Novell Solutions For Healthcare

Enforcing Privacy and Security of HITECH
# Background

**HIPAA & HITECH Act**

## The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Administrative Simplification provisions established national standards for security and privacy of health data, along with other standards designed for efficiency and effectiveness of health care.
- Covered entities include: health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers.
- Privacy Rule – regulates use and disclosure of protected health information (PHI).
- Security Rule – establishes administrative, physical, and technical safeguards for electronic PHI (EPHI).
- Limited enforcement actions until recently:
  - 2008 Providence Health – $100K
  - 2009 CVS – $2.2M plus FTC Consent Order; 20 years of external audit

## Health Information Technology for Economic and Clinical Health Act (HITECH Act)

- Promotes electronic exchange and use of health information to improve quality and coordination of care.
- Invests $20 billion in health information technology infrastructure and incentives to encourage doctors and hospitals to use Health Information Technology (HIT).
- Strengthens existing HIPAA security and privacy rules, expands HIPAA to entities not previously covered, and addresses long-standing issues with the privacy rule to better protect PHI at rest, in use, and in motion.
HITECH Act Overview — background

The recent American Recovery and Reinvestment Act (ARRA) provides a significant step toward health care information technology modernization

Facts and figures

• Obama Administration initiative
• Appropriates $787B across a broad spectrum of government programs
• Many Health and Human Service (HHS)/labor funds are passed down to states through existing mechanisms
• Health IT funding includes incentives and appropriations from the HITECH Act and other health IT initiatives such as telehealth

HITECH priority areas include:

• Electronic Health Records (EHR)
• Health Information Exchanges (HIE)
• Security and Data Privacy
• Outcome Registries
• Promotion of Health Information Technology (HIT) Standards and Interoperability

ARRA includes the HITECH Act to accelerate the adoption of interoperable electronic health records and to promote HIE.

The legislation includes provisions intended to shore up public confidence in the use of EHRs and personal health records (PHRs) by beefing up enforcement of and expanding the scope of activities covered by HIPAA Privacy and Security Rules.
## HITECH Act’s Impact on Privacy and Security and Timelines

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
<th>Effective date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New HIPAA Business Associates</strong></td>
<td>• Requires that new entities that were not contemplated when HIPAA was written (Personal Health Record vendors, Regional Health Information Organizations, HIEs, etc.) are subject to the same privacy and security rules by requiring Business Associate contracts and treating these entities as Business Associates under HIPAA.</td>
<td>February 17, 2010</td>
</tr>
<tr>
<td><strong>Breach Notification</strong></td>
<td>• Establishes a federal security breach notification requirement for unsecured protected health information (unsecured PHI) and PHR.</td>
<td>September 15, 2009; February 2010</td>
</tr>
</tbody>
</table>
| **Disclosure Restrictions**  | • An individual is permitted to request a covered entity not send its PHI to a health plan for purposes of carrying out payment or health care operations for a service when paying for the service fully out of pocket.  
• Covered entities are required to limit the use, disclosure or request of PHI to the limited data set to the extent practicable, or the minimum necessary if needed by the entity. | February 17, 2010                                                            |
| **Accounting of Disclosures** | • Covered entities must produce, upon request, an accounting of disclosures of the individual’s PHI, including routine disclosures over a three-year period.  
• Business associates must produce, upon request, an accounting of disclosures of PHI for treatment, payment, and health care operations. | January 1, 2011 through January 1, 2014, based on acquisition of electronic health records |
| **Prohibition on Sale**      | • A covered entity or business associate is prohibited from receiving direct or indirect receipt of remuneration for any PHI without a HIPAA authorization from the applicable individual subject to exceptions. | No later than February 11, 2011                                              |
| **Marketing and Fund Raising** | • Marketing and fund-raising activities now require specific authorization as they are no longer covered under the health care operations definition. Also, individuals have the right to opt out of any communication that relates to fund-raising. | February 17, 2010                                                            |
| **Enforcement**              | • Strengthens enforcement of HIPAA security and privacy rules and penalties for noncompliance.  
• Provides for enforcement of HIPAA by States Attorneys General and local law enforcement. | Increase in civil penalties and enforcement by State Attorneys General February 17, 2010  
Penalties for willful neglect by February 11, 2011 |
HITECH Act Overview
Penalties and Enforcement

**Penalties**
- New penalty tiers per HIPAA violation (max/year)
  - Unknowing ($25K)
  - Reasonable cause ($100K)
  - Willful neglect ($250K)
  - Uncorrected willful neglect ($1.5M)
- Civil and criminal liability for HIPAA violations extended to business associates
- Mandatory investigations and civil penalties for violations due to willful neglect

**Enforcement**
- Expanded resources and significant funding for HHS enforcement
- State Attorneys General authorized to pursue actions on behalf of state citizens
- Vendor breaches enforced by the Federal Trade Commission as unfair and deceptive acts or practices

**Notable Past Incidents**
- Pharmacy incident — $2.24M penalty, plus consent agreement
Top HIPAA Privacy and Security Concerns and Challenges

Based on recent studies relating to HITECH, the following are examples of the top privacy and security concerns or challenges that many organizations are facing:

<table>
<thead>
<tr>
<th>HIPAA privacy</th>
<th>HIPAA security</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Update the breach notification procedures</td>
<td>– Reduce data leakage (e.g., data sent outside the organization and/or controlling end-user behavior)</td>
</tr>
<tr>
<td>– Amend the business associate agreements and enhance third-party risk management (now subject to HIPAA privacy &amp; security provisions)</td>
<td>– Enhance role-based access control based on the minimum necessary principle</td>
</tr>
<tr>
<td>– Revise policies and procedures (e.g., accounting of disclosure, marketing, individual access to PHI)</td>
<td>– Improve logging and monitoring to detect suspicious system activities</td>
</tr>
<tr>
<td>– Refresh training to workforce members</td>
<td>– Implement encryption solution (e.g., focusing on mobile devices first)</td>
</tr>
</tbody>
</table>
## Novell Solutions For Key HITECH Security Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Novell Product Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impermissible uses and disclosures of protected health information (PHI)</td>
<td><strong>Novell Compliance Management Platform (CMP)</strong> provides identity management, audit reporting, and web access control to network resources</td>
</tr>
<tr>
<td>Lack of safeguards of protected health information such as logging and monitoring to detect suspicious system activities</td>
<td><strong>Novell SecureLogin (NSL)</strong> provides enterprise single sign-on and fast user switching for shared workstations. <strong>Novell Sentinel</strong> can provide real-time auditing, monitoring and remediation of user access to PHI with powerful correlation engine</td>
</tr>
<tr>
<td>Enhance role-based access control based on the minimum necessary principle</td>
<td><strong>Novell Access Governance Suite (AGS)</strong> can manage roles and security policies as well as access certification. <strong>Novell Identity Manager (IDM)</strong> can provision/deprovision resources based on roles and provide self-service and workflow.</td>
</tr>
<tr>
<td>Breach notification procedure updates with monitoring and reporting</td>
<td><strong>Novell Sentinel Log Manager</strong> can store and analyze who had access to what, when, where and how for all connected devices and apps</td>
</tr>
<tr>
<td>Encryption of mobile devices and other data sources storing PHI plus reducing data leakage</td>
<td><strong>Novell ZENworks Endpoint Management</strong> solutions can secure devices including USB ports, encrypt data, application virtualization, patch management and make upgrades easy (e.g. Windows 7)</td>
</tr>
</tbody>
</table>
Novell – Three Solution Areas
Helping Healthcare Providers give users simple, secure access while safeguarding patient information

Data Center
- Lower Costs
  - SUSE Linux Enterprise
  - Virtualization
  - Intelligent Workload Management
  - Business Service Management

End-User Computing
- Secure Assets
  - SUSE Linux Desktop
  - Endpoint Management
  - Manage and Secure servers and desktops
  - Secure Social Collaboration Tools

Identity and Security
- Protect Data
  - Compliance Management
  - Access Governance
  - Identity Management
  - Single Sign-on
  - Security Management