



Solving the Weakest Link in Healthcare Security: Passwords

A Digital Persona, Inc.
White Paper
February 2006

Digital Persona, Inc.
1+ 650.474.4000
www.digitalpersona.com

Table of Contents

Introduction.....	1
The Problems with Passwords.....	1
Password Costs	1
Government Regulations.....	2
Alternative Authentication Solutions.....	2
The Answer to the Healthcare Authentication Dilemma	3
Features That Ensure Security and Ease of Use.....	3
Unprecedented Control Across an Organization.....	4
Summary	5
About Digital Persona.....	5

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), makes protecting and securing confidential patient data a key concern for healthcare IT professionals. One of the main challenges is balancing HIPAA requirements of developing secure systems and procedures ensuring the confidentiality of patient medical records – without compromising the medical professional's need for quick, simple access to critical health data.

Passwords are still the most pervasive tool used to secure systems. As a result, the cost of managing password-based security represents a growing burden for the healthcare IT professional. Despite countless expenses and hours in creating guidelines, procedures and purchased safeguards, one user can still override all IT's efforts by simply sharing a password.

Many healthcare IT professionals have responded to HIPAA requirements by creating stricter password policies, effectively shifting the burden of compliance to their users. Policies include using longer and more complex passwords while still requiring passwords to be changed at regular intervals.

Unfortunately stricter password guidelines have spawned a significant increase in password-related help desk calls for healthcare organizations. Increasingly, frustrated healthcare professionals are hesitating to follow password guidelines. When a staff member cannot quickly access patient data, productivity decreases; in an emergency situation, more creative ways of accessing patient data are attempted – including borrowing another user's password.

This white paper addresses the problems associated with passwords in the healthcare organizations and describes how fingerprint authentication technology can eliminate the temptation for users to share passwords – eliminating the vulnerabilities and costs of the network's weakest link.

The Problem with Passwords

Passwords exist for two reasons: to ensure users can get into their account and to ensure that non-authorized users cannot. Under HIPAA, IT professionals often end up imposing procedures and policies that users view as being unnecessarily

complicated. When users are required to have many different passwords or to change their passwords frequently, the "human factor" begins to erode the very security benefits which passwords are intended to provide. Given the choice, users overwhelmingly choose passwords that are easy to remember, assigning the same password to multiple applications and keeping their passwords for months or years. When asked to change their passwords more frequently, they "recycle" old favorites.

- 40% of all help desk calls are for forgotten passwords.
- Each year companies spend up to \$150 per user trying to maintain secure passwords.
- Up to 15% of annual IT budget is spent on information security.

Gartner Group

"The 2002 NTA Monitor Password Survey found that the typical intensive IT user now has 21 passwords, and has two strategies to cope, neither of which is advisable from a security standpoint: they either use common words as passwords or keep written records of them. The survey found that heavy users maintain up to 70 passwords. Forty-nine percent write their passwords down or store them in a file on their PC. "

As the number of passwords per employee increases, the likelihood of them being forgotten rises. As a result, the costs of managing password-based security represent a growing burden for most organizations. In most cases, security may be abandoned for convenience.

Users also share passwords with colleagues – and not just occasionally.

"4 out of 5 workers will disclose their passwords to someone in the company if asked."

**PentaSafe Security Technologies,
CNET**

In the attempt to prevent password compromises, IT professionals develop security policies that

specify parameters for passwords and rules for using them:

- Passwords must be at least some specified number of characters long and must contain a combination of letters, numbers and symbols
- Passwords must be changed quarterly, monthly, weekly, or even more frequently
- Access to each application must be controlled by a separate password
- Passwords must be memorized

While these rules seem logical from a security perspective, the fact is that they are difficult for people to follow, difficult to enforce and not very effective. Complex password protection schemes are simply not practical for healthcare workers or for the IT departments that must enforce them. HIPAA increases the burden by requiring modes of access to be changed twice a year. Imagine the workload for a hospital administrator who must oversee the process of changing passwords and PIN codes for thousands of doctors and medical personnel, many of whom may not willingly participate in the process.

Thus, frequent password changes intended to improve password protection serve to exacerbate the problem, making passwords even harder to remember and increasing the likelihood that users will compromise their secrecy by writing them down. This could lead to passwords becoming ineffective as a method of authentication.

Password security policies rely on end-user cooperation. Healthcare information systems are only as secure as their least responsible user.

With a biometric system, frequent changes of passwords and PIN codes are not required.

Password Costs

The more complicated the password policy, the more expensive it is to implement and support. Between 25-50% of calls into help desks are for password resets. It is estimated that the typical enterprise spends an average of \$150 USD per user, per year to support password resets according to Andreas Faruke, head of Deloitte & Touche's Identity Management Services in Canada. In an organization with just 1000 users, that's \$150,000 a year – an expense that could be virtually eliminated with a truly effective, easy-to-use and implement, authentication solution.

In fact, the Department of Defense achieved a 90% reduction in their password-related help desk calls after a fingerprint biometric deployment.¹

The costs reported above do not include lost productivity due to user down-time and frustration or the forensic costs of investigating breached security – a sure nightmare for any IT organization. According to the Computer Emergency Response Team (CERT), 80% of the security attacks they investigate are password-related.

They also do not include potential loss of income. Physicians who use the system day in and day out value the ability to access applications easily and quickly; the less time they spend throughout their day trying to log on, the more time they have to dedicate to patients. Physicians often work with multiple medical facilities and must keep track of many different logon credentials and password policies. Thus, anything that makes a medical facility easier to work with is liable to encourage them to bring more patients there – and, with them, more revenue.

Using fingerprint sensors provides the competitive edge over other healthcare facilities, reducing the need for complicated, ever-cycling password policies that discourage end-users, and creating ease of access that encourages healthcare professionals.

Government Regulations

Government regulations are creating additional pressure to provide better security for private information:

- The Health Insurance Portability and Accountability Act (HIPAA) mandates that individually-identifiable health information must be kept private and secure. HIPAA, as written, affects virtually all healthcare-related information created or received in virtually any medium by the healthcare industry or an employer. Password costs are not limited to maintaining passwords, but also include the potential \$250,000 fine or imprisonment of up to 10 years or both, for wrongful disclosure with intent to sell information.

¹ FEDERAL COMPUTER WEEK, "Applications at Their Fingerprints.", 8/9/04

- The Sarbanes-Oxley (SOX) Act of 2002 requires higher security standards for data that is financial or confidential. According to this act, any public company may be liable if it has not taken adequate steps to protect this type of data. Many existing password and security policies would not be considered sufficient under SOX.

Laws such as these, coupled with stiff penalties for non-compliance, have forced healthcare organizations to take a closer look at their information security protocols.

Alternative Authentication Solutions

The past few years have seen the emergence of many alternatives to traditional password-based security. Organizations have turned to solutions such as tokens, smart cards and Single Sign-On (SSO) solutions to address the weaknesses of password-based systems.

Tokens and smart cards offer an added level of security, but also add complexity and cost. Tokens are difficult to use and, like smart cards, they require a significant up-front investment in deployment and integration with the organization's applications and network infrastructure. In many cases, tokens and smart cards have been confined to users who travel or work remotely, or who are working with the most sensitive information.

Single Sign-On has grown in popularity because of its ease of use. However, providing a single entry point via a password to multiple systems makes an organization far less secure than a separate password for each system. Organizations are often surprised to uncover the hidden costs and issues associated with setting up SSO systems, including significant costs required to integrate with each application. To address security risks of SSO, many organizations feel compelled to introduce a Public Key Identification (PKI) infrastructure, thus adding more complexity in implementation, IT management, and user requirements.

The Answer to the Healthcare Authentication Dilemma

Fingerprint authentication technology addresses healthcare security issues that other password-based systems cannot:

- Fingerprints are a credential that cannot be lost, forgotten, or easily shared.
- Using fingerprint authentication for access control helps ensure that only authorized users can gain access to personal and sensitive information.
- Protecting access with fingerprints also makes it possible to provide an accurate audit trail, an important consideration in complying with HIPAA regulations.

One large manufacturer of pharmaceutical dispensing equipment used Digital Persona's software development kit to incorporate fingerprint access into their equipment. By requiring a fingerprint to access the pharmaceuticals, they eliminated the password problem of shared passwords. Their system monitors and provides only authorized users access to medications.

Replacing password entries (and memory requirements) with a simple touch of a finger eliminates the high costs, administrative overhead and security risks associated with traditional password-based systems. Fingerprint systems are easy for users, convenient and cost-effective to implement and – most importantly – more secure.

Don Davis, the Chief Information Officer and Senior Vice-President of Information services for Rite Aid, said their decision to use Digital Persona technology in their pharmacies was based on "the efficiencies we felt we would obtain from not having to administer password resets, the speed of logging into the system, audit trail creation and compliance with role-based tasks." Rite Aid is anticipating a fast return on their investment.

Digital Persona provides fingerprint authentication solutions that offer a combination of security, convenience, ease-of-use and management tools that surpass traditional password policies. The company's flagship solution, DigitalPersona® Pro, includes a fingerprint reader and software application suite that delivers reliable, virtually impenetrable, security for an organization's most sensitive data, yet is the easiest and most cost-effective user authentication available.

With the touch of a finger, a user is automatically authenticated against their centrally managed fingerprint credentials in Microsoft Active Directory. Provided their fingerprint credentials match, their user name, password and any other logon credentials required for most applications or Web services are automatically and securely submitted without ever having to type in a password. For security and privacy reasons, the user's fingerprint

is never stored – only encrypted data collected from minutia data points on the user’s fingerprint is retained. The data points are converted into a string of numbers and then encrypted with a set of algorithms, making their misuse extremely difficult.

Features That Ensure Security and Ease of Use

In clinical trials, one California medical device manufacturer uses the fingerprint reader to keep track of who accessed and updated patient records. After signing into the application, employees continue to use the reader to initial forms and do subsequent authentication beyond the initial log on.

Among the features that differentiate DigitalPersona Pro are its password management and centralized authentication control. Using an “Identity Lockbox” feature, which is a secure and encrypted location within the Microsoft Active Directory; DigitalPersona Pro automatically stores and manages user logon names and passwords for each application being accessed. Each lockbox can only be “opened” by the person to whom it is “registered.”

Since all it takes to identify a user and gain access to the appropriate lockbox is a simple touch of a finger on a reader, users need no longer remember passwords. Thus, there is no longer any need to write them down. Furthermore, since a fingerprint cannot be shared or duplicated like a password, the risk of social engineering attacks is dramatically reduced.

DigitalPersona Pro can also be configured to automatically create and assign a randomized password for each application a user accesses. When this option is selected, passwords are automatically entered, created, updated and stored. This password randomization capability further enhances security because the end-user does not know their password. Therefore, the password can be substantially more complex than a user-selected password. This further protects organizations against brute force or dictionary attacks.

For shared workstations like a nursing station, DigitalPersona Pro Kiosk improves security and shared workstation productivity. In a hectic environment where seconds can make a difference, remembering to sign out of a patient record may be easily forgotten leaving access to confidential patient data and systems vulnerable.

DigitalPersona Pro Kiosk eliminates the need to log on and out of Windows. Kiosk provides multiple

users quick access to shared applications on a single PC by simply touching the reader.

One large California hospital system has resolved their staff’s frustration about always having to sign in and out of shared workstations with DigitalPersona’s Kiosk program. Nurses often meet with patients prior to the doctor’s visit and enter data into the patient’s record in the workstation in the examination room. With Kiosk, doctors only need to touch the same reader to quickly sign in as themselves. Often the patient’s record is already on the screen, ready to go. By using Kiosk, the hospital system has enhanced their workflow process, increased productivity, and kept an audit trail for HIPAA compliancy while eliminating a significant issue for their staff.

With DigitalPersona Pro, end-users no longer have to store and remember the myriad of passwords required to log into their applications. There is little chance that they will forget their fingers when they come to work for the day. Help desk calls plummet. The whole login experience – to the network, to applications and to Web services/Web sites – is made convenient and, users claim, fun!

Fingerprint authentication can also be enhanced with additional security layers (a practice called “two factor” security) such as adding multiple fingerprints to an authentication scheme. This is essentially a no-cost solution, although it requires users to use the fingerprint reader twice for each authentication.

Unprecedented Control Across an Organization

DigitalPersona Pro includes administrative tools that provide central control of authentication and password management policies. DigitalPersona Pro integrates with Microsoft Active Directory and Group Policy Object administration tools to allow IT personnel to set authentication policies for specific applications or users. A wizard enables administrators to create templates which can fingerprint-enable Windows, Internet or custom applications. IT administrators can create these templates without the need for programming or professional services assistance. In any healthcare environment, Pro is used to authenticate in over 75 to 125 different applications including mainframe, emulators and regular applications, through our One Touch® Sign On (OTS) software. Through our many healthcare deployments, DigitalPersona has tested our OTS with a vast array of medical software programs including Siemens, Cerner,

Meditec, McKesson, Epic Systems, IDX Systems, Per-Se and Eclipsys.

Digital Persona recently expanded their hardware support for integrated UPEC devices like tablets, thin clients, laptop PCs and mobile carts.

The seamless integration of DigitalPersona Pro with Microsoft Active Directory makes it possible for administrators to delete a user's access to all applications when needed by simply deleting that user's Identity Lockbox within Active Directory.

DigitalPersona Pro's fingerprint authentication solution scales to healthcare organizations of any size. The end-to-end solution consists of a fingerprint reader, as well as Workstation, Kiosk and Server software. Organizations large and small have found the set-up to be straightforward and far less costly than supporting passwords.

Top 5 Advantages of Fingerprint Authentication

- **Secure Authentication**
Identity is based on who you are (fingerprint) versus what you know (password)
- **Ease of Use**
Quick access to patient data
- **HIPAA Compliance**
Restricts access, protects patient data and provides audit trail (164.308 and 164.312 HIPAA standards)
- **Accountability**
Comprehensive audit trail of each user, minimizing misuse
- **Quick Return On Investment**
Reduces help desk costs and increases productivity

Summary

More than ever before, healthcare organizations are concerned about HIPAA compliance; ensuring only proper users – those who are authorized – have access to sensitive patient data and applications.

Passwords are even less secure today, despite more stringent requirements such as 90 day expirations and strings that must be a certain length. Passwords should be managed automatically, where humans aren't required to remember or keep track of them.

With the number of initiatives and tasks facing IT departments only increasing, it is imperative that solutions and procedures for simplifying the authentication process are put in place. Regardless of how secure a new technology promises to be, if it's hard to use or inconvenient for end-users, it won't be accepted. Biometrics technology has evolved to the point where it is possible for any organization to implement non-intrusive, reliable and affordable solutions that reduce cost and complexity while increasing security and compliance.

Fingerprint authentication has proven to be effective in healthcare and alleviates the IT nightmare of dealing with identity management issues. Fingerprints address healthcare's HIPAA compliance challenge of maintaining patient confidentiality while providing fast, easy access to critical health data. Digital Persona provides leading fingerprint authentication solutions that offer simplified sign-on capabilities which address user compliance, security and resolve the weakest link, passwords.

About Digital Persona

Digital Persona is the leading provider of biometric authentication solutions for enterprise networks and commercial applications. Founded in 1996, Digital Persona designs, manufactures and sells turnkey solutions that improve security and regulatory compliance while resolving password management problems. Its award-winning fingerprint technology is used worldwide by over 25 million people in the most diverse and challenging environments.

Digital Persona has strategic relationships with market-leading manufacturers and resellers including Intel, Dell Inc., Microsoft, GTSI Corp. and Hewlett-Packard. DigitalPersona® Pro, the company's flagship turnkey security solution for enterprise authentication, is used by leading organizations such as Sutter Health/CPMC, Rite Aid, the U.S. Department of Defense, Cargill, and United Bankers' Bank.

Additional information is available by contacting Digital Persona, Inc. at +1 650.474.4000 or at www.digitalpersona.com.

© 2006 Digital Persona Inc. All rights reserved. DigitalPersona and One Touch are the trademarks of Digital Persona, Inc., registered in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.