Protecting access to patient data is a must-have

Market studies show more than 85% of healthcare organizations experienced data breaches in the past two years, at an average cost of up to $2M each.¹ To avoid such losses, many hospitals, medical practices and other businesses are deploying security solutions that can encrypt data and, at the same time, manage how clinical staff access systems that use that data. This comprehensive approach makes IT security stronger, easier to manage and more affordable.

Make EHR work for doctors and nurses – Fast access to health records, more time with patients

While EHR 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, your clinical staff cannot spend their time logging on to PCs, typing passwords that change every month 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.

Comply with HIPAA/HITECH without disrupting clinical workflow and processes

When life is at stake, there is no time for changes that could affect how services are delivered. IT needs solutions that achieve compliance with regulations, while at the same time preserving the workflow doctors and nurses require.

Save money, too

Even with the risks and costs of security breaches, many hospitals and clinics struggle with small security budgets. Most organizations have fewer than two employees dedicated to taking care of their security and compliance efforts.² 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

- Get rid of common passwords and Post-it Notes
  Ensure each user has and uses his own credentials
- Use strong authentication for PCs and shared kiosks
  Deploy biometrics or other credentials, also at shared workstations
- Simplify application access with Single Sign-on (SSO)
  Allow seamless logon to all clinical applications, from any computer
- Deploy Full Disk Encryption on all laptops
  Make sure access to data is secure even if PCs are lost or stolen
- Protect remote access to the network
  Implement strong authentication for logging on through VPN
- Secure e-communications with digital signature
  Ensure authenticity and accountability of e-prescriptions and email
- Extend security to virtualized environment
  Secure and simplify access for users roaming across computers
- Tie security with user provisioning
  Seamlessly deploy credentials and apply security policies to new users
- Allow for monitoring and audit
  Make sure you know who did what and when, if needed
**Strong Authentication, SSO and Data Protection**

*Now integrated into one, single solution*

**DigitalPersona® Pro – When security and compliance require comprehensive security**

DigitalPersona Pro is a leading suite of centrally-managed security applications that protects data and controls access to PCs and applications. By combining solutions such as Full Disk Encryption, Strong Authentication and Single Sign-On (SSO), DigitalPersona Pro uniquely integrates access management and data protection solutions enabling you to achieve security and compliance with immediate ROI and lower costs. DigitalPersona Pro is the choice of thousands of businesses and government agencies worldwide.

---

**Flexible management options**

DigitalPersona Pro Workgroup is a self-contained, SQL-based solution. DigitalPersona Pro Enterprise configuration snaps into Active Directory for maximum scalability and integration.

**Centralized auditing and reporting**

Centralized event collection allows for auditing and reporting. You can run reports on the security status, investigate suspicious events, or even integrate with your existing log collection system.

**Single Sign-On (SSO) into all Enterprise applications**

With no changes to existing apps, IT can enable Single Sign-On into any Enterprise application, including Web apps, Windows applications, Terminal Services, Citrix, AS/400, and more.

**Support for shared PCs, Citrix, VMware, TS, RDP**

DigitalPersona Pro supports kiosk-style workstations where users share a common Windows account. Within thin client environments, users can log onto their virtualized desktop in a snap and keep working as they move from PC to PC.

**Full Disk Encryption**

AES 256-bit encryption locks the hard drive. Support for multi-credential authentication, including fingerprints and smart cards. Remote access recovery prevents lockout emergencies.

**50% cost savings, modular design**

Managing many security apps from one solution helps you save as much as 50% in immediate costs. With the modular design, you can start from one application now and then add more over time.

**OTP for RADIUS VPNs – without tokens**

Add one-time password security to RADIUS apps such as VPNs, Citrix, OWA. Users can use fingerprints, face recognition or cards to generate the OTP automatically, or use their smart phones or traditional hardware tokens.

**Strong authentication with biometrics, cards, tokens**

From biometrics to tokens and cards, DigitalPersona Pro makes strong authentication simple and affordable for disk encryption, PC login, Enterprise applications and VPN access. It also supports shared PCs using a common Windows account.
Preparing for a round of visits in the ward

When clinical staff prepare for visits, they log on to many applications and access patient data. With DigitalPersona Pro, logging on to any application is seamless and more secure with strong authentication and Single Sign-On. No more shared passwords, Post-it® notes or helpdesk calls.

Accessing medical records from patients’ rooms

After visiting a patient, doctors and nurses update their records and prescribe drugs from the shared thin clients available in patients’ rooms. With fingerprint biometrics, doctors just place their finger on the reader to quickly and securely log on to their clinical applications or personal virtual desktop.

Dispensing medications and drugs from carts

To provide medications or drugs prescribed by doctors, nurses often use mobile carts equipped with laptops. With DigitalPersona Pro, any authorized nurse can easily authenticate using fingerprints, smart cards or other credentials when dispensing controlled substances.

Emailing prescriptions to pharmacies

After visiting patients, it is time for office work. Doctors email prescriptions to pharmacies. Using DigitalPersona Pro, their digital signature ensures authenticity of the prescription.

Offsite patient visit

Doctors may carry laptops or tablets with patients’ records. DigitalPersona Pro protects data with full disk encryption from theft, loss or from unauthorized access. Doctors unlock disk encryption quickly and easily and then securely log on to the network using a VPN with two-factor RADIUS authentication.

Adding a new clinician to the staff

When new employees are hired, they register their fingerprints or smart cards 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.
Single Sign-On Support for Healthcare applications

DigitalPersona Pro provides support for a broad range of Healthcare and other Enterprise applications, with no change required to the existing environment. Our customers have used DigitalPersona Pro with thousands of healthcare-related applications, including:

- Allscripts
- CareFusion
- Carestream Health
- Cerner Millennium
- Cerner Proworks
- Claims Administrator
- Courion
- Dolphin Healthcare
- eClinicalWorks
- Eclipsys
- Embla
- Epic
- Fisher International
- Fujitsu Healthcare Solutions
- GE Centricity
- GE Medical
- HealthMEDX
- Horizon Business Folder
- Horizon Patient Folder
- IBM iSeries/AS400
- IBM Tivoli
- IMPAX
- Keane
- Kronos
- Magic
- McKesson
- MediTab
- Meditech
- MedPlus
- Medtuity
- MercuryMD
- Misys
- Misys Tiger
- NextGen Healthcare
- OBIX
- Paragon
- Pathways Compliance Advisor
- Pyxis
- QuadraMed
- Siemens Invision
- Softlab
- Systoc
- T-Systems
- Thomson
- WellSoft Emergency

“The DigitalPersona Pro solution provides quick, secure access to our electronic systems including our EHR, improving clinician-patient interaction at the point of care. Since deploying DigitalPersona Pro, we’ve experienced a reduction in helpdesk calls for password resets, particularly from contingent staff. This improves overall efficiency and reduces our IT costs.”

Carl Zani, IT Director, Memorial Hospital

“The DigitalPersona solution allows our staff to obtain information faster while providing a higher level of security to confidential client information”.

Janette Schroeder, RN CSU Coordinator, The Nord Center

“DigitalPersona’s strong authentication capabilities provide quick and secure access to patient data while our doctors make their rounds. Our physicians really appreciate the time it saves them.”

Richard Caldwell, VP of Support Services, Jackson Hospital

Disclaimer
THE INFORMATION IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED TO BE ANYTHING OTHER THAN THE EDUCATED OPINION OF THE AUTHOR. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT DIGITALPERSONA MAKES NO CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS, OR ADEQUACY OF THE INFORMATION. THIS INFORMATION SHOULD NOT BE RELIED UPON AS LEGAL ADVICE. DIGITALPERSONA SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS OR COMPLIANCE WITH ANY LEGAL REQUIREMENTS.

2 Id. at 1.

© 2010 DigitalPersona, Inc. All rights reserved. DigitalPersona, is a trademark of DigitalPersona, Inc. registered in the U.S. and other countries. All other brand and product names are trademarks or registered trademarks of their respective owners.