

NETWORK SECURITY & COMPLIANCE: HOW THEY DRIVE QUALITY OF CARE

July 2009

Prepared for WatchGuard Technologies, Inc. by ReymannGroup, Inc.

Table of Contents

Introduction	2
Healthcare in 2014	2
Healthcare Technology and Quality of Care Continuum	3
Security Compliance Is Paramount	3
Network Security Best Practices in Healthcare	7
WatchGuard Enables Continuous Security and Compliance	9
Take the Next Step	10

Introduction

This paper examines events that are driving the demand for increased security of protected health information (PHI) within the healthcare industry. In it, we review new laws, enhanced HIPAA mandates, increased enforcement activities, and new security guidelines from the Department of Health and Human Services (HHS).

We also describe how WatchGuard solutions can help you to create a day-to-day culture of proactive and real-time information security throughout your organization and infrastructure. Our goal is to provide a forward-looking perspective on how thoroughly securing all personal health information (PHI) and leveraging the right technology can reduce the cost of your security and compliance efforts.

Whether you have an established security program, are looking to enhance an existing program, or are trying to jump-start your efforts to create the foundation of an effective security program, this paper offers insights to help you cost-effectively enhance quality of care, protect patient and other sensitive data, and enable successful security and compliance.

Healthcare in 2014

This is what the future will look like:

- A national health information technology infrastructure will change the way healthcare providers, insurers, patients, and vendors work, interact, share protected health and financial information, and enable delivery of quality care
- Federal standards, specifications, and certification of technologies will promote security, protect health information, and render individually identifiable health information unusable, unreadable, or indecipherable to unauthorized individuals
- Healthcare agencies will be required to adopt systems and products that meet these standards and specifications
- Contracts and agreements with third parties will require private entities to also use the same systems and products
- Healthcare security and information technology risk management will be a way of life

Sound familiar? It should. This model of healthcare has been evolving for years.

Now, thanks to the American Recovery and Reinvestment Act (ARRA) of 2009 (a.k.a., Stimulus Act), we are going to experience a significant improvement in the delivery of quality healthcare and the secure sharing of protected health information.

The Stimulus Act does a lot more than stimulate spending and economic recovery. It includes specific mandates and funding to revolutionize the secure electronic data exchange in healthcare. The shift will be towards a more efficient delivery of quality care that will be enabled by the secure delivery and sharing of health records and quality services.

Healthcare Technology and Quality of Care Continuum

Healthcare has been moving toward an electronic clinical and transaction model for many years. This specific initiative for a national network began prior to the Stimulus Act. It started on April 27, 2004 with Presidential Executive Order 13335. This Executive Order called for the development and nationwide implementation of an interoperable health information technology infrastructure to improve quality and efficiency of healthcare. It outlined a plan for most Americans to have electronic health records by 2014. This Executive Order established the Office of the National Coordinator for Health Information Technology under HHS.

In the last decade, we have also seen legal mandates enacted to protect the security of health information under HIPAA and other extensive federal and state¹ laws for protecting sensitive personal information. The most recent federal law was the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) that included new updates to HIPAA.

Programs

Beyond the need to protect patient records, we have also seen a number of government and private sector programs to enhance quality of care, enable better reporting of care delivery outcomes, give providers incentives to adopt e-prescribing and improve care, mitigate the risk of medical identity theft, and strengthen hospital accreditation reviews.

Business Drivers

Common business drivers for an electronic model of care delivery and information exchange throughout the industry and among many individual healthcare organizations have included improved patient care, reduced medical errors, daily financial and medical transaction processing, compliance with regulatory issues, and communications among doctors, staff, patients, third-party providers, and payers.

The healthcare industry is evolving quickly to effectively adopt an electronic clinical and business model. The continued success of this healthcare continuum will depend on the availability of trusted and proven technology solutions that can help enable these clinical and business priorities.

Healthcare Trends

- ARRA & HITECH Act
- New HIPAA Mandates
- HIT Policy/Std's Comm.
- New HHS Guidelines
- TJC Accreditation
- Medical Identity Theft
- e-Prescribing
- Pay for Performance
- Cyber Pirates

Security Compliance Is Paramount

Among the many changes confronting all healthcare organizations today are:

- Care delivered over larger and larger geographic areas
- Increasing use of specialists and sophisticated diagnostic and treatment technology
- A need for ready access to patient and disease data as well as automated decision support tools
- Increasingly mobile medical personnel who deliver patient care, inside and outside of the hospital

¹ Most states have passed data security laws that apply to companies that do business with residents of those States. In some states, such as California, these laws apply to medical information and health insurance information. In some of the other states, the law actually states that a HIPAA covered entity is excluded. In other states, compliance with a more stringent law such as HIPAA can create compliance by default. Other states have also passed laws that mandate the encryption of such data.

Common among all of these changes is the need for enhanced and secure connectivity across a national network of healthcare delivery. The foundation of this enhanced access to critical data must be a health information technology infrastructure that allows for the secure exchange and use of information. This connectivity must support secure access to information and collaboration among mobile personnel as they perform duties throughout the expanded healthcare enterprise. It must protect the data in order to meet stringent federal and state security compliance requirements with real-time network monitoring, tracking, reporting, and continuous audit, forensic, and enforcement capabilities.

There are numerous laws, rules, events, and initiatives that are raising the bar on how well hospitals, clinicians, and other covered entities are protecting the security and confidentiality of patient health information and the increasingly connected healthcare networks. For example:

ARRA and the HITECH Act

In January 2009, the American Recovery and Reinvestment Act (ARRA) created the HITECH Act. The HITECH Act enhances the authority and resources of the HHS Office of the National Coordinator for Health Information Technology to oversee the development of a nationwide health information technology infrastructure that allows for the secure electronic use and exchange of protected health records by 2014 to improve quality of care.

HIT Policy and Standards Committee

The HITECH Act also creates a Health Information Technology (HIT) Policy and Standards Committee to make recommendations to the National Coordinator on standards, implementation specifications, and certification criteria needed for (among other things):

- Technologies that protect health information and promote security
- A nationwide health information technology infrastructure
- Use of certified electronic health records for each person in the USA by 2014 to improve quality of care
- Technologies that can render individually identifiable health information unusable, unreadable, or indecipherable to unauthorized individuals, when it is transmitted in the nationwide health information network or physically transported outside of a secured physical perimeter

The Secretary of HHS must adopt an initial set of these standards, implementation specifications, and certification criteria no later than December 31, 2009. Under these new mandates:

- Agencies will be required to use HIT systems and products that meet the adopted standards and implementation specifications
- Agency contracts or agreements shall require private entities to use HIT systems and products that meet the adopted standards and specifications
- Health information technology will be certified as compliant in accordance with specific National Institute of Science and Technology (NIST) defined certification criteria

New HIPAA Mandates

Effective January 2009, the HITECH Act amends parts of HIPAA² and includes improved security and enforcement provisions that require:

² In 1996, HIPAA established the Security Rule for Protected Health Information (PHI)—which defines PHI as any information about an individual's health status, provision of healthcare, or payment of healthcare or that could be reasonably tied to an individual by a combination of patient name and address, birth date, or social security number. This rule defines

- Application of HIPAA security provisions and penalties to "business associates" of covered entities. (Previously, HIPAA required "satisfactory assurance," only.)
- Notification in the case of a breach and posting of such breaches on the HHS public website. (This includes covered entities, business associates, vendors, and 3rd party service providers.)
- Tiered increase in potential amount of civil monetary penalties. For example, a violation due to "willful neglect" can result in at least \$50K per violation up to a total of \$1.5M in a calendar year.³
- Enforcement by State Attorneys General, in addition to the existing HHS Centers for Medicare and Medicaid Services (CMS) and Office of Civil Rights (OCR) enforcement powers.⁴

HIPAA Enforcement Highlights

From April 2003 through March 2009, HHS received over 43,000 HIPAA non-compliance complaints. More than 8,000 of these complaints have resulted in enforcement action. The most common issues investigated are (listed in order of frequency):

- Impermissible uses and disclosures of protected health information.
- Lack of safeguards of protected health information
- Lack of patient access to their protected health information
- Uses or disclosures of more than the "minimum necessary" protected health information
- Lack of or invalid authorizations for uses and disclosures of protected health information

HHS Data Breach Notification Rule and "Safe Harbor" Technology Guidelines

The HITECH Act requires HHS to issue an interim final rule to require HIPAA covered entities to provide for notification in the case of breaches of unsecured protected health information.⁵ It also requires HHS to specify technologies and methods that create a "safe harbor" from the data breach notification mandates defined in the Act.

Effective April 17, 2009, HHS published guidelines on technologies and methods that can render individually identifiable health information unusable, unreadable, or indecipherable to unauthorized individuals, when it is transmitted in the nationwide health information network or physically transported outside of a secured physical perimeter. These guidelines define encryption and destruction of data⁶ as the "safe harbor" from the data breach notification requirements.⁷

standards and specifications for administrative, physical, and technical safeguards. Exhibit I highlights several key HIPAA security standards.

³ In March 2006, HHS published its HIPAA enforcement rule that established the initial civil monetary penalty authority for a HIPAA violation. The enforcement authority is now expanded under the HITECH Act.

⁴ CMS is authorized to investigate complaints of and make enforcement decisions for non-compliance related to the HIPAA security regulations. Enforcement of the HIPAA Privacy Rule is under the authority of the Office for Civil Rights (OCR). When privacy issues occur in the context of potential security violations, CMS and OCR collaborate to enforce the HIPAA rules.

⁵ HHS is required to publish this interim final data breach notification rule within 180 days of enactment of ARRA, i.e., August 17, 2009 or sooner.

⁶ The HIPAA Security rule requires covered entities to establish policies and procedures that address the final disposition of electronic PHI and the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use. See 45 CFR 164.310(d)(2)(i) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible

The Joint Commission January 2009 Deadline⁸

In July 2008, The Joint Commission (TJC) issued updated accreditation standards that went into effect in January 2009. This requires healthcare organizations to be aware of the new information management (IM) standards and comply. Information security, privacy, and technology risk management are key among these updated standards. Hospitals must meet the challenge of enabling compliance with these newly enhanced standards. If they do not - they risk the loss of reimbursements from Medicare for such services and increased liability of insurance costs. Privacy, security, and integrity of health information are a specific focus of TJC IM standards. Exhibit I highlights the relevant TJC IM standards.

Medical Identity Theft

Medical identity theft is an emerging issue that raises concerns for consumers, healthcare providers, health plans, and others. In January 2009, the Office of the National Coordinator for Health Information Technology published its "Medical Identity Theft Final Report."⁹ This report found that the potential consequences of medical identity theft are the loss of accuracy of medical records, expenses to individuals whose identities are stolen, widespread expenses to the healthcare system, and compromised patient care if inaccurate health records are relied on at the point of care. The report includes recommendations of policy and technical approaches to address issues of prevention, detection, and remediation of medical identity theft.

HHS Incentives for Adoption of e-Prescribing

e-Prescribing is defined as entering a prescription for a medication into a data entry system – directly or via a portable device such as a PC, PDA, tablet, or smart phone – and thereby generating the prescription electronically, rather than handwriting it on a paper form.¹⁰ Ensuring that the appropriate healthcare professionals have a safe and secure network, desktop, laptop, connected PDA and smart phone technology, database security, real-time monitoring and reporting, and a HIPAA compliant information security program is key to the success of this e-prescribing initiative.

Typically, access to these online systems is authorized on a limited "need-to-know" basis with each user having role-based access to a network and applications that transmit and store data. However, this "need-to-know" access policy cannot be enforced without appropriate network monitoring capabilities that will help to prevent or identify erroneous or fraudulent access.

Pay for Performance

Pay for performance is a way to address equitable payment for quality of care. Pay for performance encourages better outcomes from medical procedures by providing financial incentives to improve care. Medicare and many commercial insurance carriers are instituting pay for performance. Providers also need timely and

disclosures of PHI. HHS has published a list of FAQs on the disposal of PHI at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaq.pdf>

⁷ A copy of the HHS HITECH Breach Notification Guidance is available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

⁸ The Joint Commission evaluates the quality and safety of care for more than 15,000 healthcare organizations. To maintain and earn accreditation, organizations must have an extensive on-site review by a team of Joint Commission healthcare professionals, at least once every three years. The purpose of the review is to evaluate the organization's performance in areas that affect care. Accreditation may then be awarded based on how well the organizations met Joint Commission standards.

⁹ A copy of the Medical Identity Theft Final Report is available at <http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf>

¹⁰ Effective in 2009, doctors will receive a "bonus" on Medicare payments for e-prescribing. After 2013, the bonus payments will be phased out and doctors will be penalized with lower reimbursement rates for not e-prescribing.

accurate reporting capabilities for all data. The security of patient care and financial information is a key component in a successful pay-for-performance program. This electronic exchange of payment information and care-provided data ensures proper reimbursement of care benefit payments. This information exchange must be accurate, eliminating the need for overpayment negotiations and possible penalties from the Medicare or Medicaid payer. If a data breach occurred that manipulated and altered the information as it flowed from the insurer to Medicare, the integrity of the information would be jeopardized and the cost to the health insurance groups could be significant.

Cyber Pirate Risks

In spite of these laws, rules, and expanded government and accreditation initiatives that promote the secure use of information technology and exchange of nonpublic personal information, almost every company has experienced a data breach or theft of its network, corporate desktops, and laptops. Today, however, the nature of these breaches has evolved from cyber crime to include cyber piracy. For example:

In May 2009, the FBI and Virginia State Police opened an investigation to search for hackers who demanded that the state of Virginia pay them a \$10 million ransom for the return of millions of personal pharmaceutical records they say they stole from the state's prescription drug database.¹¹

Such medical identity theft and ransom activities highlight the need for all hospitals and other entities in the healthcare industry to adopt real-time security controls that will protect the patient records.

As the national awareness and cost of sensitive patient and employee data breaches continues to rise, government agencies take a more active role in the security of sensitive data, and as the use of technology to exchange information grows, healthcare organizations must ensure they are enabling prudent real-time security practices throughout the healthcare continuum.

Network Security Best Practices in Healthcare

By proactively implementing best practice strategies for security and compliance across the entire clinical, business and network infrastructure, each healthcare organization will establish the parameters needed for:

- Delivering quality of care
- Assessing risk
- Securely sharing data
- Improving the effectiveness of their operations
- Avoiding disruptions in service and operations
- Enabling continuous compliance
- Reducing liability risk
- Containing cost

As a starting point to help healthcare organizations plan how to best accomplish these best practice strategies, we offer the following recommendations for each organization to consider. While this list does not cover everything that you may need to consider, it highlights several best practices that will help.

¹¹ Source is from the Privacy Rights Clearinghouse database www.privacyrights.org

Select the Right Technologies

Achieving a secure and compliant culture goes beyond a “CHECK-THE-BOX/YES/NO” audit methodology for compliance. All organizations must establish a technology infrastructure that enables the company to address the real intent of the HITECH Act and HIPAA requirements – proactive and real-time security.

HIPAA compliance requires governance over your entire IT infrastructure. Thus, it is imperative that you use technologies that address your entire network – all the data components as well as all the systems that host PHI. This allows you to achieve a broader approach to your compliance initiatives and provide maximum protection for PHI. Example technology strategies that must be implemented include:

- Installing and maintaining secure firewalls
- Encrypting across open, public networks
- Establishing a zoned network architecture
- Tracking and monitoring all access to the network and cardholder data

By automating and centralizing as much of the compliance processes and technologies as possible, you ensure agility with operating efficiency, and relieve resources to focus on clinical and other day-to-day operational initiatives. This empowers employees, makes the processes more manageable, and uses less time and capital to enable compliance.

Team with Strategic Technology Partners

Hiring consultants to perform security audits is not a cost-effective option by itself. Constant changes throughout your network and in the nature of the threats to your network and data require you to partner with strategic technology companies that provide automated and real-time security. You need to plan beyond the regular audit and establish an ongoing risk assessment culture that will enable you to maintain your strengths identified in the audit and correct any weaknesses. Outsourcing for technologies that deliver firewall, encryption, and real-time monitoring of your network is a cost-effective alternative to help you establish and maintain a secure and compliant infrastructure.

Appoint a Champion – Make security compliance more than just a periodic compliance project

One of the most valuable practices a healthcare organization could undertake would be to create a sustainable, repeatable process. Security compliance is not a point-in-time activity – it is a continuous process. Implementing formal security processes, policies and procedures and ensuring that these are followed does much more than simply satisfy the federal and state mandates - it lessens the likelihood of unauthorized access to PHI that could influence the quality of care.

Each organization should designate an individual or group with the authority and responsibility to champion a security and compliance culture. This individual should understand and stay abreast of the legal, regulatory, and other requirements, the controls needed to meet them, and actively pursue the right solutions that resolve any security issues. They can then propagate security throughout your enterprise with an employee awareness program to educate your staff on how PHI should (and should not) be handled.

Best Practices at a Glance

- Select the right technologies
- Team with strategic partners
- Appoint a champion

WatchGuard Enables Continuous Security and Compliance

All healthcare organizations must find a solution that allows them to address security of PHI and a broad range of the security compliance requirements. This will enable them to streamline their security initiatives. No one solution will be the answer, however, finding a multi-layered solution will bring new levels of efficiency to their security, compliance, and quality-of-care initiatives. WatchGuard delivers a wide range of solutions designed to help healthcare organizations address compliance and security as a whole. With WatchGuard as a strategic partner, healthcare organizations can employ a culture of security throughout their clinical and business day-to-day activities.

WatchGuard capabilities align with healthcare security and compliance requirements and include the following:

Building and Maintaining a Secure Network

The powerful application proxy technology behind all WatchGuard firewalls provides detailed granular control over which protocols, ports, and content are allowed through the firewall. Healthcare organizations can block all traffic by default and defining a proxy policy that allows only approved traffic to pass into the PCI DSS operating environment. Intrusion Prevention System (IPS) and Gateway AntiVirus (Gateway AV) subscriptions can also be used to scan allowed traffic in order to block unauthorized intrusion attempts, and monitor for threats that conform to protocol standards but carry malware.

Protecting Health Information

WatchGuard appliances support network zones, and they can be configured to create a DMZ for all public-facing servers and a Trusted zone where PHI resides. This also ensures that none of the IP addresses in the trusted zone are visible or accessible from the Internet. All management communications are done via a secure encryption-based protocol, and all e-Series and XTM appliances support IPSec and SSL VPN communication.¹²

WatchGuard also helps guard PHI over wireless networks. Wireless networks are inherently insecure, but there are some circumstances where they cannot be avoided. In these cases, the wireless operating environment must be physically segregated from the wired environment and appropriately firewalled. Wireless Firebox X Edge models support WPA2 and can be combined with either an IPSec or SSL VPN to achieve compliance and guard PHI.

WatchGuard Helps

- Build and maintain a secure network
- Protect health information
- Maintain a network vulnerability management program
- Implement strong access controls
- Regularly monitor and test networks

Maintaining a Network Vulnerability Management Program

WatchGuard unified threat management (UTM)¹³ and extensible threat management (XTM)¹⁴ solutions provide comprehensive network protection. They integrate application proxy firewall, zero day attack prevention, anti-spyware, anti-virus, anti-spam, intrusion prevention, and web content filtering on a single platform. This greatly

¹² Implementing appropriately strong encryption solutions for transmission of EPHI (e.g. SSL, HTTPS etc.) is a risk management strategy that is defined in the CMS HIPAA Security Guideline for Remote Use of and Access to electronic PHI. SSL should be a minimum requirement for all Internet facing systems which manage EPHI in any form, including corporate web-mail systems.

¹³ UTM is an all-inclusive security product that has the ability to perform multiple security functions in one single appliance: network firewalling, network intrusion prevention, gateway anti-virus, gateway anti-spam, VPN, content filtering, load balancing, and monitoring/reporting.

¹⁴ XTM is the next generation of network security products that build on UTM capabilities, but are engineered to deliver even greater security, enhanced networking capabilities, and more management tools.

reduces the time and cost associated with managing multiple point solutions and significantly improves protection from blended threats.

These solutions provide Gateway AV support that reduces the ingress of malware into the network. Automatic updates of the AV signature database help provide up-to-the-minute protection from vulnerabilities. In addition, WatchGuard updates the appliance logs whenever traffic is denied by the Gateway AV and whenever the signature sets are updated.

A WatchGuard firewall can inspect web traffic at the application layer using the HTTP and HTTPS proxies. This provides a robust mechanism to mitigate many web-based vulnerabilities (e.g., SQL injection, cross-site scripting). In addition, WebBlocker, an integrated security subscription for all WatchGuard appliances, delivers powerful web content filtering to block access to dangerous and inappropriate websites.

Implementing Strong Access Control Measures

WatchGuard appliances deliver stringent access controls with two-factor authentication, including RADIUS,¹⁵ SecureID, and individual VPN certificates. They also support authentication via Active Directory, which streamlines authentication, saving time and eliminating hassles. Organizations can implement strong controls with WatchGuard appliances as they store all password information in an encrypted format. This provides an additional layer of security. Furthermore, WatchGuard SSL 100 appliances make secure remote access easy and affordable, regardless of the network size.

Regularly Monitor and Test Networks

Secure, centralized logging and comprehensive reporting are included in WatchGuard System Manager – with no extra logging or reporting modules to buy. Clear, visually driven interfaces and plain-language log messages make it easy to validate the security policy and to make changes or adjustments as desired. Interactive tools enable you to take instant preventive or diagnostic action directly from the monitoring interface, without the need to open separate configuration screens. WatchGuard also helps monitor networks by tracing each login activity to an individual. All UTM and XTM appliances support authentication via Active Directory.

Real-time monitoring and logging provide not just an effective view of security, but also documented proof for inspectors conducting a HIPAA audit.

Take the Next Step

To learn more about how WatchGuard can help your healthcare organization have comprehensive network protection and achieve compliance, call 1.800.734.9905 or visit www.watchguard.com.

¹⁵ Implementing two-factor authentication for granting remote access to systems that contain electronic PHI and using Remote Authentication Dial-In User Service (RADIUS) or other similar tools is a risk management strategy that is defined in the CMS HIPAA Security Guideline for Remote Use of and Access to electronic PHI.



ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard has been building award-winning unified threat management (UTM) solutions that combine firewall, VPN, and security services to protect networks and the businesses they power. Our newest appliances represent the next generation of network security: extensible threat management (XTM). All of our solutions feature reliable, all-in-one security, scaled and priced to meet the security needs of every-sized enterprise. Our products are backed by 15,000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including healthcare, education, and retail. WatchGuard is headquartered in Seattle, WA with offices throughout North America, Europe, Asia Pacific, and Latin America.



ADDRESS:
1908 Blue Ridge Road
Edgewater, MD 21037
USA

WEB:
www.reymanngroup.com

CONTACT:
Phone: (410) 956 7336
Fax: (410) 956 7338
Email: info@reymanngroup.com

ABOUT REYMANNGROUP

ReymannGroup, Inc. provides finance, healthcare, energy, public sector, and retail subject matter expertise. Our firm helps companies evaluate their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. ReymannGroup provides customers with independent, highly-qualified professionals, authors of regulations and books, and subject matter experts familiar with industry regulations and best practices.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis. © 2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. WGC WGCE66638_072809