: General Data Protection Regulation*

LEVERAGE eIDAS FOR CROSS BORDER HEALTHCARE

eIDAS[2] needs to be leveraged to support cross border healthcare. To adapt to healthcare use cases, the EU and the Member States should agree on

- Specific attributes that need to be shared in the case of cross border healthcare, in addition to the current eIDAS attributes.
- The Authentication Assurance Levels (AAL) required for the various use cases: here we recommend policy makers and stakeholders to strike a balance between security and convenience – while health data are sensitive, the context in which they are used are not all at the same level of risk. As such, requesting an AAL high for all healthcare transactions might not prove useful and deter stakeholders to adopt the policy.

RAISE AWARENESS REGARDING GDPR AND ID

Healthcare professionals need to better understand how ID can help them comply with the basics of GDPR. Guidelines from the EU could help healthcare providers implement best practices in terms of:

- **data collection** and **consistent storage** in the patient's file to ensure data are properly linked to their owner,
- **user consent**: when user consent is needed, in which cases (does a patient need to give systematic consent to his GP or can this be granted for a period of time? should a patient give consent to the doctor when he is consulting abroad i.e. in the case of cross border healthcare?...) and how this is logged,
- **data protection**: strong authentication to access data should be required.

OPEN TO INNOVATIONS AND TO VARIOUS TECHNOLOGIES THAT CAN BE COMBINED (BIOMETRICS, SMART CARDS, SMARTPHONE…)

Regarding Patient ID, one needs to bear in mind that this ID needs to be checked in multiple instances: during a doctor's consultation, at hospital admission, at blood sampling i.e. when the patient is conscious and responsive but also in surgery, in emergency rooms, in cases of dementia… i.e. when the patient is unconscious and/or unable to support the process of identity verification. To that purpose, all stakeholders (policy makers, healthcare professionals and vendors, patients themselves and carers) need to realise that such Patient ID needs to take multiple forms. This can materialise into a (smart) card as commonly known but also into a wearable or a smartphone. It could also be communicated thanks to biometric verification (finger print recognition or face recognition for instance). The various forms of ID need to be adapted to the use cases. And what is true for Patient ID is also very relevant for Healthcare Professionals for whom it is essential that this ID verification be quick and efficient in all circumstances: emergency, in surgery, in mobility…

We recommend that working groups and pilots, involving all stakeholders, be carried out to help defining the most appropriate solutions depending on the use cases (some use cases are described in annex of this paper).

2. Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted by the co-legislators on 23 July 2014 / https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

IDENTITIES AND THEIR RELATIONSHIPS

Before we take a closer look at identity management, it is important to understand the different identities in use within the healthcare industry and how they relate to one another.

PATIENT ID

The most obvious identity is that of the patient, which begins at birth and follows the patient through life. The "patient ID" is very personal and strictly confidential: only patients and select healthcare providers should have access.

A secure patient ID is important for both the provider and the patient. For providers, it means consistency of care. Medical records associated with a patient ID ensure that all medical professionals have access to a complete and reliable medical history when treating a patient. For patients, it means privacy and peace of mind. Ensuring patient privacy can ease the fears of patients suffering from sensitive diseases, such as HIV, since many patients do not want their names associated with those diseases. In fact, such patients might seek treatment under aliases at different healthcare facilities in order to hide their illness from others, which could compromise consistency and quality of care.

This example raises the natural question: why can't we use our legal citizen IDs as our patient IDs as well? While it is certainly the most convenient option – and one that is in use, for example in Belgium – this solution poses both legal and privacy challenges: not all countries allow legal identities to be used in healthcare and sensitive health data may need to be kept separate. Germany for instance has chosen to not use its national smart ID card for healthcare, due to privacy concerns.

To protect privacy, the safest option is to decouple patient IDs from legal citizen identities. The idea here is to create an identity that includes everything the healthcare system needs to know and nothing that it doesn't, such as the patient's address for instance. A patient's ID would only include information needed to treat the patient within the healthcare system, limiting the risk that this information could be revealed to the public. The result would be that the information is shared within the system, cannot be tied to a legal identity, and therefore does not infringe on personal privacy.

HEALTH INSURANCE ID

In countries with state-run health insurance programmes, a health insurance identity is necessary to link people to the social security or insurance benefits to which they are entitled. Unlike patient IDs, this identity can change over time and be shared. For example, patients might switch insurance providers or lose their insurance coverage after taking up residence in another country. Health insurance IDs may need to be shared, such as is the case for children who are covered by their parents' insurance policies.

By issuing a health insurance ID that is separate from a patient ID, a patient's medical history is detached from their health insurance information and benefits, making it safer and easier to update when coverage changes and making both of them more secure to prevent fraud.

HEALTHCARE PROVIDER ID

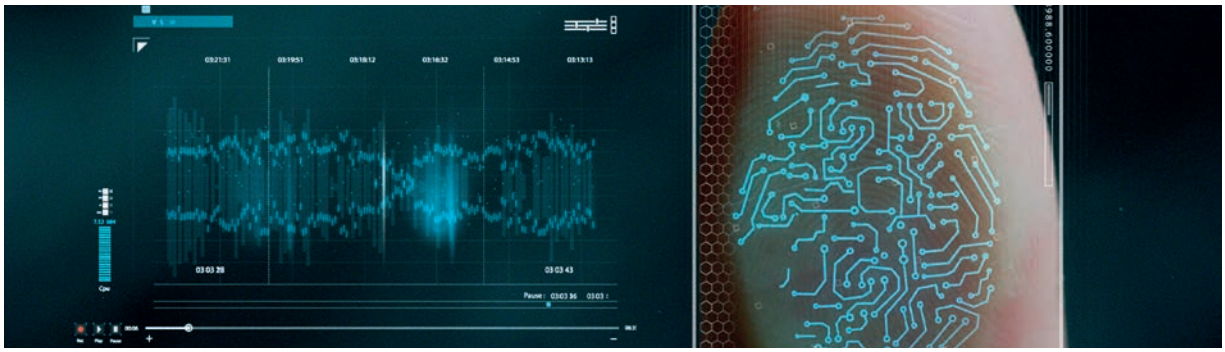
Healthcare professionals also require identities for access to healthcare systems and to determine authority, i.e. who is authorised to make certain decisions within the system, such as diagnose patients or prescribe medications. For example, radiologists are only allowed to examine and interpret X-rays and are not permitted to prescribe medications. A healthcare

provider ID should be associated with rights and responsibilities to individuals based on their position within the organisation.

This concept can also be extended to the broader ecosystem when relevant. For instance, opticians in France are now authorised to re-examine patients' visual acuity in order to provide them with just the right corrective lenses. Although not considered formal healthcare providers, opticians deliver a healthcare service and need to be granted the rights to do so.

Healthcare provider IDs are tied so closely to power and influence that they should not be merely managed through a practitioner's legal identity, which doesn't include the healthcare provider attributes, role and responsibilities. These healthcare provider IDs must be separate and carefully managed.

These three identities have clear and distinct purposes. Much like the different lives we lead and the roles we play in life, there are many good reasons to separate patient, insurance, and provider IDs in the world of healthcare, not least of which are patient privacy and improved care.



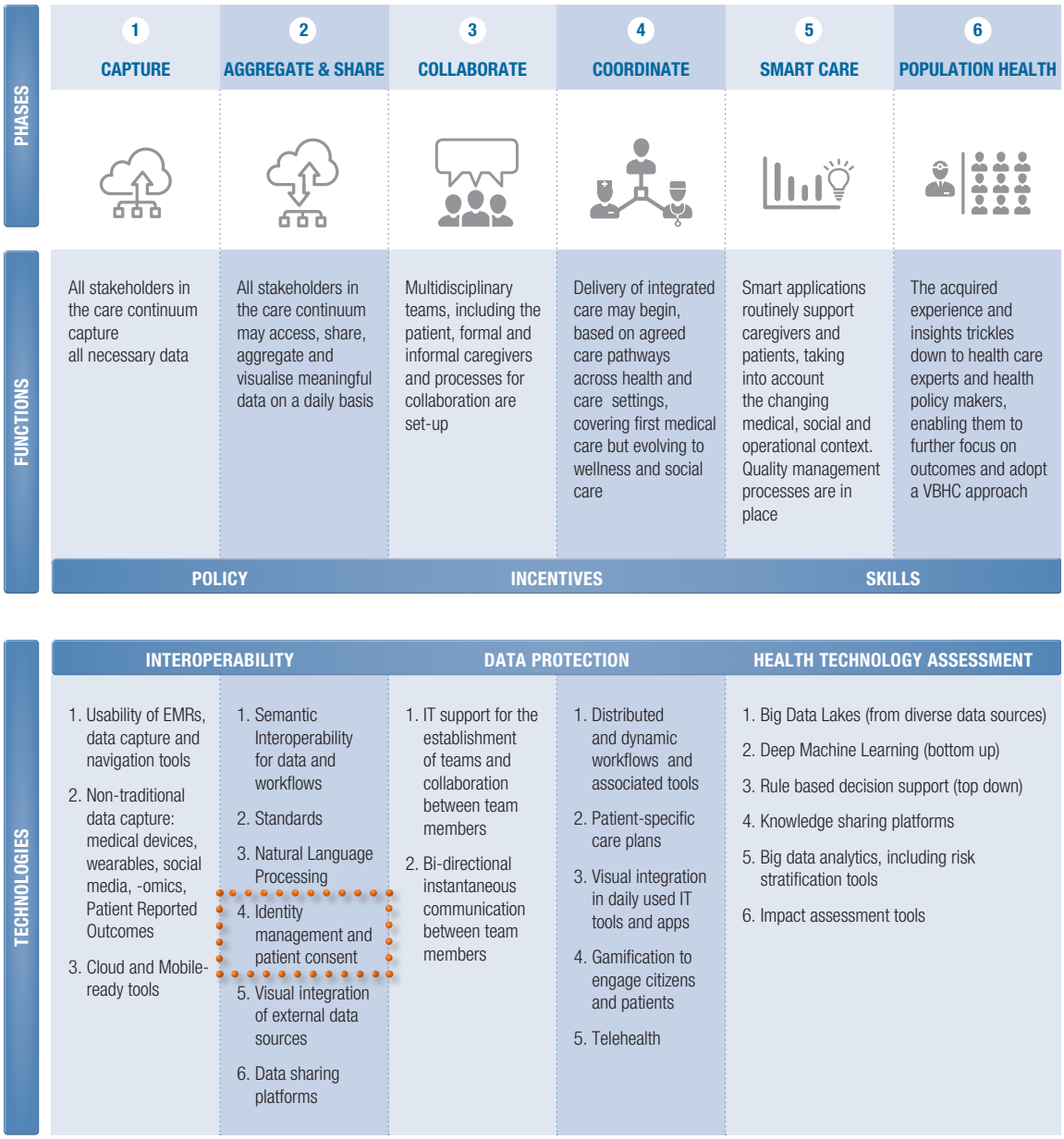
OPPORTUNITIES

An efficient management and use of these 3 types of identities would deliver tremendous opportunities to the healthcare system: starting with enabling true integrated care, this would also ensure the peace of mind and service level expected by patients. Not to mention that it would unlock the potential of cross border healthcare in Europe and support the system in its endeavor to control costs to the benefit of sustainability.

IDENTITY AND INTEGRATED CARE

The concept of integrated care is attracting a great deal of attention around the world as an important model for improving patient outcomes and developing more cost-effective health systems. But it is relatively new and has yet to be clearly defined. Though different models have been used to integrate care, what they share is the aim to design all stages of care delivery around what is best for patients. The general idea is to bring together the various healthcare professionals involved in patient care to deliver consistent and coordinated services. With chronic illnesses on the rise and populations aging around the world, the industry agrees that the often-fragmented delivery of care must be replaced by a more comprehensive approach that offers patients better quality and more efficient care.

Integrated care inherently requires integrated information – sharing patient data so that all parties are working with a patient's complete and reliable medical history. As the COCIR paper on the Digital Health Roadmap to Support Integrated Care clearly explains, trusted patient identities and data collection provide the foundation. To ensure the effectiveness of an integrated healthcare system, a solid and secure identity management solution must be in place.



Source: COCIR Digital Health Roadmap to support Integrated Care Here

Obviously, there is no sense in sharing data to coordinate care unless it is complete and correct, not to mention linked to the right patient. Trusted patient IDs must be at the heart of any healthcare system, connecting patients to their data and their individual case. By positively identifying his patient at each step of the process, the healthcare provider is ensured to access and update the correct medical file thus delivery efficient care and avoiding medical errors. The patient in turn can rest assured that his medical history is being reliably and consistently compiled and consolidated.

IDENTITY AND PATIENTS

Patients have a lot to gain from efficient identity management. In addition to security and privacy protection, such identity systems empower patients and make their lives easier.

PRIVACY EQUALS PEACE OF MIND

With trusted patient and healthcare provider IDs, healthcare systems are much more secure and patients have a lot less to worry about. Healthcare providers can be confident that the medical history they access matches the patient they are treating, and patients can rest assured that their records are not being mixed up with someone else's and that only authorised providers have access.

KHUSHI BABY - INDIA

Delivering healthcare to rural areas with illiterate populations and little to no infrastructure is a challenge many providers face around the world. In the state of Rajasthan in India, a pilot programme was started to establish a decentralised system to monitor and respond to the health of pregnant women and their newborn babies. Using the wearable technology and a mobile application developed by Khushi Baby, a US nonprofit organisation, community healthcare providers can register mothers and newborns in remote villages, monitor their health, track vaccination schedules, and more. Each patient is issued a digital medical record worn as a necklace that can be read and updated through near field communication (NFC). A secure biometric tablet is used to collect biometric information so that the next time the mother or child sees a healthcare provider a biometric scan can be used to verify that the medical record in the NFC necklace matches the person wearing it. Updates on the tablets are automatically synced to a central platform as soon as the healthcare provider has cellular coverage. This also means that no matter which provider patients visit, that provider will have instant access to their complete medical history. In just a few months the program has registered more than 30,000 mothers and babies.

Security is indeed of paramount importance in healthcare. Patients need assurance that their medical records, which may include sensitive information, will not fall into the wrong hands. Data security is also a matter of compliance. For example, the EU's General Data Protection Regulation (GDPR) mandates that data protection is designed into the development of services by default and that people have the right to access their data at any time.

Privacy equals peace of mind. Now that electronic medical records (EMRs) are standard in many healthcare systems and with medical identity theft on the rise, people are rightly concerned about who has access to their data and how secure it is. Patients suffering from diseases that may be seen as taboo or carry harsh sociocultural consequences if exposed might wish to keep this information private or choose who may or may not know about it.

PATIENT EMPOWERMENT

Digitisation is making things easier and more convenient in many industries – and that includes healthcare. As many healthcare providers strive to deliver integrated care, they are going digital – converting to EMRs and building digital networks to communicate and coordinate care. With trusted digital IDs at its core, an efficient identity management system makes it easy for patients to access their EMRs without the need for cumbersome usernames and passwords. Patients can also move freely through the system without carrying paper records or lists of medications to share with new doctors.

Digital identities are also the keys to empowerment, enabling patients to become active stakeholders in their treatment. With access to their medical records, they are able to see updates immediately and monitor their health. They can decide with whom to share their data, including with which healthcare providers or informal caregivers. And in the new age of IoT, a digital system allows patients to upload data from self-monitoring systems such as fitness trackers or other health and wellness devices.

Estonia is a good example of patient empowerment through digital technologies. Through the deployment of their national digital strategy, Estonian citizens can log into their patient portal, after authenticating strongly with their eID card, to view their medical data and related information (such as recent appointments, prescriptions) – and the records of their children. They are also able to control which doctors have access to their files.

With that level of trust, confidence and control, patients may even be more willing to share data with the scientific community for research purposes – a positive side effect with tremendous potential.

CROSS BORDER HEALTHCARE

In particular in Europe, cross border healthcare is a key lever to improve the quality of care as well as its efficiency. With the implementation of various eHealth Networks, the EU is looking at taking advantage of the medical expertise where it is for the benefit of the larger population of Europe as well as to accompany the mobility of the European citizens across Europe. Again efficient identity management and especially of all 3 types of identities (insurance, patient and healthcare provider) will support this trend:

- Identifying reliably the patient will allow the healthcare provider to access the right medical file and confirm patient's consent for his access (the latter being key to comply with privacy regulations);
- Identifying reliably the healthcare provider will ensure the patient that his data are being shared with an authorised professional and that his privacy is being protected;
- Linking the medical transaction to the insurance ID will allow the beneficiary to be reimbursed or financially subsidised according to his rights and benefits.

Managing efficiently and adequately identity in cross border healthcare provides the necessary conditions of success: the patient is secured from a medical and financial standpoint and the healthcare provider is ensured to get the data he needs to deliver care. This is vital and even more so when such cross border healthcare might be delivered remotely i.e. in the case of a patient accessing remotely to medical expertise in a neighboring EU country.

COST REDUCTION

In addition to supporting integrated care, patient empowerment and cross border healthcare, identity management also directly and indirectly contributes to controlling healthcare expenditures through 3 main levers:

- FIGHTING FRAUD
- STREAMLINING ADMINISTRATIVE PROCESSES
- REDUCING REDUNDANT TESTS.

FIGHTING FRAUD

Healthcare is expensive, which means social security programmes and insurance policies are very valuable targets and the risk of identity theft is high. By putting in place a programme to verify identities of beneficiaries before issuing health insurance ID, social protection and welfare entities can fight fraud and recoup those losses.

The system in **France** provides an excellent example. French healthcare providers are issued CPS cards (Carte de Professionnel de Santé) to authenticate and key all medical transactions. Patients receive health insurance ID cards (Carte Vitale) that convey their identity and enable to verify the benefits to which they are entitled.

The two cards when used together allow to authenticate a medical transaction and submit it to the insurance provider for reimbursement. When patients visit the doctor, their insurance ID

card is read, which links them to the treatment that follows. The provider's CPS card is used to authorise and sign the transaction before it is transmitted to the insurance provider, rendering the provider liable for proving that the service was actually delivered.

STREAMLINING ADMINISTRATIVE PROCESSES

When identities have been provisioned in an electronic and/or digital format (through a smart card for instance), some processes can be streamlined. For instance, the reimbursement claim process or the admission process can be streamlined. In France, thanks to the introduction of the Vitale Card, the reimbursement claim process could be streamlined and automated: in 2012, the GIE SEAME-VITALE reported a per transaction cost reduction of more than 80% and a savings in the range of €1.5bn.

REDUCING REDUNDANT TESTS

Once integrated care is in place and patients own their medical records, healthcare providers can take advantage of complete and reliable medical history. This should avoid the prescription of redundant tests and examinations which today represent a terrible waste. In the US, it is estimated that these redundant tests could be avoided for a savings of $8bn (*Improving Safety And Eliminating Redundant Tests: Cutting Costs In U.S. Hospitals, by Ashish K. Jha, David C. Chan, Abigail B. Ridgway, Calvin Franz, and David W. Bates.).*

Once that foundational comprehensive identity management system has been laid, both patients and healthcare professionals will be able to reap the full benefits of electronic medical records (EMRs) and integrated care, which include the following:

- A system designed around what is best for the patient
- Access to complete and up-to-date medical records at all stages of care
- Communication and coordination across a network of healthcare providers
- Reduced costs and increased efficiency by avoiding duplicate and/or unnecessary examinations and tests as well as identifying any services that may have been overlooked
- Peace of mind that records are safe and secure, that doctors have a controlled access to records and are making informed diagnoses
- A basis for establishing telehealth and mHealth programmes
- A better interface between health systems and social services.

CHALLENGES

NO REQUIREMENT REGARDING PATIENT ID

Overall, there are no or limited requirements regarding Patient ID be it at the national or EU levels. In some member states, the Patient ID exists in the form of a unique patient ID number. In others, it is mixed with the Citizen ID like in Belgium or in Estonia.

There are no or limited requirements regarding its verification i.e. its correspondence to the rightful owner of the Patient ID:

- Healthcare providers do mention that it is important to check the identity of their patients but they rarely do so and have no incentive to do so
- There is no minimum level of assurance to comply with when doing so: in the framework of cross border healthcare, this will be a key challenge to overcome. Member states should agree on the Authentication Assurance Level (AAL) to be complied with to enable cross border healthcare. Most likely they will leverage the eIDAS framework and will need to agree on additional attributes to be shared in the framework of healthcare use cases, in addition the current eIDAS attributes.

INADEQUACY OF IDENTIFICATION MEANS

The current methods of identification in most healthcare systems are at most adequate within a single care delivery organisation, with nurses manually double-checking paperwork before collecting blood or asking patients to verify such details as name and date of birth. Both examples are at best inefficient and at worst unreliable when scaled to span multiple organisations. The challenge is finding a state-of-the-art model to efficiently, securely, and reliably identify patients.

When scaled at a national level, patient matching errors present an acute problem to the healthcare industry. In a place where many people have the same names, the typical systems – based only on demographic data – has demonstrated its limits. As a result of typos or identical names, patient records are getting mixed up or left incomplete, which can lead to lethal consequences such as unwanted drug interactions, inaccurate or inadequate prescriptions, and surgical errors.

GDPR

As GDPR is coming into force, the industry as well as Member States are still struggling to interpret the regulation and to define the measures to put in place. A lot of focus and attention are paid to how to reuse medical data while complying with GDPR and to how to demonstrate privacy by design but little has been discussed about how to ensure the essence of GDPR: ensure that each and every European citizen can access the data that was collected about him. Very little attention has been paid to the fact that without identifying positively the patient, healthcare providers cannot ensure this to their patient. Indeed, how can you guarantee your patient that you can provide all his data and only his data if the link between data and his identity is not reliable? How can you ensure that data were not mixed? How can you ensure that you are pulling the right file out?

FRAUD

Fraud in healthcare is massive. In this paper we mention only 2 types of fraud: identity fraud and transaction fraud. Both result from a poor identity management of health insurance beneficiaries and healthcare professionals. Indeed, as ancillary identities compared to Citizen ID, they often do not get the attention they deserve leading to massive fraud attacks and terrible financial losses.

IDENTITY FRAUD

Medical identity fraud can stem from identity theft or the use of fake identities. In countries with state-run health insurance programmes, the rise of medical identity theft and fraud is startling, with ramifications ranging from financial to medical. The problem is particularly prevalent in the area of entitlements, such as Medicare in the US. Scammers use the stolen information to access subsidise care or medication with potential medical risk for the victim. If the fraudster's medical information is mixed up with that of the victim's, there's a risk that crucial information about the victim could be changed, such as blood type or indications for medications that could cause allergic reactions. In some countries, that type of fraud is perpetrated at such a scale that it leads to massive black markets for medications fueled by identity theft and fraudulent transactions.

In some cases, fraudsters establish entirely fake identities to access entitlements or to submit false claims. Too often the benefits are paid out before the fraud has been detected. The same applies to areas where entitlement programs are regionally bound. There we find cases of multiple registrations in different regions aimed at obtaining multiple benefits at the same time.

TRANSACTION FRAUD

Transaction fraud primarily involves healthcare providers filing social security or insurance claims for services that were never rendered. As online transactions become more popular, the fraud associated with them is also rising. With telehealth and mHealth services playing a larger role, the industry needs solid identity solutions to ensure that claims are made for real patients who are treated with real services.

IT SKILLS OF HEALTHCARE PROVIDERS

While this is evolving with the new generations, healthcare providers are still generally lacking IT skills, which most likely accounts for their lack of interest for IT security measures. While studies report that a large proportion of data breaches result from internal resources negligence or misuse, there is clearly a need to increase the level of awareness of healthcare providers but also to provide them with solutions that are both efficient and convenient.

RECOMMENDATIONS

To reap all the benefits of integrated care, we need to lay solid foundations: efficient, reliable identity management is one of the necessary pillars. Through this paper, we want to raise the level of awareness regarding the importance of identity management in healthcare and would like to recommend the following action items to support its implementation:

STRONGER POLICY REGARDING ID

REVIEW PROCESS OF ID CREATION FOR ALL 3 TYPES OF ID

The process of creation of those identities (Patient ID, Health Insurance ID, Healthcare Provider ID) should follow the same practices as the Citizen ID. For Citizen ID, it is commonly known that the end-to-end process from registration to issuance to document verification needs to be secure. At registration, this means obtaining reliable data from civil registries or national identity systems in order to ensure that newborns are properly linked to parents' health insurance plans for instance. The issued credentials (be they physical documents or digital identities) must be secure enough to prevent forgery or alteration. Identities shall be verified at the point of care with a minimum Authentication Assurance Level.

We recommend all Member States to review their processes to create, manage and verify the 3 types of identities in their countries to ensure best practices are applied to adequately support the needs of healthcare in terms of outcome, security, privacy and cost control.

INCENTIVES FOR HEALTHCARE PROFESSIONALS TO VERIFY PATIENT ID

While it makes perfect sense to check the Patient ID at the point of care, this is yet not commonly performed in practice. There is still a need to incentivise this practice until it becomes common place across the board.

We recommend EU and Member States to assess the possibility to adopt a policy enforcing the systematic strong ID verification of patients at the point of care.

LEVERAGE eIDAS FOR CROSS BORDER HEALTHCARE

eIDAS needs to be leveraged to support cross border healthcare. To adapt to healthcare use cases, the EU and the Member States should agree on

- Specific attributes that need to be shared in the case of cross border healthcare, in addition to the current eIDAS attributes.
- The Authentication Assurance Levels (AAL) required for the various use cases: here we recommend policy makers and stakeholders to strike a balance between security and convenience – while health data are sensitive, the context in which they are used are not all of the same level of risk. As such, requesting an AAL high for all healthcare transactions might not prove useful and deter stakeholders to adopt the policy.

RAISE AWARENESS REGARDING GDPR AND ID

Healthcare professionals need to better understand how ID can help them comply with the basics of GDPR. Guidelines from the EU could help healthcare providers implement best practices in terms of:

- **data collection** and **consistent storage** in the patient's file to ensure data are properly linked to their owner,
- **user consent**: when user consent is needed, in which cases (does a patient need to give systematic consent to his GP or can this be granted for a period of time? should a patient give consent to the doctor when he is consulting abroad i.e. in the case of cross border healthcare?...) and how this is logged
- **data protection**: strong authentication to access data should be required.

OPEN TO INNOVATIONS AND TO VARIOUS TECHNOLOGIES THAT CAN BE COMBINED (BIOMETRICS, SMART CARDS, SMARTPHONE…)

Regarding Patient ID, one needs to bear in mind that this ID needs to be checked in multiple instances: during a doctor's consultation, at hospital admission, at blood sampling i.e. when the patient is conscious and responsive but also in surgery, in emergency rooms, in cases of dementia… i.e. when the patient is unconscious and/or unable to support the process of identity verification. To that purpose, all stakeholders (policy makers, healthcare professionals and vendors, patients themselves and carers) need to realise that such Patient ID need to take multiple forms. This can materialise into a (smart) card as commonly known but also into a wearable or a smartphone. It could also be communicated thanks to biometric verification (finger print recognition or face recognition for instance). The various forms of ID need to be adapted to the use cases. And what is true for Patient ID is also very relevant for Healthcare Professionals for whom it is essential that this ID verification be quick and efficient in all circumstances: emergency, in surgery, in mobility…

We recommend that working groups and pilots, involving all stakeholders, be carried out to help defining the most appropriate solutions depending on the use cases (some use cases are described in annex of this paper).

CONCLUSION

If you miss the very first step, you are likely to tumble down the entire flight of stairs. Patient identity is the proverbial first step that the healthcare industry cannot afford to miss. It is the key to collecting information, protecting that information, and ensuring that it accompanies patients throughout an entire lifetime of healthcare – from pediatrics to geriatrics. It is the building block of privacy protection and patient empowerment, providing peace of mind and turning patients into stakeholders. And it is the foundation for providing truly integrated care in the digital age.

But healthcare is a complex ecosystem, in which patient IDs interact with countless actors and where secure and trusted health insurance and healthcare provider identities are also essential to an effective identity management system that serves the entire industry. Separate health insurance IDs not only link patients to their social security and insurance benefits, they allow that information to be shared or changed without risking any sensitive information included in patient IDs. Healthcare provider IDs enable caregivers to sign off on each step in the treatment process and determine who is authorised to make certain decisions within the system. Both are vital in order to safeguard the system and prevent errors.

As healthcare systems and providers around the world transform to integrated, digital models, they will first need to solve their identity problem. Once a trusted identity management system is in place, these providers will be in a position to design truly integrated care programmes centered on what is best for their patients: improving outcomes and delivering services that are consistent and coordinated from the patient's perspective. But identity is not only the key to solving these issues, it also unlocks the door to other cost control and efficiency benefits that can ultimately fuel the transformation process.

ANNEX

IDENTITY SOLUTIONS FOR INTEGRATED CARE

Here are a few of the different technology and operational models for identifying patients:

CARDS

Patients are issued a patient ID card, which they present to their healthcare providers at each visit. This solution is costly to maintain over time and there is always the risk that cards are lost or not on hand when needed.

BRACELETS

Bracelets equipped with bar codes allow providers to quickly scan and identify their patients, but are quite inconvenient in multi-facility ecosystems. Patients often feel "marked" as ill, and the bracelets can be lost easily. Most applications to date have been in single-facility situations, such as hospitals, which clearly limits scalability.

BIOMETRICS

Biometric identity tools offer a number of advantages for providers striving to implement solid identity systems and ultimately offer truly integrated care. First and foremost, biometrics are intrinsic and unique to each individual. Not only is there no need for patients to carry IDs, each person's biometric information – fingerprints, facial features, and iris patterns – are one of a kind. Biometric capturing has improved greatly in recent years, with many commercial devices available on the market that are both fast and easy to use. Biometric identity tools can speed access to patient data in emergency situations and provide a powerful method for identifying patients who are unconscious or unable to spell their names or remember who they are.

BIOMETRIC SOLUTION CASE STUDIES

The use of biometrics in the healthcare industry is still in its infancy – in some cultures the mere concept is difficult to accept. So far, we've seen biometric identity solutions deployed in either single hospitals or in groups of hospitals and primarily in the US. A number of countries, such as India, are considering biometric solutions for their national healthcare systems and/or to leverage their national biometric databases for healthcare purposes.

The following case studies demonstrate how powerful biometric technology can be to help build solid identity management systems.

KHUSHI BABY

Delivering healthcare to rural areas with illiterate populations and little to no infrastructure is a challenge many providers face around the world. In the state of Rajasthan in India, a pilot program was started to establish a decentralised system to monitor and respond to the health of pregnant women and their newborn babies. Using the wearable technology and a mobile application developed by Khushi Baby, a US nonprofit organisation, community healthcare providers can register mothers and newborns in remote villages, monitor their health, track vaccination schedules, and more. Each patient is issued a digital medical record worn as a necklace that can be read and updated through near field communication (NFC). A secure biometric tablet is used to collect biometric information so that the next time the mother or child sees a healthcare provider

a biometric scan can be used to verify that the medical record in the NFC necklace matches the person wearing it. Updates on the tablets are automatically synced to a central platform as soon as the healthcare provider has cellular coverage. This also means that no matter which provider patients visit, that provider will have instant access to their complete medical history. In just a few months the programme has registered more than 30,000 mothers and babies.

BIOMETRIC IDENTIFICATION

Biometric identification uses measurable biological characteristics such as fingerprints, facial features, and iris patterns to identify an individual. The prevalence of biometric technology in civil society has grown in recent years, with many countries using it to authenticate a person's identity before issuing passports, ID cards, voter registration cards, etc. In a nation like India with a massive and rapidly growing population, the technology has proven extremely useful for providing unique and trusted digital identities to residents. As of October 2017, the country's Aadhaar program had issued more than 1.2 billion unique IDs using biometric technology.

AIDING ALZHEIMER'S

Spain's capital Madrid is home to more than 50,000 Alzheimer's patients and some 450,000 families in the region are affected by the disease. Due to the memory loss associated with this form of dementia, there is always the risk that medical professionals will be unable to identify patients in emergencies, which means they wouldn't have access to critical medical records. To prevent this from happening, local authorities have launched a solution to offer fingerprint registration so that those suffering from Alzheimer's can be immediately identified in an emergency situation. Hospitals and ambulances are being equipped with digital fingerprint scanners to quickly and securely identify patients. The program is entirely voluntary. Patients or their guardians sign a consent form before the digital fingerprints are recorded, in accordance with Spanish data protection laws.

While patient IDs are the threads that tie all healthcare providers to their patients, it is essential to recognise the importance of healthcare provider IDs in delivering integrated care. Indeed, as healthcare data is more than sensitive, access to such data needs to be appropriately managed and this can only be done with trusted healthcare provider IDs. While patient IDs are vital to ensure coordination of care for the patient's health, healthcare provider IDs are fundamental to ensure trust and privacy for patients' peace of mind.

EFFICIENT AND SECURE ENTRY

Biometric technology can eliminate the need for logins and passwords and ease entry into restricted areas, which increases efficiency and solves many security concerns. Using fingerprint scanners to log into digital devices and iris scanners to unlock doors, medical professionals can save time and deliver faster care. And administrators no longer have to worry about forgeries and lost or stolen ID badges.

The progress made in the deployment of biometric technologies seems to indicate that multiple such technologies may be used in the future to offer more flexibility in adapting to the variety of environments in which identities needs to be authenticated in healthcare.

It is also important to pace the adoption of biometric identification with the availability of standards that ensure that the creation and access for validation of biometric identity data is open and interoperable for competitive procurements of devices and applications used in various point of care.

ABOUT COCIR

COCIR is the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries. Founded in 1959, COCIR is a non-profit association headquartered in Brussels (Belgium) with a China Desk based in Beijing since 2007.COCIR is unique as it brings together the healthcare, IT and telecommunications industries.Our focus is to open markets for COCIR members in Europe and beyond. We provide a wide range of services on regulatory, technical, market intelligence, environmental, standardisation, international and legal affairs.COCIR is also a founding member of DITTA, the Global Diagnostic Imaging, Healthcare IT and Radiation Therapy Trade Association. **www.cocir.org**

ABOUT SIA

The Secure Identity Alliance is dedicated to supporting the provision of legal, trusted identity for all, and to drive the development of inclusive digital services necessary for sustainable, worldwide economic growth and prosperity.

We bring together public, private and non-government organisations to foster international collaboration on the issues of legal, trusted identity for all, to help shaping policy and to provide technical guidance and implementation best practices for national and international ID systems.
www.secureidentityalliance.org

ID IN HEALTHCARE