IDC Technology Spotlight

Sponsored by: **Imprivata**

Authors:
Silvia Piai
Giulia Besana

May 2019

Security at Scale: How Security Changes with Healthcare Digital Transformation

Digital Transformation in European Healthcare: Where are We?

When it comes to digital transformation (DX), European healthcare organisations are at a crossroads. From a vision standpoint, they recognise DX's relevance in achieving greater value for patients in terms of outcomes, safety and experience. They appreciate how DX enables them to be able to measure where and how this patient value is created, and how to use these insights to transform and realign skills, processes and investments to maximise this value. When we look at the execution, however, this bold vision remains unfulfilled. Many European healthcare organisations are still mired in a digital deadlock, where the digital and the enterprise strategies are out of sync. Very few of them are truly data-driven, evidence-based organisations. A recent IDC survey shows that 68% of European healthcare organisations still consider their approach to digital transformation siloed, and, even when digital and enterprise goals are aligned, they are too focused on the short term.

These organisations are digitally distraught. The misalignment described above is driven by the lack of an enterprise model that defines enterprisewide objectives, accountability, integrity, talent, performance and risk governance around digital transformation. These organisations do not have the solutions in place to scale the benefits delivered by digital in some parts of the organisation, across the whole enterprise, with patients and the broader ecosystem they are working with.

Navigating the road from digital distraction to digital determination requires a high degree of mastery in accessing, managing, analysing and leveraging information.

Navigating the road from digital distraction to digital determination requires a high degree of mastery in accessing, managing, analysing and leveraging information. To drive patient value in terms of outcomes and experience, healthcare organisations rely on coordination, collaboration and integration across professionals, workflows and processes. The new digital platform should be conceived both as an internally and externally facing technology architecture where the key objective is to create an ecosystem of connected patients, employees, partners and suppliers that use the information and services available to them.

Healthcare organisations, however, have to deal with the most personal, most sensitive data — patient information. It is no surprise then that European healthcare providers consider ensuring data privacy and security a key challenge to — and a key imperative for — digital transformation. The healthcare information security model clearly needs to evolve and adapt to the needs of the DX platform. A DX security strategy needs to provide the foundation for the necessary level of "digital trust" among stakeholders and the organisation to address challenges that affect both the perceived risk and reputation of an organisation.

Challenges for Healthcare Providers in Securing the DX Platform

The unparalleled availability of technologies, new data sources and the enablement of dynamic organisational models is posing a threefold challenge to European healthcare organisations that want to secure their DX platform.

Ensuring Compliance with a Swelling Regulatory Environment

The recent enforcement of the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS) has made patient data rights more actionable, introduced more stringent requirements on data privacy, infrastructure security and business continuity provision, and has set substantial fines in case of a breach. For example, in July 2018, a Portuguese hospital was fined €400,000 by the Data Protection Authority for security deficiencies and inadequate identity access management. According to the authority, the hospital staff had access to patients' files and health-related information through false profiles, and physicians had unrestricted access to all patient files, regardless of the doctor's specialty.

Ensuring Clinical Experience When Safely Using Technologies

Clinicians frequently report challenges in the usability of healthcare applications: access to them is time consuming and distracting and requires frequent password changes to maintain security. Time spent by the medical staff in application access, password resetting and IT support requests critically hinders operational efficiency and impacts patient experience, direct care resources availability and — ultimately — clinical outcomes.

Time spent by the medical staff on application access, password resetting and IT support requests critically hinders operational efficiency and impacts patient experience.

In this environment, patients' data safety depends on access authentication and identity management compliance. Healthcare workers can enter up to 10 passwords to access different applications during their practice, and security requirements are often different for each one. As a result, doctors can be stuck in time-consuming, user-unfriendly multifactor authentication to access the EHR system, while having to change an expired password to access the pharmacy management system.

In fact, most of the time, complexity and frequent changing of passwords are basic security requirements, but those security measures make it hard for users to remember credentials. This easily leads to shortcut solutions and non-compliant ways to avoid the pain and struggle of authentication, such as sharing credentials or creating new authorised user accounts.

Adapting the Implementation of the Security Model to the New Computing Paradigm

Healthcare organisations increasingly require flexible technologies that can adapt to users, devices, environments and different levels of risk across assets and resources. The migration towards virtualised, cloud-based systems, coupled with the need to concurrently manage and protect different computing environments, devices and users, is leading to a fragmentation of the security framework that increases risk and costs.

For example, as AI technologies are increasingly adopted, what it means to be a user is no longer easily defined, with resources in the healthcare organisation and in its ecosystems that are both physical and virtual and, in many cases, software defined. The high level of mobility introduces a new threat to the traditional notions of "inside" or "outside" a trusted organisational perimeter. Boundaries are no longer easily defined, and the distinction between "inside" and "outside" are becoming insignificant when building a security strategy.

Security at Scale: The New Security Model for the DX Platform

These challenges show us how it is essential to reconsider and extend security to embrace the needs of DX, including scalability, speed, privacy and relationships. Patient value generation goes hand in hand with security and information governance capabilities, as they impact the quality of the work of the medical staff, the accuracy and integrity of information used in the care process and the trustworthiness of the organisation in safeguarding patient data rights.

According to the *IDC European Vertical Market Survey 2018–2019*, the main information security priority for European healthcare providers is the implementation of new regulations, such as GDPR, with almost 40% of respondents mentioning identity and access management (IAM) as a priority. The GDPR enforces IAM management through articles 5, 24 and 32, where it discusses personal data processes, organisational security measures and data loss/unauthorised access risk management.

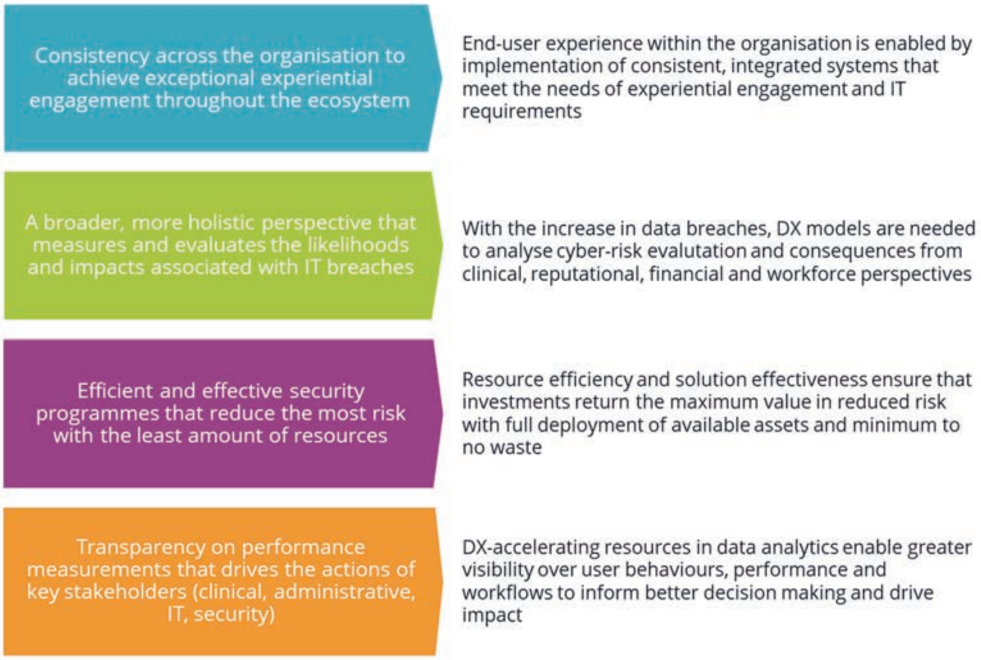
All European countries are adapting their data protection and data security frameworks, in line with GDPR. Sweden, for instance, has been revising its Patient Data Act and countries such as Germany, France and Italy are publishing guidelines and recommending best practices to help healthcare organisations define what is state-of-the-art technology implementation and adopt a security-by-design approach to comply with GDPR.

Designing security outside of a DX strategy puts the potential for return on investment at high risk, as it weakens the possible impact of new solutions and technologies, creates unnecessary process interoperability issues and, due to the misalignment with the broader environment, ultimately increases the vulnerability of the organisation.

DX calls for a new information management governance and security-by-design model that answers the need for consistency, comprehensiveness, efficiency and transparency (see Figure 1).

DX calls for a new information management governance and security-by-design model that meets the need for consistency, comprehensiveness, efficiency and transparency.

Figure 1
Information Governance and Security Needs in the DX Platform



Consistency across the organisation to achieve exceptional experiential engagement throughout the ecosystem	End-user experience within the organisation is enabled by implementation of consistent, integrated systems that meet the needs of experiential engagement and IT requirements
A broader, more holistic perspective that measures and evaluates the likelihoods and impacts associated with IT breaches	With the increase in data breaches, DX models are needed to analyse cyber-risk evalutation and consequences from clinical, reputational, financial and workforce perspectives
Efficient and effective security programmes that reduce the most risk with the least amount of resources	Resource efficiency and solution effectiveness ensure that investments return the maximum value in reduced risk with full deployment of available assets and minimum to no waste
Transparency on performance measurements that drives the actions of key stakeholders (clinical, administrative, IT, security)	DX-accelerating resources in data analytics enable greater visibility over user behaviours, performance and workflows to inform better decision making and drive impact

Source: IDC, 2018

The Role of IAM Solutions in the New Security Strategy for Healthcare DX

Identity and trust are two of the key disciplines that define how security strategies need to be applied to the new DX platform throughout its core and all service areas. Identity management ensures that the organisation can validate the source of activity and control users' access to resources. Trust management is about strengthening the legitimate source of activity. It enables technology-enabled and technology-prompted actions to be made because their digital identities have been authorised, just as a person's would be. In this way the DX platform ensures the key objectives of confidentiality, integrity and availability of information, as well as the productivity and efficiency of systems.

To serve the current need for control over patient information access and use, the new generation of IAM solutions in the market build on these two disciplines. IAM is a comprehensive set of solutions used to identify users (employees, patients, contractors, etc.) in an IT environment, and it's used to control their access to resources within that environment by associating user rights and restrictions with the established identity and assigned user accounts. The solutions leveraged for identity management include provisioning, access governance, multifactor authentication, single sign-on with federation and user behaviour analytics.

IAM functionalities can be summarised into four basic areas:

- Identification: Any user within a healthcare organisation, even across different locations, accessing sensitive data has to clearly disclose their identity.

- **Authentication:** Verifying users and their access to the information system can be done through something that the user knows (e.g., a password), something that the user has (e.g., a key or token) or through the user's fingerprint, iris or other biometrics.
- **Authorisation:** The variety, complexity and specificity of data requires that healthcare professionals are granted access only to the data they require to perform their activity.
- **Governance:** The monitoring of IT resources for performance, compliance and risk management.

Combining the concepts of identity and trust, these solutions are better suited to help healthcare organisations consistently address the risks arising from their complex and interdependent IT and organisational settings, building transparency and increasing efficiency. They enable the move away from the reactive and compliance-only driven approach, building a DX security model that leverages capabilities such as dynamic and risk-based authentication and identity federation.

Dynamic authentication applies various techniques for user and device validation during normal operations and the use of systems, often in response to perceived changes in risk, leveraging user behaviours and predictive analysis. This new generation of IAM solutions can be better integrated with new multilayered computing platforms as they are built on cloud-based architectures enabling greater speed and flexibility in providing centralised access and authentication policies across the organisation's endpoints.

Changes in healthcare service delivery models, as in the case of integrated, value-based care, requires collaboration of professionals belonging to different departments and entities. Identity federation enables users to share their ID with the healthcare organisation and easily gain access to more than one application with one sign-on. This gives them easy access to a complete view of patient information needed to safely deliver care while remaining compliant to the data security requirements.

The solutions supporting the IAM strategy need to build on each other's strengths and capability to support the healthcare organisation's evolving needs. For example, Bolton NHS Foundation Trust recently started implementing its eObservations project, a system that enables it to record and store patients' vital signs, via mobile devices. The trust has already been using Imprivata's IAM solutions (Authentication Management, Single Sign-On and Virtual Desktop Access) to improve access to the hospital information systems. As the clinical workforce was used to accessing virtual desktops only by tapping their NHS smart card, the trust worked with Imprivata to ensure that mobile access was built on the same seamless and user-friendly approach. In five weeks, the trust tested and added Imprivata Mobile Access to its eObservations system.

> *"It took no time for our clinicians to use the system."*
>
> Phillipa Winter
> CIO, Bolton NHS Foundation Trust

According to Phillipa Winter, chief informatics officer at Bolton NHS Foundation Trust, "It took no time for our clinicians to use the system, as the experience is seamless and very coherent with what they are used to." The system simplifies system access without weakening security processes or breaching audit requirements. Easy access to resources enables healthcare professionals to accurately record observations and share them in real time, enabling timely interventions when needed. As the trust continues to evolve in its role within the Greater Manchester Health and Social Care Partnership, it wants to scale up the benefits it has achieved with its IAM strategy. It is now working towards building a secure and compliant shared information governance environment, in which appropriately identified and authorised healthcare professionals belonging to different organisations and care settings will be able to share information and collaborate efficiently and securely.

Moving Beyond the Digital and Real Dichotomy: Clinical and IT are Driving and Measuring IAM Value Together

Despite its essential role in enabling the DX platform, security is still perceived as a domain where IT has exclusive decision ownership and responsibility. Security is still one of the key areas where the dichotomy between the decisions governing the organisation and the delivery of healthcare services (the reality of healthcare processes and their stakeholders) and the decisions on the "digital side" of data and related information technologies persists.

Security is still one of the key areas where the dichotomy between the decisions governing the organisation and the delivery of healthcare services and the decision on the "digital side" of data and related information technologies persists.

This separation is evident when it comes to the selection and implementation of solutions for the implementation of a security strategy, such as IAM. True digital transformation is realised when digital and enterprise strategies form a single coherent road map led with a clear mission and formal accountability. Misaligning the security strategy and the business strategy, particularly regarding its identity and trust components, impacts healthcare organisations' ability to advance more rapidly in the DX journey.

The misalignment not only increases the liability risk of the whole organisation, but also impacts patient safety and experience, affects the productivity and efficiency of clinical workflows, and endangers the digital trustworthiness of the organisation. Healthcare organisations that are at more advanced stages of digital transformation are those that have shifted their security focus, moving from a fragmented and reactive compliance approach to a more balanced, business-aligned and proactive strategy. The shift from a "surviving" to a "thriving" digital strategy has shown how balanced and organised security dynamics can foster organisational efficiency, cut costs and improve outcomes.

Organisations with a forward-thinking approach to DX know the value of IAM and see the implementation of IAM solutions as key capabilities for the readiness of the digital platform in supporting the business strategy. They approach identity management risks as business risks. For example, GDPR forces healthcare organisations to be responsible for ensuring full auditability, providing transparency, traceability and reproducibility of any authentication. With IAM, healthcare organisations can not only audit data available and recover and reconstruct an access attempt to verify its regulatory compliance, but can also use this information and analytics capability to gain greater visibility into and control of access, workflows and users behaviours. These insights better inform their decisions and help them design strategies to proactively fill existing gaps and protect from potential harm, thereby optimising their risk management.

Building a Value-Driven Business Case for IAM

The strategic alignment of clinical needs and IT transformation brought about by DX is redefining how leading healthcare organisations manage the internal discussion around value generation.

The IAM value-generation process underpins the co-creation of a meaningful, efficient and secure workflow structure that directly and consistently impacts the everyday work, interaction and success of all stakeholders in the healthcare organisation environment. The system of priorities and needs in the healthcare environment varies across professional groups and individuals. Value at work for:

- **Healthcare staff** relates to the ability to perform care tasks in an easy, secure and efficient way, ensuring the highest quality of care to the highest number of patients. Timely, easy access to secure and accurate data can be life-saving for patients and can determine failure or success for the entire care team, impacting different professionals simultaneously.
- **Organisation executives** is based on several factors relating to reputational, care quality standards, financial return on investment and future outlook of the organisation in the short, medium and long term.
- **IT executives** is dependent on the solution capability to ensure compliance to the broader spectrum of security requirements, to be consistent within broader and varied enterprise IT infrastructure, and to be sustainable over the long term while ensuring usability for the internal stakeholders they serve.

It is therefore essential for senior technical executives responsible for implementing the technology to ensure that the guiding principles in the design of enterprise IAM projects are co-developed in partnership with medical, administrative, logistics, laboratory and senior management professionals. Every player approaches the common goal of patient value from a substantially different vertical perspective. This offers an opportunity for senior IT executives to segment and address each priority through a comprehensive and coherent model that embraces the full set of processes and needs of the organisation.

It is essential for senior technical executives to ensure that the key guiding principles in the design of enterprise IAM projects are co-developed with medical, administrative, logistics, laboratory and senior management professionals.

Defining how IAM will bring value and enabling "security at the speed of business" requires organisations to prioritise the discussion around the preferences and priorities of an organisation's end users, how their different information needs will be accommodated and how clinical workflows can be transformed to optimise outcomes. Only then can the technical requirements be better defined.

This collaborative approach to IT transformation ensures that all players are involved, thereby contributing to the definition of the business case for IAM. The business case will be pragmatically built on a broader sharing and understanding of the challenges, pain points and opportunities that IT can effectively and easily tackle with the solutions available on the market and by tailoring those to the needs of each professional group.

Focus on Workflow Transformation and KPI Identification

To appreciate the impact of IAM solutions and to identify organisation-specific KPIs to measure the success of the implementation, healthcare organisations will need to analyse clinical and administrative workflows in depth.

This includes activities such as mapping, timestamp data analysis and department walkthroughs. All these should be done by simultaneously engaging technical and clinical stakeholders, as well as department management. By ensuring that technical and clinical stakeholders work together on clinical workflow analysis, organisations can assess the gap between optimal, desired workflows and actual workflows. This will help organisations to determine the essential requirements and assess what resources are already available and can be further leveraged. It is essential to identify project champions — from both disciplines — who will support the rollout of the solution and be able to articulate the business value of the initiative.

This was the approach taken by Leeds Teaching Hospital NHS Trust. The trust is committed to maximising the value of EHRs to support and improve care, and making the creation and use of patient information at the point of care easier is a key enabler of this vision. By engaging in discussions with healthcare staff, the trust's IT management was able to define the requirements of a solution that would enable it to securely connect medical devices to EHRs without slowing down healthcare staff workflow with multiple passwords and other identification techniques.

Since 2012, the trust has been using Imprivata Single Sign-On and Authentication Management solutions to ensure quick access to the EHR system in both mobile and desktop environments. Using the solution, healthcare professionals can open patients' EHRs in 3 seconds by scanning the barcodes printed on their wristbands, while the Single Sign-On solution identifies the professional.

To connect medical devices, the trust added the Imprivata Medical Device Access module to the platform. It started with the renal unit, where nurses can now walk to the dialysis machine, tap an RFID badge, access the patient's EHR via their smartphones, and upload the observation data directly from the machine. The solution has reduced the time wasted and the conflict of information, and has helped to create a richer observation data set that can be shared with all professionals involved in the patient's care. Nurses' observation frequency and accuracy increased from 55% to 97.5%.

Hemodialysis patients have a greater risk of cardiovascular disease, and after implementing the solution, the Leeds hospital has reduced the number of cardiac-arrest events. Higher frequency and accuracy of observations enables the hospital to identify earlier and then intervene when patients' conditions deteriorate. The Leeds example shows how having the clinical staff onboard in the system design is critical when it comes to achieving benefits not only from a security practice standpoint but also in how the IAM solution can contribute to care quality and clinical outcomes.

Challenges in the IAM Solutions Offering Space

When healthcare organisations choose to engage with an IAM vendor, they should keep the following considerations top of mind:

- IAM should be integrated into security architectures and the broader digital security strategy. Healthcare organisations need to be aware of consistency and interoperability risks.
- Healthcare providers' typical architectures are complex environments that try to accommodate the different needs of legacy and new applications (with large sets of APIs and several integration tools to manage) that can be run in the cloud, on-premise, etc. Not all IAM solution vendors can support this complexity.
- User behaviour analytics is becoming a popular item, but identity-driven context analytics for user behaviour is not as mature and transformational as many vendors claim.

IAM is a collection of solutions. Healthcare organisations need to define what they consider to be key requirements and look for vendors operating in the IAM market that offer products that are specific to the required functional areas. Few vendors offer solutions in all market segments. Those that do tend to have functional areas of expertise and might have products with different technological maturity.

Healthcare organisations need to define what they consider to be key requirements and look for vendors operating in the IAM market that offer products specific to the required functional areas.

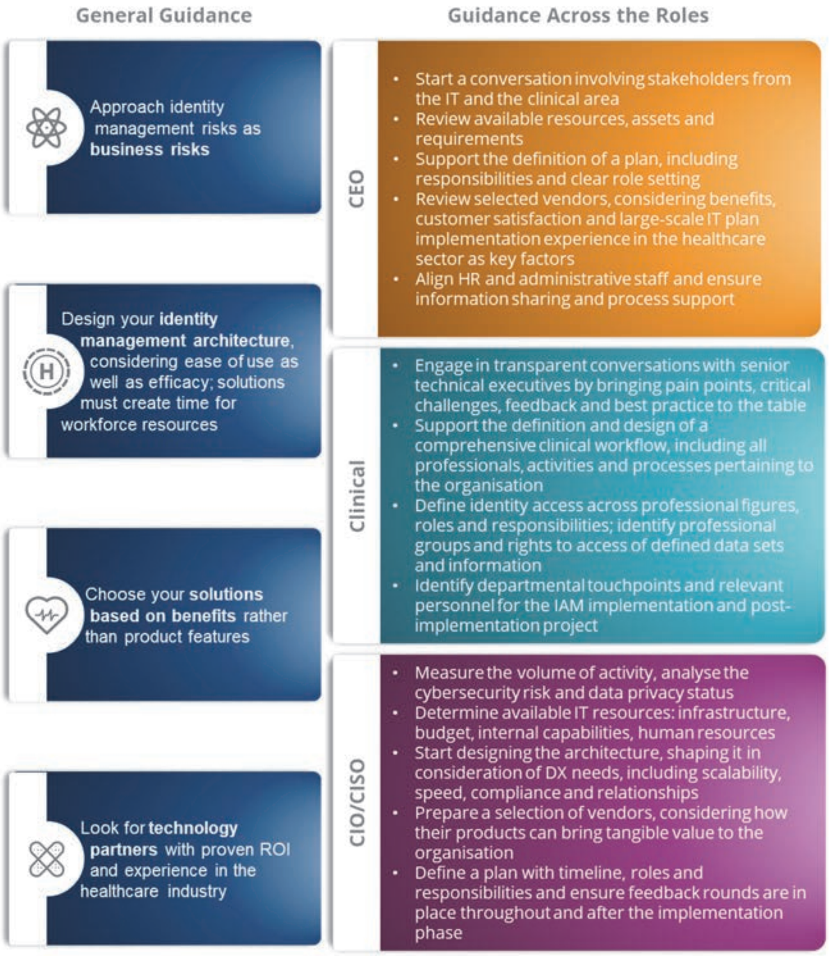
Healthcare organisations need to make sure that the vendors they engage with have specific expertise and experience in supporting implementations comparable to theirs. This should not just be a general reference to "healthcare experience", but a proven track record with organisations that are similar in size and technological maturity.

With each vendor comes a risk related to the challenges it faces as a company. Healthcare organisations should therefore look at criteria such as vendor financial viability and performance, frequency of senior management changes, talent acquisition policies, commitment to product development, and recent divestures and mergers and acquisitions.

Guidance for Technology and Business Leaders When Defining and Implementing Their IAM Strategy

The whole collaborative, business-value-driven process described above should be guided and inspired by the general and role-specific guidelines set out in Figure 2.

Figure 2
Guidance for Defining and Implementing an IAM Strategy



General Guidance

Approach identity management risks as **business risks**

Design your **identity management architecture**, considering ease of use as well as efficacy; solutions must create time for workforce resources

Choose your **solutions based on benefits** rather than product features

Look for **technology partners** with proven ROI and experience in the healthcare industry

Guidance Across the Roles

CEO

- Start a conversation involving stakeholders from the IT and the clinical area
- Review available resources, assets and requirements
- Support the definition of a plan, including responsibilities and clear role setting
- Review selected vendors, considering benefits, customer satisfaction and large-scale IT plan implementation experience in the healthcare sector as key factors
- Align HR and administrative staff and ensure information sharing and process support

Clinical

- Engage in transparent conversations with senior technical executives by bringing pain points, critical challenges, feedback and best practice to the table
- Support the definition and design of a comprehensive clinical workflow, including all professionals, activities and processes pertaining to the organisation
- Define identity access across professional figures, roles and responsibilities; identify professional groups and rights to access of defined data sets and information
- Identify departmental touchpoints and relevant personnel for the IAM implementation and post-implementation project

CIO/CISO

- Measure the volume of activity, analyse the cybersecurity risk and data privacy status
- Determine available IT resources: infrastructure, budget, internal capabilities, human resources
- Start designing the architecture, shaping it in consideration of DX needs, including scalability, speed, compliance and relationships
- Prepare a selection of vendors, considering how their products can bring tangible value to the organisation
- Define a plan with timeline, roles and responsibilities and ensure feedback rounds are in place throughout and after the implementation phase

Source: IDC, 2019

Healthcare's IAM Partner: Imprivata

Imprivata, a healthcare IT security company, provides healthcare organisations globally with an industry-specific platform that addresses critical compliance and security challenges related to IAM. Imprivata aims to establish trust and streamline clinical workflows by offering solutions for:

- Identity governance
- Enterprise single sign-on
- Multifactor authentication
- Positive patient identification

Imprivata partners with European healthcare providers looking to optimise secure access to patient information at the point of care by offering the following:

- **Enterprise single sign-on solutions:** Imprivata OneSign is designed to ease access to clinical information systems while ensuring secure, no-click access to patient information. Solutions in this area support authentication, single sign-on, virtual desktop access and mobile device access (integrating with Citrix and VMware environments, for example).

- **Multifactor authentication:** Imprivata Confirm ID and Imprivata Medical Device Access together comprise an identity and multifactor authentication platform that establishes clinical authentication workflows including remote network access and access to cloud applications, Windows servers and desktops, and other critical systems and workflows. The solutions enable the replacement of passwords with more convenient methods such as tapping a proximity badge, swiping a fingerprint or hands-free authentication. They also integrate with leading EHRs and other clinical applications provided by vendors such as Cerner and Epic. For these vendors, Imprivata also offers EHR workflow optimisation solutions.
- **Identity governance:** Imprivata Identity Governance supports the enforcement and control of user entitlement policies to meet organisations' compliance obligations. The solution replaces manual administering of user accounts with a combination of secure, role-based access controls, automated provisioning and deprovisioning, streamlined auditing processes and analytics that enable faster threat evaluation and remediation.
- **Imprivata IAM:** The complete, integrated platform brings together Imprivata Identity Governance, Imprivata OneSign and Imprivata Confirm ID to provide an integrated solution for automated identity management and secure no-click access in clinical systems and applications supporting clinical workflows.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions:

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com.