ARRA HITECH AND ACR2 HIPAA 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. Lunarline and ACR2 HSCR provide unique and cost-effective solutions that ensure compliance, maximize protection, and enable your strategic business and IT initiatives to grow securely.

WHY LUNARLINE and ACR2?

Our proposed solution brings to our customers the best value based upon our teams extraordinary expertise in IT technology security, HIPAA Security Rules compliance, NIST 800 series security requirements and a focus on ePHI security. We provide a team immersed in a culture of information assurance, risk management, risk mitigation and compliance to provide the highest quality of service to our clients, which include but are not limited to the office of the CIO for the Department of Health and Human Service and the VA administration who have the task to treat and protect the identity of our veterans.

<table>
<thead>
<tr>
<th>HSCR Benefits</th>
<th>HSCR Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>• We read the regulations, so you don’t have to!</td>
<td>• Roadmap to full HIPAA compliance</td>
</tr>
<tr>
<td>• Compliance limits liability</td>
<td>• Continuously updated using Federal standards</td>
</tr>
<tr>
<td>• Annual subscription based program</td>
<td>• Software as a Service (SaaS)</td>
</tr>
<tr>
<td>• Protects your data</td>
<td>• Secure Input (SSL)</td>
</tr>
<tr>
<td>• Auditable reports</td>
<td>• Encrypted Storage of input data</td>
</tr>
<tr>
<td>• Uses approved NIST methods</td>
<td>• Encrypted PDF Reports</td>
</tr>
<tr>
<td>• Automates time consuming processes</td>
<td>• Supports SCAP vulnerability scan import</td>
</tr>
<tr>
<td>• Automates extraction of syslog data</td>
<td>• Supports IPS/AV upload</td>
</tr>
</tbody>
</table>

Achieving HIPAA Security Rule Compliance

1. Scan the computer network using an SCAP validated vulnerability scanner.
2. Conduct a risk assessment using the NIST 800-30 protocol.
3. Implement safeguards to protect against the risks identified during the risk assessment and SCAP vulnerability scan.

With ACR2 HSCR you can:

• Comply with HIPAA Security Rules, NIST requirements and HITECH requirements
• Maximize ePHI protection and your reputation
• Confidently implement EHR/EMR compliance
• Adopt virtualization for reporting and compliance
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.

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. However, the industry has struggled with the choice of specific technologies solutions in the absence of implementation guidelines. Penalties for noncompliance 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 heightened 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.

HIPAA Security Rule Master Conditions

The Security Rule outlines four master conditions or minimum requirements that apply to business controls and processes used to address the rule’s 42 standards. These minimum requirements state that all selected controls must be:

- **Cost effective.** A company should not spend more for the control's implementation than the probable value of the information or process it is designed to safeguard.

- **Within the technical capability of the firm.** The company must be able to maintain and enforce the controls they choose without having to rely on an outside party. For instance, although a company can outsource its IT functions, it must be able to create, maintain, and enforce all IT controls if they are brought back in-house, such as access and authorization controls and audit log evaluations.
• **Within the resource capability of the enterprise.** The business should have the necessary IT resources to monitor and manage each control throughout the year.

• **Suitable when weighed against their desired results.** General IT, compensating, or alternative controls should correspond directly to the standard in question. For example, the requirement to be able to back up and restore patient data should rely on access controls, data verification and integrity controls, and storage requirements, among others.

During Security Rule compliance reviews, internal auditors need to identify how companywide IT measures and controls meet each of the four requirements.

**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.

**Regulatory Compliance Applies to:**

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

**Penalty Matrix**

<table>
<thead>
<tr>
<th>Standard of Culpability</th>
<th>Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know of the violation and by exercising reasonable diligence would not have known of violation</td>
<td>Corrective action without penalty</td>
<td>No penalty – however, subject to discretion of Secretary</td>
</tr>
<tr>
<td>Unknowing Violations</td>
<td>At least $100 per violation</td>
<td>Not to exceed $25,000 in a calendar year</td>
</tr>
<tr>
<td>Violation due to reasonable cause, not willful neglect</td>
<td>At least $1000 per violation</td>
<td>Not to exceed $100,000 in a calendar year</td>
</tr>
</tbody>
</table>
Violation due to willful neglect

<table>
<thead>
<tr>
<th>Violation due to willful neglect</th>
<th>At least $10,00 per violation</th>
<th>Not to exceed $250,000 in a calendar year</th>
</tr>
</thead>
</table>

Violation is due to willful neglect and the violation is not corrected within 30 days of the first date the person liable for the penalty knew or should have known that the violation occurred

<table>
<thead>
<tr>
<th>Violation is due to willful neglect and the violation is not corrected within 30 days of the first date the person liable for the penalty knew or should have known that the violation occurred</th>
<th>At least $50,000 per violation</th>
<th>Not to exceed $1,500,000</th>
</tr>
</thead>
</table>

**HITECH Act Highlights:**

- **EHR/EMR Funding**
- **Business Partner Compliance**
- **Risk assessments and Mitigation**
- **Breach notification**

**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.

**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 address the topic of breach notification of unsecured ePHI, 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

**STATE PRIVACY LAWS**

Although the HITECH Act asserts precedence over state laws, it also acknowledges the importance of alignment with state laws by specifying 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.

**ACR2 HSCR**

### HIPAA Security Rule Compliance Reporter

The **HIPAA Security Rule Compliance Reporter™** (HSCR) deploys state of the art enterprise risk management technology to allow you to meet the HIPAA Security Rule requirements for hospitals and their business associates. The software supports SCAP vulnerability scan data uploads and direct input or uploads of syslog data from perimeter security devices. Policy inputs include HIPAA specific questions and enhanced reporting. The HSCR console enables the monitoring of the HIPAA security rule compliance status of each business associate. The console allows for hospital access to real-time display of the HIPAA security rule compliance status of all active business associates as described in NIST 800-66.

![Fig. 1 - HIPAA Security Rule Compliance Reporter Data Entry Screen](image-url)
HSCR Benefits

- We read the regulations, so you don't have to!
- Compliance limits liability
- Annual subscription based program
- Protects your data
- Auditable reports
- Uses approved NIST methods
- Automates time consuming processes
- Automates extraction of syslog data

HSCR Features

- Roadmap to full HIPAA compliance
- Continuously updated using Federal standards
- Software as a Service (SaaS)
- Secure Input (SSL)
- Encrypted Storage of input data
- Encrypted PDF Reports
- Supports SCAP vulnerability scan import
- Supports IPS/AV upload

Achieving HIPAA Security Rule Compliance

1. Scan the computer network using an SCAP validated vulnerability scanner.
2. Conduct a risk assessment using the NIST 800-30 protocol.
3. Implement safeguards to protect against the risks identified during the risk assessment and SCAP vulnerability scan.

How it works - the technology

The overall ACR2 automated risk management process is shown in Figure 2. IPS and Anti-Virus data, network scan data, and policy data are input into the Risk Calculation Engine. This creates the Results Documentation Report and the Control Recommendations Report. The changes in controls are implemented and the changes are added to the risk engine, along with updated Scan and IPS/AV data. This cycle can be repeated as often as daily, with reports on demand, on schedule or on alarm.

Fig. 2 - HIPAA Compliance Methodology

Enterprise Compliance Console for HIPAA™

The enterprise management compliance package includes a console that allows hospitals or distributed health care enterprises to
access and view the HIPAA security rule compliance status of all of their business associates. This uses an implementation of technology developed under the sponsorship of the US Department of Homeland Security. The console allows the hospital to review and display the HIPAA security rule compliance status of each or all active business associates that have been configured and authorized access.

Glossary of Abbreviations

- AV - Anti-Virus
- IPS - Intrusion Prevention System
- NIST - National Institute of Standards and Technology
- SCAP - Security Content Automation Protocol
- Syslog - System Log output from security devices
- UTM - Unified Threat Management System

Fig. 3 - HIPAA Compliance Console