VASCO
THE AUTHENTICATION COMPANY

MYDIGIPASS™
YOUR TRUSTED DIGITAL IDENTITY

MYDIGIPASS for Healthcare

Managing Trusted Digital Identities for the Healthcare Community

MYDIGIPASS for Healthcare is a comprehensive solution for healthcare organizations, EHR and eRx vendors that helps ensure EPCS compliance for prescribers and offers enhanced security for HIE, provider and patient portal access. From identity proofing and provisioning to secure login and fulfilment – all aspects of digital identity management are covered on a single, fully integrated platform.

Prompted by regulatory requirements such as the DEA EPCS Regulation and HIPAA, along with a massive push towards electronic health records management, there is a clear need to establish digital trust in the healthcare ecosystem. MYDIGIPASS for Healthcare incorporates five critical elements to support trusted digital identities and secure information exchange within healthcare organizations and HIT providers:

1. **Identity Proofing** via an in-person video call or remotely via Knowledge-Based Authentication (KBA)
2. **Credential issuance** via hardware, software or combined authentication technology
   - **Hardware two-factor authentication** token – FIPS 140-2 Level 2 certified DIGIPASS GO7
   - **Software two-factor authentication** token – FIPS Compliant DIGIPASS for Mobile. Available for iOS and Android.
3. **Provisioning**
4. **Fulfillment and Inventory Control** with physical shipment of hardware authenticators
5. **Secure login** with two-factor authentication

MULTI-APPLICATION AND MULTI-PLATFORM SECURITY

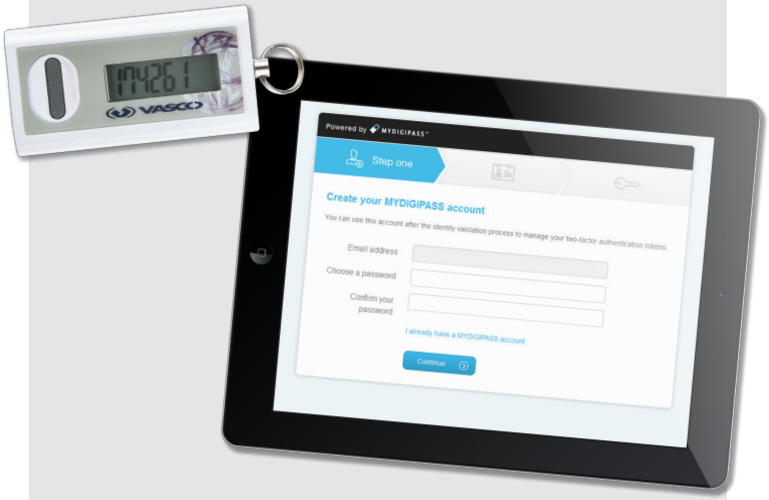
MYDIGIPASS for Healthcare offers a unified ID proofing method and authentication tool that can be used throughout all applications and platforms. It also works ANYWHERE inside the healthcare facility or off-site, even when no cellular service is available. This critical flexibility is accomplished via the following products:

- DIGIPASS GO 7, a FIPS 140-2 Level 2 Certified one-time password hardware token
- DIGIPASS for Mobile, a DEA compliant software authentication tool that does not require cellular service to operate
- DIGIPASS for APPS Push Authentication that operates using a secure communication channel and does not require cellular service to operate

WHY DO YOU NEED IDENTITY PROOFING?

For EPCS the U.S. DEA requires that individual healthcare practitioners must apply to federally approved credential service providers (CSPs) or certification authorities (CAs) to be identity proofed and obtain their two-factor authentication credential or digital certificates that meet NIST Level of Assurance 3 (LoA3).

Additionally, the U.S. Health & Human Services' Nationwide Shared Interoperability Roadmap is seeking "Verifiable Identity and Authentication of All Participants" with the 2015-2017 milestone of 65% of health care organizations permit patient access to patient portals via username and password plus knowledge-based attributes or emerging technologies in lieu of passwords to reduce vulnerabilities in identity theft. HHS's 2018-2020 milestone is to have at least 50% of health care organizations have implemented identity proofing and authentication best practices of all participants; providers, staff and patients.



VASCO
THE AUTHENTICATION COMPANY

MYDIGIPASS™
YOUR TRUSTED DIGITAL IDENTITY

Why Choose MYDIGIPASS for Healthcare by VASCO?

REGULATORY COMPLIANCE

- Two-factor authentication that meets FIPS 140-2 Level 1 Standards required by DEA EPCS Rule
- Enforcement of New York's I-STOP Law mandates that all medications be prescribed electronically
- The only one-time password hardware token that is FIPS 140-2 Level 2 Certified and satisfies DEA requirements for EPCS
- A dedicated mobile authentication module within our DIGIPASS for APPS product suite that is FIPS 140-2 Level 1 certified
- Full-service Credential Service Provider certified under the SAFE-BioPharma FICAM Trust Framework at NIST SP 800-63 Level of Assurance 3

HIGH LEVEL OF TRUST ON A SINGLE PLATFORM

End-to-end identity proofing solution that facilitates secure information exchange between all access points throughout the healthcare ecosystem. From the time a patient logs onto a patient portal; to a physician reviewing that patient's health information using an EHR system; to accessing the state's prescription drug monitoring program, to electronically prescribing medication for that patient's use, to submitting a claim to the health insurance company, all transactions and data exchange are executed with the highest level of trust.

MULTI-APPLICATION CAPABILITIES

No one wants to carry 2, 3 or 10 tokens, each assigned to a different application. To avoid this problem, healthcare organizations can equip providers and staff with a single hardware or software authentication tool that can be used to conveniently access all applications throughout the healthcare organization; essentially allowing each user to have a single, secure and trusted digital identity.

SIMPLIFIED AUDIT PROCESS

VASCO's FIPS 140-2 Level 2 Certified authenticator fulfills EPCS and Stage 3 meaningful use requirements; and the robust reporting capabilities of our backend platform deliver a comprehensive audit trail that can ease the third-party audit process.

How MYDIGIPASS for Healthcare Works

1. Physicians identity proofing at NIST Level of Assurance 3. Identity Proofing methods (selected automatically based on information input by each individual) include:
   - Knowledge-Based Authentication (KBA)
   - Live video call
2. VASCO will ship the hardware token to the user and provide activation instructions via email – and/or
3. The user will receive a link to download a free mobile app with DIGIPASS for mobile authenticator and activation instructions
4. Once a token has been received and activated, the user can start performing tasks that require strong authentication and digital identity validation such as electronically submitting prescriptions for controlled substances, accessing PHI, logging into patient portal, and more.

About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security and designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com