Ensuring Healthcare Compliance and Managing Risks with Next Generation Identity and Access Management
The challenges imposed by federal regulations including HIPAA and ARRA HITECH along with adherence to best practices have created a disruption amongst healthcare organizations nationwide. According to Gartner, “by 2018, 30% of organizations will have replaced more than 50% of manual access certification and request approvals by automated intelligent policies driven by analytics.” This paper will take a look at solutions to help healthcare organizations meet the latest regulatory mandates for security, data protection and availability.

What is HIPAA and HITECH?
To ensure a set of generally accepted security standards and requirements for protecting health information, the US Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. The scope widened in 2009 when it was extended to include digital information, known as the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Digitalization in Healthcare
As the healthcare industry began adopting electronic information systems including data entry and electronic health records (EHRs), a wave of security threats began to emerge such as stolen electronic records, tampering of data and information or public disclosure. In an effort to control/eliminate these threats, strict standards have been laid out to govern healthcare information. The cost of non-compliance fines range from $25,000 to $1.5 million per violation.

Identity and Access Management
To protect patient privacy and secure health information, healthcare organizations of all sizes must deploy a business-driven Identity and Access management (IAM) solution. With an IAM solution in place, a healthcare organization can securely manage access to sensitive patient information, deliver access in a timely manner, and ensure appropriate levels of access. In order to meet both federal regulations and organizational requirements, IAM solutions in a healthcare organizations must meet the following capabilities:

- Enterprise-wide visibility and control
- Governance
- Risk Management
- Identity Warehouse
- Access Certifications
- Policy Model
- Resource Connectors

Look at SailPoint IdentityIQ for Healthcare Organizations
IdentityIQ is the Sailpoint solution for identity and access management software. Texas-based SailPoint is one of the pioneers of identity and access governance technology.

Source: Gartner, Inc. All Rights Reserved.
Their flagship solution meets stringent identity and access management requirements. SailPoint was named a Leader in Gartner's 2014 Magic Quadrant for Identity Governance and Administration, published January 2015.

**SailPoint IdentityIQ: Setting the Standard in Identity and Access Management**

SailPoint IdentityIQ allows organizations to meet strict capabilities, maximize exponential return on investment and ensure compliance. This next generation of SailPoint identity management solutions, empower organizations to automate and streamline user management processes. By enabling automation, rigid controls are places for electronic medical systems including Epic, Cerner, GE Centricity, Siemens and others.

The following represents the solutions’ capabilities and impact within the organization:

<table>
<thead>
<tr>
<th>SailPoint IdentityIQ Capability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Warehouse</td>
<td>Rapidly creates a single repository of users and access data, creating an enterprise-wide view into users, accounts and entitlements. An Identity Warehouse resolves data inconsistencies, eliminates orphaned accounts and provides user-friendly descriptors to translate cryptic IT data into usable business information.</td>
</tr>
<tr>
<td>Access Certifications</td>
<td>Automates the creation, distribution and reporting of cross-enterprise access certification campaigns across entitlements, roles and policy violations.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Highlights key identity risk factors for users across the enterprise. Organizations are able to focus and prioritize compliance controls on high-risk populations of users. In addition, this allows for an automated view of identity risk scores for users who have not had timely certification reviews.</td>
</tr>
<tr>
<td>Policy Management</td>
<td>Automates the detection and mitigation of Separation-of-Duty (SoD) policy violations within and across enterprise IT systems.</td>
</tr>
<tr>
<td>Resource Connectors</td>
<td>Automates the collection of user account data by deploying read-only connectivity to a wide variety of enterprise systems.</td>
</tr>
</tbody>
</table>

SailPoint IdentityIQ provides healthcare organizations with automated, governance-based controls to align access policy with process across the organizations to ensure lower audit costs and improvement in oversight that significantly lower its security risk.

For more information on how SailPoint IdentityIQ can help your organization meet requirements, please contact info@columnit.com.