



WHITE PAPER

Layered Security: The Right Prescription for Internet-Based Healthcare Initiatives





CONTENTS

+ Introduction	3
+ Trends and Opportunities in Internet-Based Healthcare	3
Turning to the Web	3
The Move to Online Medical Records	4
+ The Barriers to e-Health Success	4
Patient Privacy and Identity Protection	4
Growing Regulatory Requirements	4
Fraud Prevention	5
+ Multilayer Security — The Prescription for Safe Online Healthcare	5
Authenticating the Website: SSL Certificates	6
Protecting the Transaction: SSL Encryption	6
Protecting Consumer Identity: Two-Factor Authentication	6
Protecting Against Fraud: Fraud Detection	6
+ Saving Lives and Improving the Bottom Line	7
+ Conclusion	7
+ Glossary	8
+ Learn More	8
+ About VeriSign	8



Layered Security: The Right Prescription for Internet-Based Healthcare Initiatives

+ Introduction

From Internet-based disease management to online medical records, the shift to electronic healthcare promises far-reaching benefits for all involved — from saving lives to saving dollars. And while the cost and effort of implementation can be a significant hurdle, there is one challenge that eclipses all others: security.

The unparalleled opportunity to simultaneously improve patient outcomes while cutting costs hinges on the ability of healthcare organizations to assure patients that their online confidential information is safe from prying eyes and criminals. While other industries have made inroads in establishing consumer trust — online retailers for example — today's consumers don't feel the same way when it comes to their medical data being online.

A recent survey showed that one-third of commercially-insured consumers are not sure if their health insurer is fully protecting the privacy of their personal information. The survey also showed that consumers with privacy concerns are nearly twice as likely to switch plans.¹

Piecemeal security measures are no longer enough to deliver the high standard of protection consumers demand. Healthcare organizations need a multilayer solution that delivers a systematic approach to security across the entire online transaction to mitigate threats at multiple levels. A multilayer solution establishes a continuum of protection for patients that addresses the essential components of the transaction: patient identity protection, confidential data protection, Website authentication, and fraud detection.

Using this approach, complementary security layers such as Secure Sockets Layer (SSL) certificates, two-factor authentication, and fraud detection, fortify each other to create a solution that is stronger than the sum of its parts. Only with this type of end-to-end security coverage can organizations lay the groundwork for widespread acceptance of patient-facing, e-healthcare initiatives.

+ Trends and Opportunities in Internet-Based Healthcare

Insurance companies, medical practices, hospitals, self-insured employers, and other service providers stand to gain sizeable benefits through the use of online health services and transactions. These range from improved quality and responsiveness of patient care to new levels of efficiency and cost savings.

Turning to the Web

Health plans — and self-insured employers — are leading the charge in turning to the Internet to help lower costs and improve patient care. These companies are introducing innovative new ways for patients to exercise greater control over their care and expenses. Some of the new services being made available to patients and caregivers include:

- Electronic claims and reimbursement transactions
- Member management

¹ "Privacy Concerns Hinder Health Plan Web Site Growth: Consumer-Directed Health Plan Members Struggle The Most With Privacy," Julie Snyder, Forrester, February 21, 2008

A Harris Interactive survey showed that 91% of consumers want access to their electronic medical records (EMRs)²

- Case review and utilization management
- Personalized disease management programs
- Advice programs with email to doctors and nurses
- Prescription shopping and management

Working together with medical Websites such as WebMD,[®] health plans and employers are providing private portals for members and employees to empower patients with better information for benefits, treatment, and provider decisions.

The Move to Online Medical Records

Electronic medical records (EMRs) can reduce errors, cut administrative costs, eliminate duplicate procedures, and save valuable time when it comes to emergency medical care. It also allows the patient greater participation in healthcare decisions.

In addition to healthcare providers and hospitals converting to EMRs, goliaths Microsoft[®] and Google[™] have launched their own offerings around online health record repositories. These initiatives are designed to help consumers organize and manage their personal health information, linking and importing data to build their online health record.

+ The Barriers to e-Health Success

Despite the improvements to quality of care and hard dollar savings that electronic healthcare can bring, the availability of new online services and acceptance of those services by consumers have not yet reached a critical mass. From the consumer perspective, the inhibiting factor is clearly privacy and theft concerns. Organizations are faced with a triad of issues surrounding online health transactions: assuring patients their confidential medical data is secure, complying with federal and state legislative requirements, and finding ways to detect and protect against medical fraud.

Patient Privacy and Identity Protection

Consumer uptake of online health services has been minimal. Only 6.1 million adults in the United States have electronic personal health records, according to estimates released by the Markle Foundation.³ And only 4% of adults in a survey conducted by Harris Interactive currently use electronic health services.⁴

For consumers, the overwhelming reason for hesitating to participate in online healthcare is security. Consumers are worried about unauthorized access to personal medical information as well as identity theft. According to Columbia University Professor Emeritus Alan F. Westin, a leading authority in privacy research, approximately 73 percent to 80 percent of the public will want to be assured of robust privacy and security practices by online personal health record services, if they are to join those offerings.⁵ Other studies show that identity verification is key to consumer uptake of personal healthcare records.⁶

Growing Regulatory Requirements

Healthcare organizations pursuing online healthcare transactions must also ensure those services comply with relevant laws. While the Health Insurance Portability and

² "Benefits of Electronic Health Records Seen as Outweighing Privacy Risks," Bekey Bright, *The Wall Street Journal*, November 29, 2007

³ "Tech Giants Back Online Health Records Standards," Steven Musil, CNET News, June 24, 2008

⁴ "The Benefits of Electronic Medical Records Sound Good, but Privacy Could Become a Difficult Issue," Harris Interactive, February 8, 2007

⁵ "Technology Companies, Providers, Health Insurers and Consumer Groups Agree on Framework for Increasing Privacy and Consumer Control Over Personal Health Records," Connecting for Health[™], June 25, 2008

⁶ "Solving identity crisis could spur PHR adoption, report concludes," *Healthcare IT News*, January, 25, 2008

"Consumer demand for electronic personal health records and online health services will take off when consumers trust that personal information will be protected."

— Zoe Baird, President, The Markle Foundation.

Accountability Act (HIPAA) has been in effect since 1996, there are several states actively pursuing laws specifically designed around the protection of healthcare information. California Assembly Bill 1298 is slated to address healthcare data breach as an update to SB1386, the well-known breach disclosure law. In the European Union (EU), several Directives of the European Parliament and of the Council protect the processing and free movement of personal data, including patient health care information.⁷

Fraud Prevention

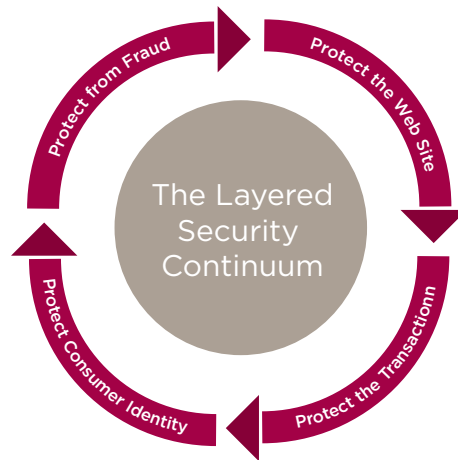
Medical fraud is rampant and on the rise, with some sources estimating fraud losses at more than \$68 billion per year in the U.S.⁸ While health plans bear the immediate burden, the high cost of fraud is eventually passed on to everyone in the healthcare ecosystem. In addition to having higher premium costs due to fraud, consumers can also get hit with paying deductibles on procedures and services they never received. The specter of potentially increasing the opportunity for fraud through online initiatives has haunted health plans' efforts to launch new e-health services.

+ Multilayer Security — The Prescription for Safe Online Healthcare

Online healthcare presents an end-to-end security problem that requires an end-to-end solution — above and beyond what single, point security products have been able to offer. That end-to-end solution is called multilayer security — protecting the transaction on multiple levels to deliver a cumulative, greater level of security.

A multilayer approach addresses the full spectrum of online challenges healthcare companies face including protection against patient identity theft, loss of privacy, and fraud stemming from online transactions. Such an approach delivers a continuum of protection across all critical areas of the online healthcare transaction: authenticating the Web site, protecting the transaction, protecting the consumer's identity, and fraud detection/protection.

Figure 1: The Layered Security Continuum



⁷ European Parliament and Council (24 October 1995): [EU Directive 95/46/EC - The Data Protection Directive](#)

⁸ "The Problem of Health Care Fraud," The National Healthcare Anti-Fraud Association, www.nhcaa.org

VERISIGN COMBINES CONVENIENCE AND SECURITY FOR MICROSOFT HEALTHVAULT USERS

Microsoft® HealthVault™ is a free service that puts consumers in control of their health information, enabling them to store, manage, and share their health records online. This service provides tremendous convenience for consumers, as it enables them to access critical healthcare information that has traditionally been controlled by outside parties. However, such convenience creates a number of potential opportunities for identity thieves. In order to ensure that consumers' valuable records remain secure amid a growing black market for health insurance policy information, Microsoft chose to deliver strong authentication through OpenID providers such as VeriSign, whose solutions include VeriSign Identity Protection (VIP) credentials.

Today, when users log into their HealthVault records, they are prompted for their OpenID user name and password, then asked for a one-time-password (OTP) generated by their VIP credential. This two-step process makes it extremely difficult for identity thieves to illegally access any sensitive medical and insurance data stored online. Moreover, Microsoft HealthVault users can utilize the same VIP credential on eBay, PayPal, AOL, and a number of other sites that participate in the VeriSign Identity Protection Network.

By enabling Microsoft HealthVault users to move their sensitive health insurance onto the Web with confidence, VeriSign helps consumers balance the convenience of total access with the privacy of a secure online experience.

Authenticating the Website: SSL Certificates

The Secure Sockets Layer (SSL) certificate enables the consumer to verify the identity of the certificate owner and ensure that the healthcare Website is indeed authentic. Many consumers are well-versed from retail and other Web sites in looking for the “https” in their browser's address bar as proof that the site has authenticated itself with an SSL certificate. Now, more advanced SSL certificates provide additional cues as well that help to extend trust online, such as turning the address bar green or displaying the name of the certificate owner.

Protecting the Transaction: SSL Encryption

SSL technology establishes a private communication channel where data can be encrypted during online transmission, protecting sensitive patient information from electronic eavesdropping. Most Internet users are familiar with the tiny lock icon that appears on pages that have been encrypted by SSL certificates. Healthcare companies should look to use at least [128-bit SSL certificates](#) or the more secure [256-bit SSL certificates](#) to enable the strongest encryption available for their customers.

Protecting Consumer Identity: Two-Factor Authentication

[Two-factor authentication \(2FA\)](#) relies on two different factors to authenticate consumer identity. Using more than one factor is also known as strong authentication and can ensure a significantly more secure experience for consumers. A criminal who steals only the first factor will not be able to forge the second factor and will be unable to authenticate. And vice versa, anyone stealing the second factor will not know the first and will be likewise unsuccessful. Two-factor authentication solutions can take the form of point-to-point products where consumers use a different credential for each Website they visit or a shared authentication network where consumers use the same credential across multiple sites.

Compared to a standalone 2FA solution, a [shared authentication network](#) delivers an extremely user-friendly and effective method of two-factor authorization that encourages and rewards consumer adoption. It enables 2FA to be both easy to use (regardless of the consumer's level of technology sophistication) and convenient, allowing the consumer to use the same credential across participating sites.

Organizations leveraging a shared authentication network benefit not only from increased consumer adoption, but the myriad advantages inherent in a hosted solution: lower costs, reduced risk, scalability, and faster time-to-market.

Protecting Against Fraud: Fraud Detection

While SSL and 2FA are proactive and visible forms of security, fraud detection is invisible to the consumer. [Fraud detection](#) technology works behind the scenes to detect anomalies that could signal potential fraud. It “learns” how each user behaves and only becomes visible to the user when additional authentication is needed based on pre-determined parameters. With healthcare fraud costing companies billions of dollars each year and rising, fraud detection and prevention should be central to any multilayer security undertaking.

+ Saving Lives and Improving the Bottom Line

Healthcare organizations that embrace multilayer security for online communications can build the trust with patients needed to gain widespread acceptance and adoption of e-healthcare initiatives. Once these initiatives reach critical mass, the resulting paradigm shift can deliver far-reaching benefits.

In addition to saving lives and improving outcomes by eliminating medical errors and providing faster access to accurate, complete patient information, electronic healthcare and online medical records create new levels of administrative efficiencies and operational savings. Storage and paper costs, which can run tens of thousands of dollars each month for a medium to large practice, can be drastically reduced or eliminated.

A December 2007 report from the Commonwealth Fund stated that in addition to efficiency, quality, and patient safety savings, \$368 billion could be saved over 10 years—through investment in and sharing of medical effectiveness and outcomes research, made possible through widespread electronic access to patient care information.⁹

Electronic healthcare can make it easier and faster for consumers and health plans to detect fraud. Access to complete medical records may make it easier for health plans to identify a fraudulent claim. Claims could potentially be validated by the patient electronically before the health plans issues payment, transforming fraud management from “pay and chase” to a “validate and pay” model.¹⁰

+ Conclusion

The opportunity awaits bold, forward-looking organizations to dramatically impact the quality and effectiveness of health care while reducing costs with innovative new online medical services. Enabling this revolution in healthcare is multilayered security — industry-leading security solutions that together provide end-to-end protection at multiple levels of the online transaction.

Through the cumulative effect of many levels of protection, organizations can offer the standard of security consumers need, while addressing regulatory requirements and fraud detection concerns. Now hospitals, practices, health plans, self-insured employers, and the other participants in the healthcare lifecycle can build consumer trust in online medical transactions to set the standard for 21st century healthcare.

⁹ “Commonwealth Fund Commission on a High Performance Health System, “Bending the Curve: Options for Achieving Savings and Improving the Value in U.S. Health Spending,” December 2007

¹⁰ “Fraud Control: New Tools, New Potential,” Susan P. Hanson and Bonnie S. Cassidy, *Journal of American Health Information Management Association*, no. 3, March 2006



+ Glossary

Authentication – The process of confirming that something is genuine. In computer security, authentication is usually an automated process of verifying the identity of someone or something, such as a computer or application.

2-Factor Authentication, Strong Authentication, Multi-Factor Authentication – All of these terms refer to the authentication practice of requiring confirmation of something you know such as a username and password and something you have such as a smart card, token or certificate.

Credential – Proof of qualification, competence, or clearance that is attached to a person. A digital certificate, token, smart card, mobile phone, or installed software are credentials that may be used to enable strong or multi-factor authentication.

Extended Validation SSL – Requires a high standard for verification of SSL Certificates dictated by a third party, the Certificate Authority/Browser Forum. In Microsoft® Internet Explorer 7, Web sites secured with Extended Validation SSL Certificates cause the URL address bar to turn green.

+ Learn More

For more information about VeriSign® layered security solutions for paperless customer communications, please call 650-426-5310 or email: identityandauthenticationservices@verisign.com

+ About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.Verisign.com for more information.