



VASCO: Compliant Digital Identity Protection for Healthcare

Compliant Digital Identity Protection for Healthcare

The proliferation of digital patient information and a surge in government regulations are forcing a shift in the healthcare industry. As the entire healthcare community adopts digital processes and web-based systems for patient data, the need for stronger security and compliance measures grows exponentially. What does it mean for the healthcare providers, pharmacies, HIT vendors and others involved in the healthcare information and data management?

Who Needs Help

VASCO's solutions support the needs of a wide variety of healthcare organizations:

- EMR/EHR software providers
- Hospitals, clinics, labs and other healthcare facilities
- Health management and insurance companies
- Health information exchanges
- Medical billing and claims processing organizations
- E-pharmacies and e-prescribing vendors

EPCS
Do I need to comply?



Problems You Need to Solve

As the healthcare industry continues to transform, practitioners and providers require advanced solutions for reducing cybersecurity threats and safeguarding patient information. Growing adoption of Electronic Health Records (EHRs) and e-prescribing places the burden on organizations to comply with EPCS, HIPAA and other federal and state regulations.

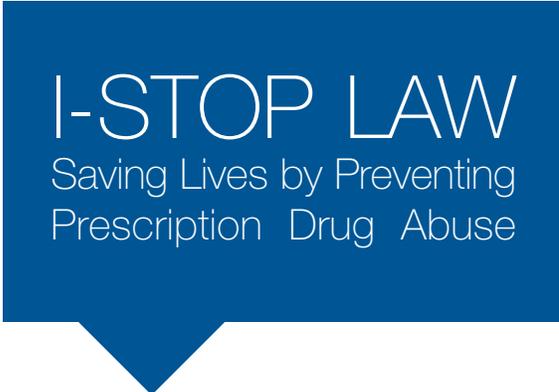
VASCO's healthcare solutions allow organizations throughout the industry to overcome their most pressing challenges, including:

- **Identity Proofing** - on-site and remotely for users accessing EHR/EMR and RX applications or patient portals
- **EPCS Compliance** for two-factor authentication
- **HIPAA and the HITECH Act compliance** for protecting patient data
- **Meaningful Use Compliance** for federal incentive programs
- **Patient Identity Theft Risk Mitigation**, fraud and medical malpractice prevention
- **Secure access to data**, without disrupting convenience for practitioners

How You Can Solve Them

VASCO offers a suite of identity and access management solutions for web-based and mobile healthcare applications (including EHRs, eRXs, HIEs, VPNs and patient portals) to help protect sensitive data and improve compliance posture. You can start your road to an interoperable healthcare system quickly, and with minimal resources thanks to the unique secure identity management platform provided by VASCO:

- Native integration with most healthcare software provider applications through an API back-end
- Vendor/application agnostic technology model to insure true interoperability
- FIPS compliant Two-Factor Authentication
- FIPS compliant Identity Proofing
- Secure Identity Federation
- Secure Single Sign-On
- Multi-application usage capabilities



I-STOP LAW
Saving Lives by Preventing
Prescription Drug Abuse

Key Building Blocks on Your Road to Secure and Compliant Healthcare System

Two-factor authentication for EPCS compliance

DIGIPASS GO 7 is VASCO's FIPS 140-2 Level 2 Certified One-Time Password (OTP) token - a single-button authenticator that generates a unique password each time a user remotely accesses a healthcare network, system or website. DIGIPASS GO 7 meets the requirements for EPCS two-factor authentication and EHR Stage 2 meaningful use, allowing healthcare providers to qualify for federal Medicare/Medicaid incentive programs and helping them to pass third-party audits.

Identity protection and validation

VASCO's Identity Proofing and Validation solutions securely confirm provider eligibility and authenticate providers to e-prescribe controlled substances. Our Identity Proofing and Validation solutions meet the NIST Special Publication 800-63 Assurance Level 3 requirements for multi-factor remote network authentication and fulfill a mandatory requirement for compliance with EPCS regulations.

Secure access

Our broad range of DIGIPASS hardware and software authenticators, as well as our IDENTIKEY Authentication Server and VACMAN Controller API, offer a turnkey solution for secure remote access to patient data, delivering unprecedented convenience for practitioners and hospital staff. We enable your staff to have one known identity, with one strong authentication method across all your applications.

Mobile EHR compatibility

Increasingly, healthcare providers are using smartphones and tablets to access clinical software. VASCO's two-factor authentication hardware tokens enable healthcare workers to securely access patient records and prescribe medications via any mobile device, while meeting the "separate authentication device" rule established by DEA for EPCS compliance.

How VASCO Enables EPCS Compliance

Electronic Prescriptions for Controlled Substances (EPCS) is a U.S. Drug Enforcement Agency (DEA) regulation that allows healthcare practitioners to write electronic prescriptions for controlled substances. In addition to reducing occurrences of fraud and prescription drug abuse, EPCS promotes the overall movement away from inefficient, paper-based prescriptions and facilitates electronic medication management.

Although DEA regulations do not mandate the use of EPCS, some states have established deadlines for requiring electronic prescriptions for controlled substances and other prescription drugs.

VASCO solutions enable healthcare providers and healthcare software vendors to rapidly implement EPCS with improved compliance and greater efficiency.



Identity Proofing Service

VASCO's Identity Proofing Service streamlines the process of third-party confirmation of provider eligibility, and efficiently authenticates providers for the electronic prescription of controlled substances. VASCO Identity Proofing solutions fulfill the NIST Special Publication 800-63 Assurance Level 3 requirements, and meet a critical EPCS compliance requirement.

Identity proofing is a critical requirement for EPCS Compliance (Electronic Prescribing of Controlled Substances). For security purposes, authentication credentials that are used to sign prescriptions can only be issued to practitioners whose identity has been confirmed and validated. Healthcare providers must offer to their prescribers both in-person and remote identity proofing that meets NIST Assurance Level 3.

Identity Proofing Service

VASCO's Identity Proofing Service for EPCS Compliance meets DEA and NIST Level 3 requirements, and is offered as part of our holistic digital identity management solution for the healthcare community. We ensure the required technical, regulatory and logistical aspects of identity validation and credential issuing are in place before authorized parties begin using the two-factor authentication protocols required by the DEA.

FIPS Level 2 Certified Two-factor Authentication

A convenient, single-button OTP (one-time password) authenticator, VASCO's DIGIPASS GO 7 provides a unique password each time the user remotely accesses a network, system or website. The DIGIPASS GO 7 FIPS 140-2 Level 2 token can be used across PC and mobile platforms, and satisfies Two-factor authentication requirements for EPCS as well as EHR Stage 2 meaningful use.



Why Choose VASCO

As global experts in identity protection and authentication, VASCO delivers best-in-class solutions that protect the most complex technical environments and improve provider workflows and productivity. Healthcare practitioners and providers that choose our products realize significant benefits, such as:

Native EHR Integration

A hassle-free native integration with most healthcare software provider applications through an API back-end, with no need for additional systems, databases, or servers, so you can get up and running quickly, and with minimal resources.

One Authenticator, Many Apps

No one wants to carry 2, 3 or 10 tokens. With VASCO's solutions healthcare providers can equip staff with a single hard or soft token that can be used to conveniently and securely access all applications.

Multiple Authentication Modalities

VASCO offers the most comprehensive portfolio of DEA-approved authentication modalities, including hardware tokens, mobile and PKI authenticators as well as provides support for biometric options. All form factors are supported on a single authentication platform.



Seamless Integration

Native integration into any on premise, cloud or mobile EHR/EMR/e-Prescribing application, so the same disaster recovery, load balancing and infrastructure you have in place today is not impacted.

Fulfillment Services

Eliminate the need to manage inventory of hardware tokens, order processing and delivery. VASCO centralizes the shipping process and monitors inventory levels to ensure adequate stock.

Customization and Packaging

Customize tokens with logos and colors or suggest custom packaging options that include user product guidelines, account registration instructions, FAQs, and other necessary information to reduce user confusion and help desk calls. Mobile authenticator customization options are also available.



About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit www.blog.vasco.com