Cloud risk 101 for health care internal auditors

Authors: Liz Norton, CPA, CISA and Arthur Sellers, CISA, CCSK, CRISC

In today's post-pandemic environment, health care organizations are challenged more than ever to deliver patient care and support business functions through flexible, high-quality solutions that are also affordable. Many health care providers are deploying new digital technologies to provide connectivity and health care options that meet the expectations of a modern patient-consumer. However, this increased reliance on patient engagement, accessible information and robotic medical devices introduces threats that cannot be ignored.

Data privacy violations or lack of system availability for connected medical devices could have serious consequences for the health care provider. In this white paper, we will present key risks associated with the use of cloud technologies and explain how health care internal auditors can play a critical role in protecting their organization at any stage of the cloud adoption journey.

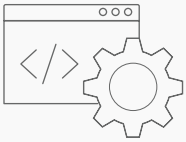
What is the cloud?

Organizations have been using cloud computing in some capacity since the internet was first introduced, but the term cloud computing was only coined in the past 20 years. Cloud computing refers to enterprise resources that are accessed through an internet connection, ranging from accessing email on a mobile device to performing surgery remotely. Cloud service providers (CSPs) continue to expand their offerings in response to shifts in business models, while cloud service customers (CSCs) have shifted from internally developed and maintained resources to greater reliance on service providers.

There are two main cloud offerings, private and public. Organizations using a private cloud are responsible for owning, operating and maintaining all equipment, but may utilize a data center company to host all of their infrastructure in a secure location. CSPs offering a public cloud provide on-demand computing resources available for anyone to purchase. Basic public cloud services are available in the following formats:

Infrastructure-as-a-service (IaaS)
Infrastructure hosted by a CSP that organizations can use for storing and processing data in place of organization-specific servers and databases

Platform-as-a-service (PaaS)
Platform offered by a CSP to enable companies to develop custom applications and programs for company use



Software-as-a-service (SaaS)
Front-end applications provided by a CSP based on a subscription model for consumption through the internet

The majority of organizations use some form of public cloud. The most common cloud providers are Amazon (AWS), Microsoft (Azure) and Google (GCP). However, VMware, Oracle and Alibaba are cloud providers that your organization might also be using depending on your global presence or SaaS requirements. It is critically important to remember that the user organization's responsibilities differ based on the service(s) used and the specific provider agreement. Common responsibilities if Microsoft is used are depicted below:

	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network controls	Microsoft	Shared	Customer	Customer
	Operating system	Microsoft	Microsoft	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical data center	Microsoft	Microsoft	Microsoft	Customer

Microsoft Customer Shared

Source: Microsoft

ahia
Assoc. of Healthcare Internal Auditors

RSM

Cloud environments in health care

Because of the complexity of the health care system and the robust regulatory requirements providers are subject to, there continues to be hesitancy to adopt cloud technologies requiring the migration of sensitive patient data. As a result, early adopters within the industry started moving business applications, such as human resources, email, desktop as a service and operational data to the cloud as a first step. Cloud offerings for critical health care applications, e.g., electronic medical records (EMRs), have provided organizations with HIPAA-compliant solutions, which increased industry willingness to migrate.

Furthermore, many providers and players in the health care space have plans to significantly increase their deployment of cloud technologies over the next five years. Cloud technology can enable patient engagement through synchronized media channels (phone, app, chat, interactive voice response, web) and can support data-mining capabilities to build an end-to-end view of the patient relationship and patient medical needs. These cloud enablers facilitate personalized experiences, improve patient outcomes through more frequent and effective patient interaction, and help providers to identify and connect with new consumer members.

One of the most noteworthy applications of cloud technology within the health care industry involves the home health model. Health care researchers estimate that nearly 70% of routine appointments do not require face-to-face interaction with a doctor. The ability to provide telehealth services on a large scale and at high availability has the potential to produce significant cost savings for providers while reaching a greater number of patients. Another important benefit for home health? Patient empowerment tools—cloud-hosted applications that help those with chronic health conditions monitor and manage their day-to-day care. Things like nutrition, exercise, medication and post-hospitalization care reminders, and blood glucose monitoring can be easily tracked through cloud-based applications, which can then provide doctors valuable data to direct and improve patient care and outcomes.

With the large, ever-increasing volumes of data that health care organizations handle and process, the cloud is an option that is both flexible and scalable. Cloud services offer affordable data storage that can scale up or down depending on the current need and high processing power to support health care functions ranging from records retention and imaging to data-intensive analytical DNA sequencing. Having data in the cloud can also help facilitate a smooth transition between consultation, treatment, insurance and payments.

The opportunity to improve patient outcomes and optimize administrative efficiency through cost-effective technologies will continue to drive the health care industry's move to the cloud.

Cloud governance critical risk areas: Common pitfalls and best practices

Two of the top concerns of any organization are managing cybersecurity risks and effectively demonstrating compliance with regulations. Cloud governance is fundamental to securing cloud systems supporting business-critical processes and managing risks holistically. In the section to follow, we present key risk areas to consider in evaluating your organization's cloud governance and its ability to safeguard data assets. Although we will cover some of the broader categories of information technology governance, our discussion will focus on the appropriate integration of attributes specific to cloud technology risks.

Internal audit insight:

Often, organizations fail to identify and effectively mitigate risks associated with cloud technologies because control processes are assumed to be the responsibility of the CSP. Even when a service is outsourced, your organization is still ultimately responsible for the safeguarding of your IT assets and your customers' data. Remember, you can outsource the process, but you cannot outsource the risk! Keep this principle in mind as we consider each of the risk areas in the discussion below—no matter what cloud services you are or are not using, your management is responsible for effective monitoring and governance.

Information (cloud) technology asset management

Every risk management strategy starts with understanding what you have in your environment and what you can do to mitigate risks while still enabling the business and culture of the organization. Without a complete and accurate inventory of IT assets, an organization may fail to implement sufficient safeguards (i.e., controls) given the level of criticality of an asset. The lack of asset management controls and tools increases the likelihood of asset mismanagement, including unauthorized use of cloud technologies, and inefficient allocation of constrained IT resources. For an organization intending to increase its adoption of cloud technologies, the lack of readily available information makes it challenging to evaluate the feasibility of migrating the data or workload to a cloud environment.

Internal audit insight:

With the disparate use of systems across related health care entities and the complexities of migrating to a cloud environment, many health care IT organizations lack confidence in the ability to completely and accurately inventory cloud assets. Reliance on automated tools to confirm network architecture and data flows can provide visibility and is an effective way of maintaining asset inventories.

In developing formal asset and data management programs, management should consider the following:

- **Cloud providers** – Understand what cloud providers your organization is using and their use cases.
- **Cloud environments per provider** – Each cloud provider managed and used in your organization can be composed of multiple cloud environments, or "accounts." Each cloud environment needs to be analyzed and categorized based on its use-cases, criticality, resilience, security and regulatory requirements.
- **Cloud services per environment** – Each cloud environment is composed of services or workloads. Each workload can have different owners/risks, use cases, data types, resources and access type (public-facing, restricted, internal, private, etc.).
- **Leverage** – Use existing capabilities to establish a centralized IT asset inventory (you may have tools such as ServiceNow tool's configuration management database or CMDB). A software tool can track hardware assets and applications, and the configuration management database can be built out to include relationships between applications and the supporting infrastructure (databases and servers), an identified owner, identification of vendor-managed and/or cloud assets, and tags to identify assets which process or store critical data.
- **Other tools** –Use other automated tools to scan network devices and traffic, to identify cloud technologies in use (or any IT assets) and true-up the CMDB and data flow diagrams (DFDs)—for example, a cloud access security broker (CASB) or the Qualys scanning tool.

Internal audit insight:

The need to rely on automated monitoring tools is a theme throughout this discussion on cloud risk. These environments are so complex and vast that it is impossible to rely on manual monitoring alone.

Data management

Patient data is sensitive and valuable, and data privacy violations can potentially have serious consequences for the health care provider. Financial data or the organization's intellectual property are also critical assets for health care providers. As mentioned in the previous section, adopting a data management strategy is a critical step in developing an effective cybersecurity program. An organization must understand its data, how it flows and apply controls to reduce the likelihood of leakage, compromise or fines by regulatory bodies.

Formal data classification standards will enable management to prioritize systems based on the sensitivity of information. At a minimum, specific labels (public, nonpublic, HIPAA, PCI, etc.) for data should be identified to support the prioritization. Management can utilize the classifications to identify key data sets and implications for moving from one environment to another.

Internal audit insight:

Data classification should drive critical business requirements when building out an end-state cloud environment. For example, electronic protected health information (ePHI) will need to be stored in a HIPAA-compliant cloud. As such, it imperative that the classifications are appropriately designed, defined and applied to data sets.

Data flow diagrams facilitate a complete and accurate understanding of where data assets are held at rest, and the connections through which critical data traverse the internal and external networks. Data flow diagrams should indicate if a system is hosted on-premises or in the cloud. Use data flow diagrams to identify endpoints requiring additional security controls and monitoring (i.e., traffic entering/leaving the internal network).

A complete data management program will also define data ownership and data custodians with their associated responsibilities and will prescribe a process to formally destroy data hosted on-premises and in the cloud. As related to cloud adoption, determine interoperability requirements for cloud workloads prior to migration to validate data can be viable on a separate cloud platform.

IT procurement and vendor risk management

For a majority of organizations, non-IT operations personnel are responsible for identifying solutions to meet enterprise objectives, which include the expanding incorporation of cloud technologies into existing business functions. Generally, business users work with a vendor management or procurement team to evaluate and select product/service providers and to work through contract execution. If a business (or any) user requests the procurement of a cloud product/service, it is critical that an evaluation following a specific risk assessment is completed in tandem by the business user (as applicable) and the IT security team to ensure the solution meets organizational requirements.

Templates for service agreements should include specific provisions for the return of hardware and data, access to data logs and ability to monitor activity logs, downtime required for upgrades and changes affecting availability of the service, and business continuity. Contract language for outsourced technology products and services should also include a specific addendum covering the required information security standards agreed to by the provider.

Organizations may develop the inherent risk assessment criteria using a cloud risk framework such as Microsoft Cloud Decision Framework, European Union Agency for Cybersecurity (ENISA) or CARAM, or perform a review of questionnaires answered by CSPs and publicly available in the CSA Security Trust and Assurance Registry (STAR).

Internal audit insight:

Service agreements between CSPs and CSCs can be extremely complex. RSM's methodology includes 20 high-risk provision areas to be assessed prior to executing a CSP contract. Engage subject matter experts upfront to limit your organization's exposure to financial, operational and data security risks.

At a periodic frequency determined based on the risk associated with the service, management will need to perform monitoring control activities to reassess the risk of conducting business with the vendor, to evaluate the vendor's adherence to contractual terms and service-level agreements, and to review independent auditor attestations over the provider's internal controls. We expect high-risk or critical vendors to be evaluated at least annually, moderate-risk vendors every eighteen months to two years, and low-risk vendors every three years. However, management's review of attest reports should occur annually.

Internal audit insight:

The primary reason monitoring controls fail is lack of established roles and responsibilities for activities throughout the contract life cycle. Who ultimately owns the broader vendor relationship as well as each individual contract? Who monitors vendor performance and what is the process to escalate for lack of adherence to service level agreements (SLAs)?

Who is responsible for reviewing third-party attestation reports for cloud vendors? For reports with user-entity controls outlined, who is responsible for identifying and implementing those controls? Are vendor management, IT and the business contract owner collaborating throughout the life of the relationship, and are all parties accountable for their role in managing the vendor?

To support the oversight of vendor monitoring activities, data related to contract management such as the executed contract, risk assessment and monitoring documentation should be retained in a centralized repository. As enterprise requirements change, contracts and SLAs may be revisited to ensure the service provider is meeting organizational needs. Changes to vendor risk based on monitoring routines should be tracked to determine if the risk associated with the vendor remains acceptable.

The usage of contractors, outsourced vendors and other third parties will require management to develop business associate agreements (BAAs) to ensure compliance with HIPAA. These agreements need to be in place for any individuals not currently employed by the organization who will be accessing protected health information. The Office for Civil Rights may fine enterprises that do not have these in place despite not having a breach or incident.

Example evaluation of technology vendor selection

Management teams have a considerable number of factors to evaluate as they choose between CSP offerings. As a practical example, below is a comparison between two different offerings and some questions that should be considered when making a decision between different CSPs.

Exhibit 1: CSP A

- SaaS solution with 99.99% uptime, which equates to slightly under five minutes of downtime per month
- Price: $300 per month per instance

Exhibit 2: CSP B

- SaaS solution with 99.999% uptime, which equates to less than one and a half minutes of downtime per month
- Price: $500 per month per instance

In evaluating the CSPs, management should consider the following questions below to determine what level of service will be needed:

Considerations
Maximum tolerable outage – Is there a baseline outage threshold in place for the environment or is it variable?
Management risk appetite – What risks are found in the environment and how could downtime exacerbate those risks?
Cost – Is there a maximum budget in place?
Usage – What will the cloud environment be used for? Is the processing critical or can increased downtime be tolerated?
Regulatory requirements (health care perspective) – Are there regulatory requirements in place that require a significant amount of uptime for data access?

Vendor management will need to determine if the extra $200 per month is necessary based on IT's requirements for the application being hosted, operation's identified maximum tolerable outage and management's risk appetite. If a critical ePHI application is being hosted by a cloud vendor, then the extra cost may be warranted, but if the application is a reporting tool used on a weekly basis, the wiser choice will be to allow five minutes of downtime.

Cloud adoption strategy

Cloud services are becoming increasingly vital to expanding the role of IT operations, enhancing data security and improving the overall patient experience. Organizations must balance the need to modernize IT environments at a rapid pace with the parallel objective of managing financial, operational and compliance risks. Without following a systems development life cycle or organization change management process providing the road map for the adoption of cloud services, technologies may be purchased and implemented without appropriate consideration of user requirements or compatibility with the current and planned IT environment. Even worse, inappropriate system changes could result in a loss of availability or potential for security vulnerabilities. Management will need to consider risks specific to cloud migration such as encryption of data being migrated, access to appropriate technical and business user SMEs and ongoing support personnel, training of risk and control owners who are managing or using the cloud technology, appropriate evaluation and selection of SaaS providers, and project management/monitoring controls over vendors assisting with implementations.

Internal audit insight:

Is your organization planning to increase reliance on cloud technologies in the near future? Ask to see a migration readiness plan; you'll learn a lot!

When designing a future-state cloud-enabled technology environment, two of the most important cyber-risk mitigation features to consider are the architecture and compatibility with automated security monitoring tools.

- **Architecture**
  Architecture is the cornerstone of cloud governance, risk management, security, cost-management and resilience. A secure architecture enables companies to have a controlled and well-managed cloud. Often, organizations cannot efficiently implement all resilience, cybersecurity or regulatory requirements in the cloud without a strong supporting architecture. As mentioned in the data governance section, focusing first on your crown jewels, or critical data assets, is important to comply with your cybersecurity and regulatory requirements. Organizations often demonstrate a focus on protecting sensitive data through segmentation and zero-trust architectures which include a landing zone or secure enclave strategy to segment workloads, data and logical access appropriately.
- **Automation**
  One of the biggest benefits of using cloud environments is enabling cybersecurity, agility and scalability with automation. Automation allows IT and cybersecurity teams to transition from routine tasks and devote more time and resources to strategic initiatives that create competitive advantages. With automation and a security-by-design culture, companies can focus on competing, meeting their business objectives and quickly moving major initiatives. Automation begins before your team deploys a new cloud workload. With automation reducing security and compliance risks, your team can address most issues prior to deployment in production and throughout the life cycle of the product or process. The other advantage of a security-by-design and an automation-first approach is that a security and configuration baseline is created in production environments. This enables monitoring solutions to alert on any anomalous change and remediate security or configuration issues automatically.

Disaster recovery and business continuity

An inability to appropriately identify and prioritize critical processes means delayed or ineffective recovery of operations in the event of a disruption. In developing a business continuity program, management should consider the following:

- Validate cybersecurity considerations and make sure they are incorporated so that management can identify reliable IT processes.
- Validate vendors so they are identified and documented in order to enable coordination with critical third parties.
- Determine the maximum tolerable outage from a financial perspective for nonpatient-facing services.
- Determine patient-care downtime levels. Some services delivered over the cloud may be a component of patient care and limited (if any) downtime may be allowed. This should be formally documented to ensure patients continue to receive necessary care.
- Foster communication between business units and IT to ensure identified recovery time objectives (RTOs) and recovery point objectives (RPOs) are reasonable and achievable.
- Define cadence for business-wide training to ensure coordination, completeness and understanding of the plan. Business impact analysis should be performed for critical vendors and bank operations to understand the RTO/RPO requirements for all functions.
- Evaluate critical processes across the enterprise in a business impact analysis and tier based on order of importance to develop a critical path to recovery IT assets.
- Determine if manual processes can be used in the event of a system-wide failure.

Internal audit insight:

A well-thought-out program won't fix any problems if it doesn't actually work in practice. It is important to test the BCP plan through tabletop exercises and to complete restore testing from end to end. Often, we see IT performing test exercises in a silo. Not including business users with precise knowledge of the data sets and system functionality has allowed downstream issues with data integrity to go undetected. Third-party vendors should also participate in testing exercises to ensure their ability to meet recovery objectives timely.

Continuous monitoring through automated scanning

Misconfigured cloud services affect data confidentiality, integrity and availability. Attackers can look for misconfigurations and vulnerabilities to gain access to data and internal networks or carry out further attacks against organizations and associated third parties. For health care providers, Internet of Things (IoT)–connected medical devices can be more vulnerable to hacker attacks because they may lack defense mechanisms and capabilities. Implementing a continuous monitoring process to identify connected devices, misconfigurations and vulnerabilities on cloud workloads reduces the likelihood of compromise. Often, organizations implement continuous monitoring in cloud environments while applying the secure-by-design model before deploying any workload. Using these two concepts, organizations can mature their environments faster and reduce security, regulatory or resilience risks.

Internal audit insight:

Automated, continuous monitoring of technical security configurations is critical to support compliance with regulatory requirements and best practices. Leverage SMEs to help execute scans, evaluate results and design customized remediation strategies. The use of automation allows monitoring of 100% of a population of IT assets, and it is imperative that IA embraces the use of automated tools and shifts away from the manual sampling approach. Additionally, performing a periodic assessment over the configurations of a cloud service will limit the potential for a successful attack.

Identity and access management

Identity and access management is a critical component of any organizational security strategy. Identity is the constant interface to organization resources and is a primary target for cybersecurity threats. With traditional network boundaries gradually dissolving by the growth of cloud, remote workforce and digital technologies, identity and access have become the first line of defence and an increasingly critical security capability for organizations. Foundational security requirements like single sign-on, multifactor authentication, individual user accounts and password/key rotation of application identities are must-have configurations critical to manage cyber-risk and compliance. Implementing these foundational requirements is only the beginning of organizations' cloud journey.

Managing corporate, application, client and vendor identities in the cloud and their interactions with other environments is where the real complexity starts. Often, organizations use legacy on-premises systems to manage employee and internal system identities, but also use cloud-native tools to manage clients, vendors and internal systems and groups connecting to cloud services to meet business goals. Here is where identity governance and administration (IGA) can help. IGA underpins secure and efficient technology and business operations, providing users, devices and processes with appropriate access to conduct daily operations. Crucial components of effective IGA include maintaining accountability for access-related decisions and timely addressing changes in responsibilities. The identity governance program is responsible for defining what constitutes an organizational identity and the relevant governance processes, workflows and certifications to protect access integrity. The program should be aligned with the organization's needs as well as incorporate the relevant regulatory and standards compliance requirements.

Finally, controlled privileged access remains one of the strongest preventive measures to significantly slow an attacker's advance on your technology environment. In a world of Ransomware-as-a-Service, limiting access to accounts that control the keys to the kingdom removes one of the most successful tools in the hacker's kit, raising a significant barrier to their progress. These individuals often take the path of least resistance and will move on to another target. Privileged access management helps to improve your internal security posture. It is also an effective way to control third-party access into your environment, which is another popular attack vector for adversaries.

Internal audit insight:

No matter who provides the software or the cloud, you will still always be responsible for who you allow to access your IT resources. Implement access administration controls for all hosted systems, including cloud (AWS, Azure) accounts.

Enterprise risk management

Senior leadership and board members require sufficient details over key risks and priorities to support adequate decision making and optimized allocation of IT resources (people and monetary funds) in support of enterprise initiatives. IT leadership should implement a formal process to periodically evaluate changes to the regulatory landscape, major IT initiatives, and known and emerging risks, and establish a cadence for reporting to executive committees or boards. The risk management program should incorporate processes to assign risk measurements for evaluation against the enterprise's tolerance limits and should require that IT/information systems management determines appropriate actions to address and monitor identified risks. Risks related to cloud migrations and adoption of cloud technologies should be included in management's risk assessments and board reporting. This includes project risk (not meeting deadlines/milestones), resource/skills constraints, misalignment of IT initiatives to overall enterprise strategic priorities, or impacts to planned spend (budget).

Risk identification and control framework

Prior to identifying and implementing controls, management should consider the inherent risks of the systems within their environment based on the results of the inventory and data mapping exercise. Formally establishing a risk appetite, approved by leadership, will reduce confusion when determining the safeguards over data. Without concrete guidance on acceptable risk, appropriate resources may not be allocated to adequately protect systems. Governance practices are challenging to quantify from an operational standpoint, and leadership may be wary of investing time and money into practices that may not increase profitability.

There are several frameworks that management can leverage to identify the appropriate controls to reduce risk to an acceptable level for a cloud implementation. The Cloud Security Alliance (CSA) is a nonprofit organization promoting best practices for security assurance within cloud computing and education on uses of cloud computing (additional information about the CSA can be found online at https://cloudsecurityalliance.org. Their control framework and additional research for performing cloud assessments can be found at https://cloudsecurityalliance.org/research/cloud-controls-matrix). While other organizations (the National Institute of Standards and Technology [NIST], International Organization for Standardization [IOS], Information Systems Audit and Control Association [ISACA], etc.) have adoptable frameworks, the CSA has developed a framework specifically designed for the cloud. Furthermore, they have mapped controls within their framework to provide coverage for organizations that already have controls in place. The most recent cloud control matrix (CCM) includes 197 controls over 17 domains, with some controls that are specific to cloud providers and cloud customers, and others that are shared between the two. Taking a top-down approach to the CCM by identifying core governance controls, moving to technical controls and determining if complementary controls are required will ease adoption.

What now?

As health care internal auditors, we are challenged to support our organizations in their mission to provide the highest standard of patient care while being perpetually compliant with ever-changing regulatory requirements. The industry is increasingly reliant on operational technologies and connectivity with outside partners, and we must be diligent in educating ourselves and our organizational leadership on evolving threats and related risk mitigation strategies. With the trend toward modernization and heavy adoption of cloud technologies delivered through third-party service providers, it is important to focus on the governance controls performed by our organization's management to safeguard our IT environment and push for scalable, automated monitoring of connected devices and their security configurations.

Internal auditors should consider how cloud services are being onboarded at their organization to determine if the current process meets enterprise requirements. For preexisting cloud services, internal audit can include new audits in their plans to evaluate how risk is being mitigated. At a minimum, we suggest incorporating the components of cloud risk into the annual IA risk assessment to determine how to manage risk in the future.

About AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare 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, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. It is meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services.

Interested? Contact a member of the AHIA White Paper Subcommittee:

Alan Henton
White Paper Chair
alan.p.henton@vumc.org

Deborah Pazourek
AHIA Board Liaison
Deborah.L.Pazourek@medstar.net

Linda Greer
lamizgre512@gmail.com

Laura L. Sak-Castellano
Laura.Sak-Castellano@aah.org

Debi Weatherford
debi.weatherford@piedmont.org

+1 800 274 3978
rsmus.com