UBISECURE®

Connecting Identity.
Transforming Digital Business.

Europe's healthcare sector

How Customer IAM drives digital transformation and information security

UBISECURE

Contents

Europe's healthcare sector

The healthcare sector is undergoing a rapid rate of digitalisation. Not only is there pressure on existing health services for digital transformation, but new players are also seizing the opportunity to bring forward new digital-first solutions.

While this is true for almost all sectors, healthcare poses unique challenges when it comes to digital transformation, notably in the areas of security, regulatory compliance, user experience and operational efficiency. Many of these relate to digital identity – how you identify and manage digital users.

In this white paper, we'll look at each of these areas in more detail, considering challenges such as:

- **Security –** high risk of data breach as protected health information (PHI) is most valuable to hackers, thus trust in who/what is accessing systems is critical. There is often the physical challenge of shared devices – many users using the same device in a healthcare setting.
- **Regulatory compliance –** from a European perspective, complying with the GDPR across often-complex IT infrastructures.
- **User experience –** services must be frictionless for all users, across locations and devices, to ensure high uptake and realise the benefits of a digital solution.
- **Operation efficiency –** facilitating access for a variety of stakeholders; "users" may include internal staff, external individuals and organisations, and connected health devices (Internet of Things, IoT).

> CIAM goes beyond internally focused IAM with specialism in external use cases

Many of these challenges can be solved with the use of a Customer Identity and Access Management (CIAM) solution. CIAM goes beyond internally focused IAM with specialism in external use cases (patients, citizens, partners, remote staff, devices), thus making it highly leverageable to healthcare organisations. CIAM covers a set of capabilities aimed at seamless and secure identification and management of who is accessing services and the level of access within those services. These capabilities include single sign-on (SSO), multi-factor authentication (MFA), identity providers, self-service account management and delegated administration.

So how do these capabilities help healthcare institutions with digital transformation and creating new eHealth solutions? Let's have a closer look at four key areas: security, regulatory compliance, user experience and operational efficiency.

Security

> Healthcare data is the most valuable on the black market

DATA BREACH RISKS

- regulatory non-compliance fines
- time and money spent resolving issues
- negative media
- loss of good brand reputation
- victim distress

Robust security is important for any digital service, but eHealth in particular must prioritise systems security as it is a popular target for bad actors. In fact, one **Trustwave report** found that healthcare data is the most valuable on the black market - up to $250 per record, compared to $5.40 for the next highest value record (a payment card).

The risks of a data breach to organisations include regulatory non-compliance fines, time and money spent resolving issues, negative media and loss of good brand reputation – not to mention victim distress. A **recent case in Finland** saw a private psychotherapy centre's database breached. A significant amount of sensitive client data was stolen, which attackers used to attempt to extort money from victims by threatening to make the information public. With a trial on the way, the CEO and board have been held personally responsible for tens of millions in damages; sadly, money won't bring back the privacy of the patients.

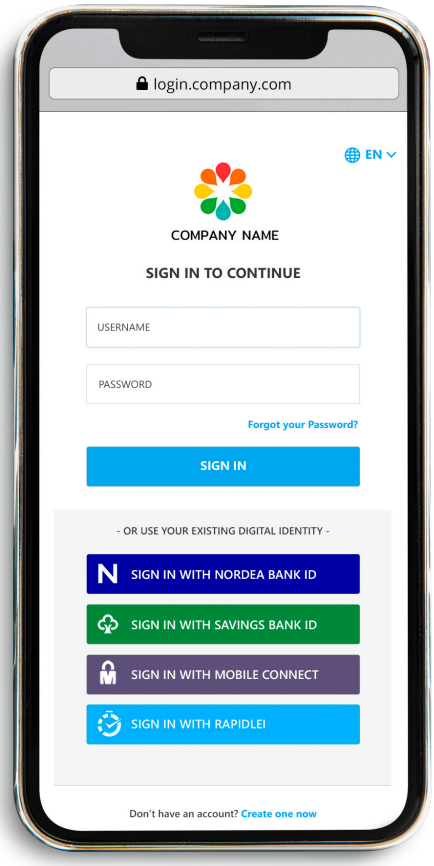
We've seen multiple healthcare data breaches make headlines in recent years, often with dire potential consequences. As Covid-19 rages on, another risk is emerging - vaccine distribution operations are under attack worldwide. In **several of these attacks**, it seems that hackers intended to steal login credentials of corporate executives and officials involved in the vaccine refrigeration process.

AUTHENTICATION

So what can be done to avoid a data breach? As **80% of security breaches** are caused by weak or stolen passwords, password-only access to healthcare systems is a major red flag that needs urgent resolution. CIAM offers alternatives to passwords (like **biometrics** and **identity providers**) which provide stronger assurance that the user logging in is who they say they are (strong authentication).

Authentication methods should be appropriate to their context. Some services only need to know that returning users are who they claimed to be when signing up (think social media sites). Other services need to know exactly who a user

is at point of signup – which is common in a healthcare setting. Since health-related data should be protected even more stridently than financial (given its high-value black market status), it then follows that healthcare providers should at minimum provide bank-level security for their customers' private data.



Example of a sign in experience using a verified identity - including bank IDs

This kind of **identity verification** could be carried out via identity providers that have completed a level of Know Your Customer (KYC) (like a bank ID), or via national level documents that can be digitally verified (using a platform like **Onfido**). Such electronic identity verification can also reduce human error, which can occur when identities are checked physically by administrative staff.

If you don't want to get rid of passwords altogether, or you want to make the authentication even stronger, CIAM enables multi-factor authentication (**MFA**). MFA requires users to authenticate via more than one means of identification, such as a password and bank ID. As it is much harder for a hacker to impersonate more than one authentication factor, this greatly increases trust in the accessing party. For this reason, **high growth** is forecast for MFA in the healthcare sector.

> **High growth is forecast for MFA in the healthcare sector**

SINGLE SIGN-ON (SSO)

Many healthcare organisations make use of single sign-on (**SSO**) – a CIAM capability which allows users to log in just once in order to gain automatic access to several applications/domains. SSO encourages users to create/manage one set of highly secure credentials, without the need to remember/manage several logins when needing to move quickly between systems. SSO can also control the use of risk-based or context-based MFA (multi-factor authentication) when access is deemed higher risk.

For example, in a patient-facing application, a patient accesses their healthcare provider's online service by authenticating with one set of credentials (with MFA where required) and can then move freely between the services that they're authorised to access. SSO reduces credential fatigue, encouraging better password 'hygiene' and uptake of optional MFA.

> **SSO reduces credential fatigue, encouraging better password 'hygiene' and uptake of optional MFA**

Additionally, SSO can be used to improve caregiving effectiveness as staff members access different systems, departments and applications. For example, federating a medical professional's identity to access different devices, medical services and data silos (such as imaging, clinical and, often, legacy applications) results in more efficient access to critical data and better overall management of medical needs. Expecting medical staff to remember multiple logins leads to inefficiencies and greatly increased breach risk – like passwords to medical systems written on sticky notes and attached to shared machines.

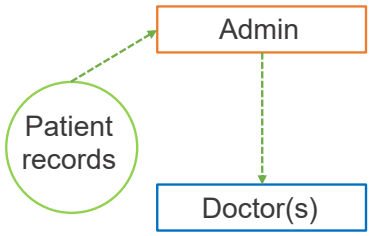
> **Without SSO, users often become lax about best-practice credential management – reusing easy-to-remember passwords across different systems, increasing the risk from 'credential stuffing'.**

SSO also has a significant security benefit when it comes to logging out; just one logout is needed for all systems, so no single service is forgotten about – a particular plus when sharing devices (think hospital admin staff). Similarly, when it comes to revoking account access (e.g. if a member of staff stops working with the organisation), just one set of credentials needs to be deprovisioned. This reduces the likelihood of human error, which could leave privileged access open beyond the necessary term.

DELEGATION

The **security of digital supply chain** processes and communications must not be overlooked. For instance, in the earlier-mentioned vaccine operations attacks, we saw how insufficient supply chain security could compromise your own information security. Such B2B workflows are far more secure when granular access control can be applied. **Delegated Authority** supports complex structures of access for all stakeholders – supply chain, partners, staff, external users and devices. Organisation-to-organisation and B2C delegation allows role-based authorisation to only necessary resources. This secure digital method of delegation also stops both data and credentials being shared in other, more vulnerable ways.

— WATCH THIS SHORT EXPLAINER VIDEO ON DELEGATED AUTHORITY.

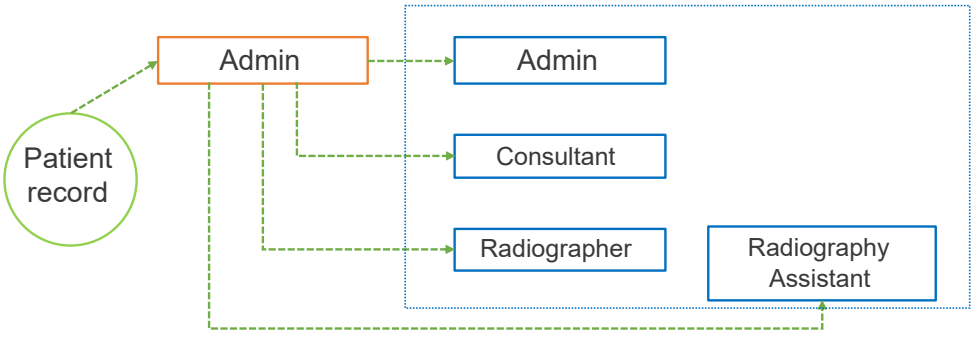


Simple delegation

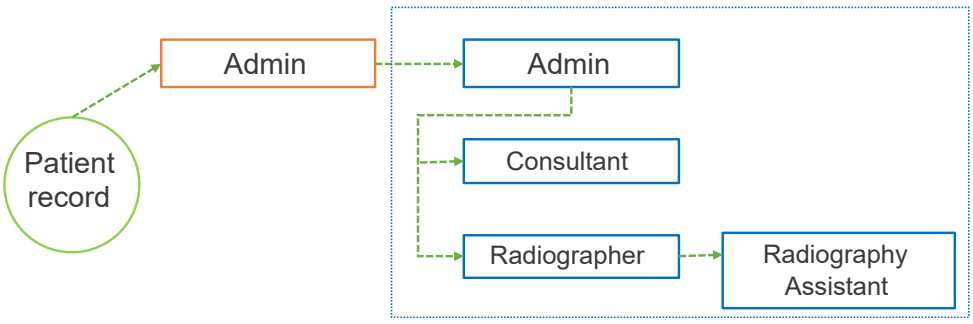
Delegated Authority can support delegation workflows from the very simple to the very complex. For example, a medical practice administrator can delegate access to patient records to a specific doctor or all authorised doctors.

However, when the situation calls for more granular control, or delegating access between organisations, CIAM can provide a streamlined solution. For example, the administrator can delegate access to an individual patient's record to an external organisation (e.g. a secondary specialist care unit). The administrator of the specialist care unit can then delegate varying levels of access to individuals within their own organisation within defined boundaries. This means that the original medical practice administrator does not need to spend time delegating access to each individual within the specialist care unit. It also stops the information needing to be sent manually – via post/phone/email, which is insecure and time-consuming.

Simple delegation to external organisation users



Delegated Authority to external organisation users



UBISECURE

Regulatory Compliance

Directly related to security is compliance, since many regulations mandate a high level of information security. Healthcare service providers in Europe, though **not generally bound by US healthcare-specific regulations** like HIPAA and EPCS, are subject to the GDPR, which essentially covers HIPAA's privacy aspects. For those organisations that are obliged to follow US regulations like HIPAA, CIAM helps you with requirements for strong authentication, granular access control and detailed user activity auditing. PSD2 is another European regulation that affects almost every organisation and is particularly relevant for healthcare organisations with an e-commerce aspect.

GDPR

When it comes to GDPR, **50% of our survey participants** said that achieving GDPR compliance without CIAM would be impossible. This is because CIAM capabilities like self-service account management, flexible logging capabilities and role-based access to data allow organisations to meet certain criteria of the regulation.

> CIAM capabilities allow organisations to meet criteria of the GDPR

One such criterion is the requirement to collect users' opt-in consent for data processing. Customer IAM helps with consent management through capabilities such as self-service account management, which gives users control over their own account settings. Through such portals, users could see/edit what identity data your organisation holds about them, and grant/revoke consent for various data processing.

Further, when users request to know all of the information you have about them, or exercise their 'right to be forgotten', some organisations find themselves unable to comply with these rights easily because they have multiple identity data siloes. CIAM can consolidate these repositories, for example by **integrating with your CRM** system. This helps organisations to comply with GDPR even alongside complex IT infrastructures. Organisations must also keep an audit of the data they collect and the purpose for processing the data. To aid this, CIAM systems have flexible logging capabilities that can capture and log any consent activity, and often include reporting tools to help with audits.

When it comes to information security, things are little more ambiguous. Article 24 of the GDPR requires that "appropriate technical and organisational measures" are taken to protect personal information. These measures are not named, but CIAM capabilities like strong authentication and/or MFA will count towards appropriate measures (see earlier security section). This also helps

organisations engaging with e-commerce to be PSD2 compliant.

At the heart of the GDPR are the concepts of 'privacy by design' and 'data minimisation' - collecting only necessary data and ensuring minimum necessary exposure of personal data. Customer IAM helps you structure your identity management workflows accordingly, also allowing you to set role-based access to data to enable the 'principle of least privilege'.

User Experience

User experience (UX) is critical to uptake of, and loyalty to, any eHealth service. Particularly when it comes to external users, if the journey through your service is not frictionless, you will not achieve the level of usage needed to fully realise the benefits. For example, if your primary goal of the digital service is to take the pressure off manual in-person services, a poor UX will cause you to fall short of that goal. This is one area in which Customer IAM, **specialised for external users** (customers, patients, residents, partners, remote workers etc.), has advantages over legacy IAM solutions (tailored to internal staff only).

— SEE MORE ON INTERNAL IAM VS CIAM

REGISTRATION

Registration is your users' very first experience with your digital service. This is a crucial point to convert users, while also needing to be tailored to your security and regulatory context. Finding this balance is what CIAM is made for.

> **45%** of users give up if the registration process is too hard

In a healthcare setting, your users are likely to be along a wide spectrum of digital literacy, as well as availability of - and preference for - different identity providers. Thus, eHealth must focus on inclusivity or risk marginalising groups from using the service. CIAM offers out-of-the-box workflows for registration that have been tried and tested in similar use cases. It allows you to tailor identity verification/authentication to your target user groups, with options to avoid a one-size-fits-all approach.

LOGINS

We saw earlier the security benefits of MFA. However, with MFA comes the potential for user friction if implemented inappropriately. CIAM providers will help you to find the correct balance of security and usability with MFA, which may include step-up authentication.

Step-up authentication introduces a second authentication factor only for certain

> With step-up authentication, security is 'stepped up' for sensitive information, while friction is reduced for low-risk resources

resources. For example, users may be able to access appointment booking after authenticating with just a username and password, but to access any PHI they will be asked to authenticate further with a bank ID. In this way, security is 'stepped up' for sensitive information, while friction is reduced for low-risk resources. This situation is comparable to contactless payments up to a certain amount, with chip and pin needed for higher-value (and therefore higher-risk) transactions.

IDENTITY LIFECYCLE

Self-service functions that aid in GDPR-compliance also make life much easier for your users (and for your staff, as we'll see in the next section on operational efficiency). By giving users control over their own account settings, it means they don't have to sit through call waiting times to speak to your IT Support desk. They can log on and update what they need to themselves.

SSO also reduces friction when users are moving between areas of your service (and even federated third-party services), increasing user retention. CIAM will help you implement a multi-channel identity solution, so that capabilities work across users' devices.

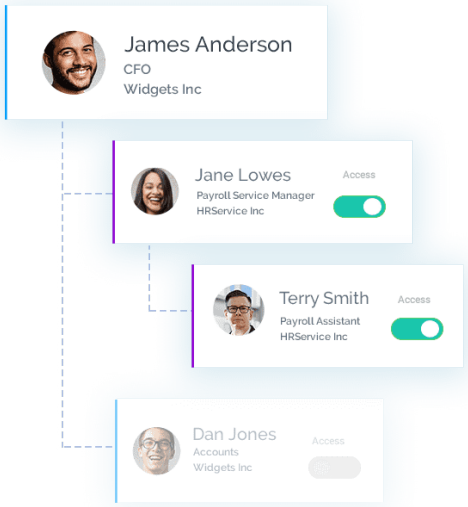
Operational Efficiency

Healthcare services often have multiple types of key stakeholders, which can require complex identity and access management workflows. These workflows may also need to span across organisations, taking into account affiliated companies, government institutions and supply chain – plus disparate systems as a result of mergers and acquisitions (M&A). Without the correct IAM solution to support (or unite) such workflows, operational efficiency can take a huge hit. With the correct IAM solution, workflows are digitised and seamless, enabling true operational efficiency.

REDUCE IT SUPPORT/ADMIN REQUESTS

According to **Forrester**, large organisations spend up to $1 million each year in staffing and infrastructure expenses to handle password resets. A CIAM staple is self-service account management – giving users control over their own account settings, including simple tasks like password resets. This takes a surprising volume of manual work away from your IT Support Desk, saving your organisation significant costs. For more about how CIAM saves organisations money (and increases revenue), download this **guide to evaluating the ROI of CIAM**.

— DOWNLOAD CUSTOMER IDENTITY AND ACCESS MANAGEMENT: INVESTMENT AND ROI



When multiple people (or devices) need access to the same data, or different levels of data, it is necessary to be able to delegate levels of access. This can be from individuals to individuals, organisations to organisations, or any combination of key stakeholders. The CIAM Delegated Authority capabilities we spoke about earlier (see Security > Delegation) are highly beneficial to operational efficiency in this regard, since they streamline complex access workflows. This saves time otherwise spent manually (and repeatedly) administering access on an individual basis.

Further, when your IT Support/Admin team does need to step in with individual support, Customer IAM can reduce the resource needed to resolve issues/requests. Firstly, the use of SSO means that there is only one set of credentials to manage per user – so if your different services required five sets of credentials previously, SSO could reduce resource for credential management by up to five times. Secondly, CIAM can help you to avoid data siloes that can occur from M&A or multiple data repositories within the organisation (e.g. by integrating CIAM and CRM systems). Therefore, by providing a single view of each user's identity, administrative staff spend far less time updating each silo, or hunting for various data sets in the first place.

ACCELERATE CHANGES

Healthcare has had to undergo rapid change in recent years, evolving to meet user demands and global situations. To keep up, new identity integrations are needed all the time – whether it be identity providers, connecting new services to the SSO capability, or federating to external services in aid of B2B relationships. To do this quickly, whilst maintaining security, purpose-built CIAM enables many integrations out-of-the-box, or will be quickly adaptable to your desired environment. This makes such solutions effectively future proof.

> **CIAM solutions adapt with your business, making them future proof**

Further, one of the biggest changes that your IT environment may undertake is as a result of M&A. CIAM can help you to integrate the resulting data siloes, merging the IAM functions quickly by drawing on vendor expertise and experience. Some organisations attempt to resolve the integration of IAM systems in-house, which can often overrun and go over budget when the complexity of the situation is realised. M&A provides a great opportunity to upgrade the CIAM system of the entire organisation, without wasting in-house development resource which could be better spent on your core business. For more on whether your organisation should build or buy its IAM solution, check out this **Build vs Buy: IAM white paper**.

— DOWNLOAD BUILD VS BUY: IAM WHITE PAPER

Summary

In summary, CIAM is a key enabler to digital transformation of healthcare services and new eHealth services. The four areas discussed – security, user experience, compliance and operational efficiency – are intertwined, with many CIAM capabilities offering benefits in all areas. For example, a better user experience will often precede more robust security practices. So if optional MFA is easy to use and offers appropriate methods to your users, it's more likely to be kept on by users – and best-practice adhered to. With the benefits spanning across your organisation – IT, Security, Marketing etc. – responsibility and ownership of CIAM must span departments and budgets.

> **Ubisecure CIAM supports healthcare needs at scale. As a European CIAM provider, we understand European organisations' needs and have 20+ years of experience in delivering proven identity solutions. Our Identity Platform can be deployed on-premises or in the cloud (Identity-as-a-Service, IDaaS), with flexibility to support hybrid IT environments and multi-cloud infrastructures.**

Find out more about how Ubisecure supports healthcare and eHealth services on **our website**, or get started with a **free 30-day IDaaS trial**.

About Ubisecure

Ubisecure provides feature rich customer identity management software and services to help companies reduce identity data breach risk, improve operational efficiencies, and improve user experience.

The company provides a powerful Identity Platform, deployed as IDaaS (public or private cloud) or on-premises software. The platform consists of productised Customer Identity & Access Management (CIAM) middleware and API tooling to enable single digital identity benefits across multiple applications. Capabilities include enabling complex authorisation and delegation workflows, single sign-on (SSO), frictionless multi-factor authentication (MFA), user identity management, and pre-established connections to dozens of third-party identity providers (social, mobile, and verified).

Ubisecure's Right to Represent is a representation governance solution offering a fast and easy way to assert and verify an individual's mandated rights to electronically represent their company, including financial, signatory, or other authority. Ubisecure's widely used Delegated Authority solution allows individuals and organisations to manage which users and organisations can act on their behalf to dramatically reduce costly, time consuming and delay-prone manual workflows.

Ubisecure is accredited by the GLEIF to issue Legal Entity Identifiers (LEI) under its RapidLEI brand. RapidLEI is a cloud-based service that automates the issuance and registration of these highly assured organisation identifiers.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com

UBISECURE UK
The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK

UBISECURE FINLAND
Vaisalantie 2
FI- Espoo, 02130
Finland

UBISECURE SWEDEN
Blekholmstorget 30 F
111 64 Stockholm
Sweden

UBISECURE DACH
Franz-Joseph-Str. 11
80801 Munich
Germany