

**NCHICA Annual Conference**  
**September 23, 2009**

---

# HITECH Compliance:

Strategies for Addressing the New Legal and Technical  
Challenges for Mobile Information Security

Steven Kahn  
Enterprise Technology Specialist

Clyde Hewitt  
Managing Consultant, Security  
Advisory Practice



# Agenda

- HIPAA and HITECH Comparison
- HHS and FTC Breach Notification Regulations
- Vendor Management
- Breach Response
- Safe Harbor
- Summary

# HIPAA and HITECH Comparison

	HIPAA before 2009	HITECH in 2009+
Applicability	Covered Entities	Added Business Associates
BA non-compliance	No responsibility if BAA in place	No responsibility if due diligence documented
Enforcement	HHS only – ‘toothless’	OCR States’ Attorneys General
Whistleblowers	Yes, but case backlog	Yes, can share in fines
Fines	Optional	Mandatory
Personal responsibility	None	Yes, up to \$1.5M

# HHS and FTC Breach Notification Regulations

- Genealogy
- Applicability and requirements
- Vendor management
- Breach response facts

# HITECH Breach Notification Genealogy

- ARRA/HITECH signed Feb 17, 2009
- HHS Draft Guidance published April 17, 2009
- NCHICA Comments provided May 21, 2009
- FTC Final Regulation published Aug 17, 2009
- HHS Final Regulation published Aug 24, 2009
- Compliance date – per HITECH Sep 23, 2009

**TODAY!!!**

# Applicability and Requirements

- HHS Regulations (45 CFR § 164) applicable to the breach notification requirements apply to all covered entities
  - Covered entities must notify their business associates and promulgate the new rules through a *Business Associate Agreement*
  - NCHICA's Legal and Pri/Sec task force is working on a new *Business Associate Agreement* template
- FTC Regulations (16 CFR § 318) apply to all organizations that have personal health information except covered entities and business associates

# Vendor Management

- Changing paradigm
- Regulatory requirements now make covered entities responsible for the actions of their Business Associates
  - Exception is if due diligence has been performed (but how?)
- Understanding the risk implications
- Requirements for a vendor management program

# Opportunities for Shared Vendor Management

- Consider the following:
  - Most business associates support many different covered entities
  - Most covered entities don't have the resource or ability to monitor multiple business associates
- What if there were a model of 'shared assessments' so that any one covered entity could get the results of a prior assessment, but it would require:
  - A common risk model
  - Common questions
  - Ability to validate evidence
  - Risk reports available, but not the actual client data
  - Ability to compare results across an industry

# Breach Response Facts

	HHS	FTC
Applicability	Covered Entities	Vendors (non-covered entities)
Subrogation	Yes - business associates must report through covered entities	Yes - ‘...or third party service providers...’ must report back to the vendors
Notification	<ul style="list-style-type: none"> <li>• Individuals</li> <li>• Media (&gt;500)</li> <li>• Secretary of HHS</li> </ul>	<ul style="list-style-type: none"> <li>• Individuals</li> <li>• Notify the media</li> <li>• Notify the FTC</li> </ul>
Timeline	60 days	60 days
Limited Data Set	No	Yes
Safe harbor	Strong encryption*	Strong encryption*
Requirement	45 CFR §164	16 CFR §318

# Safe Harbor Definition

45 CFR § 164.402

- “Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site.”

# Summary

- Any breach of identifiable health information, regardless if your organization is a covered entity or not, must trigger a response
- Any breach caused by any supporting organization (business associates or 'other third parties) must trigger a response
  - All organizations who use third supporting organizations have an obligation to perform due diligence

**NCHICA Annual Conference**  
**September 23, 2009**

---

# Mobile Data Security

## Technical Deep Dive

Steven Kahn  
Enterprise Technology Specialist  
South Central District Government, Education & Medical Region  
Intel® Americas - Enterprise Solution Sales



# Key Data Points

- NIST Compliance
- Implementation – Central and Distributed
  - Requirements
  - Use Cases
  - Operational Impact
- Notebook Hard Disk and Flash Drive Protection
- Secure Mobile Devices not just Notebooks
- Challenges

# What is the reality

- A Major Vendor of mobile encryption technology, recently surveyed 426 IT professionals worldwide.
  - >Eight-eight percent said they know large amounts of sensitive data are sitting on their employees' mobile devices. Seventy-two percent said the best way to protect that data is through encryption. But only 20% said they have actually deployed encryption on those devices!!<
- News broke recently about one of the largest known security breaches at a US University.
  - A database break-in at the University of California, Los Angeles has reportedly exposed the private information of about 800,000 people.

# Key Data Points

- **NIST Compliance**
- Implementation – Central and Distributed
  - Requirements
  - Use Cases
  - Operational Impact
- Notebook Hard Disk and Flash Drive Protection
- Secure Mobile Devices not just Notebooks
- Summary

# NIST Data Security Compliance

- Data in Use
- Data in Motion

# Data Defined Within

- “Data in motion” includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange, while “data at rest” includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method.
- “Data in use” includes data in the process of being created, retrieved, updated, or deleted, and “data disposed” includes discarded paper records or recycled electronic media

# Encryption Policy

- Government Policy = Encryption is one method of rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized persons
- To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt

# NIST Definitions

- Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52,
- Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated

# Key Data Points

- NIST Compliance
- **Implementation – Central and Distributed**
  - Requirements
  - Use Cases
  - Operational Impact
- Notebook Hard Disk and Flash Drive Protection
- Secure Mobile Devices not just Notebooks
- Summary

# Summing up the Process

- **Identify Needs.** The first phase involves identifying the needs to encrypt storage on end user devices, determining which devices and data need protection, and identifying related requirements (e.g., minimum performance).
- **Design the Solution.** The second phase involves all facets of designing the solution. Examples include architectural considerations, authentication methods, cryptography policy, and supporting security controls.
- **Implement and Test a Prototype.** The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment. The primary goals of the testing are to evaluate the functionality, performance, scalability, and security of the solution, and to identify any issues with the components, such as interoperability issues.
- **Deploy the Solution.** Once the testing is completed and all issues are resolved, the next phase includes the gradual deployment of the storage encryption technology throughout the enterprise.
- **Manage the Solution.** After the solution has been deployed, it is managed throughout its lifecycle. Management includes maintenance of the storage encryption components and support for operational issues. The lifecycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

# Operational Considerations

- Centralized management
  - Update and Patch management
    - Service releases
    - Encryption software controls
  - Authenticator management
  - Key management
  - Data recovery
  - Automation of the deployment and configuration of storage encryption software to end user devices
  - Deployment and user audit logs

# Policy Requirements

- Corporate Policy
  - End-User Awareness of policies around encryption
  - Policy around securing and encrypting end-user devices

# Single and Dual Factor Authentication

- Biometrics, Tokens and SmartCards
- PKI- Certificate Authentication
- Passwords
  - LDAP and Active Directory
  - Password transmissions
    - Don't use email passwords
    - Plain-text passwords

# Key Management

- Planning
  - User databases
  - Recovery
  - Storage
  - Destruction
- Device Control

# Device Management

- Flash Drives and Memory Cards
- Storage Encryption leveraging existing resources
  - Operating System components
  - File System Support

# Distributed Deployment

- Workers are mobile
- Devices are controlled by mobile workers
  - Hardware-based FDE can usually only be managed locally

# Key Data Points

- NIST Compliance
- Implementation – Central and Distributed
  - Requirements
  - Use Cases
  - Operational Impact
- **Notebook Hard Disk and Flash Drive Protection**
- Secure Mobile Devices not just Notebooks
- Summary

# Mobile Data Encryption

- Is file and disk encryption complicated?
- Why even bother if I can use Computrace?
- My Hard-Drive and USB Key have passwords! Is that Good Enough?

# File and Full Disk Encryption

- Files and Folders- Good
- Virtual Disk Encryption - Better
- FDE- Pre- Operating System- Best

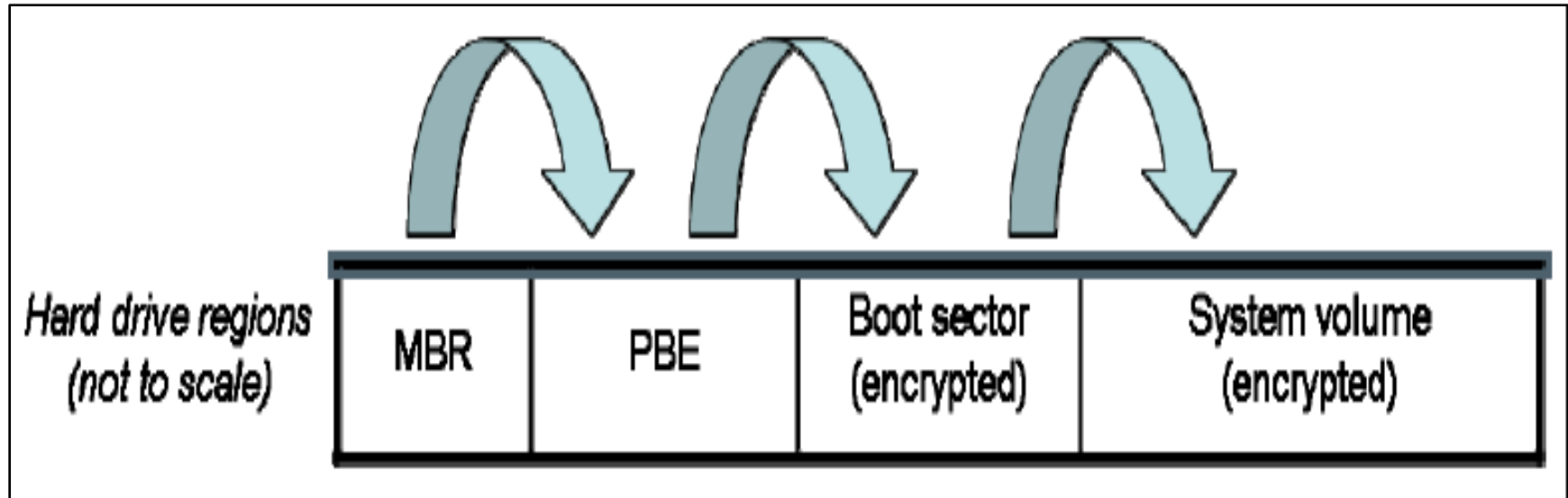
# File Based

- **File/Folder** level encryption is selective by allowing specific files to be encrypted or a container (folder or directory) to be created so that files saved there are encrypted
- File/folder encryption does not provide any protection for data outside the protected files or folders, including swap and hibernation files

# FDE and WDE

- **Full-Drive Encryption** encrypts all sectors on a disk or disk volume. This solution often encrypts operating system files, applications, system settings, and cache files, as well as, sensitive data.
  - FDE is software based encryption and policy enforcement
  - WDE- Is based in the firmware of the disk drive
    - Hardware-based FDE typically does not alter the MBR, so hardware-based FDE does not cause conflicts with software that modifies the MBR
- FDE/WDE solution leaves less doubt about all instances of sensitive data actually is encrypted.
  - Operating systems and applications write data in caches, temp directories, page files, etc. that are difficult to identify, let alone selectively encrypt<

# FDE Start Sequence



# Virtual Disk Encryption

- *Virtual disk encryption* is the process of encrypting a file called a *container*
  - Files can then be added to the container by the user as needed
  - VDE can be portable
  - containers are protected until the user is authenticated for that container
- VDE does not provide any protection for data outside the container, including swap and hibernation files that could contain the contents of unencrypted files that were being held in memory!!

# Volume Encryption

- *Volume encryption* is the process of encrypting an entire logical volume and permitting access to the data on the volume only after **proper** authentication is provided.
  - Usually this is hard drives and volume based USB drives

# What Have We Missed?

- CD/DVD Burning of Encrypted files
- File/Tape Backups
  - Encrypt the data prior and after decryption
- File Transfer and or Copy Security
  - This the most often overlooked breach
  - Files can be blocked

*Storage encryption solutions require users to authenticate successfully before accessing the information that has been encrypted*

# Key Data Points

- NIST Compliance
- Implementation – Central and Distributed
  - Requirements
  - Use Cases
  - Operational Impact
- Notebook Hard Disk and Flash Drive Protection
- **Secure Mobile Devices not just Notebooks**
- Summary

# Mobile Device Protection

- PDA
- Smartphones
- Symbian Mobile
- iPhones
- Blackberry – other Palm OS Devices

# Key Data Points

- NIST Compliance
- Implementation – Central and Distributed
  - Requirements
  - Use Cases
  - Operational Impact
- Notebook Hard Disk and Flash Drive Protection
- **Secure Mobile Devices not just Notebooks**
- Summary

# Mobile Device Protection

- Smartphone –Windows Mobile file system encryption and device locking
- Symbian- Device Encryption
- Palm OS- PIN Encryption and device locking schemes
- iPhone- Apple security policy and device locking schemes

# Notebook Safety

- Physical Theft
- Data Theft
- The Flash Drives are a key point of vulnerability-  
Secure it!!

# Key Data Points

- NIST Compliance
- Implementation – Central and Distributed
  - Requirements
  - Use Cases
  - Operational Impact
- Notebook Hard Disk and Flash Drive Protection
- Secure Mobile Devices not just Notebooks
- **Summary**

# Current State of Business

- More than 70% of surveyed have some data protection or encryption policy in place
- At least one data breach has occurred at 85% of the surveyed organizations, 22% of these had five or more!!
- 25% of the organizations use a platform approach for data encryption

# Summary & Takeaways

- Recommended Storage Encryption Applications
- Recommended Mobile Device Protection
- HHS and FIPS Supported Policy Choices

# Backup



# HITECH Compliance

- FIPS 140 -2,FIPS 199
- Common Criteria Evaluation Assurance(CC)
- GLB
- HIPAA
- FISMA
- HHS
- EAL4(Level4),EAL2

# Compliance with Encryption



# HIPAA Compliance of HHS

- The term “unsecured protected health information” includes PHI in any form that is not secured through the use of a technology or methodology specified in this guidance by the Secretary. This guidance, however, addresses methods for rendering PHI in paper or electronic form unusable, unreadable, or indecipherable to unauthorized individuals.

# PHR and PHI Breach Guidelines

- Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information
- This guidance is intended to describe the technologies and methodologies that can be used to render PHI unusable, unreadable, or indecipherable to unauthorized individuals

# Encryption Matrix

Characteristic	Full Disk Encryption	Volume Encryption	Virtual Disk Encryption	File/Folder Encryption
Typical platforms supported	Desktop and laptop computers	Desktop and laptop computers, volume-based removable media (e.g., USB flash drives)	All types of end user devices	All types of end user devices
Data protected by encryption	All data on the media (data files, system files, residual data, and metadata)	All data in the volume (data files, system files, residual data, and metadata)	All data in the container (data files, residual data and metadata, but not system files)	Individual files/folders (data files only)
Mitigates threats involving loss or theft of devices?	Yes	Yes	Yes	Yes
Mitigates OS and application layer threats (such as malware and insider threats)?	No	If the data volume is being protected, it sometimes mitigates such threats.* If the data volume is not being protected, then there is no mitigation of these threats.	It sometimes mitigates such threats*	It sometimes mitigates such threats*
Potential impact to devices in case of solution failure	Loss of all data and device functionality	Loss of all data in volume; can cause loss of device functionality, depending on which volume is being protected	Loss of all data in container	Loss of all protected files/folders
Portability of encrypted information	Not portable	Not portable	Portable	Often portable

\* These storage encryption technologies can only protect the files against some OS and application layer threats if the user has not been authenticated in this session to access the files. If a single sign-on solution is used, then generally the user is authenticated to the storage encryption technology during OS login, so the files are not protected against these threats once OS login occurs. If a separate authentication solution is used, the files are protected until that separate authentication is performed.



# TPM+KEYS

- As a security system, this approach has some wonderful characteristics. If you lose the laptop, no one can use your disk (assuming they don't know your passphrase).

If you take the disk out of the laptop and throw it away, there's no chance someone will get to the data on it because they need the keys that are stored in the hardware. The cryptography gives you the equivalent of a shredder for your old disk

# Resources

- Introduction to Cryptography - Jon Callas
- ZDNET Article:  
<http://www.zdnet.com.au/insight/security/print.htm?TYPE=story&AT=339272771-139023764t-110000105c>
- Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 / Rules and Regulations, Department of Health and Human Services
- 2009 Annual Study of US Enterprise Encryption Trends by the Ponemon Institute, Ponemon Institute
- HHS Breach Notification for Unsecured Protected Health Information - 45 CFR Parts 160 and 164
- NIST Guide to Storage Encryption of End User Devices, NIST Document Archive Publication 800-111