



Corporate Headquarters
10700 Parkridge Blvd.
Suite 400
Reston, VA 20191
703-391-2913
703-391-7807 (fax)
www.silentrunner.com



4080 McGinnis Ferry Rd.
Suite 1102
Alpharetta, GA 30005
770-663-4889
770-663-4205 (fax)
www.dcshealthcare.com

WHITE PAPER

A SILENTRUNNER® APPROACH TO HIPAA SECURITY

By Kevin Arner, Executive Vice President, DCS Healthcare

NOTICE: The contents of this briefing are not intended to serve as legal advice related to any individual situation or entity. This material is made available on an informational basis only and is provided with the understanding that DCS Healthcare, SilentRunner Inc., and Raytheon Company are not providing legal advice. If legal advice is required, the services of a competent licensed attorney should be sought.

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) – 42 U.S.C § 1320d-2(d)(2) requires all covered entities that maintain or transmit health information to “maintain reasonable and appropriate administrative, technical, and physical safeguards” to ensure the integrity and confidentiality of the information; protect against reasonably anticipated threats and unauthorized uses or disclosures, and otherwise ensure compliance. In addition § 164.530 (c)(1) of the Privacy Rule contains its own security requirements; “A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.”

HIPAA Security Liability Preys on Healthcare’s Technology Foundation

Modern healthcare is built on a technology foundation. Billions of dollars have been invested in applications, networks and data to create a pervasive environment of clinical, financial and patient health information. Improved patient care, cost control, reduced medical errors and gains in operating efficiencies are all related to the proper use and effectiveness of technology. However, these valued assets are at risk because it is this technological foundation that now presents the challenge and liability of HIPAA Security compliance.

While not all data is subject to HIPAA provisions, protecting intellectual property of all types is critical to the wellbeing of your enterprise. HIPAA wields stern responsibility and liability, yet extending beyond this is the unwavering need to maintain the integrity of trust within the patient-provider relationship. Organizations that distinguish themselves above the necessities required by HIPAA Security will foster greater trust and success in their relationships with partners, providers and patients.

Most healthcare entities governed by HIPAA are already engaged in compliance efforts. Unfortunately, many, if not most have overlooked or under estimated the diverse process, workflow, cultural and infrastructure impact HIPAA Security provisions will have on their organization. A comprehensive, cohesive, non-invasive approach is needed to assure end-to-end security and avoid HIPAA liability.

What is needed is a single solution that addresses the three basic tenets of HIPAA compliance; Policy and Procedure, Audit Ability and Defense.

Policy and Procedure Provides a Necessary but Weak First Line of Defense

Identifying potential risks and mapping procedures that parallel risk factors is a necessary and valuable first line of defense. However, the healthcare enterprise is a dynamic entity, continuously changing and ever varied in its relations with partners, physicians and patients, reducing the effectiveness of procedural measures.

Awareness Training and User Education address the elementary requirements of HIPAA policy for security training. However there is universal agreement that the greatest risk of liability stems from human error and malicious intent. Your ability to monitor compliance and avert risk must extend beyond policy, procedure and the human interface. Ultimate compliance must be governed and protected at the fundamental level of data and the flow of data in, out and within your enterprise.

The ability to passively monitor and assimilate large volumes of information serves to identify risk areas. SilentRunner’s Network Security Analysis software (“SilentRunner®”) passively monitors and analyzes network traffic in order to support Forensics visualization of “non standard” network activity, outside threats, inside abuse, and policy deviations.

PROBLEM: Policies and procedures stipulate acceptable pathways and users of Patient Identifiable Information, but do not provide protection against human error or intent.

SILENTRUNNER® SOLUTION: SilentRunner, transparently captures, maps and visualizes the movement of data throughout the enterprise and analytically alerts you to deviations in proper behavioral patterns, abnormal data use and exceptions to role-based access provisions of individual users.

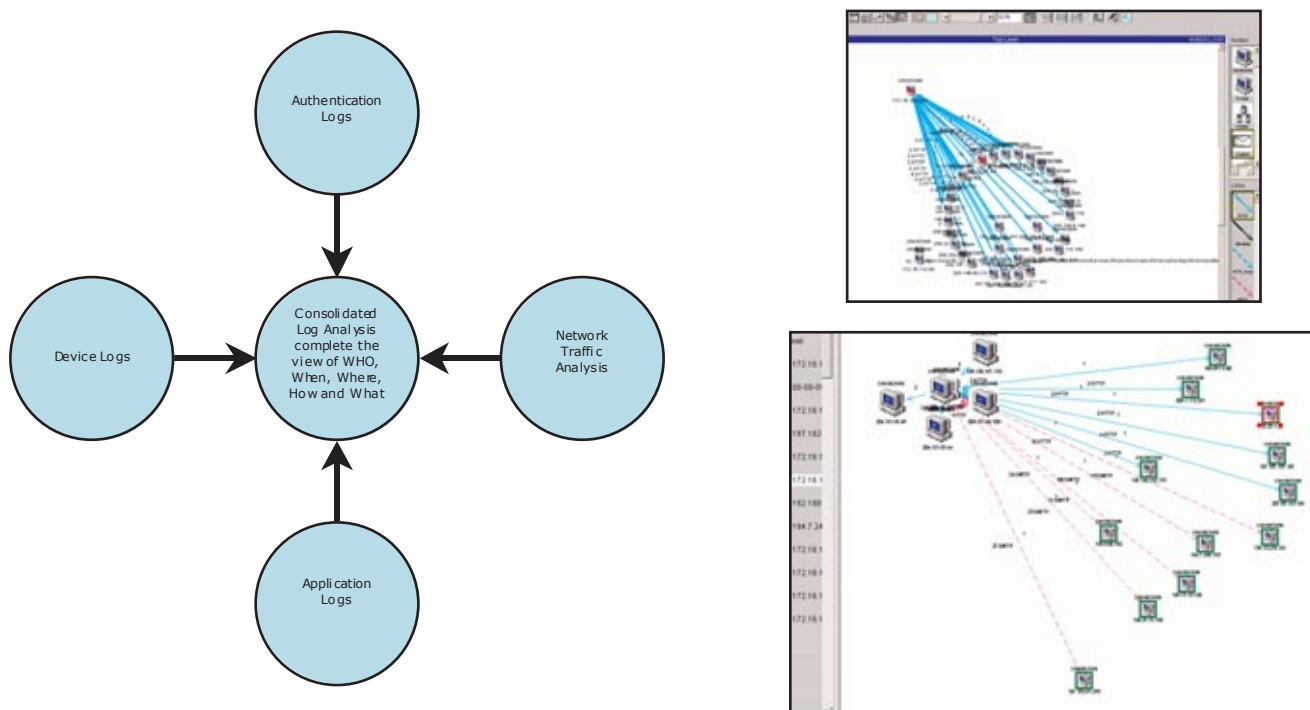
RESULT: Policies and procedures are made to be more effective, more accurate and unquestionably enforceable. Proper monitoring of policies, pre-emptive monitoring and forensic analysis greatly diminishes HIPAA liability.

A “packet level” audit trail empowers you to know Who, What, When, Where and How, before having to ask Why?

Perhaps no other component of HIPAA is as valuable or necessary as audit ability. While process and policy, authentication, and access control elements all contribute to HIPAA remediation, audit ability is the only assurance of the continual effectiveness before, during and after a breach.

Your ability to continuously monitor information exchange, between users, systems and partners provides your greatest strength to avoid risk and guide further refinement of HIPAA compliance. An effective audit instrument does not impede business activities; it provides a single-source for consolidated metadata allowing each monitoring component to contribute information which in consolidated form presents clear evidence of success or failure within appropriate standards.

Authentication logs, Device logs, and Application Logs each contain valuable audit information within the specific context of events. However, by combining network traffic analysis and consolidated log information, the individual event or breach now becomes an exemplar of knowledge in full context of time, sequence, cause and effect. A true means of audit integrity in real-time or post facto.



A single computer workstation without external connectivity and containing no data presents little or no risk. However, the power to leverage your investment in infrastructure and the interconnectivity of systems to create an integral audit capability is an immensely potent HIPAA tool, creating effective security measures of both users and data.

Although most data traversing your networks presents some potential risks, it is the specific data relevance of Patient Health Information that you are required to guard and audit. While centralized patient accounting and clinical care

related data are obviously high value/high risk, less formal data sources and elements present equal risk and are much more difficult to identify and protect.

Email messages, word processing files, electronic notes, images and other digital content can contain HIPAA regulated information. These individual objects provide indiscriminate containers that may hold and transport HIPAA data. A transparent ability to monitor the content and context of these prolific and insidious objects is fundamental to HIPAA compliance.

User and data threats come from both internal and external sources. Your security audit trail must monitor and reinforce policies and procedures, identify users, systems and data that places you at risk, and must not impede operational efficiency within the enterprise. Before you are asked “Why?”, know Who, What, When, Where and How.

PROBLEM: HIPAA demands audit capabilities to Guard Data Integrity, Confidentiality and Availability.

SILENTRUNNER® SOLUTION: SilentRunner, creates complete audit capabilities of packet level data to assure HIPAA compliance. Any and all data can be assessed whether secure or non-secure within the complete context of users, policies, content and risk vulnerability.

PROBLEM: Many varied disparate audit points diminish the overall value of audit capabilities.

SILENTRUNNER® SOLUTION: Many enterprise applications and hardware security devices provide audit capabilities, most through the use and creation of log files. With many disparate and prolific logs being created, it is difficult to analyze and maintain these data sources effectively. SilentRunner consolidates the many comprehensive log sources and analytically presents this information in the relevant context of events, data, users and time.

PROBLEM: Content is critical. Protecting HIPAA relevant data requires that you know the content and audience to properly assess HIPAA risks.

SILENTRUNNER® SOLUTION: Working from the packet level across your complete infrastructure, SilentRunner, definitively analyzes relevant data content and patterns normal behavioral utilization of information. Within this knowledge, policies and procedures can be verified, anomalies can highlight risks, and malicious use can be targeted.

Perimeter Defense Protection from the Threat Inside and Out

The threat from within is as great as the threat unknown. In a 2002 FBI/CSI study, more than 90% of companies reported internal security breaches of which 78% were attributed to employee Internet abuse.

Traditionally, an outward facing perimeter defense was considered secure. Firewalls, Intrusion Detection, Virus Scanners and the like certainly do provide some degree of defense. However, HIPAA requires protection against external threats, notwithstanding the liability of inside-out breaches of HIPAA standards. While firewalls, routers and IDS solutions are effective entry barriers, intelligence must control exit points of risk.

Content sensitive Data; the Crown Jewel of Risk and Liability

Policies instruct you not to, Audit Control confirms you did, and Perimeter Defense keeps outsiders at bay. However, the ever present risk involves sensitive data either moving internally among unauthorized parties or from an authorized internal party exploiting an exit point to forward data to an unauthorized external party.

Obvious solutions slow or impede critical information from being shared among relevant and necessary parties. The best option for securing data and monitoring vulnerable exit points, while facilitating the flow of information is low-level, passive monitoring.

By analyzing packet level data traversing the network, vulnerable data elements can be monitored, isolated and protected. Assuring proper data utilization requires you to ask three questions; 1) is critical data being moved securely, 2) is the sensitive data being moved only among appropriate authorized parties, and, 3) is the integrity of the data maintained throughout its journey?

- 1) The first question incorporates two qualifications. Is critical data being moved securely? Determining critical data requires you to know what the data is in the context of the proper authorized audience. Many systems attempt to assess data content via dictionary rules, keywords, and phrases. However in order for this method to be effective the dictionary rules must define all possible cases and exceptions, and in most cases is ineffective against encrypted messaging, multi-lingual messaging and cannot accommodate the vast language variable of the medical dialect and lexicon.

Therefore the appropriate technology must be able to associate patterns of data within the context of content and audience to determine whether critical data is trafficked among appropriate authorized communities of users.

- 2) The second question requires associating data content and users with behavioral patterns of data use and authorization. Behavioral patterns are a normal consequence of proper data traffic. Medical staff converses with Medical staff, Facilities personnel converses with Facilities staff, and likewise Patient Accounting staff converses with Patient Accounting personnel. These “inter-functional” patterns simplistically define normal utilization of data among appropriate audiences. However, the requirement is greater than patterns alone.

Satisfying HIPAA Security does not impart the need to associate like users, but rather, it requires users of sensitive data to communicate only among pertinent entities. Therefore in order to avoid breach of these provisions, you must combine the monitoring of the behavioral patterns of data traffic with the knowledge of whether the data shared among the entities is sensitive.

- 3) The third qualification of proper HIPAA data utilization demands that you protect the integrity of data and information. Most healthcare entities have approached this requirement at the application database record level and within the scope of encrypted transactions and messages. Albeit the degree of protection is necessary and meaningful, but the risks penetrate deeper. Packet level protection and monitoring is needed to assure the integrity of data at its most vulnerable state while in transit internally or externally.

Conclusion

The movement and use of health information is critical to the efficacy of a modern healthcare enterprise. However, be aware the pathways through which data moves are complex, far-reaching, often riddled with risks, and are typically very dynamic in nature. Networks, wireless devices, and the Internet are repeatedly interconnected. Email, Web pages, EDI transactions and raw data continuously traffic a maze of applications, users and trading partners. **THE ONLY TRUE AND EFFECTIVE MEANS TO MONITOR, SECURE AND AUDIT HIPAA SECURITY IS TO DO SO AT THE PACKET LEVEL OF YOUR TECHNOLOGY INFRASTRUCTURE.** Being able to monitor, analyze and audit all connectivity and data within the context of who, what, when, where and how is a single, permanent means of assuring proper, long-standing HIPAA compliance.

Know that HIPAA liability is averted by:

- Assuring only proper methods of secure and non-secure connectivity are used across 1500+ protocols of communications
- Know that the entities that are exchanging data are appropriate within the relevance of data content
- Know that enterprise applications that are sharing and exchanging data are doing so in a secure mode

- Know that your audit capabilities can clearly determine internal and external risks, and that all of your infrastructure is working in concert to provide a complete security watch

Don't allow your technology to be complicit in HIPAA liability whether derived from user error or intent, data misuse, or external threat.

SilentRunner, Provides HIPAA Security Confidence



Four components enable its use as an effective HIPAA Security tool.

Identify. Network security analysis begins with knowledge. SilentRunner gathers data about your network, its structure, its traffic and its users by analyzing raw network packets. The raw packets are assembled and organized into a knowledgebase, which provides a detailed display representation of the network.

Correlate. The ability to import, display and simultaneously correlate data from several sources (SilentRunner collected data, Firewall logs, IDS logs, etc.) enables the examination of real-time suspicious events across multiple platforms and environments.

Analyze. SilentRunner is the lens into your network ensuring proactive assessment of network weaknesses and vulnerabilities. The ability for three-dimensional visualization of activity within the network provides unparalleled knowledge of what issues pose the greatest risks to critical data assets.

SilentRunner uses n-gram analysis to determine relationships between like types of information. N-Gram Analysis is a method of breaking up text-based documents into n-number long character words. The statistical similarity of occurrences of N-grams in the source texts ultimately leads to similarities allowing you to associate specific types of data content with common communities of users. This approach provides statistically significant results with much greater speed than simple word comparisons and eliminates the limitations of linguistic analysis.

Inform. SilentRunner supplies the crucial decision making information required when making network security decision support prior to, during and after an incident.

Thanks to our pioneering solution customers can advance their ability to cost-effectively safeguard their electronic property by correlating remote and internal communications and data into critical decision-making information. Coupled with state-of-the-art visualization technology organizations are now empowered to solve complex problems by expediting network security and network management decision-making efforts.

As a logical next step to enhance legacy security technologies, SilentRunner provides an unparalleled view into the security of your healthcare enterprise information. For executives who must ensure the welfare of their intellectual assets, avoid HIPAA liability and maintain the successful management of their enterprise networks, SilentRunner® delivers patented products for advanced Network Security Analysis.

About DCS Healthcare

DCS Healthcare is a leading expert in the use of SilentRunner technology providing innovative healthcare solutions for HIPAA Security and Enterprise Application Integration that leverages existing infrastructure to enable efficiencies with effective security measures. For more information please contact DCS Healthcare at 770-663-4889, or visit us at www.dcshealthcare.com.

QUICKVIEW OF DCS Healthcare SECURITY SOLUTIONS

ASSESSMENT, PLANNING AND POLICY

- Policy review and applied evaluation
- Internal Network & Host Intrusion Testing and Assessment
- External Network Penetration Vulnerability Testing and Assessment
- Internet Vulnerability
- Email Vulnerability Testing
- Extranet & Trading Partner testing and verification
- HIPAA Compliance Testing, Planning & Policy

IMPLEMENTATION, DEVICE PROVISION, AND REMEDIATION

- Biometric, Secure Token and Smart Card Devices
- Public Key Encryption
- Security Certificate Authority Services
- Trading Partner Security Verification
- Email Content Verification (including Healthcare Specific Libraries)
- Encrypted messaging

MONITORING SERVICES AND CSO SUPPORT TOOLS

- Managed Intrusion Detection Monitoring
- Managed Penetration Detection Monitoring
- Executive Security Alert Service
- Cohesive Physical and Automated Security Measures