VASCO

Trusted Digital Identity

What every healthcare organization needs to know

Trusted Digital Identity and Healthcare

A digital identity is a set of attributes related to a person, organisation or device that can be used to authenticate that entity to a computer system. A "trusted" digital identity is one that has been verified as belonging to the authorized entity.

In the physical world, people need **trusted** credentials to **prove** they are who they claim to be.

Government-issued ID (e.g. driver's license)

Insurance card

In the digital world, healthcare organizations can protect themselves with trusted digital identities by managing a four-step process.

VALIDATE USERS – "Identity proofing"

ISSUE CREDENTIALS – Hardware or mobile authenticators

PROVISION CREDENTIALS – Bind user to trusted device

AUTHENTICATE USERS – Multi-factor authentication

Trusted digital identities help **prevent**:

Data Breaches

Medical Identity Theft

Fraud

Fines

38 % of large data breaches in healthcare in 2015 were caused by unauthorized access or disclosure.[1]

48 % percent of consumers would consider changing healthcare providers if their medical records were lost or stolen.[2]

1 Forbes.com: *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015*

2 Ponemon Institute *Fifth Annual Study on Medical Identity Theft*

This infographic illustrates **six** areas where trusted digital identities are essential for healthcare organizations.

Secure Access for Patients

Portals provide patients and their authorized representatives with an online means to view, download and transmit healthcare data.

Patient portals improve patient satisfaction, reduce costs, and help address industry regulations and guidelines.[3] Trusted digital identities **protect patient** information from cybercriminals.

IDENTITY PROOFING

MULTI-FACTOR AUTHENTICATION

CHALLENGES

- Process must be easy
- Must validate identity remotely
- Patients have diverse personal devices

3 For example, Netherlands: Idensys; UK: Patient Online; United States: CMS.gov
Meaningful Use Stage 2 – Patient Ability to Electronically View, Download & Transmit (VDT) Health Information.

Secure Access for External Healthcare Partners

Healthcare organizations rely on a wide variety of external healthcare partners to deliver services to patients. Privacy legislation such as HIPAA and the General Data Protection Regulation require that the healthcare organizations and their service providers and "business associates" work together to safeguard patient information. Trusted digital identities are essential for ensuring that only trusted entities can access systems containing patient data.

CONSULTANT

HEALTHCARE SERVICE PROVIDER

CYBERCRIMINAL

IDENTITY THIEF

PHARMACY BENEFITS MANAGER

CLAIMS PROCESSOR

HACKTIVIST

CHALLENGES

- Many service providers to manage
- Each provider accesses multiple health applications
- Cost of educating and monitoring many providers
- Healthcare organization blamed for any failure

Secure Access for Practitioners

Doctors, nurses, technicians, administrators and other staff all need access to information in electronic systems – often many electronic systems on the same day. Strong security is essential, but convenience and ease of use have a direct impact on productivity, morale and cost.

SYSTEM 1

SYSTEM 2

SYSTEM 3

SYSTEM 4

SYSTEM 5

SYSTEM 6

CHALLENGES

- Need access to multiple "siloed" systems
- Many practitioners and staff to manage
- Sign-ons must be lightening fast
- Smartphones banned inside some facilities

Protecting Electronic Prescriptions

In the United States, the Electronic Prescribing for Controlled Substances (EPCS) rule of the Drug Enforcement Administration allows health practitioners to electronically write prescriptions for controlled substances. The DEA requires the use of trusted digital identities for this activity. To obtain authentication credentials the practitioner must apply for identity proofing to an approved credential service provider or certification authority, and multi-factor authentication must be used before signing prescriptions.

Electronically Writing a Prescription

Review patient's health information on EHR → **Accesses state's prescription drug monitoring program** → **Electronically write medication** → **Send prescription to pharmacy**

R_x

Practitioners must apply for credentials through an approved service provider whose identity proofing process adheres to NIST SP 800-63-3 Identity Assurance Level 3.

The practitioner must use multi-factor authentication to access secure systems. If a hardware device is used, it must meet at least FIPS 140-2 Security Level 1 requirements.

CHALLENGES

- Over 25 percent of doctors fail to answer the questions correctly on the first try [during the identity proofing process].[4]
- An eRx vendor can be shut down if identity proofing and multi-factor authentication don't meet DEA requirements—affecting millions of patients.

4 Quoted in DrFirst white paper: The Evolving EPCS Landscape: A Prescription for Stopping Opioid Abuse

Compliance

The healthcare industry continues to increase the number of initiatives centered around strong identity management. Many industry standards and government regulations recommend or require identity proofing, multi-factor authentication, and implementation of a trusted digital identity management program.

REGULATIONS

HIPAA

EU Regulation No 910/2014 (eIDAS)

EU General Data Protection Regulation (GDPR)

DEA Electronic Prescribing for Controlled Substances (EPCS)

New York I-STOP Act

Maine Act to Prevent Opiate Abuse

STANDARDS

NIST SP 1800-1

FIPS 140-2

NIST SP 800-63-3

INITIATIVES AND ROADMAPS

ONC Nationwide Shared Interoperability Roadmap

EU Code of Conduct on privacy for mHealth apps

NHS Patient Online

SAFE-BioPharma FICAM Trust Framework

Office of the National Coordinator for Health Information Technology (ONC)

Personally Controlled Electronic Health Record (PCEHR)

White House Precision Medicine Initiative

Surescripts Identity Proofing Requirements

Idensys

NemID

HIMSS ID Management Task Force (IDM TF)

HIMSS ID Management Task Force (IDM TF)

Identity Ecosystem S teering Group (IDESG)

National Strategy for Trusted Identities in Cyberspace (NSTIC)

Safeguarding Mobile Health Apps

Mobile health (mHealth) apps are revolutionizing patient care, customer service, and medical research. But when anyone can log on, from anywhere, with any device, at any time, healthcare organizations face new challenges protecting patient data and preventing the unauthorized manipulation of mHealth apps.

At home

On the go

At remote offices

CHALLENGES

- Balance between security and ease of use
- Diverse users
- Diverse devices
- Diverse apps

Criteria for Choosing a Trusted Digital Identity Solution

- A single integrated solution for identity proofing, credential issuing, and strong multi-factor authentication
- Simple remote identity proofing services adhering to NIST SP-800-63 Level 3
- Convenient and user-friendly multi-factor authentication for practitioners, patients and external partners
- Advanced hardware and software authentication options that enable secure access to multiple healthcare applications
- Bank-level security for mobile health apps, including FIPS 140-2 Level 2 certified authenticators
- Compliance with dozens of key regulations and healthcare initiatives around the world

VASCO protects the world's most sensitive data and offers a suite of strong, scalable, and easy-to-deploy solutions tailored to help healthcare organizations protect identities, safeguard patient records, and enable compliance with regulations. Our diverse portfolio provides a one-stop shop for security solutions across all types of organizations in the healthcare ecosystem.

Learn More: VASCO Healthcare Solutions

https://www.vasco.com/solutions/healthcare-information-security/index.html

VASCO