

VASCO Solutions for Healthcare Providers

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 offers a suite of two-factor authentication solutions for web-based and mobile healthcare applications (including EHRs, VPNs and patient portals) to help providers protect sensitive data and improve compliance posture. Additionally, VASCO delivers an easy, no hassle integration with most healthcare software provider applications. Through an API back-end and vendor/application agnostic technology model, as well as secure identity federation, SSO and multi-application usage capabilities, you can start your road to an interoperable healthcare system quickly, and with minimal resources.

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.



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, mobile and PKI authenticators, all supported on a single authentication platform.