

# Trusted Identities for the Healthcare Industry

Building healthcare's foundation of trust.



**ENTRUST**

SECURING A WORLD IN MOTION

# Trusted Identities – the Need of the Hour

Healthcare data is among the most sensitive and most targeted in the world.

Healthcare is unlike any other industry. It serves people at every stage of life, from birth to ongoing chronic care to end-of-life decisions. Patients place enormous trust in their providers: trust that the right doctor has access to the right information, that their personal health data stays private, that their insurer has accurate records, and that the systems supporting their care are always available when needed.

This trust has to be earned, and protected, at every point of care, and healthcare organizations carry this responsibility across every level of their operations.

Clinicians need fast, secure access to patient records. Patients expect seamless, secure experiences whether they're checking in at a clinic or consulting a physician remotely. Administrators need to ensure that sensitive data is accessible only to those who are authorized. And then there is compliance with regulations like HIPAA.

There is pressure to deliver on all of these demands simultaneously, with zero tolerance for downtime, data breaches, or identity errors. This is what makes trusted identity solutions critical infrastructure for today's healthcare.

Entrust helps healthcare organizations meet this challenge. With a single trusted vendor, providers can manage issuance and badging, secure patient onboarding, control access to sensitive data and protect the systems that house that data, and support continuous compliance, all built on a foundation of trust.



# \$7.42M

Average cost of a healthcare data breach – the highest of any industry for 12 consecutive years.

Source: IBM Cost of a Data Breach Report, 2025

# Accelerating Data Access for Better Patient Outcomes

Trusted identities enable quick identification and ensure accurate medical information reaches the right provider at the right time.



## Identify and authenticate the patient

Patient misidentification has been a significant issue within the healthcare system, carrying serious consequences for patient safety and quality of care. With increasing patient volumes and more complex care pathways, there's a need to clearly define and verify the identity of healthcare professionals, patients, and visitors. Identity solutions give healthcare institutions the ability to establish a trusted patient identity for administering care and ongoing treatment.

## Streamline the registration process

Trusted identities streamline the registration and onboarding process by automating the input of and access to patient information. Healthcare institutions can quickly confirm a patient's identity and support instant verification of insurance and benefits eligibility. This helps decrease patient wait times and improve the quality of care.

## Direct patients to appropriate doctors and treatment

Clinicians can direct patients to appropriate clinics and care pathways using securely stored identity information. Trusted identities also support tracking of patients from registration to consultation to payment.

## Quick access to medical information in case of emergencies

Trusted identities enable first responders to identify a patient immediately and access potentially lifesaving information and perform correct procedures with appropriate medication. This is particularly beneficial if the patient has lost consciousness or the ability to communicate their medical situation accurately.

# Securing Critical Assets and Patient Information

Trusted identities support healthcare institutions to authenticate employees and monitor their access rights to protect critical assets and patient information.



## Secure patient records and healthcare data

Considering the amount of sensitive data that healthcare facilities work with, providing secure access to medical information poses a unique challenge, and failure to protect it puts healthcare organizations at risk of losing their credibility. Using trusted identities, healthcare facilities can help ensure only authorized doctors have access to patients' personal information, health records, and other confidential healthcare data stored on the systems.

According to IBM's 2025 Cost of a Data Breach Report, healthcare breaches take an average of 279 days to identify and contain, which is more than five weeks longer than the global average. The longer a breach goes undetected, the greater the risk to patient privacy, organizational credibility, and regulatory standing.

## Authorized access to healthcare assets

Asset protection is a major concern for medical facilities, as prescription medications, medical supplies, and equipment are potential targets for theft and misuse. With trusted identities, healthcare organizations can automate the assignment and withdrawal of access privileges across the entire network, quickly and accurately.

## Enable remote consultation

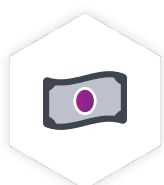
Telehealth and remote consultation have become a permanent and growing part of modern healthcare delivery. While telemedicine bridges the distance between doctors and patients, healthcare providers are susceptible to potential security risks. Trusted identities facilitate quick, accurate, and seamless identity proofing of patients and doctors by providing digital identity verification, secure credential issuance, and authentication of healthcare transactions.

Source: IBM Cost of a Data Breach Report, 2025 (page 7)

# Working “Smart” – Benefits of Implementation of Trusted Identities

In an environment as complex as a healthcare facility, trusted identities help mitigate fraud risks and maintain healthcare systems’ integrity, while simultaneously maintaining the required level of accessibility and openness. The rapid adoption of electronic health records, patient terminals, and telehealth has only accelerated the need for secure, reliable identity solutions across the entire care continuum.

A trusted identity solution brings the following benefits to healthcare organizations:



## Cost reduction

Legacy healthcare systems rely heavily on data that is collected through manual processes. This mode of collecting and managing data is proving to be unreliable, risky, and time-consuming; it often results in data loss, theft, and added cost. Having a simplified and secure identity issuance strategy boosts efficiency by drastically reducing the likelihood of human error and reducing labor costs and time spent on rejected insurance claims owing to incorrect or missing information.

Additionally, with mobile identity solutions healthcare institutions can create a sense of self-sufficiency that many patients prefer. With self-service kiosk systems, patients can handle their own registration and check-in, and this can be another contributing factor to lowering labor costs.



## Optimize processes

Healthcare processes are routinely slowed by redundant forms, repeated identity checks, and requests for information already on file. Trusted identities improve healthcare processes by automating and streamlining identity and document authenticity.



## Ensure patient safety

Mistaken identity can lead to unnecessary or potentially harmful medical procedures and an inaccurate medical history record that can jeopardize future care for the patient to whom the record belongs. Trusted identities help ensure that a patient's personally identifiable information (PII) is accessible only to authorized clinicians and that critical activities like medical procedures and prescriptions are always performed for the correct patient.



## Enhance patient satisfaction

Trusted identities help ensure the right treatment reaches the right patient at the right time, improving engagement across the entire care journey. As trusted identities expedite the processes and provide a secure and easy environment, they minimize patient inconvenience and maximize the quality of the patient's interaction with the provider across all delivery channels, be it on-premises, online, or off-premises.



## Support compliance with regulations

Healthcare is one of the most highly regulated industries, and trusted identities can help make it much easier for healthcare institutions to stay compliant with various regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). One of the key provisions of the HIPAA Privacy Rule is to assure an individual's health information is protected and they can control how their health information is accessed and used.

In the first five months of 2025 alone, the HHS Office for Civil Rights entered into 10 HIPAA resolution agreements, with penalties ranging from \$25,000 to \$3 million - each tied to failures in basic Security Rule compliance.

Trusted identities can help bolster regulatory compliance by providing healthcare institutions the tools to implement comprehensive security, audit, and access policies.



## Protect organizational reputation

Identity theft is one of the most reported cybercrimes, and one that can have devastating effects on reputation. By establishing a strong security and compliance posture that defends the healthcare enterprise against breach and loss, trusted identities help protect credibility and deliver real and perceived benefits that can help create competitive differentiation.

Source: <https://ogletree.com/insights-resources/blog-posts/2025-enforcement-trends-risk-analysis-failures-at-the-center-of-hhss-multimillion-dollar-hipaa-penalties/>



# Entrust Solutions for the Healthcare Industry

With Entrust, healthcare providers can create, deploy, and support identities that are built on trust, enabled by digital and physical issuance systems, and backed by digital signing, encryption, and authentication technologies.

## Credential Issuance

Enable clinicians, patients, and visitors with trusted identity in the form of a physical card and/or embedded within a mobile application.

Entrust provides both physical identity and digital identity in a single form factor (smart card or mobile).

## Identity and Access Management

Facilitate secure and authenticated access to patients and clinicians to healthcare applications or services.

Entrust offers cloud-based identity and access management (IAM) solution with multi-factor authentication (MFA), credential-based passwordless access, and single sign-on (SSO).

## Electronic Signature and Digital Signing

Extend the capability to create and sign tamper-evident documents that can be validated easily.

Entrust helps protect PHI and critical workflows with certificate-based encryption, digital signatures, and secure document sealing.

# Entrust Solutions for the Healthcare Industry

## Public Key Infrastructure (PKI)

The basis of trusted identity that helps bring security and accountability to hospital information systems.

Managed PKI Services, Cryptographic Security Platform PKI, and PKI as a Service.

## Hardware Security Modules (HSMs)

Ensure secure and tamper-resistant storage of the keys used to establish the trusted identity.

Entrust nShield HSMs are available in a range of FIPS 140-2 & 140-3 certified form factors and perform cryptographic functions such as generating, managing, and storing encryption and signing keys.

Entrust offers end-to-end solutions for healthcare providers to protect patient data, reduce risk, and help demonstrate compliance while improving patient experience and organizational efficiency. Key features include:

- Issue trusted identities to ensure proper access control and accountability.
- Protect patient health records by making them inaccessible and unusable to attackers.
- Safeguard medical devices to ensure maximum uptime and reliability for patient care.
- Provide tamper-proof documents and ensure authenticity in transactions including teleconsulting, e-prescription signing, and insurance claims.
- Facilitate compliance with HIPAA and other healthcare and/or government data privacy mandates.

# Complete Identity Security for Healthcare

Trust is the foundation of every patient relationship. From the moment a patient walks through the door – physically or virtually – to every interaction with their data, their care team, and their insurer, identity is at the center of it all.

Entrust offers end-to-end identity solutions designed for healthcare. With a single trusted vendor, healthcare providers can issue and manage credentials, secure patient onboarding, control access to sensitive data, protect the systems that house that data, and support continuous compliance, all while improving patient experience and organizational efficiency.

The result is a healthcare environment where clinicians can focus on care, administrators can focus on operations, and patients can focus on getting well.

Learn more about how Entrust supports healthcare organization.

[Learn More](#)



## ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit [www.entrust.com](http://www.entrust.com)