



## SOLUTION OVERVIEW



# Security Solutions

to Support Compliance with the Health Insurance  
Portability and Accountability Act (HIPAA)



Where it all comes together.™



## KEY BENEFITS

### *Supports Rapid, Cost-Effective Compliance*

VeriSign security solutions help healthcare organizations achieve compliance with §164.308 and §164.312 of HIPAA Security Standards.

### *Minimizes New Security Investments*

Healthcare organizations can reduce the costs of planning, developing, and implementing a security infrastructure needed to help achieve HIPAA compliance.

### *Establishes a Flexible, Extensible Security Program*

VeriSign solutions help establish policies, procedures, guidelines, and technologies for complying with HIPAA and other regulations and achieving business priorities.

As healthcare organizations move information online to automate business processes, streamline communications, and improve customer service, safeguarding electronic data has evolved from an internally defined business practice to an externally imposed requirement of the federal government. Health plans, clearinghouses, healthcare providers, Medicare/Medicaid agencies, and other healthcare organizations must comply with federal Health Insurance Portability and Accountability Act (HIPAA) regulations regarding the confidentiality, integrity, and availability of private health information. To comply with these mandates, healthcare organizations must assess risks, correct weaknesses, and establish mechanisms for proving regulatory compliance.

The U.S. Department of Health and Human Services issued the Final Rule on HIPAA Security Standards in February 2003 (45 Code of Federal Regulations [CFR] Parts 160, 162, and 164). Most healthcare organizations were required to comply with the Final Rule on Security Standards by April 21, 2005. As noted in the Final Rule on Security Standards, “[T]he implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as the lack of adequate security can increase the risk of violation of the privacy standards.”

VeriSign offers a suite of services to support healthcare organizations in complying with HIPAA Security Standards:

- **VeriSign® Managed Security Services** – Support compliance with security management requirements, through 24/7 management of the network security infrastructure, as required by 45 CFR Parts §164.308(a)(1) and §164.308(a)(6)
- **VeriSign® Global Security Consulting** – Enables organizations to conduct risk analysis and implement risk management measures as required by §164.308(a)(1)
- **VeriSign® Unified Authentication** – Enables healthcare organizations to establish procedures for person and entity authentication, as required by §164.312
- **VeriSign® Managed Public Key Infrastructure (Managed PKI)** – Enables healthcare organizations to address integrity control and encryption as required by §164.312

## + Compliance and Risk Assessment

VeriSign leverages deep expertise, proven methodologies, and state-of-the-art tools to thoroughly assess the current state and vulnerability of existing network security implementations including policies, technology, operations, use, performance, and physical security. VeriSign identifies immediate security concerns, and then pinpoints gaps between the current infrastructure and identified requirements for HIPAA compliance, overall system security, and projected growth. Using the assessment and gap analysis, VeriSign provides prioritized recommendations for improving performance, mitigating risk, and ensuring compliance with the identified requirements.

## + Security Management Process

To comply with HIPAA, healthcare organizations must “implement policies and procedures to prevent, detect, contain, and correct security violations” (§164.308 [a][1]). In addition, they must be able to maintain audit trails for all data activity and system events (§164.312 [b]). The VeriSign Managed Security Services suite enables organizations to delegate security infrastructure management to a team of experts whose core business is security.



### CASE EXAMPLES OF HIPAA COMPLIANCE

- A Fortune 500 healthcare provider uses VeriSign Managed PKI and VeriSign Secure Sockets Layer (SSL) certificates to accept digitally signed and validated prescriptions from caregivers.
- A leading pharmacy benefit management provider uses VeriSign digital certificates to authenticate group administrators to its extranet.

The suite of services (e.g., firewalls, intrusion detection systems, intrusion prevention, and log monitoring), which can be used individually or as a set, includes assessment, monitoring, management, and reporting. Working from globally linked VeriSign Security Operations Centers (SOCs), security teams use sophisticated tools to monitor, correlate, and analyze data across multiple levels of the organization in order to rapidly identify and prevent attacks. Organizations maintain full control of security policies and decisions and can access network data 24/7 via the Web-based VeriSign® Enterprise Security Portal.

#### + Secure Communications, Transactions, and Data Exchange

VeriSign digital certificate services, based on Managed PKI, provide mechanisms for compliance with §164.312. Using digital certificates, healthcare organizations can perform the following tasks:

- **Authentication** – Validates the identity of employees and partners, as well as applications
- **Encryption** – Ensures that information is not viewed or tampered with during transmission
- **Non-repudiation** – Establishes an irrefutable, time-stamped audit trail
- **Digital signing** – Attaches legally binding electronic signatures to documents and forms

In addition, the Managed PKI service provides out-of-the-box integration with leading messaging programs (such as Microsoft® Exchange, IBM® Lotus Notes®, and AOL® Instant Messenger™), enabling healthcare organizations to send and receive digitally signed and encrypted messages. With VeriSign solutions, healthcare organizations can rapidly strengthen security and compliance while minimizing the costs associated with developing, deploying, and maintaining in-house digital certificate services.

The HIPAA mandates also apply to automated data-sharing among applications. To comply with these regulations, healthcare providers, insurance carriers, and other organizations must ensure that machine-to-machine communications can reliably secure data, validate the identity of applications, check the integrity of data, and log and archive system activity. VeriSign's industry-leading SSL certificates enable healthcare organizations to extend application integration initiatives to partners, colleagues, and suppliers with complete confidence that valuable data is protected from end to end.

#### + Authentication and Access Control

To ensure that only authorized users access electronic protected health information (§164.312 [a][1]), healthcare organizations must be able to control not only who accesses networks, applications, facilities, and other resources, but also which resources each user can access. VeriSign Unified Authentication enables healthcare organizations to significantly reduce the risk of unauthorized access. Along with its technology partners, VeriSign enables healthcare organizations to easily deploy and manage a variety of strong authentication solutions such as digital certificates, smart cards, universal serial bus (USB) tokens, and biometrics. In addition, Unified Authentication can be seamlessly integrated with leading access-control and directory applications.



The VeriSign® Identity Protection (VIP) suite of services is designed to strengthen and protect consumer's digital identities and is for healthcare organizations and other companies that interact electronically with consumers' personal data. The VIP suite is comprised of VIP Fraud Detection Service and VIP Authentication Service. These complementary services form a flexible, layered solution that provides both visible and invisible mechanisms for securing online transactions and preventing identity theft. VIP Fraud Detection Service provides invisible server-side monitoring capabilities. VIP Authentication Service provides a more visible, standards-based strong authentication solution for online commerce applications. Both services help ensure that a person is who he or she claims to be.

### + Learn More

For more information about VeriSign Security Services, please call 650-426-5310, email [enterprise\\_security@verisign.com](mailto:enterprise_security@verisign.com), or visit us at [www.Verisign.com](http://www.Verisign.com).

### + About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions everyday across the world's voice and data networks. Additional news and information about the company is available at [www.verisign.com](http://www.verisign.com).

## Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.

This Solution Overview provides only a general description of VeriSign services for informational purposes and does not comprise a legal opinion or representation regarding the status or sufficiency of the VeriSign services under any applicable law. Customers should obtain independent legal advice on the scope and applicability of any legal requirements to which they may be subject.

©2006 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. IBM, Lotus Notes, and Tivoli are trademarks of IBM Corporation. Microsoft is a trademark of Microsoft Corporation. AOL and Instant Messenger are trademarks of AOL. All other trademarks are the properties of their respective owners.

00017474 08-05-2006