intercede

SECURE HEALTHCARE PROVISION
Identity and Authentication

WHITE PAPER

Chris Edwards
Chief Technical Officer, Intercede

About the Author

Chris has over 35 years' experience within the IT industry, 18 of them at senior level within the security sector. He was responsible for the initial design of Intercede's MyID product and retains overall responsibility for the architecture and technology within it.

Chris was instrumental in making MyID the first electronic personalization system to achieve FIPS 201 accreditation as part of the FIPS201 (PIV) Approved Products List and has substantial experience of working on both US and UK government and commercial security projects.

Chris is directly responsible for Intercede's R&D team, with a special interest in mobile identities, IoT and credential convergence.

About Intercede

Intercede® is a cybersecurity company specialising in digital identities, derived credentials and access control, enabling digital trust in a mobile world.

Headquartered in the UK, with offices in the US, we believe in a connected world in which people and technology are free to exchange information securely, and complex insecure passwords become a thing of the past.

Through our MyID® software platform we have been delivering trusted solutions to high profile customers for over 20 years. Our software is used by governments, most of the largest aerospace and defence corporations, major financial services, and healthcare organizations around the world to issue and manage millions of digital identities.

For more information visit: intercede.com

Contents

2 **Introduction**

3 **Setting the scene**

3 Patients

4 Physicians, consultants, medical technicians and nurses

6 Hospital administrators

6 Hospital IT staff

6 Non-person entities

7 Health insurance providers

8 Pharmacists

8 Regulators

9 **Use Cases**

9 Employee computer and network access

10 Clinician authorizing a prescription

11 Pharmacist correcting a prescription

11 Clinician managing their relationship with insurers

12 Access to shared medical equipment

12 Identifying a patient

13 Consultant signing patient discharge records

13 Clinician and Pharmacist DEA registration

14 Pharmacist annual DEA report

14 **Potential models**

15 Core requirements

16 **Health Passports**

17 **Call to Action**

Introduction

This is the second in a series of whitepapers outlining the current state and likely direction of identity, authentication and related security issues as they affect a number of important markets. In this paper we explore the diverse and complex demands of the healthcare sector, embracing the needs of healthcare professionals, patients, regulators, insurance companies, equipment, and ancillary service providers. In particular, we examine the competing requirements for risk mitigation and convenience in the context of a number of representative use cases.

The need for an organization or system to be able to identify an individual reliably and quickly has been an element of almost every human transaction since the dawn of the human race. Until the last 40 years or so however, our society and its technology were such that relatively low fidelity methods of identification were sufficient for most cases. ('Halt! Who goes there! Friend of foe?" springs to mind).

As travel, communication and automation expanded however, traditional methods of identification were no longer adequate. We needed some form of secure, verifiable token in which we could place a high degree of trust. The first driver here was inevitably financial, with chipped bank cards emerging through the 1990s. Towards the end of the decade, the need to protect other digital assets and devices gained traction in sensitive industries such as defense and aerospace.

It would be a few years though until the importance of protecting personal data, especially medical records, would emerge to encourage large scale health providers such as the UK NHS to undertake a healthcare workers' electronic identity card program to protect patient records and medical services.

In commercial healthcare systems, an early imperative for strong authentication was seen to be the reduction in fraudulent insurance claims due to impersonation. A number of pilot schemes explored the opportunity for biometric identification to reduce the problem.

In decentralized healthcare markets such as the US however, the number of independent players has made it impossible to deploy such a universal credential so far. Policy setting organizations such as SAFE BioPharma helped by establishing trust frameworks within which providers and suppliers sign transactions and exchange data, but the widespread adoption of a convenient, interoperable secure means of identification has, until now, largely eluded the sector. The landscape has changed however, as affordable, secure technologies such as mobile authentication, ubiquitous connectivity

and convenient identity and access management platforms have matured.

This is now set to change though. A number of recent security breaches and the subsequent legal cases have introduced powerful financial incentives for the industry to fix the problem. Concurrently, we have seen ransomware attacks, faked ePrescriptions for controlled substances, growth in medical devices that need to be identified and secondary effects of medical-related identity theft escalating to the point where they can no longer be ignored as a side issue. Legislation has been introduced that will compel behavioural changes within the healthcare market to address these concerns.

Over the next few years, we can expect to see significant growth in the healthcare identity, access management and cyber-security industries and industry related standards as the players agree and implement the processes and technologies needed to operate beyond 2020. This will be accelerated by the extreme demands for remote working as we learn to live and work effectively in a pandemic-aware society.

The focus of this paper will be on the US healthcare market, although many of the observations could apply equally to other countries.

Setting the scene

As noted above, the healthcare market is hugely complicated with multiple operators within numerous categories all needing to undertake trusted, secure transactions at enormous scale.

Let's take a look at a selection of the players in this ecosystem, to see how they interact with each other and the IT data systems.

Patients

In any healthcare system, patients are at the heart of the system, with their safety of paramount concern to every health delivery organization and their suppliers. Patients own their data, which is arguably the most important asset to protect. There are two facets to this data. Firstly, we have Personally Identifiable Information (PII), which tends to be of a more general nature. Secondly, we have the more sensitive 'Protected Health information' (PHI). Although PHI has been the main focus for security, more stringent data privacy legislation means the we have to consider all PII as potentially having a high value.

In commercial healthcare systems, they have relationships with insurers – directly, via one or more employer, or through state-funded provision such as Medicare and Medicaid.

Patients clearly have relationships with the primary providers and administrators, but in many cases, this can extend to their family members. It is not uncommon for these important yet indirect relationships to depend on context too. For example, a person may have their main insurance through their employer but acquire cover for dental work via their spouse's employer's policy.

Identifying patients is important to minimise fraud through impersonation, to establish entitlement and to ensure the reliable association of each person with their medical records. The ability for each person to control the sharing of distribution of specific elements of their data is also an important principle. This may also need to reflect the level of anonymity associated with some forms of sharing (for example, to share raw information to a central statistical database while participating in a medical trial).

Physicians, consultants, medical technicians and nurses

These 'front-line' professionals are responsible for primary care delivery. This may be through consulting sessions, medical procedures or just daily care and monitoring. They all require secure access to patient records and numerous other data services such as diagnostics reports, imaging databases, appointment systems and prescribing applications.

Technicians may need to have controlled access to equipment (scanners etc.), while nurses have to record medication details and consultants need to sign-off patient discharge notes and authorize prescriptions.

One important consideration is that many devices are 'multiuser' shared devices – for example, a tablet used on a ward that is accessed by multiple individuals on different shifts. Some equipment controllers may need to be left running but 'locked' until an authorized operator authenticates.

There may also be interactions with private and state insurers to authorize payments, and liaison with post-operative convalescence and social care providers.

Hospital administrators

Administrators are responsible for a broad range of interactions that are vital to the smooth running of the

One important consideration is that many devices are ‘multiuser’ shared devices – for example, a tablet used on a ward that is accessed by multiple individuals on different shifts. Some equipment controllers may need to be left running but ‘locked’ until an authorized operator authenticates.

system. They need to access patient records so that they can arrange appointments, schedule procedures and manage in-patient resources, taking into account the specific needs of each person.

When patients arrive at a facility, administrators need to verify their identity to ensure the correct association with medical notes and financial authority.

Administrators are also the interface between a medical facility and its suppliers, directly responsible for large budgets and multiple providers of equipment and services.

Some will also of course be responsible for administering the enrolment, on-boarding and off-boarding of personnel. This may involve background checks and verification of formal qualifications.

Hospital IT staff

Medical facilities are complex IT environments with sophisticated networks and many thousands of connected devices. Securing the infrastructure is a seriously challenging problem, entrusted to IT staff, in whom a high degree of trust and authority is placed.

It is therefore of paramount importance that all privileged systems access is achieved as a result of strong authentication to achieve the necessary confidence that only authorized individuals are able to access the infrastructure for administrative purposes.

IT staff are also likely to be responsible for configuring any credential issuance and validation systems so again, strong authentication is a pre-requisite for this level of access.

Non-person entities

With equipment becoming increasingly autonomous and fully connected, we must address the identification of non-person entities with as much care as we do for actual people. This is especially important as so many of the devices operating within the network have historically paid limited attention to security.

Network devices range from biometric monitors (including wearables) through bedside units such as infusion pumps, access devices (workstations, tablets, cell phones) and communications peripherals right up to major equipment like x-ray, MRI and CT scanners.

Each one of these devices has a set of permissions and a level of authority associated with it. Can it upload to the imaging database? Can it record to this patient's log? When data is transmitted to a monitoring service, should it be digitally signed to guarantee its authenticity and integrity? The risk of a rogue device getting onto the network is clear.

Associated problems arise when you consider the need to maintain and upgrade devices. A recent NIST report highlighted the importance of improving the security of infusion pumps in this respect.

It is also increasingly common (and generally desirable) for physical access controls to share the same network infrastructure. With advances such as PKI-at-the-door and NFC capable door readers, the levels of integration needed for comprehensive identity and access management are huge.

To support these requirements, a universal means of identifying the make and model identifier of any piece of equipment is important. A possible model to emulate here is the FIDO authenticator assertion certificate.

Health insurance providers

Insurance providers also sit at a communication and transactional nexus in the healthcare ecosystem. They require trusted, secure communications with patients, employers and providers. Some relationships may be direct, others via an organization. For example, liaising with a hospital over charges for post-operative care, but directly with surgeons and consultants for clinical authorization.

The vast amount of personal data they maintain requires them to implement strong authentication and access controls for all of their employees and contractors.

This means for example that there is a need for each insurance provider to manage independently the authentication and trust relationship with each of the physicians with whom they contract.

Each US state also acts as an insurance provider in their administration of Medicare and Medicaid.

Pharmacists

Each pharmacist will have relationships with hospitals, patients, pharmaceutical manufacturers and prescribing physicians. They are also accountable to regulatory bodies who oversee the distribution of controlled substances. These people need to be able to assert their identities and authorization, but also must be able to validate the authenticity of any instructions in the form of prescriptions for example.

Regulators

Each country has national healthcare and treatment regulators – NICE in the UK, FDA in the US etc. These are responsible for overseeing the legitimate operation of healthcare delivery and in particular, the regulation and approval of drugs and appliances. The ability to verify the authenticity of drugs and other medical supplies is an important role; one that involves authentication of individuals, non-person entities and trusted manufacturers.

HIPAA compliance for the protection of patient data is a key area of regulation. It is expected that as strong authentication and access control becomes the norm, proof of compliance should get easier through continuous audit and exception reporting applications. HIPAA is administered by the Department of Health and Human Services (DHHS).

Additionally, the FDA administers the rules around product labelling, including the electronic labelling of connected devices and the listing of these within a Global Unique Device Identification Database. However, the scope of such labelling is very limited and does not relate to any form of verifiable assertion of device authenticity or identity.

Public health insurance (Medicare, Medicaid) is delivered at state level, but overseen by the Social Security Administration (SSA).

Every prescribing practitioner is assigned a 'DEA number' (by the DEA!). At present, simply knowing this number - which must appear on the physical paperwork - is sufficient to enable fraudulent impersonation for the purposes of obtaining controlled substances. Providing a means of cryptographically signing instructions with a certificate that binds to that number would be a major advance.

Looking at the above, even in this simplistic overview, it is evident that there are significant challenges with identity, authentication and trust within the healthcare ecosystem. A single federated identity approach is unlikely to work, as there are far too many one-to-one relationships that require specific

conditions and independent validation. Conversely, requiring every relationship to have a unique, dedicated authenticator creates a huge management challenge and, depending on the authenticator form factor, an impossible logistical challenge (I can only fit so many smart cards in my wallet).

To address these problems then, we will need to adopt a hybrid approach to identity, authentication and authorization. This means that we need common technical standards and a well-defined trust framework, but it must have the flexibility to accommodate multiple credential providers, federation servers for specific communities of interest, and have exceptional levels of interoperability.

The solution must also be auditable and accountable, with compliance measures to mitigate the risk of misconfigured systems and rogue actors.

Use Cases

There are a huge number of potential use cases that require strongly authenticated trust in a healthcare context. A number of these are described below to give the reader a feel for the range and scope of interactions that must be considered for such a framework. This is not intended to be an exhaustive list of cases, as any one operational area could generate an entire paper analysing the complex interactions between people, devices, physical premises and information systems. We hope however that some of the examples given will resonate with the readers' own environments and requirements.

Employee computer and network access

This case applies to employed and contracted staff working for organizations involved in healthcare. Working on the assumption that there is likely to be PHI on the network, or access to restricted services, it is reasonable to apply strong multi-factor authentication to logons and to VPN access. Additional authentication may be needed to access specific services.

The technology needed to achieve this is well tried and tested. The use of PKI smart cards, virtual smart cards (VSC) or mobile PKI over Bluetooth are all established, reliable means of access that have been in use for many years through the PIV programme. It might in general be beneficial to advise the use of PIV technology for this however, as that avoids the need for additional

middleware and is also compatible with a growing number of physical access door readers.

The basic use case for a smart card login is:

1. A user inserts their card into a reader
2. The user enters their PIN to activate signing with the private key
3. The computer verifies the signature and authenticates the use login

Extensions to this use case include:

a. Pre-login out of band secondary authentication to unlock a blocked card

b. Pre-login out of band secondary authentication to issue and personalize a new card

A related use case if that of connecting to a virtual private network (VPN) using PKI authentication. This is also readily achievable on PKI-enabled operating systems. When connecting to a VPN, the user is simply prompted to sign the request with their card or VSC, which requires a PIN input before connecting. The user experience is very simple.

Provisioning and issuing PIV cards is supported by a number of CMS platforms, making this use case simple to realize. With the forthcoming release of the updated FIPS201-3 standard, we expect the use of other form factors such as mobile and USB tokens to expand rapidly over the next few years. This presents a great opportunity to overcome the physical constraints of smart cards and move on to more flexible and appropriate authentication devices for each specific environment. This is especially important when considering their use in biologically sterile environments for example. At the forefront of alternative technologies are a large (and still growing) range of FIDO-compliant devices

The use of non-PIV smart cards (for example, mini-driver devices) and other less standardized devices is also possible, although this could limit some other aspects of interoperability.

Clinician authorizing a prescription

When controlled substances are prescribed for a condition, the clinician must authorize a pharmacist to deliver the drugs by signing the prescription. With the introduction of electronic prescriptions for controlled substances (EPCS – as regulated by 21 CFR part 1311) and the imminent strengthening of legislation in this area, there is now an important use case for digitally signing these transactions.

To achieve this, a clinician would use an application to generate an electronic form, which would then be signed with their

PKI certificate, incorporating his/her DEA number. The transaction may take place on a desktop computer, mobile device or a combination of these.

Typically, we would expect a prescribing clinician to run an application of the device of their choice and fill in the details of the instruction to be presented to the pharmacist.

The form would then be digitally signed with the clinician's certificate, which includes their DEA number as an attribute.

When using a desktop or laptop computer, a smart card or secure USB token would be needed to perform the signing operation. On a phone or tablet, a mobile PKI credential could be used.

In either case, direct client signing or indirect signing using a 'cloud resident' credential could be used, with the user strongly authenticating to the cloud service via a secondary credential on their device.

In all cases, 2-Factor Authentication must be used as a minimum to ensure the integrity and non-repudiation of the instruction.

Pharmacist correcting a prescription

Numerous studies have shown that prescribing clinicians generate erroneous prescriptions in 5 to 15% of cases. (https://ejhp.bmj.com/content/22/2/79) This worrying statistic is mitigated however through the corrections applied by the dispensing pharmacists, who trap and amend the vast majority of these errors.

This means however that there is an additional authorization process needed to ensure that prescription changes are fully accountable. The pharmacist must therefore perform a similar signing operation to the originating clinician so that the change can be clearly identified and attributed.

Clinician managing their relationship with insurers

Clinicians require secure communications with the medical insurance providers to exchange information (that include PHI) in support of claims for treatment and risk assessments for premiums.

They will typically connect to an online portal to exchange such data. However, existing password mechanisms no

longer offer adequate protection and must be upgraded to cryptographically secured 2FA models.

Each insurer has relationships with a large number of providers and must manage these accounts carefully. Hat means that each organization is responsible for account security and hence and credentials they may need to issue to enable that trust.

Conversely, each clinician will have relationships with multiple insurers, leading to the need for multiple authenticators or an agreed federated authorization service.

It is therefore expected that on attempting to access the clinical support portal, you will be asked to present your card, USB token or mobile identity to validate your entitlement. This will include the presentation of a PIN or biometric to the authentication device.

Access to shared medical equipment

Devices such as x-ray, CAT or MRI scanners typically have a control system on a dedicated computer, to which access must be managed. However, it is extremely inconvenient if operators have to log off and on to the computer between use, especially as this is likely to require a restart of any equipment management applications.

An alternative means of locking access and unblocking through a secure roles-based model is needed to optimize the secure transition of operators through a typical working day.

Identifying a patient

When a patient presents at a medical facility (or even where they the subject of a first-responder emergency), there is often a requirement to verify their identity for the purposes of association with known medical records and, potentially, to verify eligibility for treatment.

This use case can be very simple in theory – where the patient is attending a planned appointment and arrives with their proof of ID for example. Even here though, identity verification to prevent fraud is important, as mistakes at this stage can have far-reaching consequences. Existing paper-based solutions are becoming increasingly insecure, as fraudsters can fabricate false documentation with relative ease.

It must be recognized however, that in more extreme situations, such as where the patient is unconscious or does not carry any formal ID, this can be very difficult to assert with any level of confidence. A mobile phone with verifiable identity credentials available from the lock-screen may provide a useful solution here. These are currently limited to basic textual data, so therefore have limited authentication capability.

Supply chain management

Each facility's supply chain needs to be secured against fraudulent access. This applies to hospitals, trauma centers, pharmacies, laboratories, and numerous other establishments. With service portals becoming more commonplace (e.g. https://www.supplychain.nhs.uk/), being confident in the identity of a visitor to the website is an important step to improving overall system security and confidentiality.

These portals handling procurement, bid submissions, orders, tracking, returns and many other aspects of the supply of goods and services to a healthcare facility.

Given the large sums of money involved, a secure authentication solution is needed. When a supplier accesses the portal, they will be changed to present a strong credential that maps them to their account on the system. A self-registration scheme may also be needed. In most cases it is expected that the hospital themselves will manage the association of an issued credential with an actual account held on the system.

Consultant signing patient discharge records

When a course of in-patient treatment has concluded, a clinician will complete and sign a 'patient discharge' form. This will often be bound to a prescription for ongoing medication and then forms part of the patients' medical records. Discharge forms may be cited in medical negligence cases or health insurance claims, so strong non-repudiation is important. A move towards digital signatures would be very beneficial for this situation.

Clinician and Pharmacist DEA registration

Every prescribing clinician and pharmacist has a unique DEA number that is used to identify them on prescriptions for controlled substances. At present, anyone discovering a valid DEA number is potentially able to generate fraudulent prescriptions. There would seem to be little if any emphasis on treating the DEA number as sensitive data, as it must appear clearly on paper prescriptions.

It would be highly beneficial if each practitioner were to be issued with a cryptographically secured credential that asserts their DEA number.

Pharmacist annual DEA report

Each year, pharmacists are obliged to generate inventory reports of all controlled substances. To maintain integrity and authenticity, it would be appropriate to digitally sign these reports.

Potential models

The United Kingdom National Health Service (NHS) solution to this challenge only needed to address a small subset of the problem. It was able to roll out a universal smart card (the 'SPINE' card) to all 1.3 million NHS employees, and use a single, private certification authority to authenticate users, with an authorization token to grant access to resources. This could be used to authenticate to computers, networks and services, but was also extended into applications such as document signing for patient discharge records and prescriptions at some facilities.

This simple model was only really feasible due to the public ownership of the NHS and the principle of universal access, free at the point of delivery. That would clearly not work in the USA today.

If we look at existing multi-player strong authentication solutions, one obvious starting point is the US Federal PIV programme. This was based on the 'federal Bridge' PKI hierarchy, with common, enforced standards for identity proofing, credentialing processes, smartcards and (more recently) mobile credentials. It is especially pertinent as some federal agencies play a major role in the regulation and delivery of healthcare in the US (FDA, DEA, VA, SSA).

This has been largely successful, but the concept falters when you try to make a comparison with the healthcare market. The absence of an overarching body with the power to compel so many different players to agree such a universal set of processes and technologies makes the federal government model potentially unworkable. At best, it could take many years to agree on standards. As if to reinforce this, the government recently decoupled the bulk of the healthcare PKI infrastructure from the federal bridge due in part to the challenges of ensuring universal policy compliance.

There are however some essential authorities that will need to be universally recognised. Oversight of the Electronic Prescription of Controlled Substances (EPCS) legislation by the DEA demands a tightly managed identity and credentialing process for clinicians and pharmacists for example. When we look at medical equipment and drugs, the FDA is responsible for regulation and approval.

Core requirements

So, let's itemize the core requirements for a viable identity and access management solution for the healthcare market. If we take the lessons learned from PIV, we can shortcut a lot of the evolutionary steps to accelerate delivery.

It would appear that we need to meet the following goals to achieve the desired objective of a proportionately secure, efficient health delivery system:

1. Agreed levels of authority needed for each business function or transaction
2. Agreed levels of identity proofing for each level of authority
3. Minimum standards of authentication – 2-factor, probably aligned with NIST SP800-63
4. Multiple form factors for authenticators – cards, hardware tokens, mobile devices, virtual smart cards
5. Controlled release of personal data so that privacy can be maintained
6. Agreed standards for federated authorization servers and token content
7. PKI as the preferred format, but also allow privacy-enhanced formats such as FIDO
8. Mix of credential issuers to service large (dedicated) and small (shared) consuming organizations
9. An approval / trust framework accreditation scheme for identity and access service providers
10. High integrity root of trust for medical devices approved by the FDA
11. Prescription signatures to meet EPCS rules enforced by the DEA
12. Strongly authenticated logon to equipment and networks from a range of client devices
13. Physical access to buildings and other secure areas
14. Extensive lifecycle management of credentials in a range of form factors

15. Efficient, cost-effective credential management processes – preferably self-service

16. Compatibility with related identity ecosystems and shared services – for example, mutual recognition of credentials to administer pharmacist registration details.

From the above it is clear that a large amount of work is needed on the policies and practice statements. Fortunately, there may be a reasonable baseline for this
in the existing SAFE BioPharma trust framework that has been operating in the pharmaceuticals industry for many years. This obviously will need a lot of extensions and alterations, but it may well reduce the scale of the overall task.
Similarly, we should be able to leverage the work done by NIST on identity and authentication to provide the definitions and templates for identity proofing and authenticator implementation. Ideally, these would be a direct reference to the imminent FIPS201-3 driven standards for the broadest possible set of devices and processes.

Existing software products such as Intercede's MyID can comfortably fill the role of credential manager, while there are numerous enrolment and identity verification solutions that could provide consistent levels of trust based on specified breeder documents.

It is important to determine the rules that will directly impact the hardware and software needed to support the final scheme at an early stage in development, so that engineering work can proceed in parallel with policy discussions. In doing so, we must also consider emerging standards in other industry sectors such as the mobile driver's license (ISO18013-5), as this is likely to become a de facto proof of identity for many use cases.

Health Passports

With the emergence of the COVID-19 pandemic, the need for a universally recognised and verifiable 'health passport' is becoming more apparent. This must of course rely on technology to strongly bind such passports to the bearer and to provide standards-compliant, convenient ways to verify the authenticity of the credential when it is presented. However, the solution should protect privacy as far as possible. There is no need to expose an individual's identity to anyone wanting to check a vaccination status for example – the passport holder should only need to present a verifiable photograph bound to the vaccination certificate without revealing any other personal information.

This will need infrastructure and services in place to support identity proofing, credential issuance and verification. Different form factors will be needed as a reliance on mobile phones would disenfranchise large numbers of people.
In the absence of any viable, global standards however, it is likely that a plethora of solutions will be developed in parallel that aim to solve the problem within a specific geopolitical region. Without agreed standards on interoperability and level of assurance, they will though be of limited use when it comes to international travel for example.

It may be more effective for each national government to provide a verification service that can confirm vaccination status against an individual's national passport. This would be acceptable in locations such as national borders where passport or national ID card is expected, but is likely to meet resistance in more local settings where privacy concerns and the inconvenience of carrying your passport would be prohibitive.

In these cases, the ability to derive a verifiable credential from your official national record may be a route to take. In the same way that a secure mobile PIV credential can be generated based on a one-time assertion of your primary PIV card, it would be possible for a national service to deliver a verifiable 'vaccination certificate' through an app that only shows the owner's photograph and status, with a scannable barcode to validate against the service. This is not dissimilar to current implementations of Mobile Driver's Licenses.
This highly topical aspect of healthcare security will undoubtedly focus a spotlight on secure identity technology providers and regulators as the world tries to get back to some semblance of normality in the wake of the pandemic.

Call to Action

Once the ground rules for policy and processes have reached a reasonably stable state, it will be possible to start work on the necessary infrastructure for delivery.
To deploy a coherent, industry-wide solution we need to build out services, hardware and software components to fulfil each of the requirements. This will include:

- Identity proofing services (shared and private)
- Certification services and associated infrastructure

- Credential issuance and management services (shared and private)
- Federated authentication and authorization services (public and local)
- IAM components for devices (apps, credential providers, client modules)
- Compliance and interoperability testing
- Business applications to create / extend for the new credentials and authenticators
- Interoperable 'health passports' to enable unrestricted global travel and local access

Constructing this sort of ecosystem at scale is a significant undertaking that will require high levels of collaboration between all of the players in the healthcare market. This inevitably requires major strategic investment in policy definition, legislation, software, hardware and services. The big question is 'who pays'?

Healthcare spending per capita in the USA is the highest in the world by a considerable margin, but with a high proportion of that expenditure being commercially driven, adopting the sort of standards necessary to achieve the security, integrity and privacy aims of such a programme will inevitably rely on legislation to require compliance to agreed standards.
In the case of national and international health passports, it seems likely that these will require national, government-driven initiatives to realize. In turn, international standards bodies will have to be involved to ensure high levels of trust and interoperability.

In much the same way that PIV standards were defined, and compliant systems deployed, there needs to be a coordinated strategy to evolve the regulatory systems that are in place today. They must address an increasingly complex and threatening cyber world where malicious actors have already shown no respect for the norms of a civilized society in pursuit of their criminal goals. Technology providers are ready to meet this challenge now – we just need an agreed strategic direction coupled with the political and commercial desire to deliver the solution.

Acknowledgements

I would like to thank Kyle Neuman, Managing Director at SAFE Identity for his contribution to this white paper.

Through SAFE Identity's work on digital identity and cryptography in the healthcare sector, Kyle is well versed on the important considerations and challenges healthcare organizations face.

SAFE Identity is an industry consortium and certification body who support the advancement of digital identity and cryptography in healthcare by enabling trust of digital credentials.

intercede

@ intercedeMyID

e info@intercede.com

w intercede.com

UK

Lutterworth Hall, St. Mary's Road,
Lutterworth, Leicestershire
LE17 4PS UK

t +44 (0)1455 558 111

US

Suite 920, 1875 Explorer Street,
Reston, VA 20190 USA

t +1 888 646 6943