

# Simplifying Compliance with HIPAA and HITECH Security and Privacy Rules



August 2010

## HIPAA and HITECH: Setting security standards for healthcare

The Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 have raised the bar of security within the Healthcare industry.

New standards have been put in place aimed at protecting Electronic Health Records (EHR), Personal Health Records (PHR), and Protected Health Information (PHI). Hospitals, clinics and other healthcare providers are now responsible for security violations occurring within their or their business associates' organizations.

HIPAA and HITECH include various requirements that are often grouped into two main categories:

- Security Rules
- Privacy Rules

Security Rules describe how healthcare providers should protect access to sensitive information, such as PHR or PHI. Privacy Rules determine patients' rights to confidential treatment of their health-related information and specify the duties healthcare providers have to ensure such confidentiality.

The consequences of not complying with HIPAA or HITECH are substantial. Consequences for violators may include civil and criminal charges, fines, obligations to notify the public or even the media of the incidents, and more.

### Access control and data protection are requirements for compliance

At a very high level, the HIPAA and HITECH Security and Privacy Rules require the adoption of

comprehensive security measures that include access control and data protection solutions.

For example, HIPAA sections 164.300 *et seq.*, 164.400 *et seq.* and 164.500 *et seq.* clearly indicate that healthcare providers should not limit themselves to either access control or data protection solutions, but rather adopt a more comprehensive approach to security:

Section	Requirements
164.308(a)(3)(i) Workforce security	Access control, data protection
164.308(a)(3)(ii)(B) Workforce clearance procedures	Access control
164.308(a)(3)(ii)(C) Termination procedures	Access control
164.308(a)(4)(ii)(B) Access establishment and modification	Access control
164.308(a)(5)(ii)(C) Log-in monitoring	Access control
164.308(a)(5)(ii)(D) Password Management	Access control
164.310(b) Workstation use	Access control, data protection
164.310(c) Workstation security	Access control, data protection
164.312.(a)(1) Access control	Access control
164.312.(a)(2)(ii) Emergency access procedure	Access control
164.312.(a)(2)(iv) Encryption and decryption	Data protection
164.312.(b) Audit controls	Access control, data protection
164.312.(d) Person or entity authentication	Access control
164.312.(e)(2)(ii) Encryption	Data protection
164.404 <i>et seq.</i> Notifications to individuals	Data protection
164.500 <i>et seq.</i> Uses and disclosures of protected health information	Data protection

### HIPAA and HITECH compliance with DigitalPersona® Pro

DigitalPersona Pro provides businesses of all sizes with a powerful, flexible solution for preventing unauthorized access to data and computer systems.

DigitalPersona Pro provides efficient management of multiple security and authentication applications, simplifying healthcare providers' efforts to achieve security and compliance. In addition, its low Total Cost of Ownership and compatibility with existing

infrastructure enable organizations to boost the return on investment of their existing systems.

The following examples show how DigitalPersona Pro can assist organizations with HIPAA requirements.

The screen images shown are from DigitalPersona Pro Enterprise, which provides Active Directory based management of security and authentication policies to organizations of any size. Most capabilities are also available in DigitalPersona Pro Workgroup, which provides easy-to-manage, affordable, out-of-the-box security for small businesses and departments within larger organizations.

### Case 1. Compliance with HIPAA 164.404 et seq.: Notification to individuals

HIPAA 164.404 requires organizations to notify individuals if unprotected, health-related personal identifiable information is lost or stolen. A typical case might be a doctor who loses his laptop containing patient records or information.

However, hospitals, clinics and other businesses can avoid having to notify individuals – thus escaping the associated costs – if the lost personal identifiable information was properly encrypted according to standards imposed by the National Institute of Standards and Technology (NIST)<sup>1</sup>.

DigitalPersona Pro can help meet the requirements imposed by HIPAA 164.404 by providing several security methods to protect all data stored on a computer.

<sup>1</sup> *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009*, Department of Health and Human Services.

With DigitalPersona Pro, IT Managers can enforce encryption of the entire hard drive on managed computers by implementing DigitalPersona Pro's Full Disk Encryption feature.

Once the hard drive is encrypted, users will be required to provide proper authentication credentials (password, fingerprint or smart card), according to policies specified by the IT manager, before the Windows operating system starts (i.e. pre-boot authentication).



For convenience, once the drive has been unlocked using proper credentials, DigitalPersona Pro provides the option for authorized users to automatically log on to Windows without further authentication by using the Single Sign-On feature called One-Step Logon.

DigitalPersona Pro's Full Disk Encryption meets the technical requirements mandated by NIST for both data at rest and data in motion, which include AES algorithm and/or FIPS 140-2.

### Case 2. Compliance with HIPAA 164.312(d): Person or entity authentication

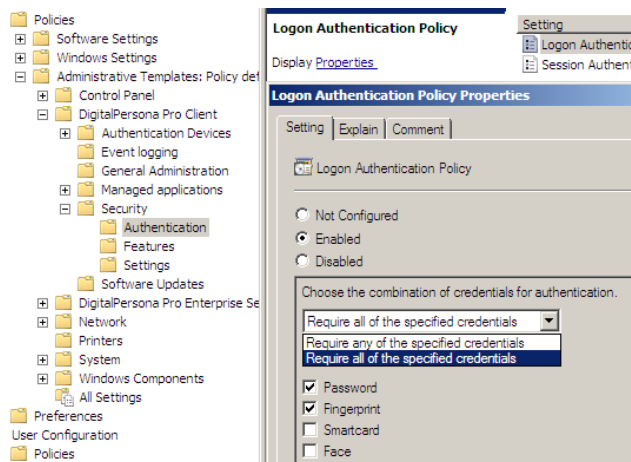
HIPAA 164.312(d) requires organizations to “[...] implement procedures to verify that a person or an entity seeking access to electronic protected health information is the one claimed [...]”. A typical case

might be two doctors sharing credentials to log on to computers or applications.

DigitalPersona Pro supports strong authentication which helps IT Managers meet the requirements imposed by HIPAA 164.312(d). Two-factor authentication, including biometrics, makes it more difficult for users to share credentials, thus reducing the risk of unauthorized access. DigitalPersona Pro also supports shared workstations and kiosks.

With DigitalPersona Pro, IT Managers can select and enforce authentication policies for computers and application logon in just a few steps. For example, to mandate a two-factor logon policy requiring a password and a fingerprint, IT Managers can use DigitalPersona Pro Enterprise to:

1. Go to the Active Directory **Group Policy Management Editor**
2. Browse to **Computer Configuration > Policies > Administrative Templates > DigitalPersona Pro client > Security > Authentication**
3. Double-click the **Logon policy** policy object
4. Select **Enabled**
5. Select **Require all of the specified credentials**
6. Select **Password and Fingerprint**

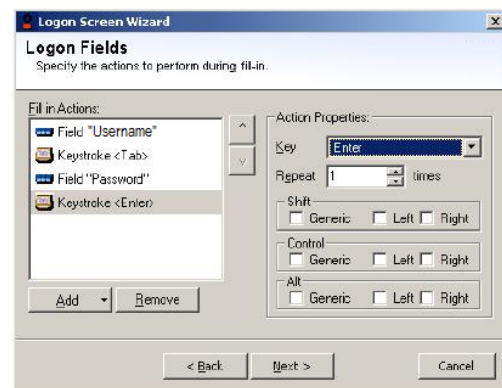


### Case 3. Compliance with HIPAA 164.308(a)(5)(ii)(D): Password management

According to HIPAA 164.308(a)(5)(ii)(D), organizations should use “[...] procedures for creating, changing and safeguarding passwords [...]”. A typical case might be the need of enforcing strong passwords to log on to enterprise medical applications.

DigitalPersona Pro can help meet the requirements imposed by HIPAA 164.308(a)(5)(ii)(D) by allowing IT Managers to configure password management and Single Sign-on to all enterprise applications. IT Managers may even want to randomize passwords, thus making it difficult to share credentials.

With DigitalPersona Pro Enterprise, IT Managers set up application logons through a simple wizard. Setup only takes a couple of minutes per application and requires no changes to the existing application. Support extends to virtually all applications, such as Citrix®, Epic®, Meditech® and SAP®, as well as Web, Windows and terminal applications.



IT Managers can also choose to configure authentication policies for managed applications to require no credentials (i.e. Single Sign-On) or any combination of passwords, smart cards, and biometrics, such as fingerprints.

Once the logon is configured, IT Managers can deploy this information to managed workstations through Active Directory Group Policy Objects.

#### Case 4. Compliance with HIPAA 164.312

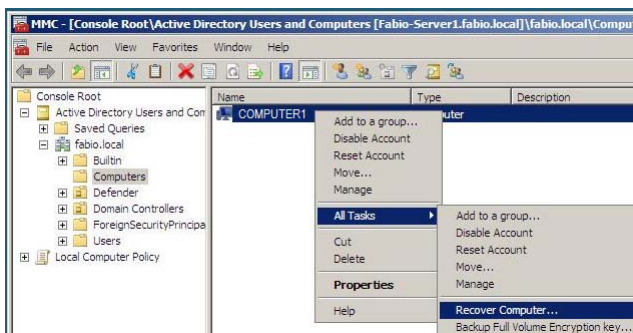
##### (a)(2)(ii): Emergency access procedure

HIPAA 164.312(a)(2)(ii) requires subject organizations to “[...] establish [...] procedures for obtaining necessary electronic protected health information during an emergency [...]”. For example, a hospital may need to access information stored on an off-duty doctor’s computer.

DigitalPersona Pro can help meet the requirements imposed by HIPAA 164.312 (a)(2)(ii) by allowing IT Managers to recover access to managed computers, even if they are protected with BIOS-level security, full disk encryption, multi-factor authentication and no network connectivity is available.

With DigitalPersona Pro Enterprise, IT Managers can retrieve emergency access codes in just a few steps:

1. Go to **Users and Computers Snap-in** in MMC
2. Browse to **Computers** and select the PC to be recovered
3. Right-click > **All Tasks > Recover Computer**
4. Type or provide to the user the one-time access code displayed in the dedicated dialog box



By typing a one-time access code as a password at computer logon (BIOS, full disk encryption or Windows authentication), users are able to get access to the medical records stored on the encrypted PC.

#### To Learn More

For more information about DigitalPersona Pro, visit [www.digitalpersona.com/pro](http://www.digitalpersona.com/pro) or contact us at:

- Email: [sales@digitalpersona.com](mailto:sales@digitalpersona.com)
- In North America, call: +1-650-474-4000
- In EMEA, call: +44-203-286-4004

Free trials are also available.

#### About DigitalPersona

DigitalPersona, Inc. is a global provider of authentication and endpoint protection solutions that make security simple, practical and affordable for businesses of all sizes. The company helps enterprises, government agencies, custom application developers and independent software vendors to efficiently address growing security, compliance and fraud-prevention demands. DigitalPersona’s award-winning technology is offered by market-leading computer manufacturers and solution providers around the world.

#### Disclaimer

THE INFORMATION IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. 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. DIGITALPERSONA SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

© 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.