



# DigitalPersona® for Healthcare Organizations

## **RAPID, SECURE AUTHENTICATION FOR MEDICAL PROVIDERS AND STAFF**

Secure Access to Electronic Health Records

---

Streamline Clinical Workflow

---

Reduce Cybersecurity Costs

---

Protect Patient Data

---

# Protecting and Simplifying Access to EHRs

## PROTECTING ACCESS TO PATIENT DATA IS A REQUIREMENT

Market studies show more than 85% of healthcare organizations that experienced breaches incurred a remediation at an average cost of up to \$2M each.\* To avoid such losses, hospitals and medical practices are deploying strong authentication solutions that can manage how clinical staff access systems that use that data. This approach makes IT security stronger, easier to manage and more affordable.

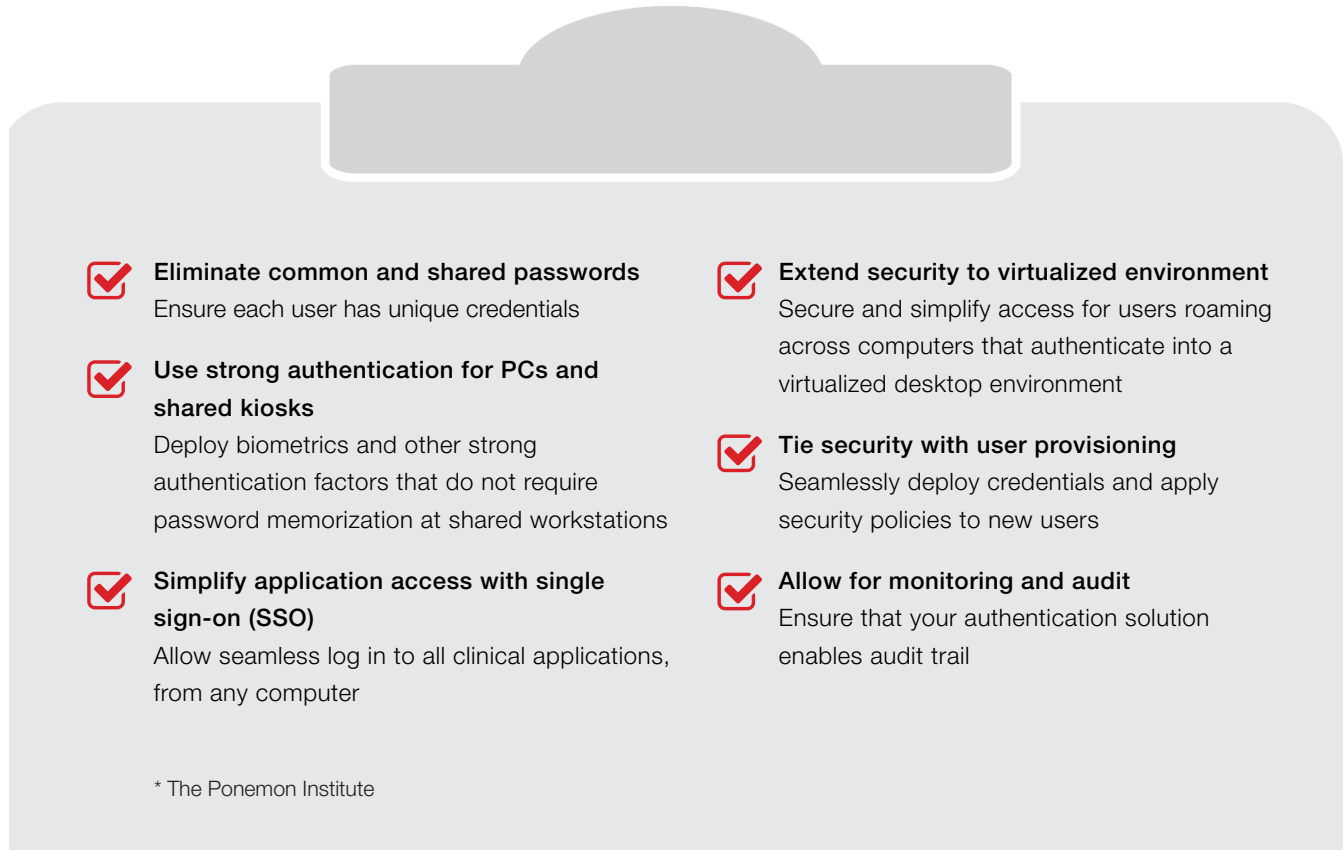
## FAST ACCESS TO HEALTH RECORDS, REGULATORY COMPLIANCE

While Electronic Health Record (EHR) and clinical systems are intended to make crucial information available to medical staff when they need it most, traditional security mechanisms often get in the way. When lives are at stake, clinical staff can't afford time needed to reset forgotten passwords or fumbling with cards or tokens. They need secure ways to get immediate access to data and applications – from any computer, at any time. The result is more time with patients, higher quality patient care and more satisfaction among clinical staff and patients. IT needs solutions that achieve compliance with regulations, while preserving the workflow doctors and nurses require.

## SECURITY INFRASTRUCTURE COST CONTAINMENT

Even with the risks and costs of security breaches, many hospitals and clinics struggle with tight IT security budgets. Most organizations have fewer than two employees dedicated to taking care of their security and compliance efforts. Strong security is a must; but to be practical, it also has to be affordable and easy to manage for IT and end users.

# Healthcare Security Checklist

- 
- ☒ **Eliminate common and shared passwords**  
Ensure each user has unique credentials
  - ☒ **Use strong authentication for PCs and shared kiosks**  
Deploy biometrics and other strong authentication factors that do not require password memorization at shared workstations
  - ☒ **Simplify application access with single sign-on (SSO)**  
Allow seamless log in to all clinical applications, from any computer
  - ☒ **Extend security to virtualized environment**  
Secure and simplify access for users roaming across computers that authenticate into a virtualized desktop environment
  - ☒ **Tie security with user provisioning**  
Seamlessly deploy credentials and apply security policies to new users
  - ☒ **Allow for monitoring and audit**  
Ensure that your authentication solution enables audit trail

\* The Ponemon Institute

# Composite Authentication for Healthcare

DigitalPersona is used by clinics and hospitals worldwide for more secure, compliant, easy and rapid authentication of medical providers and back-office staff into critical applications, workstations and networks. Leveraging your existing infrastructure, there is no ripping and replacing. DigitalPersona's technology integrates seamlessly with all environments – both cloud and client-server – to fit your existing workflows and supports all operating system platforms.

KEY BENEFITS FOR HEALTHCARE ORGANIZATIONS	
Increase Security And Reduce Fraud	Multifactor authentication that supports the widest range of authentication credentials, including biometrics which provide proof of presence.
Centralized Control for IT	IT managers use familiar Active Directory tools to centrally control security policies and authentication events.
Support Regulatory Compliance	The ability to use multiple factors and create complex passwords that users do not have to remember assists with meeting HIPAA and HITECH mandates. Event logs provide audit trails of who accessed what and when.
Eliminate Forgotten Passwords and Boost Productivity	Easy to use. Users simply scan a finger instead of remembering and entering complex passwords. Increases productivity.
Reduce IT Support Costs	The average cost of a password-related IT support call is \$70 (USD). DigitalPersona composite authentication significantly reduces the frequency of these types of calls.

## A BROAD ARRAY OF AUTHENTICATION FACTORS



### WHAT YOU KNOW

Password  
PIN  
Recovery Questions



### WHO YOU ARE

Fingerprint



### WHAT YOU HAVE

Smartcards and USBs  
Contactless Card  
Proximity Card  
Bluetooth Device  
One-Time Password



### WHAT YOU DO

Keystroke  
Behavioral  
Biometrics\*



### WHERE YOU ARE

GPS Location  
IP Address  
Geo-Fencing



### WHEN YOU ACT

Time Frame  
Geo-Velocity

TRADITIONAL FACTORS

RISK-BASED FACTORS

# DigitalPersona Architecture

DigitalPersona is an advanced authentication solution that fits well into healthcare environments. It deploys into any type of hospital environment – complex or simple – working with back-end systems to scale up to any size. The wide range of authentication methods ensures healthcare workers receive quick, secure access to the critical systems they need.



**DigitalPersona** provides a flexible, scalable and secure architecture that allows hospitals and healthcare organizations to deploy strong multifactor employee authentication to shared computing resources, applications and workflows.

Covered applications include: Allscripts, CareFusion, Cerner Millennium, Epic, GE Centricity, Kronos, McKesson, Meditech, Pyxis, QuadraMed, Softlab and more.

## Authentication Workflow



### Password Manager Controls The Traditional Login Screen

The ability to manually input a user ID and password can be disabled so that the DigitalPersona solution is now managing a randomized complex password that requires no memorization.



### Users Authenticate Rapidly

The user provides their assigned credential, such as a fingerprint, card, PIN or one-time password (OTP) to rapidly complete authentication. Security is further protected.



### DigitalPersona Completes Application Login

Once authenticated by the DigitalPersona authentication server, the user's credentials are automatically populated to complete the login process.

# Composite Authentication Use Cases for Healthcare



## **Preparing for Rounds**

When clinical staff prepare for visits, they log in to many applications and access patient data. With DigitalPersona, logging in to any application is seamless and more secure with strong authentication and SSO. No more shared or memorized passwords, notes or helpdesk calls.



## **Accessing Medical Records**

After visiting a patient, doctors and nurses update their records and prescribe medication from the shared thin clients available in patients' rooms. With fingerprint biometrics, authorized personnel quickly and securely log in to their clinical applications or personal virtual desktop.



## **Dispensing Medications**

Nurses often use mobile carts equipped with laptops. With DigitalPersona randomized complex password, which does not need memorization if a biometric authentication factor is in place, any authorized nurse can easily authenticate using fingerprints, smart cards or other easy credentials when dispensing controlled substances.



## **Offsite Patient Visit**

Doctors may forget their passwords when using laptops or tablets offsite. DigitalPersona provides an access recovery feature to avoid lockouts due to forgotten passwords. No network or Internet connection is required.



## **On Boarding New Staff**

When new employees are hired, they register their fingerprints or other approved credentials as part of the regular HR process. Their credentials are automatically provisioned throughout the environment so they can access their accounts, applications or virtual desktops from any computer.



---

**Crossmatch**

3950 RCA Boulevard, Suite 5001

Palm Beach Gardens, FL 33410

Tel: +1 561 622 1650

Fax: +1 561 622 9938

**crossmatch.com**

## About Crossmatch

Crossmatch helps organizations solve their identity management challenges through biometrics. Our enrollment and authentication solutions are trusted to create, validate and manage identities for a wide range of government, law enforcement, financial institution, retail and commercial applications. Our solutions are designed using proven biometric technologies, flexible enrollment and strong multi-factor authentication software, and deep industry expertise. We offer an experienced professional services capability to assess, design, implement and optimize our identity management solutions for a customer's individual challenges. Our products and solutions are utilized by over 200 million people in more than 80 countries.