Trend Micro Enterprise Security For the Healthcare Industry

A Trend Micro White Paper

Assuring regulatory compliance, ePHI protection, and secure healthcare delivery

July 2010

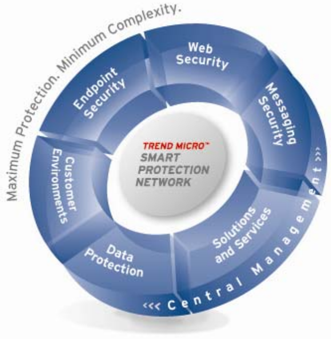
TREND MICRO ENTERPRISE SECURITY FOR THE HEALTHCARE INDUSTRY

I. HEALTHCARE REQUIREMENTS AND TREND MICRO ENTERPRISE SECURITY

The healthcare industry is in a time of great transition, with a government mandate for EHR/EMR systems, increasing security regulations, and greater compliance scrutiny and punitive actions. While EHR systems will ultimately lead to more efficient and effective patient care, they also increase the criminal appeal of attack and an institution's vulnerability to large-scale ePHI breach. Moreover, increased reliance on IT and EHR systems for mission-critical operations means that any attack or infiltration has the potential to be catastrophic. Compliance with security regulations will guide providers of all types to mitigate their risk, but maximizing protection of these complex operations requires a broader strategy.

Trend Micro Enterprise Security provides unique and cost-effective solutions that ensure compliance, maximize protection, and enable your strategic business and IT initiatives. With Trend Micro you can:

- Comply with HIPAA, HITECH, and PCI regulations
- Maximize ePHI protection and your reputation
- Confidently implement EHR modernization
- Adopt virtualization and cloud computing strategies
- Consolidate and simplify your security infrastructure



US Healthcare Regulation	Trend Micro Enterprise Security				
	Endpoint Security	Web Security	Messaging Security	Data Protection	Vulnerability and Threat Management
HITECH Act					
Breach notification for unsecured ePHI	●	●	●	●	●
Encryption ("safe harbor" from breach notification)	●		●	●	
Extend HIPAA requirements to business associates	●	●	●	●	●
HIPAA (Health Insurance Portability and Accountability Act)					
Protection of ePHI confidentiality, availability, and integrity	●	●	●	●	●
Minimize data collection and use	●				
Transmission security			●	●	
Integrity	●	●			
Access control and authentication	●			●	
Device and media controls	●			●	
Security awareness, training, incident procedures	●			●	●
Security management process	●	●		●	●
Protection from malicious software	●	●	●		●
PCI DSS (Payment Card Industry Data Security Standard)					
PCI compliance (see appendix)	●	●	●	●	●

Trend Micro Solutions for HIPAA, HITECH, and PCI Requirements

II. THE HEALTHCARE COMPLIANCE LANDSCAPE

Patient data privacy and security regulations along with compliance enforcement have evolved for over a decade, but new, more stringent guidelines, mandates for electronic record modernization, and government funding are compelling the industry to make significant investments in modernizing and securing their operations.

Regulatory Compliance Applies to:

- *Covered entities including health plans, health care clearinghouses, and health care providers*
- *Business associates of these entities.*

THE HIPAA RULES – PROTECT ePHI

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 states that "covered entities" are required to employ safeguards that "ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI)"[i] under their control[ii]. However, the industry has struggled with the choice of specific technologies solutions in the absence of implementation guidelines. Penalties for non-compliance or actual ePHI breach have been minimal as compared with other regulations (e.g., PCI), causing many organizations to delay or insufficiently secure ePHI systems.

ELECTRONIC MEDICAL/HEALTH RECORDS (EMR/EHR) – MORE REWARD, MORE RISK

A 2004 presidential mandate called for all health records to be electronic by 2014, in hopes of driving improved efficiency and lower costs in healthcare delivery and information management. However resistance to EHR modernization has been considerable due in part to costs, practitioner resistance to change, and the heighted security risks of large-scale breach of digital records.

NIST 800-66 – IMPLEMENTATION GUIDELINES FOR HIPAA SECURITY RULE

More recently in 2008, the National Institutes of Standards and Technology (NIST) authored "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule", as a framework for federal agencies to achieve HIPAA compliance.

Though NIST guidelines do not claim to supersede HIPAA Security or other related rules, the HHS interim final regulations specifically call out NIST and its various publications as trusted resources for technology implementation guidance in key areas such as encryption. As a result, many non-government agencies can also benefit from the technical specifications highlighted in this guide.

HITECH ACT OF 2009 – THE NECESSARY INCENTIVES

Title XIII of the American Recovery and Reinvestment Act of 2009 is also known as the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The HITECH Act further reinforces the 2014 EHR mandate and provides the necessary incentives to accelerate EHR adoption and clarify key HIPAA security requirements.

Funding: Most significant in the Act is actual funding support for EHR conversion via ARRA funds. While specific amounts and qualification criteria continue to be determined, there is clear government support for migration to EHR, *including* the implementation of appropriate security systems.

HITECH Act Highlights

- *EHR Funding*
- *Business Partner Compliance*
- *Risk assessments*
- *Breach notification*
- *Safe harbor through encryption*

Risk Assessments: Risk Assessments can be used in both proactive and reactive ways. The Act specifically identifies risk assessments as necessary in determining, after the fact, whether an incident is indeed a breach of unsecured ePHI and whether even the leak of a subset of an individual's ePHI could be used to identify the individual. These nuances point to the need for visibility into data and some level of forensics to determine the nature and extent of potential data breaches.

Breach Notification Requirements: The HITECH Act[iii] address the topic of breach notification of unsecured ePHI,[iv] or ePHI that is 'not secured through technology or methodology' for covered entities and for the first time, business associates. Not only do the disclosure requirements subject the organization to public scrutiny on the data breach, but also the costs associated with notifying affected individuals can be significant. Any breach of unsecured ePHI must be disclosed and acted upon as follows:

- Covered Entity: Notification to affected individuals and Secretary of HHS
- Business Associates: Notification to affected Covered Entities
- Secretary of HHS: Post on HHS website if >500 individuals are affected

"Safe Harbor" Through Encryption: The Act defines 'secured' ePHI as data that is either encrypted or destroyed. It goes further to state that if secured ePHI is involved in a data breach, *notification requirements do not apply*. This is a significant directive, specifically prescribing encryption as both a preferred means to enforce confidentiality and as a relief from breach notification requirements. The Act also highlights NIST guidelines[v] on end user device encryption as a resource for implementation strategy. The ultimate benefit of these specifications to the healthcare organization is specific guidance on how best to protect both patient privacy and the institution's reputation.

STATE PRIVACY LAWS[vi]

Although the HITECH Act asserts precedence over state laws, it also acknowledges the importance of alignment with state laws by specifying[vii] a 'harm' threshold', which would notify the affected individual if a specific level of breach has occurred. The ultimate benefit of this consistency is simpler implementation of security controls and fewer notifications. Some laws have extended requirements to encryption of confidential data, bringing Federal and State laws closer and simplifying compliance efforts.

PCI ENFORCEMENT LOOMS

Healthcare institutions that accept credit card payments are obligated to comply with the Payment Card Industry Data Security Standard (PCI DSS) [viii]. Health insurance premiums, medical services, and even retail shops located on hospital premises are examples of scenarios where the security of cardholder data is required. PCI enforcement continues to increase and healthcare institutions are well advised to design and implement a security framework that addresses both HIPAA and PCI DSS.

III. HEALTHCARE SECURITY & COMPLIANCE CHALLENGES

Maintaining regulatory compliance and maximizing security is especially demanding in today's evolving healthcare industry. Trend Micro understands the challenges and offers solutions that enable you to confidently secure the business and IT initiatives that support your strategic business goals.

PROTECT ePHI – AND YOUR REPUTATION

While perimeter and content security provide important safeguards, HIPAA and HITECH make it clear that encryption is the only way to ensure the ultimate protection of ePHI and avoid costly disclosures. Effective encryption deployment also requires a data loss prevention (DLP) solution to discover where ePHI is stored and ensure its encryption when transmitted. However, conventional encryption and DLP solutions suffer from major drawbacks that impede their success and widespread adoption by employees:

- PKI-based email encryption is burdensome and complex to administer and use
- Endpoint DLP solutions typically have a negative performance and usability impact

Trend Micro secures sensitive data with endpoint DLP, email encryption and content filtering solutions that emphasize both security and ease-of-use. Identity-based, universal-reach encryption will ensure adoption of secure data policies across your entire medical ecosystem.

SECURE LAPTOPS, PDAS, AND SMART PHONES

Mobile laptops, PDAs, and other devices are quickly becoming mainstays of EHR-based care systems and essential to the daily tasks of nurses, physicians and other healthcare professionals. These devices are at extreme risk for attack and ePHI loss, but cannot be adequately protected by network-based solutions.

Trend Micro OfficeScan and the Smart Protection Network keep wireless, mobile, and fixed devices of all kinds protected from malware both on and off network. Trend Micro Data Encryption and DLP solutions continuously protect endpoint data while allowing secure communication from any location.

PROTECT HEALTHCARE WEBSITES AND PORTALS

EHR promises efficient patient and partner data access, however websites have proven to be extremely vulnerable to attack and hijacking, using SQL injection and other techniques. Inadequate website security puts your reputation at risk by exposing patients, their data, and entire databases to attack.

Trend Micro Deep Security and Vulnerability Management Services secure patient/partner communication by protecting websites and portals from infection, day-zero threats, and the vulnerabilities introduced by ever-changing web content.

SECURE CRITICAL MEDICAL DEVICES

Medical devices for patient evaluation and diagnosis are increasingly network-connected and run on general-purpose operating systems such as Microsoft Windows. While greatly improving patient care, these devices are now at risk for compromise and failure due to malware infections or external hacks.

Trend Micro Deep Security and OfficeScan minimize the risk of compromise on medical device systems that run on general-purpose operating systems. And for networked devices that cannot be directly secured, Trend Micro Threat Management Services identifies compromises and aids in remediation.

CONFIDENTLY IMPLEMENT EHR/EMR INITIATIVES

Implementing an EHR system provides a strategic opportunity to improve care while fostering loyalty in a wide network of independent physicians and practices. Securely operating this extended infrastructure requires a security partner capable of protecting operations from hospital floor to cloud-based data centers.

Trend Micro Enterprise Security provides comprehensive content and data security for the entire provider ecosystem—across physical, virtual and cloud-based environments. With Trend Micro you can confidently go digital and adopt the latest workplace and technology innovations to support your business initiatives.

ADOPT VIRTUALIZATION & CLOUD COMPUTING

EHR modernization and “green IT” practices are driving the healthcare industry to adopt server virtualization to enable cost efficient and flexible datacenters and to pave a path toward integrated cloud computing. And desktop virtualization promises new economies and tighter security and policy control. But the complexity and fluidity of virtual environments pose special challenges, rendering traditional IPS, firewall, and antivirus protection insufficient to prevent attacks on virtual servers that process or host ePHI/PCI data.

Trend Micro Deep Security provides advanced software-based security that protects physical, virtual, and cloud-based servers with agentless anti-malware, integrated IPS, firewall, integrity monitoring, and more. Along with supplemental malware protection from Trend Micro Core Protection for Virtual Machines, Trend Micro provides a comprehensive software solution for securing complex virtual and cloud environments.

CONSOLIDATE AND SIMPLIFY SECURITY INFRASTRUCTURE

Over the years, healthcare and benefits providers have built a patchwork of security products in an effort to deal with evolving threats and regulations. The government’s EHR mandate and funding efforts along with the clarity of the HITECH act provide the opportunity for institutions to build a consolidated and simplified security infrastructure in conjunction with their IT new modernization initiatives.

Trend Micro solutions are designed to provide comprehensive and consolidated content and security that minimizes the number of products and vendors you must deploy. And with Trend Micro Endpoint Security Platform, you can manage both security and systems using a single integrated application.

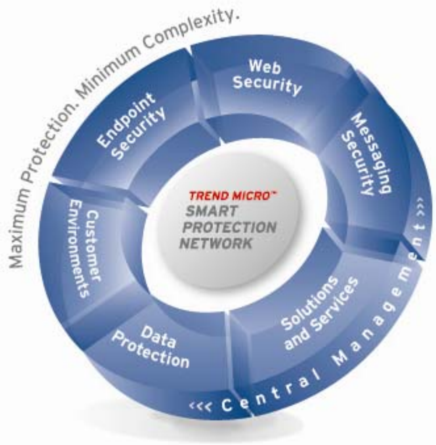
AUTOMATE IT RISK MANAGEMENT PROCEDURES

While the HITECH Act identifies risk assessment as a *reactive* measure to identify the nature of a breach, most IT organizations recognize the need to *proactively* avoid data breaches and hacks. Both for corporate governance and HIPAA compliance, organizations should employ risk management practices to identify and assess the vulnerability of critical assets, evaluate infiltrations, and apply additional preventative measures.

Trend Micro Vulnerability Management and Threat Management Services support Healthcare IT Risk Management by utilizing cutting-edge analysis of malware behavior and advanced threat correlation to uncover, contain and remediate network infiltrations undetected by perimeter and content security. Going further, Threat Management Services provide root-cause analysis and consultative planning to strengthen your security posture.

IV. TREND MICRO ENTERPRISE SECURITY

Trend Micro Enterprise Security is a tightly integrated offering of content and data security solutions and services, powered by the Trend Micro Smart Protection Network™. Together they deliver maximum protection from emerging threats while minimizing the cost and complexity of security management.



Trend Micro enables you to go beyond addressing fundamental HIPAA and HITECH compliance with practical solutions that truly safeguard your critical operations and infrastructure and enable your strategic business and IT initiatives.

Trend Micro Enterprise Security Solutions	Description
Smart Protection Network	
Trend Micro Smart Protection Network	Trend Micro Enterprise Security products and services are powered by Smart Protection Network—a next-generation cloud-client infrastructure that combines sophisticated cloud-based technology, feedback loops, and the expertise of TrendLabs researchers to deliver real-time protection from emerging threats.
Data Protection	
Trend Micro Data Loss Prevention	Provides data loss prevention with extremely accurate and effective detection and protection of sensitive data on the endpoint. Sophisticated fingerprinting, statistical algorithms and small footprint ensure high scalability, while HIPAA and PCI templates and reports simplify tracking and protection of ePHI and cardholder data.
Trend Micro Email Encryption	Advanced *identity-based* encryption allows universal reach without pre-registration. Unlike conventional PKI encryption, Trend Micro email encryption uses cloud-based key management to generate keys on demand without the need for certificates and per pair pre-registration. End-user encryption as well as policy-based, automated gateway encryption ensure that all sensitive data is protected and your communications are compliant.
Messaging Security	
Trend Micro InterScan Messaging Security	Smart Protection Network provides antispam, anti-phishing and anti-malware protection as well as outbound content filtering and automated encryption for enterprise email. Multiple deployment modes include virtual appliance.
Trend Micro Communication & Collaboration Security	Provides dedicated anti-malware protection for Microsoft Exchange, Office Communication Server (IM), SharePoint and Lotus Domino.
Endpoint Security	
Trend Micro OfficeScan	Provides superior defense against threats—both on and off the corporate network—combining top rated anti-malware with innovative in-the-cloud protection from the Smart Protection Network. File Reputation moves the burden of signature management into the cloud, freeing endpoint resources. Web Reputation protects endpoints by blocking access to malicious sites. OfficeScan offers a single compliance solution to protect desktops, virtual desktops, laptops, servers, storage appliances, PDA devices and more.

Trend Micro Deep Security	Provides software-based comprehensive security and compliance for critical business servers operating in standalone, virtual, and cloud-based environments. Key protection capabilities include: deep packet inspection (enabling IDS/IPS, network application control, and web application protection), firewall, integrity monitoring, and log inspection. .
Trend Micro Core Protection for Virtual Machines	Provides automated anti-malware protection designed specifically to meet the unique needs of the virtual environment. Features include: active and dormant VM protection, vCenter management integration and a performance-optimized architecture.
Messaging Security	
Trend Micro InterScan Messaging Security	Provides Smart Protection Network-based anti-spam, anti-phishing and anti-malware protection as well as outbound content filtering and automated encryption for enterprise email. Available in a variety of deployment models including virtual appliance.
Trend Micro Communication & Collaboration Security	Provides dedicated anti-malware protection for Microsoft Exchange, Office Communication Server (IM), SharePoint and Lotus Domino.
Web Security	
Trend Micro InterScan Web Security	Provides immediate protection against web threats by integrating multiple layers of protection at the internet gateway. It combines anti-malware and antispyware with Smart Protection Network Web Reputation and URL filtering to detect and block threatening web site access based on reputation and company policy. Advanced reporting capabilities provide detailed monitoring and analysis of employee activity.
Trend Micro OfficeScan, Deep Security and Vulnerability Management Services	Together these products enable secure and compliant website operations and web-based communication and collaboration by protecting websites and portals from malware infection, day-zero and targeted threats and the exploitation of vulnerabilities introduced by web applications and ever-changing site content.
Risk Management	
Trend Micro Vulnerability Management Services	Delivers total control over software and system vulnerabilities, web content vulnerabilities, and IT policy compliance
Trend Micro Threat Management Services	Manages breach risk with unique services to discover targeted and zero-day infiltrations that perimeter and content security has failed to detect. Powered by the Smart Protection Network, it features cutting-edge analysis of malware behavior, advanced threat correlation and consultative planning services to ensure compliance and maximize ePHI protection.
Central Management	
Trend Micro Endpoint Protection Platform	Provides a unified platform for managing security and systems compliance across all clients and servers regardless of location or network connectivity. Key components under management include Core Endpoint Security and Web Protection, Data Loss Prevention, Patch Management and Power Management
Trend Micro Control Manager	Provides centralized management of many Trend Micro products, simplifying configuration and updates and coordinating threat reports and analysis.

V. HEALTHCARE REGULATION COMPLIANCE WITH TREND MICRO ENTERPRISE SECURITY SOLUTIONS

Please see Section 4 for a detailed overview of Trend Micro Enterprise Security products highlighted below.

Healthcare Regulation	Trend Micro Solutions and Mapping Justification
HI TECH Act of 2009—Breach Notification for Unsecured Protected Health Information	
HITECH § 13402 Notification in Case of Breach **HITECH § 13404** Application of Privacy Provisions and Penalties to Business Associates of Covered Entities **HITECH § 13407** Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities **45 CFR parts 160 and 164** (Interim Rule) Issued following updates to HIPAA: **HIPAA Subpart D** Notification in the Case of Breach of Unsecured Protected Health Information **HIPAA §164.404** Notification to Individuals (Description of type of unsecured ePHI involved in the breach)	**Trend Micro Enterprise Security Solutions for Endpoint, Messaging, Web, and Data** provide essential functionality to meet ePHI breach notification requirements through security monitoring, threat prevention, and data encryption. **Monitoring** ▪ Monitor files on servers known to contain ePHI for tampering, copying or removal with **Trend Micro Deep Security**. ▪ Routinely discover where ePHI is stored with **Trend Micro DLP**– to identify which systems need to be secured and also to determine the possible sources of a breach should it occur. ▪ Monitor systems – on-site, remote, or off-line for unauthorized copy of ePHI to external devices or transmission via common applications such as Web, email, and instant messaging with **Trend Micro DLP**. ▪ Monitor end-user systems for access to malicious websites or email suspected of hosting data-stealing malware with **Trend Micro OfficeScan** and **InterScan Web and Messaging Security.** ▪ Monitor email traffic for ePHI leaks and block inbound spam containing data-stealing malware with **Trend Micro InterScan Messaging Security.** ▪ Monitor network traffic for evidence of active malware infections that have infiltrated the network with **Trend Micro Threat Management Services.** **Prevention** ▪ Prevent end users—whether on-site, remote, or off-line—from copying or transmitting ePHI to external devices or unauthorized locations with **Trend Micro DLP** ▪ Prevent sending of emails to outside entities if they contain unencrypted ePHI in the message or attachments with **InterScan Messaging Security.** ▪ Prevent end-user systems from access to malicious websites or email suspected of hosting data-stealing malware with **Trend Micro OfficeScan and InterScan Web and Messaging Security**. **Encryption** *(see Safe Harbor section below)*
HI TECH Act of 2009—"Safe Harbor" or exemption from breach notification if PHI is secured using encryption	
45 CFR parts 160 and 164 (Interim Rule) (Encryption and destruction for rendering ePHI unusable, unreadable, or undecipherable to unauthorized individuals.) **45 CFR parts 160 and 164** (Interim Rule) (Keep encryption keys on a separate device from the data that they encrypt or decrypt) **HIPAA §164.304 Definitions** (Encryption)	Trend Micro offers encryption solutions which enable covered entities to protect ePHI and forego breach notification requirements: ▪ Enforce automated encryption of email messages and attachments containing unsecured ePHI with **Trend Micro Email Encryption**. ▪ Cloud-based key management safeguards keys and generates keys on demand without the need for certificates and per pair pre-registration for all **Trend Micro Encryption Solutions**.

Healthcare Regulation	Trend Micro Solutions and Mapping Justification
HIPAA Security Rules—A subset of the HIPAA rules, covering technical safeguards for PHI data.	
§ 164.306(a)(1) (Protect ePHI: Facilities must protect the confidentiality, availability, and integrity of all ePHI created, received, maintained, and transmitted.)	When implemented using the recommended risk assessment and best practices from the NIST "Introductory Guide to Implementing the HIPAA Security Rule" (recommended in the Interim Rule), **Trend Micro Enterprise Security Solutions for Endpoint, Messaging, Web and Data** help address confidentiality, availability, and integrity of ePHI.
§ 164.308 (a)(1) Security Management Process (Includes required risk analysis and risk management)	IT risk management involves inventory of all assets and related vulnerabilities, threats, likelihood threats, and countermeasures. **Trend Micro Enterprise Security Solutions** can help in key areas of the risk management process: ▪ Discover all enterprise systems which store ePHI data – or assets – with **Trend Micro DLP.** ▪ Scan internal and externally facing systems for vulnerabilities and IT policy compliance with **Trend Micro Vulnerability Management Services.** ▪ Scan external facing healthcare websites and portals with **Trend Micro Vulnerability Management Services**to identify vulnerabilities that could be exploited to gain access to ePHI data. ▪ Monitor end-user systems for access to malicious websites or email suspected of hosting data-stealing malware with **Trend Micro OfficeScan, InterScan Web Security, and InterScan Messaging Security**. ▪ Detect and remediate active malware infections using **Trend Micro Threat Management Services.** Provides network risk assessment audit logging and offers advanced reporting and audit trail to demonstrate infection-free environment.
§ 164.308 (a)(5)(i) (Security awareness and training) **§ 164.308 (a)(6)** (Policies and procedures to address security incidents)	▪ Use **Trend Micro Threat Management Services** to detect and remediate active malware infections as well as implement a security strategy and training plan that continually improves security posture. ▪ Notify users of unauthorized use of ePHI while they are attempting the action using **Trend Micro DLP**. Display a popup window with the appropriate ePHI protection guidance.
§ 164.308 (a)(5)(ii)(B) (Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software)	▪ Monitor and block malicious software from infiltrating end user systems, critical servers, and block malicious email and Web exposure with **Trend Micro Endpoint, Messaging, and Web Security solutions**
§ 164.308(b)(1) (Business associate will appropriately safeguard information)	▪ **Trend Micro Enterprise Security solutions** can be implemented by business associates to secure their operations and protect ePHI. Minimally, **Trend Micro Email Encryption** can provide secure communications between covered entities and their business associates.
§ 164**.310(d)(1) Device and Media Controls** (Policies and procedures that govern the receipt , removal and movement of hardware and electronic media containing ePHI)	▪ Maintain a current inventory of ePHI on the network with discovery scanning using **Trend Micro DLP**. IT change management can include review of discovery reports in order to properly handle systems storing ePHI.

§ 164.312(a)(1) Access Control (Allow access only to those persons or software programs that have been granted access rights)	▪ Control access to servers or applications using **Trend Micro Deep Security**, which enables communications to be restricted or allowed based on MAC and IP addresses. ▪ Role-based access controls (RBAC) and delegated administration using **Trend Micro Deep Security** to support separation of administrative duties with respect to creating, deploying, and auditing security policy and events that violate the policies. ▪ Perform regular discovery of ePHI systems with **Trend Micro DLP** to determine where access controls must be in place.

Healthcare Regulation	Trend Micro Solutions and Mapping Justification
§ 164.312(c)(1) Integrity (Protect ePHI from improper alteration or destruction)	▪ Monitor the integrity of files containing ePHI data with **Trend Micro Deep Security**, alerting any modification or deletion.
§ 164.312(e)(1) Transmission Security (Guard against unauthorized access to transmitted ePHI)	▪ Secure emails between employees and external recipients with **Trend Micro Email Encryption.**
§ 164.514(d) (Collect and use the minimum data necessary)	▪ Discover duplicated and unsecured ePHI on laptops, desktops, file servers and databases on a regular basis with **Trend Micro DLP**.
NIST Guidelines— Examples of NIST guidelines intended to help federal government institutions secure ePHI.	
NIST Publication 800-66 (For implementing HIPAA Security Rules) "Use a combination of security software, such as antivirus…, personal firewalls, spam and Web content filtering,… to stop most attacks, particularly malware;"	▪ **Trend Micro OfficeScan, Deep Security, InterScan Message Security, and InterScan Web Security** directly address these requirements. ▪ **Trend Micro Threat Management Services** provides antivirus detection for devices and systems that cannot directly host antivirus security software, e.g., MRI scanners, bedside monitors, and legacy devices and systems.
NIST Publication 800-66: 4.13. Device and Media Controls (§ 164.310(d)(1)) (What data is maintained by the organization and where?...)	▪ Maintain a current inventory of ePHI on the network with discovery scanning using **Trend Micro DLP**. IT change management can include review of discovery reports in order to properly handle systems storing ePHI.
NIST Publication 800-66: 4.14. Access Control §164.312(a)(1)) (Have all applications/systems with ePHI been identified?, Where is ePHI …currently housed?)	▪ Perform regular discovery of ePHI data on enterprise systems with **Trend Micro DLP** to determine where access controls must be in place.
Payment Card Industry Data Security Standard (PCI DSS)—Compliance Requirements	
Twelve categories of controls to protect cardholder data	▪ **Trend Micro Enterprise Security Solutions** address most PCI requirements. Please see white paper, "Trend Micro Solutions for PCI DSS Compliance"

For more information please call or visit us at.

www.trendmicro.com/go/enterprise

+1-877-21-TREND

VI. FOOTNOTES

[i] HIPAA security requirements detailed in “Title 45 – Public Welfare Subtitle A – Department of Health and Human Services Part 164 – Security and Privacy”, http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html

[ii] Department of Health and Human Services, “Health Insurance Reform: Security Standards; Final Rule.” *Federal Register*, vol. 68, no. 34 (Feb. 20, 2003), pg. 8341. (http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf)

[iii] “Department of Health and Human Services | 45 CFR parts 160 and 164 | Breach Notification for Unsecured Protected Health Information; Interim Final Rule”, August 24, 2009 http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

[iv] “Department of Health and Human Services | 45 CFR parts 160 and 164 | Breach Notification for Unsecured Protected Health Information; Interim Final Rule”, http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

[v] NIST Special Publication 800–111, “Guide to Storage Encryption Technologies for End User Devices”, November 2007, http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

[vi] Refer to Section 5 for more details on healthcare regulations/requirements mappings

[vii] “Department of Health and Human Services | 45 CFR parts 160 and 164 | Breach Notification for Unsecured Protected Health Information; Interim Final Rule”, page 6, http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

[viii] For more information, refer to the white paper, “Trend Micro Solutions for PCI DSS Compliance – Addressing PCI DSS Requirements with Trend Micro Enterprise Security.”