The New **Healthcare Interoperability** Rules
A Risk & Compliance Perspective

January 2021
Introduction

Interoperability is a regulatory push by the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) that aims to alter the way the healthcare industry shares data by moving from a system whereby healthcare organizations are permitted to share data in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and towards one where healthcare organizations must share relevant information with each other and consumers can better dictate who has their health information and how it is used. The alteration will enable healthcare data to move with customers (patients or members) from provider to provider and from health plan to health plan.

The first set of interoperability requirements affecting health providers, health IT companies, and health information exchanges ("HIEs") will be effective on April 5, 2021. Payer-specific requirements are effective on January 1, 2021, but will be enforced beginning on July 1, 2021, with additional requirements becoming effective during the next two years. (Figure 3)

As payers and providers mobilize to meet the new interoperability requirements, early engagement by risk and compliance teams is critical to building a successful program and establishing control-enabled processes that create value while minimizing risk.

Figure 1. Key requirement summary

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Payer</th>
<th>Provider</th>
<th>HIT Vendor</th>
<th>HIE/HIN 3rd Party App Devs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital ADT Notification</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EHI Exports</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Digital Contact Updates for NPPES</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ePrescribing</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Blocking</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Patient Access API</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provider Directory API</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payer to Payer Data Exchange</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improving the Dual Eligible Experience</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

API = application programming interface, CMS = Centers for Medicare & Medicaid Services, FHIR = Fast Healthcare Interoperability Resources, HIE = health information exchange, HIN = health information network, HIT = health information technology, MMA = Medicare Prescription Drug, Improvement and Modernization Act of 2003, ONC = Office of the National Coordinator for Health Information Technology
Despite the urgency, not all industry participants may be prepared to meet the deadlines. A PwC Health Research Institute executive survey conducted in August and September 2020 (Figure 2) found that almost 80% of provider and payer respondents reported having prepared for new processes and that about half have mapped out their data to understand potential impacts. While the issue is clearly top of mind, more than half of the respondents said they have not yet identified leaders who will be responsible for aligning and governing those efforts across their organization.

Without clear leaders or governing bodies, the risk of gaps in planning and implementation efforts increases as teams press forward—sometimes focused only on their own priorities, whether that involves meeting the minimum compliance requirements or building an architecture to enable future business use cases. In addition, we believe interoperability represents an opportunity to reassess enterprise strategy and develop leading capabilities, and remaining idle may make it more difficult to compete in the future healthcare ecosystem; however, less than a quarter of executives said they view the issue as a strategic opportunity.

**Figure 2. PwC Health Research Institute executive survey, August—September 2020**

<table>
<thead>
<tr>
<th>Interoperability Readiness Activity</th>
<th>Entity</th>
<th>% of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Reviewed business partnerships in this new regulatory environment</td>
<td>Payers</td>
<td>67%</td>
</tr>
<tr>
<td></td>
<td>Provider</td>
<td>68%</td>
</tr>
<tr>
<td>2. Prepared for new processes</td>
<td>Payers</td>
<td>79%</td>
</tr>
<tr>
<td></td>
<td>Provider</td>
<td>79%</td>
</tr>
<tr>
<td>3. Identified a leader</td>
<td>Payers</td>
<td>42%</td>
</tr>
<tr>
<td></td>
<td>Provider</td>
<td>45%</td>
</tr>
<tr>
<td>4. Mapped out your data to see what’s affected</td>
<td>Payers</td>
<td>48%</td>
</tr>
<tr>
<td></td>
<td>Provider</td>
<td>58%</td>
</tr>
</tbody>
</table>

None of the above

Payers | 2%
Provider | 5%

**Figure 3. Interoperability compliance timeline**

- May. 1, 2020 - CMS and ONC Rules Published in Federal Register
- Nov. 1, 2020 - Digital Contact Information must be available in NPPS
- Jan. 1, 2021 - Patient Access API must be available
- April 5, 2021 - Public Reporting and Information Blocking
- May. 1, 2021 - ADT Event Notification must be active
- July. 1, 2021 - Patient Access API
- May. 1, 2022 - ADT Event Notification
- Apr. 1, 2022 - Improving Duality Eligible Expenses - Frequency of Federal/State Data Exchanges
- Early 2021 - Public Reporting of Providers without Digital Contact Information in NPPES

Note: Enforcement can be retroactive to Compliance date.
Which best describes your organization’s view of the new federal rules for interoperability?

<table>
<thead>
<tr>
<th>Response</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>We view them as something we have to comply with</td>
<td>76%</td>
</tr>
<tr>
<td>We view them as a strategic opportunity</td>
<td>24%</td>
</tr>
</tbody>
</table>

Note: Based on a sample size of 153 providers and 128 health plans (281 total).

Risk and compliance considerations

Interoperability will require a cross-functional response from an entire organization to ensure that the right people, processes, and technologies are in place to meet the new requirements. Risk and compliance leaders have the unique role of ensuring that the new or updated capabilities are working as intended and that any risks or issues get quickly identified and addressed. Planning and implementation efforts are underway at most organizations aiming to meet the rapidly approaching compliance and enforcement deadlines, but time is short. Programs that embark on a pathway without the involvement of their risk and compliance functions often face challenges and incur costs that could have been avoided, such as (1) misinterpretation of the requirements, (2) gaps in controls and (3) new processes and technologies that didn’t consider the broader universe of state and federal laws, thereby exposing the organization to unintended issues, including reputational, financial, and compliance risks.

This paper sets forth key risk and compliance considerations for affected entities across the following five dimensions that we see as critical in the implementation of a successful interoperability program.

Strategy & Governance
Overall enterprise goals for interoperability compliance and capabilities

Compliance, Security, & Privacy
Interoperability requirements, privacy, and security

Program Design
Program management to coordinate cross-functional delivery teams, decision making and escalation, and performance tracking

Technology & Data
Data ingestion, integration, and sharing considerations, including controls and infrastructure

Operational Readiness
Process and workflow changes to comply with regulations and develop additional business value
Strategy & Governance

Leading healthcare companies are viewing interoperability as a key enabler of their enterprise strategy. As each member’s healthcare information will soon move with them, capabilities that can quickly absorb and interpret that content to deliver differentiated experiences will be crucial.

PwC’s own market experience confirms interoperability is more than a core compliance concern and carries deep strategic implications. Understanding the impact to strategy will require a holistic review that takes into account an organization’s market position, explicit and implicit business priorities, applicable use cases, and acceptable risk tolerances.

Independent of the interoperability strategy pursued, bringing the right stakeholders to the discussion early is key to minimizing unexpected risk while preparing the organization for the risks it is ready to manage.

A fast follower action is the creation or adaptation of the right governance model that aligns stakeholders. This will oversee the program structure that coordinates and prioritizes planning, funding, integrated roadmap and implementation that meets both compliance and strategic requirements.

Defining value measures and key performance indicators (KPIs) for compliance and business outcomes will also help an organization monitor progress toward key milestones and clearly demonstrate success stories that drive broader adoption.

Further, as an organization moves further down the implementation roadmap, risk teams should stay close, providing input and advice as decisions get made regarding technology, processes, controls, and monitoring. Successfully engaging and aligning a broader stakeholder group early on can help ensure that the overall interoperability response gets carefully managed, adheres to strategic guiding principles, and demonstrates success through measurable outcomes.

One regional health plan decided to use interoperability as a strategic differentiator; by including business teams in the design of its interoperability infrastructure, the plan ensured that the infrastructure properly delivered business value by enabling specific use cases that benefited from new information and capabilities.
Program Design

Beyond establishing a technical infrastructure and capabilities, many activities across business functions are needed to support adherence, minimize risk, and achieve desired outcomes. Examples of such activities are the updating of privacy policies, the enhancement of consent management capabilities, development of customer educational materials, changes to service-level agreements with existing vendors, the creation of KPI dashboards, and the formulation of an onboarding process for third-party developers wanting access to data through the new APIs. As with any large, cross-functional initiative, setting up a formal program facilitates project planning and management, stakeholder involvement, and visibility at the executive level.

Setting up a successful program starts by establishing a core management function that can inventory and coordinate all of the in-flight projects affected, new projects needed, and any dependencies, synergies across the portfolio, and risks. Some aspects of the rules are somewhat ambiguous, requiring compliance and/or legal involvement to confirm terms and establish common understanding. Next, aligning on an integrated work plan, a delivery method, and ways of working can provide both flexibility and visibility across all projects and teams—and help identify risks early. Securing the internal and external resources with the right skills may be a challenge, making capacity bottlenecks a risk that should be closely monitored.

Clients we have worked with have set up programs that include cross-functional teams with IT, risk, compliance, and business representation.
Operational Readiness

Interoperability requires buy-in and commitment from all business areas. Policies, processes, and procedures will have to be updated. And personnel, including physicians, will require training at the appropriate time. Both employees and customers will have to be educated on the benefits—and the risks—of sharing data, whether among providers and payers or among patients sharing data with third-party apps.

Customer-facing employees will have to be prepared to answer inquiries around privacy rights, consent, and even recommended apps. They will have to know how to update consent selections, how to address completeness and accuracy issues identified by the customer, and how to communicate the reason specific access requests were denied or information was omitted.

The introduction of new business activities and third-party developers will require new processes for (1) assessing the risk of permitting access to APIs, (2) providing the appropriate level of documentation and support for those developers, and (3) sufficiently documenting activities or events that could be interpreted as information blocking. Most providers say they believe that EHR vendors would handle most such activities, but EHR vendors may not account for all requirements. Multiple functions will certainly have roles in measuring and monitoring adoption, performance, and compliance. Defining an operating model and a change management plan with risk and compliance in mind will help an organization become ready to support the business and its customers as it adjusts to this industry wide transformation.

In addition, hospitals will have to send electronic patient admission, discharge, and transfer event notifications to other healthcare facilities, community providers, and practitioners, which will improve care coordination, but processes and workflows will have to be designed and implemented for utilization of the notifications in meaningful ways.

Interoperability is expected to increase staff productivity and reduce costs by eliminating administrative burden on providers and payers, by facilitating value-based care delivery, and by accelerating the adoption of value-based reimbursement models. Organizations we have worked with on interoperability strategy and readiness have typically identified more than 50 use cases to drive business value.
Technology & Data

Accessible, reliable data constitutes the fuel that powers the benefits of interoperability. The infrastructure that organizes, moves, and protects data is what is needed to turn that fuel into real value for businesses, consumers, and the broader community.

The designing of capabilities that enable the future scalability and retrieval of multiple data types and sources will be at the forefront of this infrastructure. Standard protocols must be implemented to avoid human errors as well as data breaches by bad actors. Audit and risk teams can support that work by helping identify—within the planned infrastructure and in the development of controls and process—the potential soft spots that increase risk.

Interoperability will push providers and payers to better manage and share existing data and to encourage the integration of information—including member and patient matching—from an increasing number of outside sources. As data becomes more portable, the number of data-generating sources to enrich the customer experience and, ultimately, health outcomes, also increases. For example, the ability to incorporate data from a new member’s previous health plan and wellness apps can lead to more-successful care plans from day one. The possibilities of incorporating lifestyle, social, and mobile health data to enhance benefit and care management, ancillary services, and cost-benefit sharing mechanisms are all parts of a truly transformed customer health journey.

Upcoming regulations require that data be made available faster and be more reliable. Claims, encounters, and clinical data maintained by payers must be made available to customers within one business day of processing—regardless of whether the plan or a delegated vendor adjudicated the claim. Although the rule specifies the required timelines of making data available to members or exchanges, it does not prescribe the timelines of sharing between delegated vendors. We recommend that processes and service-level agreements with delegated vendors be aligned to meet the

A multiregional insurer faced disparate data sources with unique and complex formats, the inability to reuse existing investments, a lack of clinical data integration, and significant technology debt. Their journey toward interoperability was led by a team that included IT, risk, compliance, and business members. The team designed a future-state architecture that accounted for new data source ingestion and data integration that both addressed timeliness requirements and enabled business use cases. By taking a comprehensive approach and achieving cross-functional buy-in, the insurer was able to overcome its initial challenges and realize the value of data and technology solutions designed for the whole business.
interoperability timeliness requirements and to adjust batch processes accordingly. Given the rapid turnaround, organizations may have to review their current contractual agreements and processing schedules. Additionally, CMS requires that plans and providers retain and share five years of data. To manage those requirements, organizations will likely have to update their data retention policies and infrastructures. Healthcare organizations should confirm that their infrastructures and processes are compliant and working as planned, and existing monitoring and maintenance programs will have to be reassessed. Successful organizations will monitor KPIs and issues reported by customers or third parties to quickly identify and remediate data quality issues. Operational performance testing on a regular schedule should be included as part of a quality assurance plan. Given the review of the ways data is being received, created, stored, managed, and exposed, other downstream impacts should be considered. For example, the reduction of latency allowed one organization to reduce the refresh rate of a heavily relied upon encounters dashboard from two weeks to daily. In doing so, the plan improved its ability to target members for their prospective risk adjustment activities. Helping the business understand the impacts of the requirements can inform use cases that translate this significant undertaking into measurable business value.
We have discussed the long-term goals and benefits of preparing a healthcare entity for interoperability, and we’ve noted various challenges to collaborations across all business areas in order to realize business value. However, that business value cannot be achieved without first meeting compliance requirements and mitigating new risks for impacted people, processes, and technologies.

While enforcement of Information Blocking rule is somewhat more explicit for providers and HIT companies, we expect CMS will enforce aspects of the rules for health plans through its existing approach to each specific underlying area. For example, we anticipate that CMS will enforce network accuracy through inclusion of the provider directory information through its ongoing audits of network accuracy (e.g., CMS Online Provider Directory Review Reports). For other aspects like the new data-sharing requirements, we expect CMS to expand existing oversight activities (e.g., accuracy of cost sharing, complaints to Medicare, sales and marketing complaints, and claims timeliness) or to develop new, specific oversight activities.

On the following page you will find a summary of requirements, with their associated compliance dates and key considerations for affected organizations.
<table>
<thead>
<tr>
<th>Regulation area</th>
<th>Overview</th>
<th>Compliance date</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient access API</td>
<td>Payers must make claims, encounter, clinical, and formulary data available to members through FHIR APIs</td>
<td>January 1, 2021</td>
<td>Payers should determine ownership and define an overall onboarding process for 3rd party interoperability-related applications and inquiries (e.g., requesting access to FHIR APIs). Ensure that a developer portal, API implementation guides, and an attestation process (e.g., CARIN Trust Framework) are included as part of the onboarding process. Identify sources and timeliness of all claims data, inclusive of claims processed by delegated entities. Identify existing clinical data assets based on USCDI, including quality reporting datasets, HRAs, and/or other datasets obtained from providers.</td>
</tr>
<tr>
<td>Provider directory API</td>
<td>Payers must provide public access to a complete and accurate directory of their contracted providers through an API</td>
<td>January 1, 2021</td>
<td>Ensure processes are in place to track provider directories are updated within 30 days of new information.</td>
</tr>
<tr>
<td>Payer-to-payer data exchange</td>
<td>Payers are required to send and receive clinical data as their members move between health plans</td>
<td>January 1, 2022</td>
<td>Payers should consider how the inbound payer-to-payer data exchange be customized or integrated into existing claims, care management, and other internal systems to support continuity of care.</td>
</tr>
<tr>
<td>Hospital ADT notifications</td>
<td>Providers must be able to send ADT notifications through their EHRs to all practitioners identified by patients to support care coordination</td>
<td>May 1, 2021</td>
<td>Aside from compliance, providers should revisit ways to take advantage of the receipt of ADT notifications to provide better, more effective patient care.</td>
</tr>
<tr>
<td>EHI exports</td>
<td>EHI must be provided directly for a patient or designated personal representative (DPR) as an export and in a timely manner</td>
<td>December 31, 2023</td>
<td>This requirement has a longer compliance timeline. Patient information that gets created or received by a healthcare provider and those operating on their behalf; includes protected health information (PHI) as well as health insurance, billing, and payment information.</td>
</tr>
<tr>
<td>Information blocking</td>
<td>A practice by a healthcare provider, HIT developer, or HIE/HIN that, except as required by law or specified by the secretary as a reasonable and necessary activity, is likely to interfere with, prevent, or materially discourage access, exchange or use of EHI</td>
<td>April 5, 2021</td>
<td>A healthcare provider is subject to the information blocking provisions agnostic of their use of certified health IT. If a healthcare provider is found to be knowingly interfering with the access, exchange, or use of EHI, then that provider may become subject to an information-blocking complaint. However, there are eight exceptions a provider can meet that justify information blocking: health IT performance, content and manner, fees, licensing, preventing harm, privacy, security, and infeasibility. Ensuring that accurate identification and documentation of exceptions will facilitate compliance. Regulatory boards have proposed that instances of violations can be determined through audits or by way of user-reported complaints.</td>
</tr>
<tr>
<td>e-prescribing</td>
<td>Providers must send e-prescription transactions by using the new National Council for Prescription Drug Programs SCRIPT standard 2017071 to align with Part D e-Rx and mental health standards</td>
<td>November 2, 2020</td>
<td>Although regulations and guidelines have been in place since 2008 with the passage of MIPPA, internal data integrations will have to be updated based on requirements, with specific attention to security so as to prevent the diversion of controlled substances.</td>
</tr>
<tr>
<td>Digital contact updates for NPPES</td>
<td>Providers, individuals or organizations, must update the NPPES database with their digital contact information to facilitate the sharing of health information and to increase provider directory reliability and accuracy. Changes in contact information after initial input must be completed within 30 days</td>
<td>Early 2021</td>
<td>CMS will publicly report providers that do not list their digital contact information. Consider using the NPPES API directory API to confirm the information listed for your providers.</td>
</tr>
</tbody>
</table>

ADT = admit, discharge, transfer, API = application programming interface, EHI = electronic health information, EHR = electronic health record, FHIR = Fast Healthcare Interoperability Resources, HIE = health information exchange, HIN = health information network, HIT = health information technology, MIPPA = Medicare Improvements for Patients and Providers Act, NPPES = National Plan and Provider Enumeration System
Security

Third-party developers will disrupt the ecosystem with data-powered innovations and new market plays through the new and unprecedented access to consumers’ medical and health data.

Because CMS has not released certification criteria for selecting and integrating third parties, payers and providers will have to develop their own scalable and timely vetting processes to ensure compliance with all security and control requirements inclusive of certification of underlying data, document verification, and API classification. Payers cannot deny access, but third parties that represent challenges may invoke a warning from payers to consumers during the consent process. Similarly, this presents an opportunity to identify new partners and create preferred app listings for trusted third parties.

Ensuring that consumers trust health plans and systems with their sensitive information and their healthcare is key to long-lasting relationships. Payers will have to establish criteria for a breach by setting baseline controls within all implemented APIs and by developing informative, real-time alert systems that notify pertinent staff members. Security staff members will have to be trained in quickly identifying the level of potential risk and implementing corrective-action plans. Of all breached US organizations, it took an average of 245 days to identify and contain a breach last year. In addition, organizations that are able to contain breaches in less than 200 days spent an average of $1.2 million less than organizations that took 200 days or longer. Accordingly, a data breach plan that gets reassessed periodically will ensure proper actions are taken immediately following a breach.

According to a Ponemon Institute Report, the costs of lost or stolen records are increasing and in 2019 were estimated to be $429 per record.

1https://healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record
### Privacy

**Figure 4. Consumers are becoming less and less comfortable sharing their medical and health information among healthcare organizations**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>To improve coordination of my care</td>
<td>63%</td>
<td>55%</td>
<td>55%</td>
<td>58%</td>
<td>45%</td>
</tr>
<tr>
<td>To support real time decision making for my care</td>
<td>55%</td>
<td>43%</td>
<td>44%</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>To measure how well my doctor does his or her job</td>
<td>35%</td>
<td>36%</td>
<td>28%</td>
<td>25%</td>
<td>20%</td>
</tr>
<tr>
<td>To identify patients who are at risk for developing a disease</td>
<td>30%</td>
<td>27%</td>
<td>24%</td>
<td>17%</td>
<td></td>
</tr>
<tr>
<td>To help companies develop new treatments or diseases</td>
<td>20%</td>
<td>17%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Consumer education and transparency should be key considerations for any privacy activity. As shown in the above figure (Figure 4), consumers have grown less comfortable with sharing their protected information among healthcare organizations, which is detrimental to the success of interoperability. In addition to stressing to consumers the advantages of sharing data, it will be critical to communicate to consumers their rights and responsibilities.

We believe that a central portal where consumers can access all terms and conditions, indicate consent, view their current permissions, and make updates and changes to their privacy settings in an easy and timely manner would be the best approach.

Consumers should be encouraged to take ownership of their data, understand who they are sharing it with and how it will be used. They should also be encouraged to share their information as they see fit, but they also have to understand the potential ramifications. For example, consumers should be made aware that data cannot be clawed back once shared, and turning off data sharing may not be an instant process.

Consent management will have to be built in accordance with consent management guidelines and the Consent2Share platform, which are currently being formalized.
How can Internal Audit and Compliance help?

An effective interoperability implementation will require a cross-functional approach to focus an organization’s efforts and resources in a concerted manner, and Internal Audit and Compliance are critical components.

We’ve laid out the key next steps for engaging with the broader interoperability program below:

**01: Get involved early**

Collaborate with Business Operations and IT to develop a program strategy and roadmap to align efforts to be compliant with interoperability requirements. Be a key driver of discussions around developing control-enabled processes in a scalable and sustainable fashion.

**02: Map risks and controls**

Given the large number of new processes and capabilities, help identify risks and key controls necessary to ensure sustained compliance with interoperability requirements within IT and business operations.

**03: Plan to audit**

Conduct in-flight readiness assessment and/or add an interoperability compliance assessment / audit to your work plan for 2021. Probe into specific requirements during risk assessment discussions.

Internal Audit and Compliance can help ensure sustained compliance by working with IT and the business to develop effective monitoring of the new capabilities established.

Over time, interoperability will change the healthcare industry in major ways and empower consumers more than ever before. Organizations should weigh the pros and cons of different interoperability strategies before making decisions. Regardless of the ultimate strategy an organization pursues, time is of the essence. Don’t wait until requirements are getting enforced; early action will provide the best opportunity build a successful program that minimizes risk, and may even prove to be a market differentiator.

For more information, please bookmark pwc.com/us/interoperability.
Questions?

Dave Curé  
Partner  
(401) 338 6439  
dave.cure@pwc.com

Kelly Tsaur  
Principal  
(617) 251-3929  
kelly.tsaur@pwc.com

Fran Grabowski  
Director  
(617) 784 6028  
fran.grabowski@pwc.com

James Lin  
Director  
(714) 206 2150  
jam.lin@pwc.com
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.

Subcommittee:

Alan Henton, White Paper Chair, alan.p.henton@vumc.org
Linda Greer, lamizgre512@gmail.com
Debi Weatherford, debi.weatherford@piedmont.org
Laura L. Sak-Castellano, Laura.Sak-Castellano@aah.org
Deborah Pazourek, AHIA Board Liaison, Deborah.L.Pazourek@medstar.net