Trustwave®

Health Care Technologies

SAFEGUARDING PROTECTED HEALTH INFORMATION

Count on Trustwave to guard your infrastructure, networks and data by building a defense-in-depth security strategy to protect your vital assets.

Securing Patient Care

Quality patient care includes fortification of sensitive and valuable medical information. Healthcare is being flipped as providers and payers embrace electronic health record systems, mobile devices and other technologies for efficiency and to improve patient treatment. However, data privacy of protected health information (PHI) and basic security of personally identifiable information (PII) is often overlooked in clinical and administrative environments.

Trustwave can enable your teams to make the most of technologies, protect against malicious attackers and maintain regulatory compliance through automated and managed security solutions.

Employ the Right Technology—implement real time detection of devices to prevent threats, authenticate users, and protect data against loss or theft.

Know Your Data—understand risk, locate information and categorize data that needs protection.

Maintain Compliance—implement policies and leverage technology to remedy compliance gaps.

Automate and Manage Security—gain insight and centrally manage controls, policies and procedures through our cloud-based TrustKeeper platform and managed security solutions.

Enjoy smart security on demand and maintain compliance with the help of Trustwave technologies and services.

Testing and Threat Response

Critical to understanding your ongoing security posture is to test and retest. Intelligent organizations conduct regular penetration testing and simulate attacks on their most sensitive network segments and key applications. Trustwave SpiderLabs is an elite team of ethical hackers and researchers that identify root causes of incidents and communicate responses in a way that clinical staff, management and IT staff can understand.

Managed Security Testing—allows continuous, static, and dynamic testing for identification of gaps and alerts you to vulnerabilities in network architecture or application code bases.

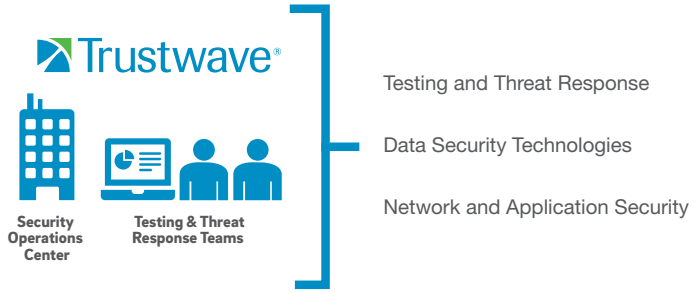
HIPAA citations §164.308(a)(1)—Security Management Process

Incident Readiness Service—offers business training, documentation development and review, simulated attacks, plus on-demand and on-call services.

HIPAA citations §164.308(a)(6)—Security Incident Response

Internal/External Vulnerability Scanning—provides a hackers view of vulnerabilities behind your firewall and network vulnerabilities exposed to the outside world from inside the corporate firewall.

HIPAA citations §164.308(a)(8)—Evaluation



Data Security Technologies

A data breach or loss of sensitive information can be devastating to an organizations brand and reputation. Align the protection of sensitive information to strategic business objectives, corporate security policy and compliance obligations with the help of Trustwave data security solutions.

Secure Web Gateway—enables safe access to the web, giving protection through our patented malware entrapment engine.

HIPAA citations §164.312(e)(1)—Transmission Security

Secure Email Gateway—delivers improved policy enforcement and data leakage protection; a secure messaging solution that protects against email borne threats including phishing, blended threats, and spam.

HIPAA citations §164.312(e)(1)—Transmission Security

Data Loss Protection—defends against data leakage by detecting and identifying data to classify, correlate, capture and control info outflow with encryption, quarantine or blocking.

HIPAA citations §164.312(b)—Audit controls
HIPAA citations §164.312(c)(1)—Integrity

Security Information & Event Monitoring (SIEM)—Having vision into and preparing for evolving threats empowers you to collect, analyze, and assess security and non-security events for rapid identification, prioritization and response. A variety of SIEM deployment options are available including software, managed and CPE appliances.

HIPAA citations §164.308(a)(6)—Security Incident Response

Encryption—provides an integrated solution for encryption of disks, persistent files on shares, desktops, laptops, USB devices and email attachments.

HIPAA citations §164.312(a)(2)(iv)—Access Control

Network and Application Security

Data is the lifeblood of your business. Malware, advanced persistent threats, malicious snoopers and inattentive insiders all pose threats to sensitive data. Trustwave integrated solutions for content security have been designed to combat common assaults, sophisticated hackers and misuse of information while providing control over the confidentiality, integrity and availability of data as it's being accessed, shared, moved and stored.

Unified Threat Management—provides a comprehensive set of integrated network security technologies designed to defend against external threats, while also offering protective measures from inside the network out. Features include:

- Stateful Firewall
- Deep Inspection Intrusion Prevention
- Web & Email Anti-Virus
- Web Content Filtering
- Rogue Device and Wireless Access Point Detection
- Internal Vulnerability Scanning
- Virtual Private Networking
- Wi-Fi Hotspot

HIPAA citations §164.308(a)(1)—Security Management Process
HIPAA citations §164.308(a)(6)—Security Incident Response
HIPAA citations §164.308(a)(8)—Evaluation

Intrusion Detection and Prevention Systems—monitors traffic passing through at the application layer, blocking data flows with malicious intent, ensuring protection at key entry and exit points so your business continues without interruption.

HIPAA citations §164.308(a)(1)—Security Management Process
HIPAA citations §164.308(a)(6)—Security Incident Response

Web Application Firewall—continuously monitor your applications, instantly detect and prevent threats, mitigate the risk of data breach and address compliance.

HIPAA citations §164.308(a)(1)—Security Management Process
HIPAA citations §164.308(a)(6)—Security Incident Response

Network Access Control—prevents the spread of malware and other threats with granular control over network access and continuous monitoring of corporate or user owned device endpoints.

HIPAA citations §164.308(a)(4)—Information Access Management
HIPAA citations §164.312(a)(1)—Access Control

Two-Factor Authentication—secure access to networks and applications to protect users and address compliance requirements for the protection of regulated data, supporting authentication from the corporate desktop, remote locations, employee laptops and mobile devices, such as smartphones and tablets.

HIPAA citations §164.308(a)(4)—Information Access Management
HIPAA citations §164.312(a)(1)—Access Control

Trustwave®

For more information: www.trustwave.com