IMAGEWARE® SYSTEMS

GoVerifyID®

Accelerate your Authentication Journey with our 2FA, Biometric, and MFA Solutions

2FA and Biometric Authentication for Healthcare

GoVerifyID addresses your two-factor and multi-factor authentication requirements and protects your sensitive healthcare data.

ImageWare's GoVerifyID can easily add two-factor and biometric user authentication to your healthcare systems, EHR applications, and clinical environments. ImageWare provides biometric user authentication for America's largest integrated healthcare system.

Medical identity theft is on the rise. An estimated 2.3 million Americans had their identities stolen during or before 2014.[1] The healthcare industry is perhaps the most vulnerable to data security breaches. Ponemon Institute's research reported that data breaches cost the healthcare industry up to $6.2 billion each year.[2] The number of reported major cybersecurity events attributed to ransomware by health care institutions increased by 89 percent from 2016 to 2017.[3]

GoVerifyID brings security and convenience to your healthcare organization by using the second factor or biometric of your choice. Patients and healthcare professionals simply swipe a finger, take a selfie, show their palm, speak a phrase, or respond to an alert on any connected device to authenticate themselves, anywhere, anytime.

With GoVerifyID, you can assure the right person gets access to the correct healthcare information.

Features

- Streamlined login
- Superior accuracy
- Seamless integration
- Highly scalable

Benefits

- Accurate patient identification
- Prevent medication errors
- Safeguard Personal Health Information (PHI)
- Reduce medical billing fraud

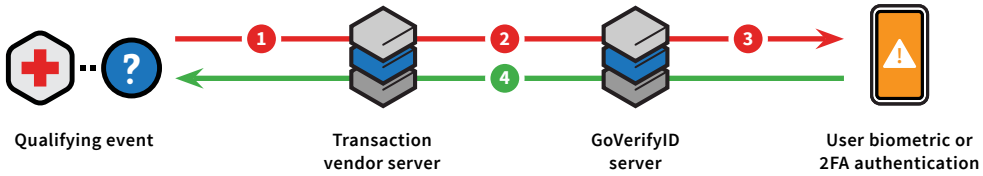
[1] Ponemon Institute's Fifth Annual Study on Medical Identity Theft, 2015. **http://goo.gl/PkPD1o**

[2] Ponemon Institute's Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, 2016. **http://goo.gl/pHwmrr**

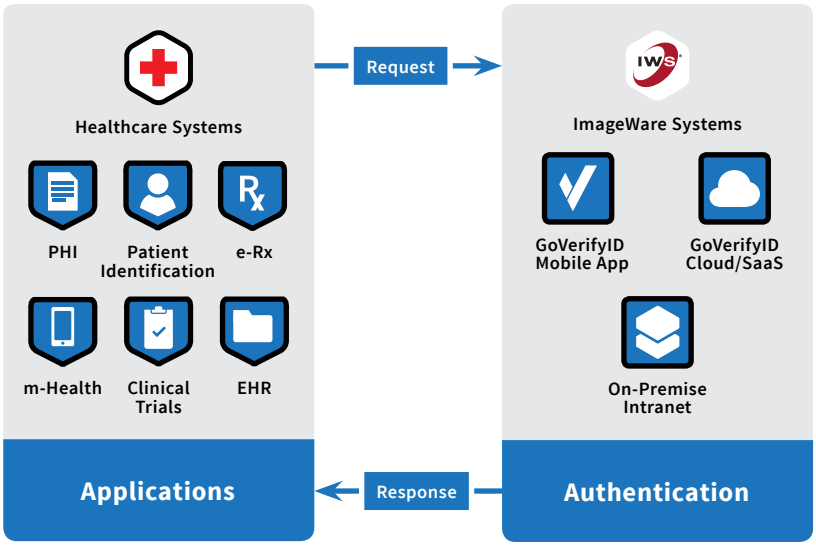
[3] CryptoniteNXT Special Report – Health Care Cyber Research Report for 2017

Mobile 2FA and biometric user authentication: How it works

1. A qualifying event (like a medical record request) starts the process.
2. The transaction vendor server (like a hospital) pings the GoVerifyID server for an authentication request.
3. The user is asked to submit their biometrics or 2FA response for authentication.
4. Based on the results from the servers, the authentication is approved or denied.



Biometric authentication in healthcare: Examples



Use Cases

- A physician or other hospital staff requesting access to a patient's Electronic Health Records (EHR) or Personal Health Information (PHI).
- A physician sharing patient records with other staff within the same health system.
- Physicians submitting electronic prescriptions (e-Rx) for controlled substances and e-Prescription renewals.
- Physicians entering orders into Certified Physician Order Entry (CPOE) systems.
- Patient check-in using biometrics to more easily and accurately identify your patients.
- Nurses or care workers visiting a patient's home using connected mobile health applications to monitor and track PHI.
- Physicians' remote access from PC or mobile devices to remote presentations, clinical portals, and shared workstations.
- Doctors accessing a patient's biographic data (vital signs) from wearable apps and other remote wireless monitoring devices.
- Internal password reset requests within hospitals and clinics.
- Hospitals and clinics offering patient portals to provide remote access to review lab results, Personal Health Information (PHI), and to schedule appointments.
- Hospitals and clinics providing mobile health applications to communicate, monitor, and support patients.
- Identifying patients in clinical trials, providing surveys and collecting patient status during the clinical trial.

For more information, contact us at (858) 673-8600 or sales@iwsinc.com

IWS IMAGEWARE SYSTEMS, INC.
Authentication Assured™

V180901