HIPAA and HITECH Compliance Simplification

Sol Cates
CSO
@solcates
scates@vormetric.com
Quick Agenda

- Why comply?
- What does Compliance look like?
- New Cares vs Rental Cars vs Custom Cars
- Vormetric
- Q&A
HIPAA/HITECH Act Requirements

- Notify individuals of breach of unsecured health information
- Information is only secured if it is encrypted or destroyed
- Encryption must meet NIST 800-111 encryption requirements
- Keys must be kept on a separate device than the data
- Only FIPS approved encryption algorithms can be used
- Omnibus Rule - Expands HIPAA requirements to business partners of payers, providers and clearinghouses
Potential Consequences of Non-Compliance: Increased Enforcement and Penalties (fines)

- HITECH Act included provisions for increased enforcement of HIPAA Privacy and Security Rules:
  - 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.
# My Simple View of the World

<table>
<thead>
<tr>
<th>Category</th>
<th>Technology</th>
<th>Required or Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Controls</td>
<td>Unique User ID</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Emergency Access Procedures</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Automatic Log-off</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td>Encryption and Decryption</td>
<td>Addressable</td>
</tr>
<tr>
<td>Audit Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>Authenticate Electronic PHI</td>
<td>Required</td>
</tr>
<tr>
<td>Person or Entity Authentication</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>Transmission Security</td>
<td>Integrity Controls</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>Addressable</td>
</tr>
</tbody>
</table>
### Where is the Data?

#### Data Centers
- Physical
- Virtual
- Outsourced

#### Clouds
- Private, Public, Hybrid
- Multiple vendors

#### Big Data
- Sources
- Nodes
- Results

#### Physical Servers
- Local offices and retail locations
- Labs

---

Vormetric.com
Challenges in complying with HIPAA/HITECH

- The security requirements, taken independently of one another, can prove costly and time-consuming to implement adequately.
  - Typically, various solutions may have to be integrated to provide adequate protection for dispersed data and implementations can prove to be very complex.

- Protecting unstructured data.
  - While some types of data, such as credit card data or social security numbers, can be readily located and protected, unstructured data frequently found in EMRs can be more difficult to protect.

- The data may consist of a variety of file types.
  - Patient record forms, medical imagery files, and other file types that are not easily protected due to being highly distributed environments.

- Controlling access to ePHI
  - While encryption protects data, robust policy and encryption key management is required to prevent unauthorized access or disclosure of PHI.
Simplifying with Vormetric
Partnerships and Certifications
Assures high performance and confidence
Vormetric Data Security Platform
Solves inefficiencies of point product solutions

**Vormetric Transparent Encryption**
- Structured Databases
- Big Data
- Unstructured Files
  - File and Volume Level Encryption
  - Access Control
  - Audit Logs

**Vormetric Application Encryption and Tokenization with Dynamic Data Masking**
- Applications
- Big Data
- PaaS, IaaS, SaaS
  - Field Level Data Encryption
  - Field Preserving Tokenization with Dynamic Data Masking

**Vormetric Cloud Encryption Gateway**
- S3 and Box
- Encryption, Control, Audit Trails

**Vormetric Key Management**
- KMIP Compliant
- Oracle and SQL Server TDE
- Certificate Storage

**Vormetric Data Security Manager**
- Key and Policy Manager

**Vormetric Security Intelligence**
- Splunk
- HP ArcSight
- IBM QRadar
- LogRhythm
- Intel Security ESM
- FireEye TAP

**Environment Support**
- Public Cloud
- Hybrid
- Private Cloud
- Data Centers

Vormetric.com
**Data Security as a Service Offerings**

**Vormetric Cloud Partners**

<table>
<thead>
<tr>
<th>CenturyLink™</th>
<th>rackspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>QTS</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>firehost</td>
<td>at&amp;t</td>
</tr>
<tr>
<td>CloudHesive</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>D+H</td>
<td>BAE Systems</td>
</tr>
<tr>
<td>virtustream</td>
<td>IBM® SoftLayer</td>
</tr>
<tr>
<td>Google Cloud Platform</td>
<td>CIRRITY</td>
</tr>
</tbody>
</table>
Using Vormetric to Comply with HIPAA HITECH

- A comprehensive solution for protection of ePHI in any environment on any data.
  - Applications, file types, and even operating systems.
  - Structured and unstructured data, including big data and databases (DB2, Oracle, SQL, Informix etc.)
  - Private, Public and Hybrid Clouds

**Vormetric Data Encryption offers:**
- Strong data security controls, leveraging both encryption and policy-based access controls,
- separation of duties
- Auditing Capabilities
- Heterogeneous systems
- Managed via a centralized policy and key management console

**Whitepaper:**
Questions?

Sol Cates
CSO
@solcates
scates@vormetric.com