# Beyond HIPAA compliance: Aligning IT audit and information security to manage information risks

Guidance for health care internal auditors and information security professionals

**Table of contents**



## Executive summary


The process and technical requirements of the Health Insurance Portability and Accountability Act (HIPAA) are not new to information security and privacy professionals. A well-managed information security function needs to be in place to protect a health care organization's investment in technology and processes, while also protecting sensitive data such as electronic protected health information (ePHI). However, emerging technologies and the continual increase in the depth and quality of regulatory audits and reviews require organizations to be agile—addressing emerging areas such as medical device security, vendor management and business associate security.

Mature health care organizations can also leverage the power of a well-tuned IT audit function to fully understand and manage the organization's risk posture. Often the status quo approach results in functions such as IT audit, IT security, and health care


ahia
Assoc. of Healthcare Internal Auditors

RSM

compliance and privacy operating in silos. However, optimal results are obtained when there is a robust partnership between these groups.


Recent rule changes and more aggressive regulatory enforcement have significantly increased financial fines for noncompliance and the pressure on organizations to "get security right." Recent sanctions have been severe and reflect several security or privacy process failures, including:

- A $4.8 million fine against New York Presbyterian Hospital and Columbia University for poor server management that exposed PHI
- A $4.3 million fine against Cignet Health of Maryland for multiple HIPAA violations, including $3 million for willfully ignoring investigators
- A $1.7 million fine against WellPoint, Inc. for insecure servers and ineffective administrative and technical safeguards that left ePHI exposed
- A $1 million fine against Massachusetts General Hospital after sensitive documents were left on a train by an employee

Health care organizations can become noncompliant for several reasons. Many failures are education-based, with employees simply not aware of potential risks or requirements. Some organizations are overconfident, while others lack the proper level of executive leadership to manage processes or commitment because of the costs involved with implementing an effective information security and compliance framework.

However, the costs related to securing sensitive data and devices pale in comparison to the repercussions of noncompliance and deficient controls. Health care organizations must consider the risks of a data breach, including severe financial sanctions, the cost of responding to the breach, reputational damage following bad press, and in a worst-case scenario, patient safety put in jeopardy.

The good news is that even with a rapidly changing information security landscape, organizations can leverage existing resources to work toward more effective collaboration between IT audit and IT security to increase enterprise security and HIPAA compliance. The HIPAA security and privacy requirements align well to the standards (i.e., ISO27001, NIST, COBIT) created to structure and manage the related organizational risks, regardless of the industry. The work of understanding and managing these risks effectively in a health care setting simply needs to be applied with more rigor.

## The critical role of IT security

Technology is evolving quickly, and regardless of the size of a health care organization, there is increased pressure to leverage technology to improve information integration affecting outcomes and quality of care. One example is "meaningful use" regulations that require providers to utilize a certified electronic health record (EHR) and electronic medical record (EMR) system to increase access and efficiency, while maintaining the security of health information.

The increased use of technology helps health care organizations on several levels, from achieving better clinical outcomes by implementing innovation for enhanced patient care, to avoiding regulatory sanctions.

Today, any health care visit or interaction results in several data points. These points ideally come together to develop a comprehensive view of a patient, from general health information to what medications are being taken and any harmful interactions to specific treatments or prescriptions. This information is not only utilized by a local physician or health system, but also downstream by insurers and pharmaceutical companies. A wide range of organizations also purchase health data in large sets to perform analytics for selling and marketing drugs and improving clinical outcomes.

However, the migration from paper-based records to electronic data storage is a new world for many health care organizations. For example, organizations once maintained paper records locked in cabinets or warehouses. Select individuals had keys, and people that needed to view files were required to fill out a form. Security measures centered on which employees had access to the files and who had keys. New digital record formats require a new skill set and approach to manage the

risks to electronic health information as organizations develop new processes to understand, control and secure sharing of information.

Health care risks are exacerbated because of an increased patient expectation that everything be connected and a need for provider efficiency. The convenience, connectivity and potential for better care that comes with smarter devices and physicians with tablets instead of clipboards brings additional vulnerabilities. People are suddenly a target, and interconnected devices and networks present more opportunities for more frequent and larger-scale breaches.

In addition to maintaining patient safety, remaining in compliance and managing reputational risks, organizations want to maintain control over health care information because it is valuable. For example, with today's technology and greater analytics capabilities, organizations can compile data together with patients in the same ZIP code, and start to draw conclusions on population health.

These trends and market changes highlight the challenge of the advanced use of technology, data and needed implementation of sufficient security measures:

- With new technology capabilities, the natural progression is that data is being used more and has become critical to health care service delivery. However, with increased utilization, data may become a *single point of failure* where data corruption or loss directly affects patient care. Therefore, the nature of threats has changed, and organizations must take more thorough measures to secure electronic data and focus on both compliance and patient safety.
- With health care data becoming more expansive, information security has become more complex as devices that directly support patient care are networked. These devices typically have many of the same, or even more, vulnerabilities as the endpoints, servers or workstations within an enterprise. Organizations make headlines when attackers access patient data on a server, but now, a more dangerous threat to be considered and addressed is a malicious attack on medical devices that directly affects patient care.
- Health care data is a valuable input to financial and clinical management processes, but it is also at risk on a constant basis as a commodity for information thieves. An underground economy has developed for buying and selling personal, health and financial information, with complete health records having the greatest monetary value. Patients that have their information breached can suffer various identity, medical record and credit complications.

## The evolving nature of security threats

The threat landscape is evolving rapidly, and organizations must be aware of vulnerabilities to a variety of attacks, including advanced persistent threats (APT), social engineering, spear-phishing and ransomware.

- APTs use sophisticated, well-organized and often multi-faceted methods to exploit vulnerabilities, such as the placement of remote administration software on networks for use in future exploits. They are often difficult to detect, and organizations can be silently breached for months.
- Social engineering occurs when criminals directly interact with employees and manipulate them into surrendering sensitive information or credentials. It can be a fairly simple process, but it often involves complex psychology and is difficult for the organization to anticipate, diagnose and prevent.
- Spear-phishing involves a targeted attack on an individual, with a specific, seemingly official email that attempts to deceive a user into transferring money or credentials, or downloading malware that can be used as a portal to the network. Criminals can simply identify individuals to target through an organization's website or a social networking site such as LinkedIn.
- Ransomware is malicious software that denies victims' access to their own data or system. Often it will encrypt the victim's files and require a ransom to be paid to the attacker to decrypt the files. In February 2016, the Hollywood Presbyterian Medical Center in Los Angeles was forced to pay approximately $17,000 in ransom to cybercriminals as the result of a ransomware attack which disabled access to employee email and the EHR platform.

## Catching up with security

Health care organizations are historically "behind the curve" with IT security when compared to other industries. The industry has driven the sharing of information for patient care and research, in contrast to companies in industries such as financial services that have a "locked down" mentality to avoid information sharing and which have also dealt with heavy regulation for decades. However, in the last five to 10 years, health care has undergone a paradigm shift with IT security expectations growing and regulatory enforcement becoming both more commonplace and costly in the event of noncompliance.

In many ways, health care has experienced a natural progression and a journey to increased information security. As industry automation grew, organizations discovered how to use computers and devices to perform important tasks better. They then continued to refine what systems and data are used for, and now leverage advanced techniques for telemedicine, financial modeling and predictive medicine. Innovation and care have been the main priorities, and security was not necessarily an afterthought, but certainly not a priority when designing the systems.

However, as highlighted previously, where the risks in other industries are mainly profit-related, with health care, financial risks are an important consideration, but the key risk is patient health and well-being. The primary reason security is coming to the forefront and receiving more regulatory attention is the potential for a security incident that results in the mishandling or misuse of patient information, missed treatment opportunities, adverse health consequences or in an extreme instance, a loss of life.

When systems failures result in adverse health effects, a spotlight will fall directly on IT security and the administration leaders that neglected this risk area. The result will be a response that creates a cascading impact on operations, investment and strategic plans. Therefore, it is critical to understand threats and implement a proactive structure to avoid security risks.

## Hazard costs versus opportunity costs

As mentioned earlier, the costs of a breach or security incident are often steep. In addition to potential fines for non-compliance, organizations are typically concerned with hazard risks, such as devices and systems failing and causing financial damage and interruptions to operations. However, health care organizations must also consider opportunity risks.

A health care organization's focus should be controlling risks, implementing corrective actions and avoiding regulatory sanctions, but at the executive level, opportunities must be monitored to ensure the business is functioning well and progressing in alignment with strategic plans. If an organization does not have a mature IT security and IT audit function, the need to respond to a breach could easily result in missed business opportunities. This is because the costs of reactively responding to a major breach during an emergency are almost always significantly higher than the costs associated with proactively building and maintaining robust IT audit and IT security functions. In an increasingly competitive health care environment, having to allocate the time of critical employees and capital to address security remediation efforts may directly reduce investments in longer-term items critical for growth or the ability to identify and pursue new opportunities.

In addition, with increased consolidation in the market, health care is more of a consumer product than it has ever been. People increasingly shop for health care services, and negative press for security lapses with patient data can result in consequences for organizations. A negative perception or a recent publicized breach may also adversely affect the ability to attract highly qualified personnel.

## HIPAA Security Rule requirements

The HIPAA Security Rule has been in effect since 2003, but compliance was not always strongly enforced; however, that has been changing rapidly. The Security Rule itself has not changed, but the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2013 enhanced enforcement, expanded regulations to certain business associates and increased penalties for noncompliance.[1]

1 "A HIPAA Security Rule Overview," American Health Information Management Association, accessed Feb. 10, 2016, http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050540.hcsp?dDocName=bok1_050540.

As organizations continue to transition to electronic systems for health information management, new technologies introduce security risks, especially as organizations utilize a growing number of outside vendors for hosting software, data storage and transmission. Understanding and implementing HIPAA Security Rule compliance across the entire health system, including business associates, is important to protect patient information and subsequently avoid enforcement actions.

The Security Rule establishes both technical and non-technical safeguards for covered entities and business associates to protect ePHI. Covered entities include all health care providers, clearinghouses and health plans that electronically transmit health information. A business associate is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." For example, this would typically include data center hosting services, medical records and billing services, and document shredding companies, among others. The rule aims to safeguard patient health information while organizations implement new innovations to improve patient care.

The Security Rule requires organizations to implement appropriate security measures or safeguards—administrative, technical and physical—to protect ePHI.

**Administrative safeguards** include guidelines for security management processes, security personnel, information access management, workforce training and periodic evaluation. **Physical safeguards** provide guidelines for facility access and control, and workstation and device security, while **technical safeguards** detail requirements for access controls, audit controls, integrity controls and transmission security.

Specifically, covered entities must:

1. Ensure the confidentiality, integrity and availability of all ePHI they create, receive, maintain or transmit
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information
3. Protect against reasonably anticipated, impermissible uses or disclosures
4. Ensure compliance by their workforce[2]

### Regulatory impact

For the purposes of the Security Rule, confidentiality refers to protecting ePHI from access by unauthorized parties. In addition, integrity refers to information not being altered without proper need or permission, and availability dictates that information must be readily accessible by authorized personnel.

Many health care organization IT, audit or security functions do not realize the extent of HIPAA Security Rule enforcement or which agencies are involved with enforcement. Government officials from the Centers for Medicare and Medicaid Services (CMS), Office of the Inspector General (OIG) and Office for Civil Rights (OCR) are performing HIPAA compliance audits, and as data security focus, and the federal investment in the industry, becomes even greater, the rate of investigations is unlikely to slow. Enforcement actions can vary, with four tiers of penalty amounts that quickly escalate and can reach $1.5 million for each separate violation.

In addition, the government distributed significant incentive payments through the Patient Protection and Affordable Care Act for organizations to implement electronic records and secure that data (meaningful use). As a result, government agencies are performing audits to ensure compliance with regulatory requirements. Organizations must monitor compliance to avoid forfeiting those funds and potentially suffering additional sanctions.

Unfortunately, many organizations struggle to implement processes and controls that comply with HIPAA Security Rule requirements. However, several existing security frameworks that are already defined, widely implemented and fully functional can help health care organizations become compliant with HIPAA and realize several additional security benefits throughout the enterprise.

---

2 "Summary of the HIPAA Security Rule," U.S. Department of Health & Human Services, accessed Feb. 17, 2016, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/.

Such frameworks which include pertinent security management processes include:

- International Organization for Standards (ISO)
- Control Objectives for Information and Related Technology (COBIT)
- National Institute for Standards and Technology (NIST)

## CIS critical security controls

| CIS critical security control | NIST core framework | ISO 27002: 2013 | HIPAA | COBIT 5 |
|---|---|---|---|---|
| **Secure configurations for software and hardware** | PR.IP-1 | A.14.2.4<br>A.14.2.8<br>A.18.2.3 | 164.310(b): Workstation use – R<br>164.310(c): Workstation security – R | AP013: Manage security<br>DSS05: Manage security services<br>BA110: Manage configuration |
| **Continuous vulnerability assessment and remediation** | ID.RA-1<br>ID.RA-2<br>PR.IP-12<br>DE.CM-8<br>RS.MI-3 | A.12.6.1<br>A.14.2.8 | 164.310(b): Workstation use – R<br>164.310(c): Workstation security – R | AP013: Manage security<br>DSS05: Manage security services |
| **Email and web browser protection** | PR.IP-1 | A.14.2.4<br>A.14.2.8<br>A.18.2.3 | 164.310(b): Workstation use – R<br>164.310(c): Workstation security – R | AP013: Manage security<br>DSS05: Manage security services<br>BA110: Manage configuration |
| **Malware defenses** | PR.PT-2<br>DE.CM-4<br>DE.CM-5 | A.8.3.1<br>A.12.2.1<br>A.13.2.3 | 164.308(a)(5): Security awareness and training – Protection from malicious software A<br>164.310(d)(1): Device and media controls – Accountability A<br>164.310(b): Workstation use – R<br>164.310(c): Workstation security – R | AP013: Manage security<br>DSS05: Manage security services |
| **Data protection** | PR.AC-5<br>PR.DS-2<br>PR.DS-5<br>PR.PT-2 | A.8.3.1<br>A.10.1.1 – A.10.1.2<br>A.13.2.3<br>A.18.1.5 | 164.308(a)(4): Information access management – Isolating health care clearinghouse function R<br>164.310(d)(1): Device and media controls – Accountability A<br>164.312(a)(1): Access control – Encryption and decryption A<br>164.312(e)(1): Transmission security – Integrity controls A<br>164.312(e)(1): Transmission security – Encryption A | AP013: Manage security<br>DSS05: Manage security services |

## Effective information security governance

While HIPAA compliance is obviously important, effective information security should be the organization's focus and must go beyond simply meeting regulatory demands. Implementing any of these trusted frameworks helps to establish a strong security foundation to protect patients and sensitive data across the organization.

From a HIPAA perspective, a security officer must be defined within the organization, with a formally documented job description. In most organizations, the chief information security officer (CISO) role resides in IT and reports to the chief information officer (CIO) or chief technology officer (CTO). However, alternative options exist for reporting structures, providing differing challenges and benefits.

The advantage of having the CISO as part of the IT organization is that he or she will be "close to the ground" and know the tactical risks that often result in incidents and compromises. However, by moving the CISO up to a more enterprise function, he or she has more authority to increase awareness and affect change. The CISO role is typically more effective when it is elevated, but CISOs must retain visibility into and understanding of IT to communicate tactical risks and share that information with executives. The IT function and network operations must be completely transparent to the CISO.

Some organizations are moving the CISO role out of IT and positioning it as a first line of defense for risk management, with reporting directly to the chief operating officer (COO) or even the CEO. The main reasoning behind this move is to avoid the security function being seen as only a technology imperative, and to remove the possible conflict with technology investment and issue escalation. Moving the CISO enables a more enterprise-wide view of risk, which is especially important considering how threats have evolved from remote attacks against an organization's firewall to more severe concerns such as social engineering, spear-phishing attacks and more complex, cutting-edge attacks.

Stronger security demands require a more pervasive mentality that crosses all lines of the enterprise, and the CISO can no longer be solely technology-focused. While the CISO's role is dependent on the authority they are given, their job responsibilities should center on three key principles, regardless of where the position resides in the organization:

1. The CISO must be independent and possess sufficient resources (e.g., access to personnel, budget) to effectively execute the information security agenda
2. The CISO must take an organization-wide consideration of IT security risk
3. The CISO must have access to executives, and in turn, provide input across the organization

An effective CISO is important for HIPAA compliance, but also for a more effective overall information security framework. However, an often overlooked opportunity is the potential to partner with IT audit and leverage its holistic view of risk to think beyond the basic HIPAA risk assessment and implement a stronger holistic security posture across the organization.

## Making room at the table for IT audit

A robust partnership between the IT audit function, the overall IT function and IT security can benefit a health care organization in several ways. Each of the functions should share some common goals, and coordinate work efforts. For example, when IT security is implementing a new initiative, IT audit should be involved in the planning stages to help ensure that appropriate control design considerations are taken into account.

IT audit should have acquired an understanding of the organization's entire ecosystem; it should therefore be charged with bringing additional value across the portfolio. As part of the IT risk assessment and formulation of the IT audit universe, collaboration between these three functions—audit, IT and security—allows for risks to be identified and managed collectively. IT audit can work strategically as an advisory group that goes where risks reside or are emerging, partnering with IT, understanding security risks and tailoring the audit plan accordingly without limiting itself to "boilerplate" audits. Too often IT audit has executed these boilerplate efforts, engaging in general control reviews that are effective for certain basic compliance exercises, but fall short of the needed risk-based approach. For example, robust IT audit functions may consider conducting internal audits or participating in projects in areas of emerging threats such as social engineering controls or medical device security.

### Moving beyond IT general controls and compliance: A partnership model

One of the biggest values that executives cite from having an IT audit function is that it serves as the eyes and ears of organization leadership. Therefore, it's important for IT audit to have a close relationship with IT security to understand current initiatives and target audits based on the specific risks that emanate from those projects instead of taking a more generic approach to risk identification.

Many health care organizations place information security in one silo and IT audit in another, with the two not effectively engaging or collaborating. A classic example is IT security implementing new cutting-edge tools such as security information and event management (SIEM) appliances while leaving IT audit out of the conversation. There is a mismatch between what the IT auditors are looking at and what IT security is planning to implement, and that can result in vulnerabilities and suboptimal audit insight. Worse, this results in audit assessing risks without considering IT's perspective on risk and the planned management of the threats.

Instead of working in a silo to evaluate risks to consider over the next six to 12 months in a tactical audit plan or simply checking off a list of compliance activities or general systems audits, a partnership model should be employed. This partnership model should provide a more targeted and comprehensive approach based on technology risk across the enterprise, involving both IT security and IT audit. Organizations employing this partnership model between the information security and IT audit functions will not only more easily maintain HIPAA Security Rule compliance, but will also be much nimbler in identifying and proactively mitigating tomorrow's emerging security threats.

## IT risk assessment to drive audit planning

Organizations must undergo a certain level of risk identification and quantification in order to select the optimal audits. A risk assessment is the very first requirement of the HIPAA Security Rule, and seeks to identify threats or dangers to the confidentiality, availability or integrity of sensitive information. It's typically a broad exercise, because it must encompass the entire scope of people, processes and technology that can be threats to the security of ePHI. An organization can achieve a powerful understanding and documentation of risks by combining the tactical inventory of risks required by HIPAA and often managed by IT, with the organizational perspective of risk insight provided by internal audit.

Areas identified as high risk may be reviewed more often than lower risk areas. For example, a high-risk area should be part of an annual audit plan. In contrast, a medium-risk area may only need to be reviewed every 18 months and a low-risk area may need review every two years. Of course many risks, and the subsequent audit activities, will emerge in real time and be integrated into the audit plan throughout the year.

Health care organizations often keep and transmit information on laptops, so a high risk may be the threat of a lost laptop containing ePHI. As the risk assessment proceeds, organizations must identify countermeasures, and how they address the risk. For example, a common strategy is encrypting laptops, and then making sure that control is implemented and it is free of any obvious errors.

Following in the footsteps of the risk assessment, an IT audit should evaluate the strength of laptop encryption. Is it effective enough to stand up to current threats? Is it being managed properly? Are the processes in place to maintain compliance? Do the processes align with the documented policy?

In addition to the risk assessment, many health care organizations are not aware they must also undergo a HIPAA compliance assessment. Section 164.308(a)(8) of the HIPAA Security Rule mandates that security safeguards are evaluated either internally or externally.

While the risk assessment is a high-level look at risks to protected information in an organization's environment, the compliance assessment considers the established criteria within HIPAA and the audit procedures to verify whether the organization meets the specified criteria from all three HIPAA rules. The risk compliance assessment provides an organization with an "OCR Audit Readiness" perspective and should leverage the OCR Audit Protocol.

Per the regulations, HIPAA risk assessments must be performed and updated by an organization once a year at a minimum. To gain more value from the required risk assessment, the IT audit group can also further leverage that information. Even though it is not all encompassing, if the assessment is done well, it will provide a significant level of detail that highlights assets, threats, vulnerabilities, controls and residual risks within the areas that it does cover. While it can't be used as the complete IT audit risk assessment, it can be a powerful tool to provide greater insight and save time during that process.

Unfortunately, the IT audit risk assessment and the HIPAA risk assessment are often not coordinated well. In some cases, IT audit may not review or leverage the HIPAA risk assessment, and key information is discovered in the assessment by compliance only after a breach has occurred. Therefore, a leading practice is for organizations to utilize the HIPAA risk assessment as a component of broader enterprise risk management (ERM), made available and leveraged as needed by various stakeholders throughout the organization, especially by IT audit.

## A practical walk-through

To begin to implement a more formalized and effective framework for HIPAA compliance and greater organizational security, the first step is establishing a strong tone at the top. Organizations need executive buy in to implement ERM processes and drive a new line of thinking that health information security is a business problem and not just a technology problem.

The importance of the risk function must be elevated, including risk identification, management, measurement and response processes. In addition, the internal audit function must also be assigned a significant degree of priority in these conversations, with an honest assessment of the organization's ability to act on the risk assessment, and manage and respond to risk. While organizations may not be prepared to implement an ERM program, integrating current risk assessment programs, such as the IT audit annual risk assessment and the HIPAA required risk assessment, will provide value to both programs.

Organizations must fully understand the risks to their environment and their security capabilities, in coordination with the IT group's understanding of risk. They then have to encourage the implementation of a framework or a set of standards that equate to thorough security measures and support the investment in these measures.

An organization's IT audit group must have an appropriate scope for reviews. If they only evaluate a third of the environment because that is what HIPAA requires, the organization may be compliant, but not have a strong security environment. Ultimately the weakest point in the security model may produce a breach that is enterprise-wide.

Finally, an organization should choose audits collaboratively in a partnership model with input from the CISO and IT group and an understanding of where IT audit can add the most value and help security capabilities mature. This process also helps build a stronger relationship between the IT group and the IT audit group.

For example, instead of the IT group independently deciding to implement ISO and choosing specific controls or IT audit performing an ISO audit, the process should be collaborative. IT audit should consult IT and the CISO when considering the biggest potential risks to the organization and the IT group should consult audit in the selection of a framework and the implementation plans.

After discussing the risks and benefits of potential audits, the parties should work to ensure enterprise alignment on the selection of audits (although the internal audit group must retain its independence and objectivity). Alignment of IT risk identification and management with the organization's overall strategy is crucial.

## Conclusion

The recent rise in HIPAA sanctions against health care organizations and data breach and ransomware media coverage is a stark reminder of the importance of effective data security. Unfortunately, many organizations lack effective security controls and processes and are susceptible to significant fines amid a more aggressive enforcement environment. Others may be HIPAA compliant, protecting against those risks, but exhibiting security deficiencies in other key areas of the enterprise that could be damaging.

When managing HIPAA compliance demands, health care organizations should not lose sight of the importance of a holistic view of information security. Compliance is important, but the overall security of the organization is the goal. When properly executed, implementation of an information security management program will address all related regulatory requirements, including HIPAA.

As health care environments become more integrated and technically sophisticated, proactive and thorough security measures are critical for reputational, financial, operational and patient safety reasons. If deficient organizations do not address their environments, a breach or a regulatory review will eventually force this security measure. Data supports that it is far costlier to react to security issues than to invest in the development of a mature program.

Regardless of an organization's data security processes and controls, several strategies can be employed to better secure the environment. Implementing an existing, formalized framework can help strengthen security measures and align with HIPAA compliance demands. An effective, formal program also elevates the role of the security officer and increases the visibility of risks and can open the lines of communication between IT, internal audit, information security and executives.

Indeed, one of the most effective steps a health care organization can take to manage organizational risk is to increase collaboration and alignment between IT security and IT audit. A stronger partnership between the two roles brings more consistency to risk management initiatives, and it allows the organization to manage HIPAA compliance risks and general controls while also taking a broader view of enterprise-wide risk.

## Key takeaways for critical risk functions

| | |
|---|---|
| IT  | – Keep a thorough and current risk assessment in full compliance with the HIPAA Security Rule.<br>– Leverage internal audit and the skills of internal audit to evaluate security investments and strategies. |
| Information security  | – Holistically frame the scope of security issues from an enterprise, business and operations standpoint.<br>– Focus on all aspects of security risk to the organization and at all levels, not just at the administrative level, but also at clinical levels.<br>– Leverage internal audit to evaluate security performance and programs. |
| Compliance officers  | – Don't underestimate the complexity of the Security Rule; be more connected with the CISO and understand the organization's risk assessment and how effectively the Security Rule is being implemented within the environment.<br>– Don't neglect preparations for the HIPAA Breach Notification and Privacy Rules. |
| Internal audit  | – A holistic risk-based approach should frame the selection of internal audits, not traditional focus on IT compliance and IT general controls.<br>– With the comprehensive view of the organization, serve as the driver in the partnership model with IT security.<br>– Drive the collaborative risk assessment and risk management process through the organization. |
| Audit committee  | – Ensure there is oversight and measurement of identified IT risks and risk identification is a collaborative process with IT, internal audit, operations and clinicians.<br>– Hold people accountable for remediation efforts for the gaps that have been identified.<br>– Understand and communicate the HIPAA compliance assessment is not all encompassing of your information security risks and capabilities. |

## Prepared by:

Greg Vetter, Director, RSM US LLP
greg.vetter@rsmus.com, +1 212 372 1624

Adam Harpool, Manager, RSM US LLP
adam.harpool@rsmus.com, +1 212 372 1773

Adam Keagle, Manager, RSM US LLP
adam.keagle@rsmus.com, +1 312 634 5352

Jonathan Dreasler, Supervisor, RSM US LLP
jonathan.dreasler@rsmus.com, +1 563 888 4113

**AHIA**

Todd M Havens, Chair
(610) 805-8458
todd.havens@vanderbilt.edu

Mark Ruppert, Publications Committee Chair
(323) 866-6900
Ruppertm@cshs.org

David Stumph, Executive Director
(888) ASK-AHIA (888-275-2442) xt.6111
dstumph@kellencompany.com

Dennis Smyser, Board Liaison
Dennis.Smyser@Brooksrehab.org

Michelle Cunningham, Account Executive
(888) ASK-AHIA (888-275-2442) xt.6120
mcunningham@kellencompany.com

Linda McKee
(757) 455-7777
lsmckee@sentara.com

Michael Fabrizius
(704) 512-5900
michael.fabrizius@carolinashealthcare.org

Mark Eddy
Nashville, TN 37203
mark.eddy@hcahealthcare.com

Debi Weatherford
(770) 801-2566
debi.weatherford@piedmont.org

**About AHIA**

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced health care internal auditing professionals who come together to share tools, knowledge and insight on how to assess and evaluate risk within a complex and dynamic health care environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of health care internal auditors with executive management and the Board. If you have a stake in health care governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network.

**+1 800 274 3978**
**www.rsmus.com**



WP-NT-RAS-HC-0116

ahia
Assoc. of Healthcare Internal Auditors

RSM