



The Impact of HITECH Act on HIPAA Compliance and Data Security



VORMETRIC

Marc J. Zwillinger
Rebecca C. Fayed

Your Speakers



[Marc J. Zwillinger](#)

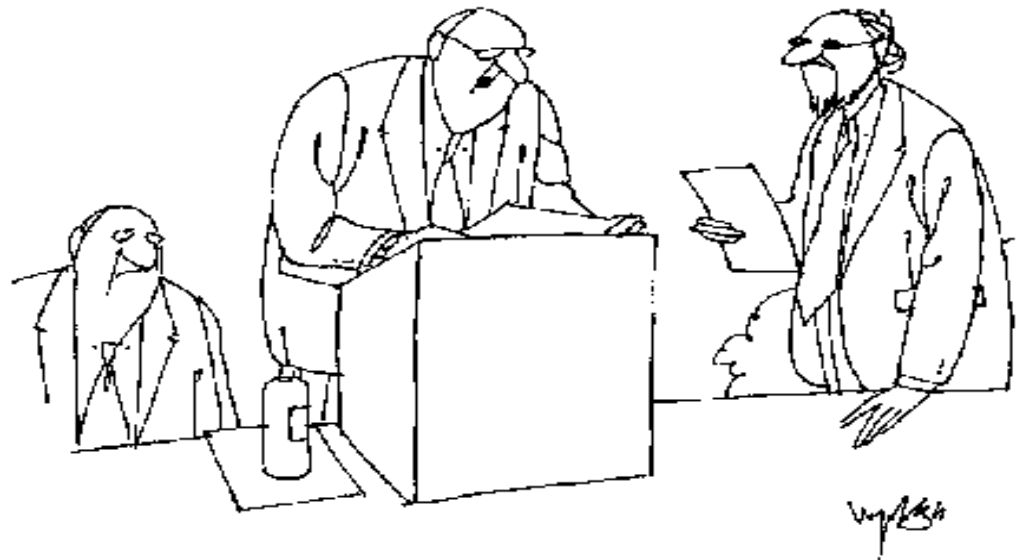
Chair of Sonnenschein's Internet, Communications and Data Protection Group (“ICDP”)



[Rebecca C. Fayed](#)

Leading expert on HIPAA privacy and security issues

HEALTH CARE
• PRIVACY AND SECURITY •
SEMINAR



"Our next speaker's remarks are encrypted. Those of you with handhelds may log on if you have the password."

AGENDA

- HITECH Act's Breach Notification Requirements
- HHS and FTC Breach Notification Rules
- Avoiding the HITECH Act's Breach Notification Requirement - Securing PHI
- HITECH Act's Changes to the HIPAA Privacy and Security Rules
 - Expanded Applicability to Business Associates
 - Limitations on the Use and Disclosure of PHI
 - Additional Individual Rights
 - Increased Penalties and Enforcement



HITECH Act Breach Notification Requirements & HHS and FTC Breach Notification Rules



www.vormetric.com

Sonnenschein.
SONNENSCHN NATH & ROSENTHAL LLP

Breach Notification Provisions in the HITECH Act

- Before the amended CA breach statute took effect on 01/01/09, only Arkansas included medical information in the definition of “personal information” triggering breach notification obligations.
- Breaches of medical information that did not involve financial information often went unreported.
- California amended statute to include both “medical information” and “health insurance information” in 2008.
- HITECH Act imposes breach notification requirements on all HIPAA-covered entities, business associates, PHR vendors and PHR related entities.
- HIPAA Covered Entities and Business Associates: HHS issued interim final rule on August 24, 2009, effective September 23, 2009. (Although HHS will use its “enforcement discretion” and not impose sanctions for 180 days.) Comments due on or before October 23.
- PHR Vendors and PHR Related Entities: FTC issued final rule on August 25, 2009, effective September 25, 2009. (Although FTC will use its “enforcement discretion” and full compliance not required until February 22, 2010.)

HHS Breach Notification Rule

Breach of Unsecured PHI

- Breach: Acquisition, access, use, or disclosure of PHI (either electronic or hard copy) not permitted by the Privacy Rule which compromises the security or privacy of PHI (i.e., it poses a significant risk of financial, reputational, or other harm to the individual).
- Applies to both hard copy and electronic PHI.
- 3 Steps to determine if it's a breach:
 1. Impermissible use or disclosure of PHI under Privacy Rule?
 2. Compromises the privacy or security of PHI by creating significant risk of harm?
 3. Is the incident excluded from the definition of a breach?
 - **An unintentional use of PHI by a workforce member acting in good faith and within the scope of his or her authority, and the PHI is not further used or disclosed improperly;**
 - **An inadvertent disclosure of PHI by an authorized person to another authorized person, and the PHI is not further used or disclosed improperly; or**
 - **A disclosure of PHI to an unauthorized person where there is a good faith belief that the unauthorized person would not reasonably have been able to retain the PHI.**

HHS Breach Notification Rule

Breach of Unsecured PHI

- Congress strongly disagrees with HHS significant harm standard for breaches.
- October 1, 2009 – House Committee on Energy and Commerce sent letter to HHS expressing “deep concern” about the “high bar” HHS set with its significant harm standard.
 - HITECH Act does not imply a harm standard.
 - Congress specifically rejected harm standard.
 - Mandatory notification meant to be incentive for health care entities to protect data through encryption or destruction.
 - Urged HHS to revise or repeal the harm provision at the soonest appropriate opportunity.

FTC Breach Notification Rule

Breach of Unsecured PHR

- Breach: Acquisition of unsecured PHR identifiable health information without the authorization of the individual.
 - Unlike HHS Breach Notification Rule, does NOT include a harm standard.
 - Acquisition: FTC provides important guidance on what constitutes unauthorized acquisition -- “Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information.”
 - Access to information creates presumption of unauthorized “acquisition” but can be rebutted by proof that it could not have reasonably been acquired.
- Personal Health Record: An electronic record of identifiable health information about an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

HHS & FTC Breach Notification Rules

Notice of Breach

- Notice must be provided to the individual “without unreasonable delay” and no later than 60 days after breach is discovered.
- Via first-class mail unless the individual has specified a preference for email.
- If the contact information for ten or more individuals is found to be outdated or insufficient, the entity must provide substitute notice in one of the following forms:
 - Conspicuous posting on the home page of its website for a period of 90 days; or
 - In major print or broadcast media, including in the areas where the affected individuals likely reside. Such notice must include toll-free phone number where individuals can call and learn whether they are affected by the breach. The phone number must remain active for at least 90 days.

HHS & FTC Breach Notification Rules

Notice of Breach

- Media notice – If PHI or PHR of more than 500 individuals in one state is breached, the entity must notify “prominent media outlets” in the state.
- HHS notice – Covered entities must notify HHS of the breach:
 - More than 500 affected individuals – must notify HHS contemporaneously with notification to the individual.
 - Less than 500 affected individuals – must notify HHS via an annual log of events no later than 60 days following the end of the calendar year.
- FTC Notice – PHR vendors and PHR related entities must notify FTC of the breach:
 - More than 500 individuals – must notify FTC within 10 business days after discovery of the breach.
 - Less than 500 affected individuals – must notify FTC via an annual log of events no later than 60 days following the end of the calendar year.
- HIPAA Business associates must notify the covered entity of the breach.
- Third party service providers must notify the PHR vendor or PHR related entity.

HHS & FTC Breach Notification Rules

Content of Notice:

- Description of facts about breach.
- Type of PHI involved.
- Steps individuals should take to protect themselves.
- What the covered entity is doing to investigate the situation and prevent future breaches.
- Contact information for individuals to ask questions.

Practical Guidance – What do I do now?

- Identify systems that have covered data.
- Secure your PHI – Encrypt or Destroy. (See next section)
- Evaluate existing privacy and security policies and procedures and assess whether current administrative, technical and physical safeguards are sufficient to protect the privacy and security of PHI.
- Adopt Incident Response plan with breach notification policy.
- Establish procedures and incident response team to respond to breach.
- Assign internal roles and responsibilities, and identify external vendors.
- Consider incident response insurance policies.

What about HIPAA? What Role Does it Play in Security Breaches?

- The HIPAA Privacy Rule requires covered entities to:
 - Mitigate – Must mitigate any harmful effects of unauthorized disclosure (police reports, notification).
 - Sanction – Must apply appropriate sanctions against employees who fail to comply with privacy and security policies and procedures.
 - Account for Disclosures – Unauthorized disclosures of PHI must be accounted for on accounting log.
- Other Compliance Efforts:
 - Training – Retrain employees.
 - Policies and Procedures – Evaluate effectiveness of and modify, if appropriate, policies, procedures and safeguards.
- In the event of a breach, likely that covered entities will receive a request from HHS-OCR asking for a description of the incident and details regarding the safeguards that were in place or have been put in place since the breach to protect the privacy and security of PHI.

Avoiding the HITECH Act's Breach Notification Requirement: Securing PHI



www.vormetric.com

Sonnenschein.
SONNENSCHN NATH & ROSENTHAL LLP

Avoiding Breach Notification: Securing Your PHI

- HITECH Act breach notification requirement applies only to the breach of unsecured PHI.
- HITECH Act required HHS to issue guidance specifying technologies and methodologies that would render PHI “unusable, unreadable, or indecipherable” to unauthorized individuals.
- If PHI is rendered “unusable, unreadable, or indecipherable” to unauthorized individuals, it is secure.
- The breach of secure PHI is not subject to the breach notification requirement.
- Avoid having to comply with the breach notification requirement by **SECURING** your PHI.

Avoiding Breach Notification: How to Secure PHI

- HHS issued guidance on April 17, 2009 setting forth an exhaustive list of what technologies and methodologies will render PHI secure.
- HHS provided additional guidance on August 24, 2009.
- Technologies and Methodologies that will render PHI secure:
 1. Encryption.
 2. Destruction.
- **Nothing else will render your PHI secure.**
- In most recent guidance, HHS:
 - Rejected access controls, such as firewalls, as a method for securing PHI.
 - Rejected redaction as a means of securing PHI, and clarified that only the destruction of paper PHI will render that PHI secure. (HHS did state, however, that if PHI is properly redacted so as to be fully deidentified, the breach of the deidentified information will not trigger the breach notification requirements under the Breach Notification Rule.)

Avoiding Breach Notification: Encryption

- EPHI must be encrypted in accordance with the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning a meaning without use of a confidential process or key and such confidential process or key that might enable encryption has not been breached.”
- Most recent HHS guidance clarified that encryption keys must be kept on a separate device from the data that they encrypt or decrypt.

Avoiding Breach Notification: Most Recent HHS Guidance

- Clarified the following:
 - Data in motion includes data moving through a network, including wireless transmission;
 - Data at rest includes data residing in a database, file system, flash drive, memory or any other storage device;
 - 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.

Avoiding Breach Notification: Encryption Safe Harbors

- The following processes have been judged to meet the encryption standard set forth in the HHS guidance:
 - Valid processes for encryption of stored PHI include those consistent with NIST Special Publication (“SP”) 800-111, *Guide to Storage Encryption Technologies for End User Devices*, including (but not limited to) full disk encryption, volume encryption, virtual disk encryption, and file/folder encryption.
 - Valid processes for encrypting PHI during transmission would be those complying with the requirements in Federal Information Processing Standard (“FIPS”) 140-2, including NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*, 800-77, *Guide to IPsec VPNs*, or 800-113, *Guide to SSL VPNs*.
 - For example, validated processes for symmetric key encryption include the Advanced Encryption Standard (“AES”), Triple-DES, and Skipjack algorithms.

Practically Speaking

- Compliance with NIST/FIPS Standard is not a simple checklist.
 - Each standard specifies means of compliance that may differ in particular situations.
 - Example: full disk encryption may be a valid way to secure data against third parties, but not against unauthorized insiders who share a laptop or computer with authorized users.
 - File/Folder encryption may be better way of 'securing' data in that scenario.

Avoiding Breach Notification: Destruction

- To comply with the destruction guidance, the media on which the PHI is stored or recorded must be destroyed in the following ways:
 - Hard copy media (such as paper and film) must be shredded or destroyed in such a way that PHI cannot be read or otherwise reconstructed.
 - Electronic media must be cleared, purged, or destroyed so that the PHI cannot be retrieved, consistent with the NIST SP800-88, *Guidelines for Media Sanitization*.

What to do now?

- Work with your Chief Information Officer or IT/IS Managers to determine whether you currently encrypt or have the capabilities to encrypt PHI.
 - The cost of encryption likely is less expensive than addressing a security breach.
- Review your medical record retention and destruction policies to confirm that data is being destroyed properly.
 - To reduce risk, do not retain medical records longer than necessary.

Changes to the HIPAA Privacy and Security Rules:

Applicability to Business Associates



www.vormetric.com

Sonnenschein.
SONNENSCHN NATH & ROSENTHAL LLP

HIPAA Applies to Business Associates?

- Prior to the HITECH Act
 - Not directly subject to HIPAA.
 - Reasonable Assurances in the form of a BA Agreement.
 - Liability limited to breach of contract.
- HITECH Act expanded the reach of the HIPAA Privacy and Security Rules.
- Effective February 16, 2010.

HIPAA Applies to Business Associates?

- HIPAA Security Rule
 - BAs must comply with the HIPAA Security Rule.
 - Conduct a security risk assessment.
 - Implement administrative, physical and technical safeguards.
 - Have policies and procedures in place to protect the security of PHI.

HIPAA Applies to Business Associates?

- HIPAA Privacy Rule
 - BAs still are NOT required to comply with the HIPAA Privacy Rule.
 - BAs must continue to provide reasonable assurances in the form of a BA agreement.
 - If a BA violates any provision of the BA Agreement, will be subject to the same civil and criminal penalties for HIPAA violations as covered entities.

Practical Effect

- Business associates will need to be revised to incorporate the new HITECH Act requirements.
 - Breach Notification Obligations
 - Compliance with Security Rule
 - New Penalties for Breaches
 - Changes to Individual Rights

Changes to the HIPAA Privacy and Security Rules: Additional Limitations on the Use and Disclosure of PHI



"Normally, I'd discuss your condition with these first-year residents, but because of confidentiality restrictions, all I can really tell them is that you're a shoo-in for an invasive procedure."

Additional Limitations: Marketing

- Privacy Rule: The following communications are not marketing:
 1. Description of a health-related product or service (or payment for such product or service) provided by, or included in a plan of benefits of, the covered entity making the communication;
 2. Treatment related communications; or
 3. For case management, care coordination or to recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

Additional Limitations: Marketing

- HITECH Act placed limitations on the marketing exception.
- If payment received for making the communications, the communication is marketing, unless the communication:
 1. Describes a drug currently prescribed and payment is reasonable;
 2. Is made by the covered entity pursuant to an authorization; or
 3. Is made by a business associate in compliance with its BA agreement.

Additional Limitations: Minimum Necessary

- Privacy Rule requires covered entities to disclose only the minimum amount of PHI reasonably necessary to accomplish the purpose of the permitted use or disclosure of PHI.
- Criticized as one of the most vague and difficult-to-implement components of the Privacy Rule.
- HITECH Act requires HHS to issue guidance on the minimum necessary standard by August 17, 2010 – Guidance has not been issued.
- Until HHS guidance issued: Use or disclose a limited data set, *to the extent practicable*, or if necessary, to the minimum necessary to accomplish the intended purpose.
- Just as difficult to implement?

Additional Limitations: Health Care Operations

- House and Senate bills originally required HHS to review the definition of health care operations and eliminate activities that could be conducted with deidentified health information or should require an authorization.
- This provision caused the most angst in the health care industry.
- Provision was NOT included in the final HITECH Act.
- The HITECH Act does not require the Secretary to review and modify the definition of health care operations.

Individual Rights: Accounting for Disclosures

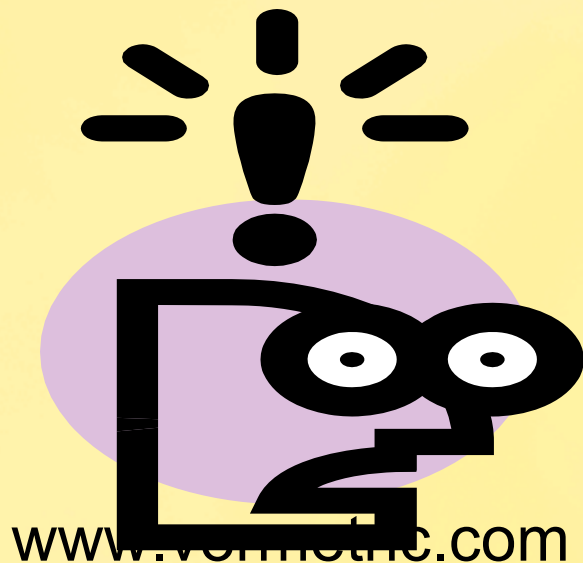
- Privacy Rule currently excepts from the accounting requirement those disclosures of PHI made for purposes of treatment, payment and health care operations.
- HITECH Act eliminates TPO disclosure exception for disclosures made of an EHR.
- 3 Year Reporting Period vs. 6 Year Reporting Period
- Compliance Date:
 - January 1, 2014 - Covered Entities who began using EHRs prior to January 1, 2009.
 - January 1, 2011 - Covered Entities who acquire an EHR after January 1, 2009 (or the date they acquire the EHR thereafter).

Individual Rights: Restrictions on Disclosures

- Privacy Rule currently provides individuals with a right to request a restriction on a covered entity's use or disclosure of PHI for purposes of treatment, payment or health care operations purposes.
- Covered entities have no corresponding obligation to agree to that request.
- HITECH Act imposes a new obligation on covered entities to agree to a requested restriction if the disclosure is to a health plan for purposes of payment or health care operations *and* the PHI relates to a health care item or service for which the health care provider has been paid out of pocket in full.

Changes to the HIPAA Privacy and Security Rules:

Increased Enforcement and Penalties



www.verimetric.com

Sonnenschein.
SONNENSCHN NATH & ROSENTHAL LLP



Increased Enforcement

- HHS-OCR enforces Privacy Rule and Security Rule.
- HITECH Act:
 - Requires HHS to formally investigate any complaint of a violation of HIPAA if a preliminary investigation indicates a possible violation due to willful neglect, and to impose civil penalties for these violations.
 - Allows state Attorneys General to bring civil actions in federal court on behalf of state residents if there is reason to believe that the interest of one or more residents has been threatened or adversely affected by a person who violates HIPAA.

Increased Penalties

- HITECH Act created tiered approach to civil monetary penalties for violations of HIPAA. INCREASED PENALTIES CURRENTLY IN EFFECT.
 - If the person did not know (and by exercising reasonable due diligence would not have known) that he or she violated the law:
 - Minimum: \$100 for each violation not to exceed \$25,000 for all such identical violations during a calendar year.
 - Maximum: \$50,000 for each violation not to exceed \$1.5 million for all such identical violations during a calendar year.
 - Violation due to reasonable cause and not willful neglect:
 - Minimum: \$1000 for each violation not to exceed \$100,000 for all such identical violations during a calendar year.
 - Maximum: \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement during a calendar year.

Increased Penalties

- HITECH Act created tiered approach to civil monetary penalties for violations of HIPAA. INCREASED PENALTIES CURRENTLY IN EFFECT.
 - Violation due to willful neglect AND the violation was corrected:
 - Minimum: \$10,000 for each violation not to exceed \$250,000 for all such identical violations during a calendar year.
 - Maximum: \$50,000 for each violation not to exceed \$1.5 million for all such identical violations during a calendar year.
 - Violation due to willful neglect and not corrected,
 - Minimum: \$50,000 for each violation not to exceed \$1.5 million for all such identical violations.
 - No maximum.



Vormetric Overview

Vormetric Overview

Enterprise Encryption Simplified

▼ Mature and Proven

- Expertise in both security and enterprise systems since 2001
- Over 500 enterprises successfully deployed

▼ Innovative Architecture

- Transparent to applications, databases, storage and users
- High performance, extendible, and rapidly deployable

▼ Strong and Growing

- Unparalleled partnerships
- Profitable, 77% revenue growth year over year

Strong Partner Validation



- THE solution for DB2 and Informix



- THE solution for NetBackup



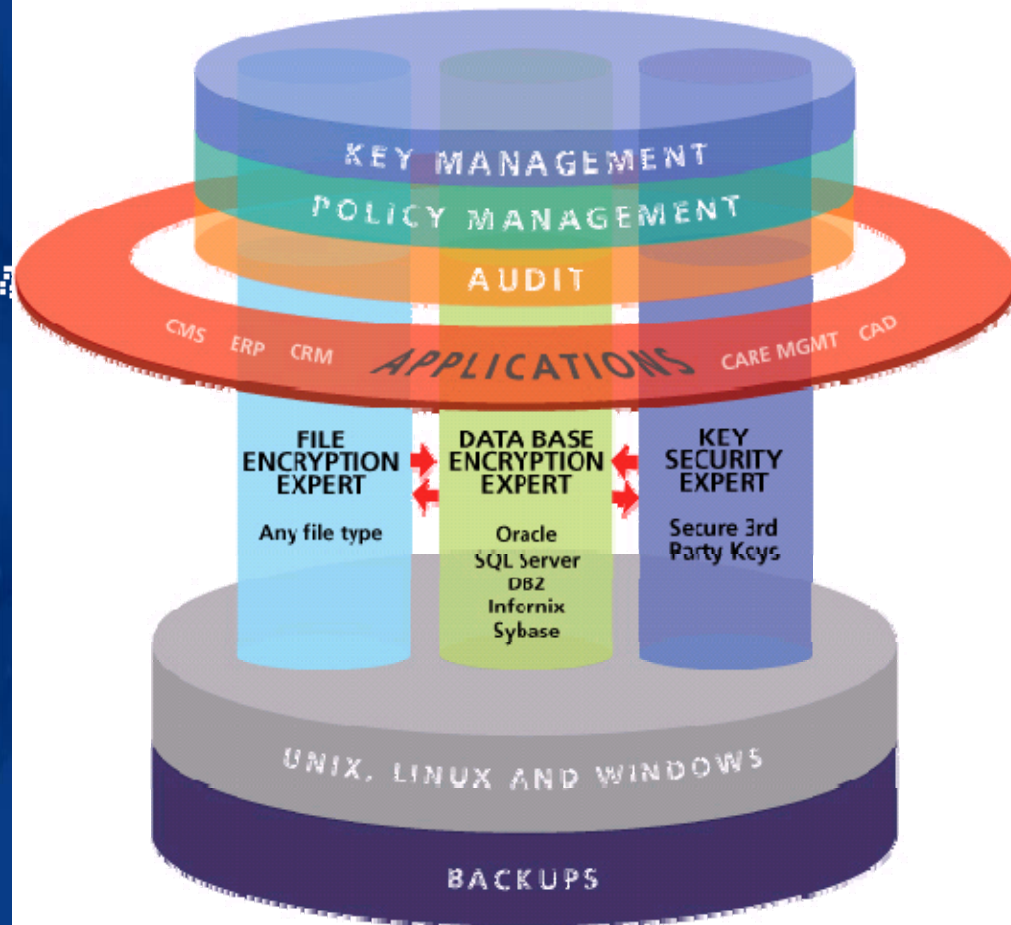
- THE solution for securing the execution environment for Oracle DataVault

Vormetric Customers



- ▼ Including 6 of the Fortune 10
- ▼ Top names in healthcare, outsourcing, insurance, government
- ▼ Used by the US Government
- ▼ IP protection, Compliance, Consumer information protection

Vormetric Data Security



Any File, Any Database, Any Application, Anywhere!

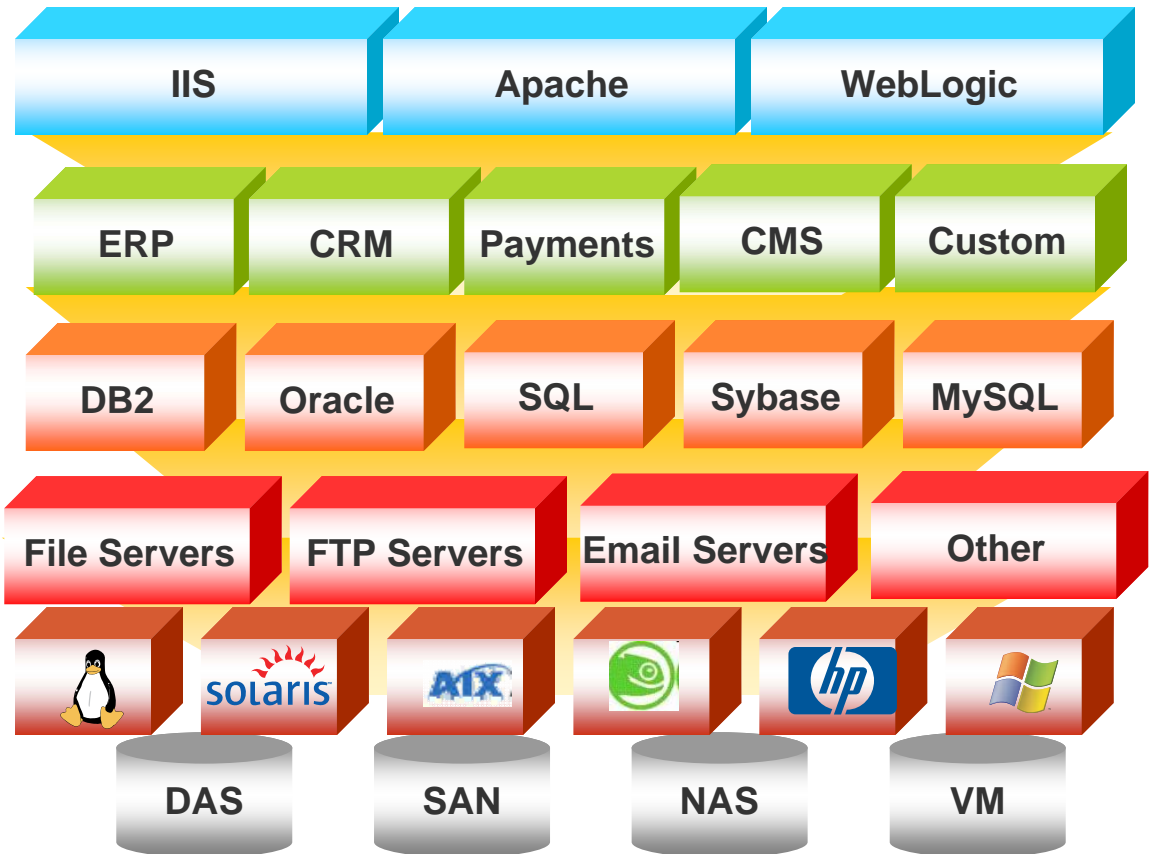
- ▼ Secure, centralized policy and key management
- ▼ High performance
- ▼ Heterogeneous
- ▼ Rapidly deployable
- ▼ Extensible

Vormetric's Extensible Solution

- Log Files
- Password files
- Configuration files
- Archive

- Data files
- Transaction logs
- Exports
- Backup










- File shares
- Archive
- Content repositories
- Multi-media



“ *Future scalability to apply this solution where additional needs may arise was a significant consideration* ”

Thomas Doughty, CISO, Prudential

Vormetric for HITECH Act Safe Harbor

FIPS Certified Encryption	
Secure Key Management	
Meets NIST 800-111	
Proven Performance	
Encryption + Access Control	
Audit	
Separation of Duties	
Low TCO	
Rapidly Deployable	

“Vormetric encrypts in a way to minimize performance overhead. It also offers separation of duties, centralized key management and policy management”

**Noel Yuhanna
Forrester
Research**

Learn More and Register for a Chance to Win!

WWW.VORMETRIC.COM/NOAPPAIN



DISCLAIMER

- These materials should not be considered as, or as a substitute for, legal advice and they are not intended to nor do they create an attorney-client relationship. Because the materials included here are general, they may not apply to your individual legal or factual circumstances. You should not take (or refrain from taking) any action based on the information you obtain from these materials without first obtaining professional counsel. The views expressed do not necessarily reflect those of the firm, its lawyers, or clients.

Questions?

Marc J. Zwillinger

mzwillinger@sonnenschein.com

202-408-9171

Rebecca C. Fayed

rcfayed@sonnenschein.com

202-408-6351

Vormetric

info@vormetric.com

888-267-3732

Suggest our next HITECH
Webcast!
ghellman@vormetric.com

Sonnenschein
SONNENSCHN NATH & ROSENTHAL LLP