Executive Summary

The Health Information Technology for Economic and Clinical Health Act (HITECH) has made significant changes to the Health Insurance Portability and Accountability Act (HIPAA). Previously a reactive and vaguely defined statute, the HITECH act brings depth of requirements and steps up enforcement and penalties to HIPAA violations. In addition, HITECH extends HIPAA coverage to related entities. For example, a healthcare provider is now responsible for the HIPAA posture of its out-of-house pharmacy services, billing services, claims processing services and overseas support desks. The updates reflect the reality of the increasingly distributed and interconnected reality of most healthcare organizations. As a result, HIPAA compliance has become more important (and challenging) than ever.

The act will impose more stringent regulatory and security requirements to the privacy rules of HIPAA, such as extending the covered entities to include business associates and related third-party vendors in the healthcare industry, increased audit requirements, more proactive measures to protect personal healthcare information (PHI), increased civil penalties for a compliance violation of HIPAA and stricter notification requirements of security breaches of protected information.

The result should be better governance and risk management, but it will come at the cost of increased challenges for covered organizations. IT Security and business unit stakeholders in particular, will be challenged in a variety of ways. Compliance with guidelines can be difficult for organizations without strong access governance processes and policies. Complicating matters, demonstrating compliance through an annual user access review and certification process can be even more complex and time consuming, which results in less time available for organizations to focus on patient care and related activities. The net result is higher operational and regulatory risk exposure.

One area that leads to a significant number of audit findings — access change management — will become even more of a challenge under the more stringent guidelines of HIPAA. To practice effective access risk management, organizations will need to shore up processes governing initial access requests (joiners), changes to access due to transfers (movers), and termination of access (leavers). The joiner/mover/leaver framework provides a useful mechanism for entities to use as a basis for a risk-based approach to access governance.

It follows that forward thinking organizations should use the passage of the HITECH as an opportunity to take a more risk-oriented approach by implementing an access governance framework and modernizing how patient information is stored and accessed through electronic health records (EHR). Such an approach will yield increased customer trust, decreased operational burden, streamlined operations and superior access risk management — all of which leads to improved organizational value.
Background

The digital revolution in healthcare has provided an opportunity to greatly streamline operations and increase levels of patient care and efficiency. But it has not been without consequences. Risks of compromise of PHI are very real. The Identity Theft Resource Center estimated that healthcare organizations were responsible for 20.5% of all data breaches in 2008, and the prevailing causes of these issues, while difficult to solve, are well-known. Access governance is at the core of this issue. At the 2008 HIMSS Conference, 64% of audience members identified user access as their number one IT security concern.

Legislative bodies have long recognized the importance of risk management in healthcare. HIPAA was passed by congress in 1996 as a means to amend existing regulation to reflect the realities of modern healthcare. The act recognized the need to move towards freer but more secure exchange of PHI, and included specific provisions aimed towards administrative simplification and the privacy/security of electronic data interchange (EDI).

Although well intentioned, the act was fraught with several problems. As with many regulatory mandates, the specific privacy and security components were exceedingly vague. Well-intentioned (but perhaps understaffed) organizations, in the absence of specific prescriptive controls definitions, often struggle to determine what the appropriate level of control should be. This can lead to over-controlled or, more frequently, under-controlled environments. Neither is efficient.

With the vacuum left by vaguely worded requirements, organizations were left to fill the middle ground with interpretations of best practice. Partially as a result, the privacy and security components of the act did not become effective until 2003-2005. Enforcement of the Act didn’t begin until 2006, a full ten years after its passage. When enforcement of HIPAA began, the penalties were not severe enough to encourage full and widespread adoption and compliance. As a result, security and privacy suffered.

The HITECH Act was passed as part of the American Recovery and Reinvestment Act of 2009, and addresses the major shortcomings of the HIPAA Act, while updating the regulatory framework to account for changes in technology. The act imposes more stringent regulatory and security requirements to the privacy rules of HIPAA, such as extending the covered entities to include business associates and related third-party vendors in the healthcare industry, more proactive measures to protect PHI and increased civil penalties for a compliance violation of HIPAA. Additionally, the HITECH Act authorizes state attorney general’s to bring civil actions on behalf of state residents adversely affected or threatened by violations of HIPAA.

One particularly interesting aspect (and potentially challenging aspect) of HITECH is increased focus on audit and notification. Part of HITECH enforcement that will impact covered entities is on-demand audit requests from patients with regard to who had access to their PHI. As a result, organizations need to be continually ready to demonstrate compliance. Related notification requirements have been stepped up, and organizations are required to not only notify potentially compromised patients, but provide a full accounting of the incident (what was compromised, when and by whom).
Regulatory Oversight

The Department of Health and Human Services (HHS) maintains the bulk of regulatory oversight duties for HIPAA compliance. Enforcement is now handled by the Center for Medicare and Medicaid Services (CMS). Fines can be substantial (up to $250,000), and criminal penalties can also be imposed. Enforcement, which was previously inconsistent, has been noticeably ramped up with the passing of the 1996 enforcement deadline and the HITECH Act.

At the same time, high-profile violations have been becoming more prevalent; and as public concern over privacy becomes more widespread, the publicity of a HIPAA violation can impart significant reputation and brand damage. At the University of California Los Angeles (UCLA), university staff took advantage of inappropriate access to leak information on celebrities to the press, creating a serious HIPAA violation, and damaging the reputation for the university. The long-term effects of such an incident can easily eclipse any regulatory fines and penalties.

From an information security audit standpoint, organizations are required to demonstrate compliance with several basic tenets and requirements within the security and privacy rules. The rules describe, at a high level, best practices that organizations must adopt to protect the confidentiality, integrity and availability of electronic protected health information.

Within the broad security rule classification, safeguards are segregated into three types of standards:

- Administrative Safeguards describe high level procedural and strategic control
- Physical Safeguards describe "brick and mortar" safeguarding of facilities and records
- Technical Safeguards describe specific technology controls that govern the access of electronic health records

To show compliance with the three standards of the security rule, organizations need to demonstrate mechanisms for the security and confidentiality of all healthcare-related data, complying with the following minimum requirements:

- The confidentiality, integrity & availability of all PHI
- Protection against reasonably anticipated threats or hazards to the PHI the entity creates, receives, maintains or transmits
- Protection against reasonably anticipated uses or disclosures of PHI
- Visibility, control & auditing into and of all information flow
- Workforce compliance with HIPAA and minimization of the threat of data being stolen for financial gain
- Periodic review of security measures as needed to ensure reasonable and appropriate protection of PHI
Getting Compliant

Healthcare organizations often struggle to maintain a consistent approach across information resources to govern user access, and as a result, may have an incomplete or fragmented posture of compliance throughout the organization. Reasons for this generally include the sheer volume of change and churn in the user population of a large organization. User relationships and roles are constantly changing as employees move into and out of different job functions and operational groups. Healthcare systems are often fragmented and widely diverse, with patient data being stored in multiple systems and locations. The trend for outsourcing patient data is often stored outside the organization with outsourced providers such as billing services. This fragmentation and distribution further complicates the ability for an IT team to gain a clear picture of the access reality and ensure that entitlements are governed accordingly.

Change becomes such an overwhelming force in most organizations that the process for governing access is unable to keep up with reality. In the joiner/mover/leaver control framework, organizations frequently do an adequate job controlling initial access requests. When new patient billing processors do not have access to the information resources they need, they are certain to raise the issue to appropriate resolution. Users that transfer or terminate their relationship with the organization are more problematic, as most organizations lack a standardized process for dealing with these access change events, which can lead to orphaned accounts, segregation of duties violations and other audit related problems.

Certification and review are the standard safeguards against access violations from poor change management. Often, these are manual processes performed in spreadsheets, which can be laden with error. Even when manual processes do detect error, these safeguards are detective in nature, not preventative, and catch problems long after the fact. The complexity, fragmentation and manual processes that are used to manage access change make compliance with such safeguards a significant undertaking.

HIPAA security requirements, although high level, are largely overlapping with other best practice access governance frameworks and regulations.

For organizations with fragmented control frameworks in place, HIPAA/HITECH presents an excellent opportunity to proactively implement an access governance framework that leverages the overlap with other common control standards such as ISO 27001/2 (formerly 17799), COBIT, NIST or ITIL or in other regulatory obligations such as Sarbanes Oxley.
Entities who manage information security and regulatory compliance need to perform due diligence to account for subtleties present in the HIPAA standard, but the groundwork for the majority of requirements should exist in such entities.

As such, an initial HIPAA compliance program should start with a readiness assessment and gap analysis, followed by a mapping exercise to the existing control framework. Organizations with a comprehensive control framework in place will have a leg up on the process, but for other entities this can represent an opportunity to build such a framework. As we will discuss later in this paper, implementing such a control framework for access governance will pay dividends both in terms of operational and compliance risk reduction as well as in a reduction of the operational overhead required with ongoing compliance processes. Regulatory compliance management is an ongoing process and should not be treated as a one-time project.

<table>
<thead>
<tr>
<th>Administrative Safeguards</th>
<th>Standards</th>
<th>Sections</th>
<th>Requirements</th>
<th>Addressed by RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Safeguards</td>
<td>§ 164.304</td>
<td>• Administrative Actions, Policies &amp; Procedures to Protect Health Information</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Security Management Process</td>
<td>§ 164.308(a)(1)</td>
<td>• Risk Analysis &amp; Management</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Workforce Security</td>
<td>§ 164.308(a)(3)</td>
<td>• Authorization and/or Supervision • Workforce Clearance Procedure • Termination Procedures</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Information Access Management</td>
<td>§ 164.308(a)(4)</td>
<td>• Isolate Health Care Clearinghouse Functions • Access Authorization • Access Establishment &amp; Modification</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>§ 164.308(a)(8)</td>
<td>• Testing</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Technical Safeguards</td>
<td>Access Control</td>
<td>§ 164.312(a)(1)</td>
<td>• Unique User Identification (App &amp; Entitlement) • Emergency Access procedure</td>
<td>✓</td>
</tr>
<tr>
<td>Audit Controls</td>
<td>§ 164.312(b)</td>
<td>• Visibility into Access</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

An initial HIPAA compliance program should start with a readiness assessment and gap analysis, followed by a mapping exercise to the existing control framework.
Access Governance Requirements

A Unified View of Access Reality

To become compliant with specific HIPAA security requirements, organizations first require a unified, enterprise-wide view to user access. Without this unified view, it is impossible to manage authorization requests under requirement 164.308(a)(4). A single view of user access is almost impossible for most organizations without a centralized access governance framework in place, as they tend to manage access at the information resource level (application, data, system, host). Having such a framework in place provides a comprehensive view of enterprise access reality - understanding who has what access to what information resources and what they can do at a fine-grained entitlement level. Since most organizations manage access in an ad hoc and siloed manner, there is no easy way to aggregate user access data to get a consolidated view. And managing access at an application or technical level (user provisioning) only provides a coarse-grained view, which will not provide the fine-grained view required for compliance.

An access governance system that spans applications’ information resources enables a foundation for providing the audit access required in 164.312(b). The standard requires a mechanism in place that can record and examine all activity in any information system containing PHI. In a siloed environment, such audit access can quickly become prohibitively expensive or outright impossible. Controls can be applied at the application or resource level, but it becomes difficult to implement controls spanning multiple applications. This can easily lead to SOD violations, because controls instantiated in a McKesson application, for example, have no visibility into the access rights granted in a Eclipse application.

A unified view providing a window into the access reality and a single system of record for access governance, also provides the ability to satisfy HIPAA requirement 164.312(a)(2)(i), which stipulates a unique identifier for tracking enterprise user identity. In complex environments, specifically those with legacy systems, it can be nearly impossible to correlate a single point of user access across the entire enterprise. HIPAA requires the ability to correlate any single-user identifier with all instances of access to information resources for that same user. In fragmented environments, this is extraordinarily difficult, but with a single correlated view of user access it becomes a reality.

"Rubber stamping" is a common occurrence in organizations with poor access governance. It occurs due to a language gap between business stakeholders, who are required to certify compliance, and the technical view of access entitlements they are forced to use to do their certification. Because entitlements are represented in a cryptic security syntax, business stakeholders that must certify access don’t have the context to understand what the entitlement means. A common language for describing access must be provided to bridge the language gap between the business and IT security teams, ensuring that violations are identified and remediated.
Dynamic and Preventative Access Controls

Formalizing an access risk management program is also a core requirement of the security rule, covered in requirement 308(a)(1). Additionally, Segregation of Duties (SOD) is required in 164.308(a)(4)(ii)(A), where organizations are required to segregate access between users who have access to PHI and members of the larger organization who do not. Under HITECH, this scope has been expanded, and organizations now must ensure that appropriate controls for access extend between themselves and their outsourced functions (e.g. patient billing and collection processing).

Most organizations rely on manual, detective controls in this area, catching potential violations through periodic audit and review processes. Automated preventative controls are far superior, and a strong access governance program should contain the ability to stop segregation of duties violations and toxic combinations from being granted in the first place. A roles-based approach to access change management will reduce the administrative burden involved with access delivery. As a result, fewer control violations go unnoticed and access reviews and risk management efforts become much less labor intensive.

A roles-based approach provides a preventative safeguard at the place of change. Rules are run dynamically at the point of request. For instance, when a mover changes roles, this approach will ensure that it does not cause a toxic combination. Rules can be used to automatically spawn an approval process at the point of request, providing a preventative control before any toxic combination is created. The result is that control violations are avoided in the first place, rather than being detected after the fact at the next periodic review cycle. From a risk management standpoint, this is a far superior approach.

Automated Audit and Evaluation

Evaluation, as detailed in 164.308(a)(8), is a critical component of the HIPAA security rule and often proves problematic for organizations that have fragmented and complex enterprises. Business-reviewing managements need to make sense of siloed user access data from disparate sources in disparate formats in order to certify the appropriateness of a user’s access. The data then needs to be collated and the findings presented in a logical context. Manual generation of such reports can be a long and expensive process. Worse yet, a static audit report is out of date shortly after it’s produced, due to the pace of user access change. The net effect is an audit review process that is manual, error-prone and lacking in control rigor.

The process can be made far less painful with a roles-based approach to access governance. Roles can reduce organizational burden. Roles provide a way to reduce this burden, enabling the organization to certify access by role rather than individual. For an example, a department of 300 users might be represented by four or five business process roles. By certifying the role structure — the specific entitlements that make up the role — the amount of effort and time required by the business for certification goes down dramatically. If no member of the role has entitlements outside of the role, and the entitlements within the role structure are in compliance, then everyone that is a member of that role automatically inherits the compliance.

Evaluation under HIPAA is also eased by the dynamic, rules-based approach to change management outlined previously. Such an approach can automate a set of processes for event-driven reviews that require a review of access only when it changes. As a result, user access that has been subject to the dynamic rule at the point of change can be excluded from the next audit review cycle (within a certain period).
**Automation is the Solution**

To meet the objective of being auditably compliant in a cost-effective and streamlined fashion, organizations should invest in an automated access governance program with regulatory compliance as a core component. The automated access governance framework should provide:

- Enterprise-wide visibility to user access aggregated and correlated to present a unified view and business friendly context
- A regular automated access reviews and certification processes
- Dynamic and preventative access controls
- Role-based access
- Closed-loop access rights remediation and validation
- An auditable system of record
- Metrics and reporting for access decision support

An automated approach to role-based access governance reduces compliance fatigue by automating the function and audit of risk-management controls. This approach will ease both the initial setup of a HIPAA compliance program, as well as streamline the ongoing maintenance, reducing organizational costs and mitigating access risk exposure.

With such an access governance framework in place, healthcare organizations will be well on their way to managing the business and regulatory risks of inappropriate access to its information resources. The right solution requires a strategic approach to access governance based on auditable business processes that provide complete visibility and accountability for user access.
<table>
<thead>
<tr>
<th>HIPAA Administrative Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td>Administrative Safeguards § 164.304</td>
</tr>
<tr>
<td>Security Management Process § 164.308(a)(1)</td>
</tr>
<tr>
<td>Risk Management § 164.308(a)(1)(ii)(B)</td>
</tr>
<tr>
<td>Workforce Clearance § 164.308(a)(3)</td>
</tr>
<tr>
<td>Termination Procedures § 164.308(a)(3)(ii)(C)</td>
</tr>
<tr>
<td>Information Access Management § 164.308(a)(4)</td>
</tr>
<tr>
<td>Isolating Healthcare Clearing House Functions § 164.308(a)(4)(ii)(A)</td>
</tr>
<tr>
<td>Standard</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Access Authorization § 164.308(a)(4)(ii)(B)</td>
</tr>
<tr>
<td>Access Establishment &amp; Modification § 164.308(a)(4)(iii)(C)</td>
</tr>
<tr>
<td>Evaluation § 164.308(a)(8)</td>
</tr>
<tr>
<td>Unique User Access Identification § 164.312(a)(2)(i)</td>
</tr>
<tr>
<td>Emergency Access Procedure § 164.312(a)(2)(ii)</td>
</tr>
<tr>
<td>Audit Access § 164.312(b)</td>
</tr>
</tbody>
</table>
About RSA

RSA is the premiere provider of security, risk and compliance solutions, helping the world’s leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, providing compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.