



Tripwire Software Protects Data And Network Integrity, Helps Healthcare Systems Meet HIPAA Privacy And Security Standards

Table of Contents

- > Summary
- > How Tripwire Applications Help Meet HIPAA Privacy and Security Requirements
- > Intrusion Detection
- > Damage Assessment and Recovery
- > Forensics
- > Policy Compliance
- > Software Verification
- > Conclusion



Summary

Best practices for assuring both data and network integrity differ little from industry to industry. Any organization managing critical electronic information understands the importance of protecting their data and networks from intrusion and abuse.

Healthcare providers face particularly difficult challenges due to the sensitive nature of the data they are responsible for safeguarding. In their environment, corrupted data can have grave consequences. Recognizing this gravity, legislators have taken steps to make the security and privacy of healthcare data a legal requirement.

The result of their concern is a broad new regulatory initiative that protects the confidentiality and integrity of electronically-stored personal health information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) set in motion the process of establishing privacy and security standards for individually identifiable health information¹. Meeting these standards demands due diligence from data and network managers throughout the healthcare industry.

Fortunately, there are many software and tools available today that will help protect this sensitive data, and assist healthcare organizations in getting a head start with their compliance. One of the tools necessary to meet these requirements is readily available to Information Technology (IT) managers. The Tripwire[®] software line of data integrity assurance products verifies the integrity of data at rest and notifies system administrators of any changes to data or system files. Patient data that is stored on servers, in databases, and required to be kept confidential can be monitored to a level of stringency that the IT manager desires. This means that unwanted changes to the data can be detected and corrected in acceptable time frames.

In addition, Tripwire software can act as a monitor to other critical healthcare systems such as firewalls and network intrusion detection appliances, ensuring that perimeter defenses have not been compromised. The ability to detect and track attacks—either through the firewall or from within the system—is a fundamental Tripwire capability on which users build many different types of security functions. As a result, information gathered by using Tripwire software is the foundation for a wide range of applications. IT managers planning a response to HIPAA Privacy and Security regulations will find that Tripwire solutions are valuable tools for helping to ensure data integrity. This paper discusses five areas where Tripwire software can help an organization meet HIPAA requirements: (1) intrusion detection, (2) damage assessment and recovery, (3) forensics, (4) policy compliance, and (5) software verification².

¹ HIPAA Privacy rules are the second final regulation to be issued in the package of rules mandated under Title II Subtitle F Section 261-264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, titled "Administrative Simplification." This rule implements the privacy requirements of the Administrative Simplification requirements. DHHS web site: www.aspe.os.dhhs.gov/adminsimp

² Specifically, Tripwire will respond to the requirements of 45 CFR, Part 164, "Security and Privacy, Subpart E, "Privacy of Individually Identifiable Health Information, part 164.530, "Administrative Requirements, subpart, (c) (1) "Safeguards" 45.164.530(c)(1). It should be noted that CFR 45.164.530 (c)(1) is referenced back to detailed security requirements which are still in "Proposed" form. It is expected that sometime early in 2001, proposed Security rule, 45.142.308, "Security Standard" will be published. This paper has drawn conclusions from the details of 45.142.308 based on the presumption the detailed administrative security requirements will be the "HIPAA Security Standard".



Tripwire Software Applications Help Meet HIPAA Privacy and Security Requirements

Administrative Procedures (Proposed CFR 45.142.308) To Guard Data Integrity, Confidentiality, and Availability		
Tripwire Software Applications Key: ID=Intrusion Detection; DAR=Damage Assessment & Recovery; F=Forensics; PC=Policy Compliance; SV=Software Verification		
Requirement	HIPAA Implementation/Description	Tripwire Application
Contingency Plan	Applications and data critical analysis – An entity’s formal assessment of the sensitivity, vulnerabilities, and security of its programs.	ID, DAR, PC, SV
Contingency Plan	Data backup plan – A documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information.	ID, DAR, PC, SV
Contingency Plan	Disaster recovery plan – The part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of a fire, vandalism, natural disaster, or system failure.	ID, DAR, F, PC, SV
Contingency Plan	Emergency mode operation plan – The part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure.	ID, PC, SV
Contingency Plan	Testing and revision procedures – The documented process of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.	ID, PC, SV
Information Access Control	Access Authorization – Information-use policies and procedures that establish the rules for granting access, for example, to a terminal, transaction, program, process, or some other user.	ID, PC, SV
Information Access Control	Access establishment – Security policies and rules that determine an entity’s initial right of access to a terminal, transaction, program, process or some other user.	ID, PC, SV
Information Access Control	Access modification – Security policies and rules that determine the types of, and reasons for, modification to an entity’s established right of access, to a terminal, transaction, program, process, or some other user.	ID, PC, SV
Internal Audit	In-house review of the records of system activity (such as logins, file accesses, and security incidents) maintained by an organization.	ID, PC, SV
Security Configuration Management	Hardware and software installation and maintenance review and testing for security features – Formal, documented procedures for connecting and loading new equipment and programs, periodic review of the maintenance occurring on that equipment and programs, and periodic security testing of the security attributes of that hardware/software.	ID, PC, SV
Configuration Management	Security testing – Process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment; this process includes hands-on functional testing, penetration testing, and verification.	ID, DAR, F, PC, SV
Configuration Management	Virus checking	ID, PC, SV
Security Incident Procedures	Report procedures – Documented formal mechanism employed to document security incidents.	ID, DAR, F, PC, SV
Security Incident Procedures	Response procedures – Documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report.	ID, DAR, F, PC, SV
Security Management	Risk analysis – A process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.	ID, DAR, F, PC, SV
Security Management	Risk management – Process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.	ID, DAR, F, PC, SV
Security Management	Security policy – Statement(s) of information values, protection responsibilities, and organization commitment for a system. This is the framework within which an entity establishes needed levels of information security to achieve the desired confidentiality goals.	ID, DAR, F, PC, SV
Training	User education in importance of monitoring log in success/failure, and how to report discrepancies.	ID, PC, SV



Technical Security Mechanisms To Guard Data Integrity, Confidentiality, and Availability

Tripwire Software Applications Key: ID=Intrusion Detection; DAR=Damage Assessment & Recovery; F=Forensics; PC=Policy Compliance; SV=Software Verification

Requirement	HIPAA Implementation/Description	Tripwire Application
Communications/Network Controls	Integrity controls – A security mechanism employed to ensure the validity of the information being electronically transmitted or stored.	ID, DAR, F, PC, SV
Communications/Network Controls	Alarm, Event reporting and Audit trail	ID, DAR, F, PC, SV
Communications/Network Controls	Encryption	ID, PC, SV
Communications/Network Controls	Entity authentication – A communications or network mechanism to irrefutably identify authorized users, programs, and processes and to deny access to unauthorized users, programs, and processes.	ID, PC, SV
Communications/Network Controls	Audit trail – A network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information.	ID, PC, SV
Communications/Network Controls	Event reporting – A network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information.	ID, PC, SV

Technical Security Services To Guard Data Integrity, Confidentiality, and Availability

Tripwire Software Applications Key: ID=Intrusion Detection; DAR=Damage Assessment & Recovery; F=Forensics; PC=Policy Compliance; SV=Software Verification

Requirement	HIPAA Implementation/Description	Tripwire Application
Audit Controls	Mechanisms employed to record and examine system activity.	ID, DAR, F, PC, SV
Authorization Control	Role-based access	ID, PC, SV
Authorization Control	User-based access	ID, PC, SV
Authorization Control	Data Authentication – The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.	ID, PC, SV
Authorization Control	Unique user identification – A combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity.	ID, PC, SV

Intrusion Detection

All of Tripwire software's capabilities are based on its fundamental role as an intrusion detector. This facility ensures that no one, internally or externally, can alter critical system files without being noticed. Using this capability, Tripwire software effectively addresses all four key areas defined in the HIPAA Privacy and Security requirements (summarized in the addendum 3 Security Matrix) which specifies intrusion detection for all servers and workstations.

Tripwire software resides at an organization's heart, protecting the servers and workstations that make up its information infrastructure. Tripwire software works by first scanning each computer and creating a database of files, a compact digital "snapshot" of the system in a known secure state. The user can configure Tripwire software very precisely, specifying individual files and directories on each machine to monitor, or creating a standard template that can be used on all machines in an enterprise.

Once this baseline database is created, a system administrator can use Tripwire software to check the integrity of the system at any time. By scanning the current system and comparing that information with



data stored in the database, Tripwire software detects and reports any additions, deletions, or changes to the system outside of the specified boundaries. If these changes are valid, the administrator can update the baseline database with the new information. If Tripwire software uncovers malicious or undesired changes, the system administrator will instantly know which components of the network have been affected.

Because Tripwire software detects file system changes from any source, it has many advantages over other types of security software. Other intrusion detection tools use anomaly detection, searching for attacks based on a catalog of known attack signatures. This strategy often fails, however, because hacker exploits literally change on a daily basis, and no anomaly detection tool can keep pace with this high-speed evolution. In addition, anomaly detection software and appliances only detect attacks that come through the firewall, ignoring attacks that originate within the system. Tripwire software detects any change to a protected system, regardless of the source of the attack, the method used, or the intent. This fundamental difference has already established Tripwire software as the industry's best-of-breed choice for intrusion detection.

Using Tripwire software throughout the network gives administrators a high level of confidence in system integrity, and will allow organizations to meet HIPAA Privacy and Security requirements, enabling administrators to prove their systems and data integrity have not been compromised.

Further, by working with applications that protect systems or applications from modifications, information provided by an intrusion detection tool (such as Tripwire software) can play a valuable role in implementing policy under HIPAA Administrative Procedures. Technically enforcing a written policy is always a formidable challenge, but with a flexible product like Tripwire software, the job just got easier.

Damage Assessment and Recovery

As many system administrators have discovered from painful experience, detecting that an intrusion has occurred is only the beginning. After a hacker has broken in, the questions begin: Which systems have been affected? Which files have been altered? Tripwire software is the most useful tool a system administrator can reach for to answer these questions. By immediately identifying which files have been compromised, Tripwire software makes it easy to focus recovery efforts where they are needed, without immobilizing the entire network.

Tripwire software, in tandem with regular backups of systems and data, allows immediate re-structuring of systems if they do go down or are compromised. Whatever alterations may have been made, Tripwire software provides the best possible roadmap to a rapid and precise recovery. This type of damage assessment and disaster recovery capability is a key element required to meet HIPAA Privacy and Security requirements.

Tripwire provides powerful tools to help manage disaster recovery efforts, data backup, testing, and revision. As part of the Security Management procedures, Tripwire software will assist in the role of response procedures, reporting procedures, risk management, and of course as an integral part of a security policy.

Another important step in recovering from an intrusion is the removal of any "back doors" that the hacker has created. The attacker may have installed a rootkit, network sniffer, or other pieces of malicious code, allowing him to gather information about your network and re-enter at will. Obviously these programs must be found and removed, but because they can be disguised as legitimate system files they are difficult to detect. Because Tripwire software uses cryptographic algorithms to scan the contents of files on a



system, it will detect changes to files that have been sabotaged even if the hacker has changed names or access times to cover their tracks. Using Tripwire software cryptographic algorithms to scan the suspect data and comparing it to archived data will quickly yield which data has actually been compromised.

For the healthcare administrator striving for HIPAA compliance, being able to recover from the incidents that do get past other security controls in a timely manner is key. For management, showing that due care and due diligence have been performed in both the prevention *and* recovery of threats to sensitive patient data will be critical to any successful HIPAA compliance plan.

Forensics

Just as damage assessment and recovery is an important part of a security incident procedure and contingency plan, so is forensics. A system that has been hacked is a crime scene. During the course of the recovery process, the system administrator should gather evidence needed to prosecute the intruder if they are found. For instance, if a hacker installs malicious programs on a system, and these same files are later found on a suspect's computer, this digital "fingerprint" can be an important piece of evidence. Tripwire software is an important forensic tool for collecting evidence at the scene of the crime, and for establishing a chain of evidence from the hacked system to the courtroom.

Tripwire software acts as a virtual camera at the scene of a crime, collecting evidence and allowing the reconstruction of the crime scene after the fact. Immediately after an intrusion is discovered, Tripwire software can be used to create a "post-attack" database for each system that has been affected.

Preserving evidence is important for any crime scene and must be done prior to system recovery efforts. With Tripwire software, all backups can be signed, (by multiple witnesses if possible) dated, and time-stamped. By following this procedure, Tripwire software serves not only as the camera at the crime scene, but also as the mechanism to prove that the evidence has not been altered.

Within the confines of the HIPAA Addendum 3 Security Matrix, Tripwire software's forensics application is crucial in the evidence-gathering role in the event of a compromise. As part of the addendum's Administrative procedures, forensics is given a large role in disaster recovery plans, internal audits, personnel security, security incident procedures, security management, and termination procedures. Tripwire software's forensics application is also valuable in the event of a security breach resulting in the modification of systems or applications. It can be key in the areas of Technical Security and Services, providing key audit trails, event reporting, integrity controls, and is also helpful in disaster recovery.

As all healthcare organizations will become aware, non-compliance with HIPAA will be very costly to offenders caught in the act. Entities compromising your compliance with the law will be prosecuted.

Be sure you have the correct tools to make a foolproof case for your organization.

Policy Compliance

When an organization installs new systems and applications and sets new policy, they need tools that will help keep that policy enforced, and then notify management if breaches occur. HIPAA Privacy and Security requirements set many such new policies into motion, and Tripwire software's policy compliance role can be utilized in virtually every area of the security matrix. Policy compliance and periodic auditing are key to Administrative Procedures, Technical Security, and Technical Security and Services.

Tripwire data integrity assurance solutions are already popular because IT managers have discovered that preventing system intrusions is much less expensive than responding to them. Because a heterogeneous system environment increases the number of exploits, security administrators know that an effective way



to prevent intrusions in a large enterprise is by standardizing the configuration of machines. An important part of this strategy is enforcement of a configuration policy that prevents users from changing their configuration. Tripwire software can be an effective tool for enforcing an enterprise-wide configuration policy by detecting changes to configuration settings on all levels.

When it is time to audit systems, Tripwire software can be used as a tool to help pass that audit. Tripwire software can easily verify that systems are HIPAA-compliant, using many of the same techniques developed to verify Y2K compliance. When companies issued software lock-downs prior to Y2K, Tripwire software was their primary enforcement tool. After making the initial investment to certify that systems were Y2K compliant, administrators used Tripwire software to determine which, if any, of the systems had been changed at a later date. Isolating the changes to a Y2K-compliant system in this way greatly reduced maintenance costs associated with re-certification.

Managers and technology departments pursuing HIPAA compliance have a wealth of options for customizing the performance or operation of their system. While this is a useful tool for ensuring successful integration, malicious software can use this same mechanism to subvert security. As part of a well-designed security policy, Tripwire software can be used to monitor individual computers across the enterprise, ensuring that neither malicious software nor uninformed users open the system to intrusions. This will offer those managing technology in healthcare IT departments the ability to manage-at-a-distance in distributed environments.

Software Verification

To meet HIPAA Privacy and Security requirements, most organizations are acquiring new systems and applications, and those installations will have to be verified. Tripwire software's ability to detect minute differences between supposedly identical systems makes it indispensable for software verification, and applies to nearly all of the HIPAA requirements for Administrative and Technical security. With so many new systems and applications going into service, Tripwire software's ability to verify that they were rolled out properly will be very powerful. With its wide range of cryptographic algorithms, Tripwire software can scan files that have been copied or downloaded to ensure that no changes occurred during the transfer. Tripwire software can also be used to monitor the software installation process to verify that a program has been configured correctly.

Using Tripwire software to roll out these systems and applications will allow system administrators to be sure that they were not modified between test system and actual production system. Once those applications and systems are in place, Tripwire software can be used to periodically audit them to make sure there have been no modifications to their integrity.

Conclusion

In enacting HIPAA, Congress recognized the fact that administrative simplification cannot succeed if the industry does not also protect the privacy and confidentiality of individually identifiable health information. The provision of high-quality health care requires the exchange of personal, often-sensitive information between an individual and a skilled practitioner. Vital to that interaction is the patient's ability to trust that the information shared will be protected and kept confidential.

Tripwire leads the industry in the assurance of data and network integrity, and has expanded from its original role as an intrusion detection tool to meet many needs in the field of security and other areas of system administration. Now, as HIPAA privacy and security requirements are implemented, Tripwire software will continue to be a fundamental tool for use at every point where data is at rest and ensure the ongoing integrity of data in the healthcare industry.

