SUPPLY CHAIN

7%

Presented by: Stephen C. Grothouse
and Erin M. Rozycki

HALL RENDER
KILLIAN HEATH & LYMAN

MAXIMIZING SUPPLY CHAIN EFFICIENCIES WITH LEGAL ENGAGEMENT

Chicago Metro Chapter Association for Healthcare Resource & Materials Management Spring Meeting

April 18, 2019

CHICAGO METRO CHAPTER AHRMM

Presented by:
Stephen C. Grothouse and Erin M. Rozycki

HALL RENDER
KILLIAN HEATH & LYMAN

ARE YOU A BLOCKBUSTER? OR NETFLIX?

Related Topics

- Supply Chain Impact
- Regulatory Watchlist
- Value Stream Mapping
- Trending Now – Risk Management
- Popular Focus Areas
- Supply Chain Efficiencies

Supply Chain Impact

Continue watching

- Cost – Supply chain costs comprise **30 to 50 percent** of a health care organization's budget – Second only to labor
- Patient – 20% (**1 in 5 clinicians**) could recall a scenario in which a patient was harmed because the facility did not have the right supplies for a procedure
- Regulatory – Numerous potential pitfalls from which regulatory penalties and compliance costs could arise
- Risk – Regulatory, financial, operational and physical

Hospitals have an unrealized $25.4 billion supply chain opportunity

BY ALEX KACIK | OCTOBER 18, 2018

Continue watching "The Regulatory Watchlist"?

Continue watching

Exit

- Anti-Kickback Statute
  - Discounts/Rebates
  - Warranties
  - GPO
- HIPAA, GDPR & State Privacy Laws
- Physician Payment Sunshine Act
- Systems and Device Security
- Physician-Owned Distributorships ("PODs")
- FDA

ET Healthworld
From The Economic Times

Pfizer to pay $785 million for overcharging US government on drugs

Wyeth, the unit, was accused of knowingly reporting to the government false and fraudulent prices for two forms of Protonix, a drug notably used to treat symptoms of acid reflux, from 2001 at 2006, before it was acquired by Pfizer in 2009, the Justice Department said.

AFP | April 28, 2016, 13:52 IST

Olympus to Settle Charges It Bribed Doctors

By Joseph Walker

The U.S. unit of **Olympus** Corp. admitted it paid bribes to U.S. doctors and hospitals to promote sales of its medical devices, and agreed to pay $623.2 million in civil and criminal penalties as part of what prosecutors called the largest-ever settlement under federal anti-kickback laws.

Olympus's Latin American unit also will pay $22.8 million in U.S. criminal penalties to resolve allegations it paid nearly $3 million to government-employed health-care practitioners in Latin America to increase sales there. Prosecutors alleged, and Olympus admitted, that the payments violated the U.S. Foreign Corrupt Practices Act, which bars using bribes or gifts to foreign officials to win or keep business.

The settlements resolve charges brought against the company by the U.S. attorney's office for the District of New Jersey. The government alleged the U.S. bribes caused health-care providers to bill government health-care programs in violation of the False Claims Act.

"There was a relatively widespread pattern of the company using various forms of financial benefits—cash, trips, consulting agreements—to induce doctors, hospitals and other health-care providers to buy their stuff," Paul J. Fishman, the U.S. attorney for New Jersey, told The Wall Street Journal.

Mr. Fishman said the settlement was the largest amount paid in U.S. history for violations of the federal Anti-Kickback Statute, which forbids payments to induce purchases by federal health programs. It also is the largest-ever settlement by a medical-device company, he said.

"Olympus leadership acknowledges the company's responsibility for the past conduct, which does not represent the values of Olympus or its employees," Nacho Abia, chief executive of Olympus Corp. of the Americas, said in prepared remarks Tuesday.

As part of the settlement, Olympus admitted in court documents that its senior employees and executives conspired to pay kickbacks to U.S. physicians in the form of consulting fees, trips to Japan, "lavish meals, ballooning, winery tours, golf and spa treatments."

The company also gave cash grants and equipment loans to hospitals with the aim of retaining their business and winning new contracts, Olympus admitted.

Wall Street Journal - March 2, 2016

Data Breach Costs

- The average cost of a data breach is now $3.86 million across all industries
- Cost per individual record by top industries:

- Average OCR HIPAA resolution amounts:
  - 2015: $1M
  - 2016: $1.8M
  - 2017: $1.9M
  - 2018: $3.2M (including the Anthem penalty)
- State Attorneys General are becoming more active in their enforcement

New Jersey fines Virtua Medical $418,000 for HIPAA breach

By **Jessica Davis** | April 09, 2018 | 02:28 PM

The penalty highlights the need for healthcare providers to thoroughly vet third-party vendors to ensure security best practices.

The New Jersey Attorney General fined Virtua Medical Group for more than $418,000 after a misconfigured database breached the protected information of 1,654 patients in January 2016. 1,617 of those patients resided in the Garden State.

The attorney general found that Virtua failed to conduct a thorough analysis of the risk to the confidentiality of patient data sent to its third-party vendor. Further, officials said the medical group didn't implement security measures that would reduce that risk, which violated HIPAA.

"This enforcement action sends a message to medical practices that having a good handle on your own cybersecurity is not enough. You must fully vet your vendors for their security as well."

– Sharon M. Joyce, acting director of the Division of Consumer Affairs

Indiana health network pays about $55,000 ransom to hackers

By Associated Press | January 17, 2018

(Updated at 4:05 p.m. ET)

A suburban Indianapolis health network said it paid a $55,000 ransom to hackers to regain access to hospital computer systems, making it the latest health system around the globe targeted by money-seeking hackers.

Hancock Health said an "unidentified criminal group" initiated the attack late last week and targeted more than 1,400 files. The health system said it was given seven days to pay a ransom in bitcoins, and after the virtual currency was transferred, its staff regained access to the computer systems.

Hancock Health said it found no evidence that patient information was adversely affected. At the time of the transfer, the four-bitcoin ransom was worth about $55,000, The Daily Reporter of Greenfield reported.

RELATED CONTENT

Healthcare data breaches caused by hacks are on the rise

Florida hack exposed files of up to 30,000 Medicaid patients

The frightening new frontier for hackers: Medical records

NEWS

Hacking pacemakers, insulin pumps and patients' vital signs in real time

At the recent Black Hat and Def Con events, researchers showed how they are able to hack pacemakers, insulin pumps, and patients' vital signs in real time.

Medical device insecurity was covered at the recent Black Hat and Def Con security conferences in Las Vegas. One set of researchers showed off hacks to pacemakers and insulin pumps that could potentially prove lethal, while another researcher explained how hospital patients' vital signs could be falsified in real time.

Pacemaker and insulin pump hacks at Black Hat USA

A decade has passed since we learned about pacemaker hacks, but still implantable medical devices that can save patients' lives can be hacked to potentially kill them. Even now, as was highlighted at Black Hat USA, attackers can cause pacemakers to deliver a deadly shock to the heart or deny a life-saving shock, as well as prevent insulin pumps from delivering needed insulin.

Value Stream Mapping – Organizational Engagement

Identify Resources

Find the right resources within the organization and team up

Obtain Buy-In

Work with those key stakeholders – gain trust and confidence

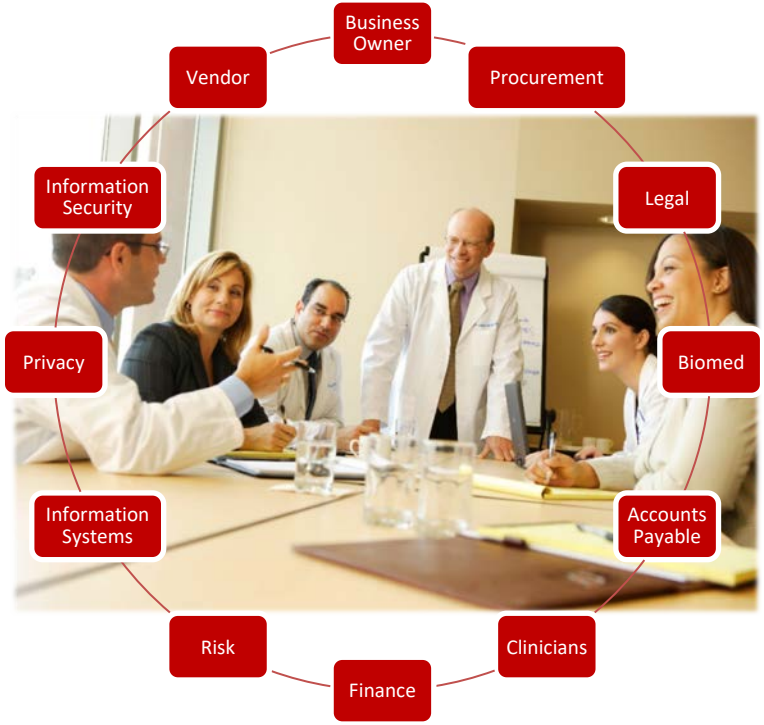
Set Objectives

Together set goals and strategy to reach them – discuss risk

Value Stream Mapping: Explained

- What is "Value Stream Mapping"?
  - Method of analyzing current state and designing a future state with less “waste” than the current map
- Why Value Stream Mapping?
  - Issues: Identify issues and create efficiencies in the supply chain process
  - Stakeholders: Give key individuals and decision-makers supply chain visibility and stake
  - Objectives: E.g., manage regulatory risk, reduce average contracting timelines
- VSM Process
  - Stakeholders meet to discuss and analyze current process
  - Identify obstacles and issues affecting each department
  - Identify opportunities for shared efficiencies and gains
  - Develop strategies to take advantage of those opportunities and realize results

VSM: Identify Resources and Obtain Buy-In



- Identify key stakeholders in organization
- Identifying obstacles and areas of exposure and pain
- Develop collaborative process among stakeholders
- Communicate and consistently improve the process

VSM: Obstacles

- Not enough documentation at onset of vendor negotiations
- Business owners not fully engaged in vendor contracting process
- One-sided vendor contracts and excessive vendor redlines to contract templates
- Significant lag time with each department requiring review
- Technical/security assessments completed late in negotiation
- Most communication occurring via email – not enough in-person/collaborative interaction between the teams

VSM: Resulting Opportunities

- Require business owner to complete routine vendor onboarding form
- Develop evaluation mechanisms to identify/manage potential regulatory risks
- Optimize collaboration/negotiation approaches (phone, software tools, in-person)
- Develop "short form" purchase contracts for low-risk/low-value projects
- Engage Risk Management to develop new insurance requirement grids, taking project risk and vendor size and maturity into account
- Information Security to develop multiple security assessment forms/modules targeted to scope and risk of project to be administered prior to negotiations
- Establish procurement governance committee to track project status

VSM: Setting Objectives and Realizing Results

- Define and measure success
- Use vendor pre-qualification processes to ensure certain "inviolable" risk factors are not present
- Build vendor onboarding process to identify interested stakeholders and identify all risk factors
- Legal and Information Security conduct periodic meetings with strategic sourcing department(s) personnel and/or leadership
- Develop vendor management lifecycle process, potentially integrating with specialized software tools

Trending Now – Risk Management

- Recalls
- Warranty Management
- Cybersecurity
- Risk-Sharing

Risk Management – Recalls

- Tracking recalled devices
- Necessity of patient notification
- Accounting for costs attributable to recalled devices
- OIG Audits
- Contract language: *Supplier shall reimburse Customer for all costs associated with any product corrective action, withdrawal, or recall requested by Supplier or required by any governmental entity*

Risk Management – Warranty Management

- Document, track and enforce
- Warranty Management software programs
  (utilize UDI information to document and track relevant data)
- Monitoring and tracking warranties and recall data for medical devices can result in significant savings for a hospital or health system
- Enforcement starts with the contract – what are the vendor's responsibilities in the event of a warranty claim or recall of a device?

Risk Management – Cybersecurity

- Practical Cybersecurity Risks
  - Physical and Remote Systems Access
  - Data transmission and hosting security
  - Misuse of data properly received and stored
  - Equipment and medical device controls and connectivity
  - BYOD and take-home devices
  - Data intake – viruses and ransomware

- Collaborative Cybersecurity Risk Management Process
  - Involve information security and legal/compliance from the outset
  - Evaluate vendor security in accordance with scope of engagement and data/systems access
  - Establish system for scoring and managing vendor security risk

Risk Management – Risk-Sharing

- In September 2018, the OIG approved the first of its kind risk-sharing program (AO 18-10)
- Warranty program for joint replacement implants, wound therapy and anti-microbial dressing
- If a patient is readmitted into the same hospital within 90 days of the joint replacement surgery, the vendor will refund the hospital the aggregate purchase price for all 3 items
- Although it does not satisfy the Warranty Safe Harbor, the OIG concluded it represents a sufficiently low risk of fraud and abuse
  - None of the products are separately reimbursable
  - Vendor will meet all obligations of "Seller" under the Warranty Safe Harbor
  - Clinicians retain clinical decision-making
  - Overall objective of reducing readmissions – positive clinical outcomes
  - No exclusivity

Popular Focus Areas

- Tools
- Training
- Process
- Templates
- Metrics

Tools

- Vendor Management Policies
- Vendor Pre-Qualifications
- Vendor Onboarding Form
- Contract Management and Risk Management Software Solutions
- Contracting Templates and Guides
- Lifecycle Process – Decision Trees

Trending: Software Tools

- Contract Management Software
  - Automate vendor intake and negotiation process
  - Allows business owners to search for contracted vendors and contracts
  - Monitor contracts that are up for expiration/renewal or periodic reporting
  - Identify business and supply chain points of contact for ongoing vendor review
  - "Flag" contracts that need periodic quality reviews (Joint Commission, SLAs, KPIs)
- Security Risk Management Software
  - Automate vendor security risk evaluation
  - Automate and manage vendor security risk scoring standards
  - Catalogue vendor security risk assessments and risk sign-off over time

Templates

- Vendor Management Policies
- Vendor Onboarding Forms
- Capital & Consumable Agreements
- Evaluation Agreements
- Consignment Agreements
- IT and other Purchased Services
- Cloud Services Agreements
- Software and Technology Agreements
- Data Transfer/Sharing Agreements
- BAAs and DPAs

Training

- Importance of training
  - Impact of turnover on departments
- Understanding contemporary contracting approaches

Upcoming Webinar: Shared Risk Contracting: Provider and Supplier Perspectives
Learn how sharing the risk of product or service outcomes is becoming more common in healthcare and how providers and suppliers can work together to generate financial, operational, and clinical value.

When: 3/14/2018
Time: 12 PM CST
Cost: Free for AHRMM members | $99 for non-members

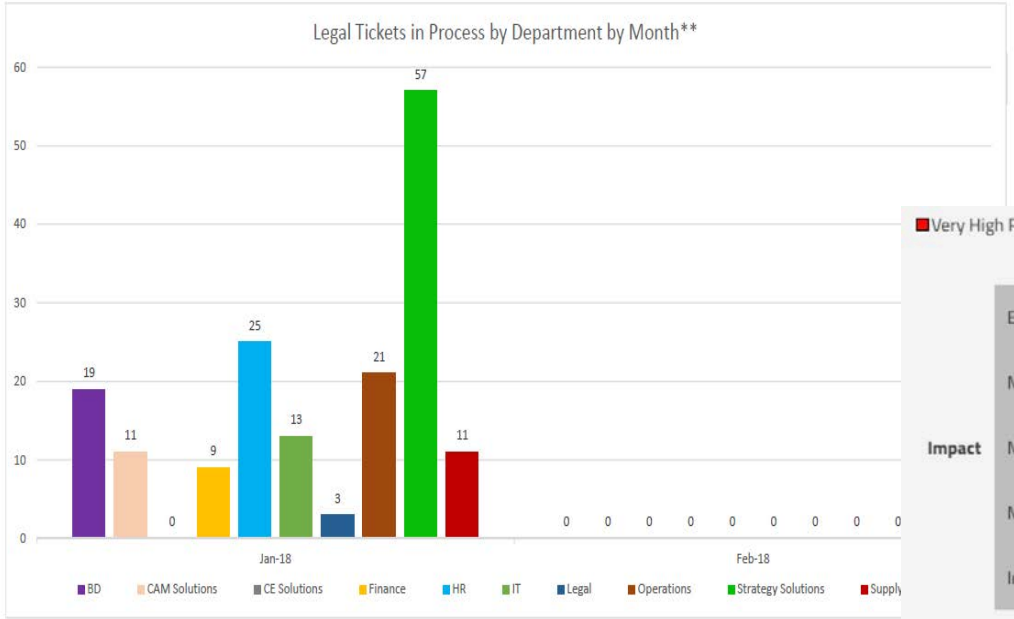
Register Today

New Webcast: Aligning Patient Data to Help Decision Makers Improve Care
Watch as Jill Cotchen, Product Executive, Vizient Inc., discusses how data crosses over departments and is interpreted to address real-life scenarios, and the necessity to take into account different benchmarking and costing methodologies to accurately quantify cost and impact to your organization.

Watch Now

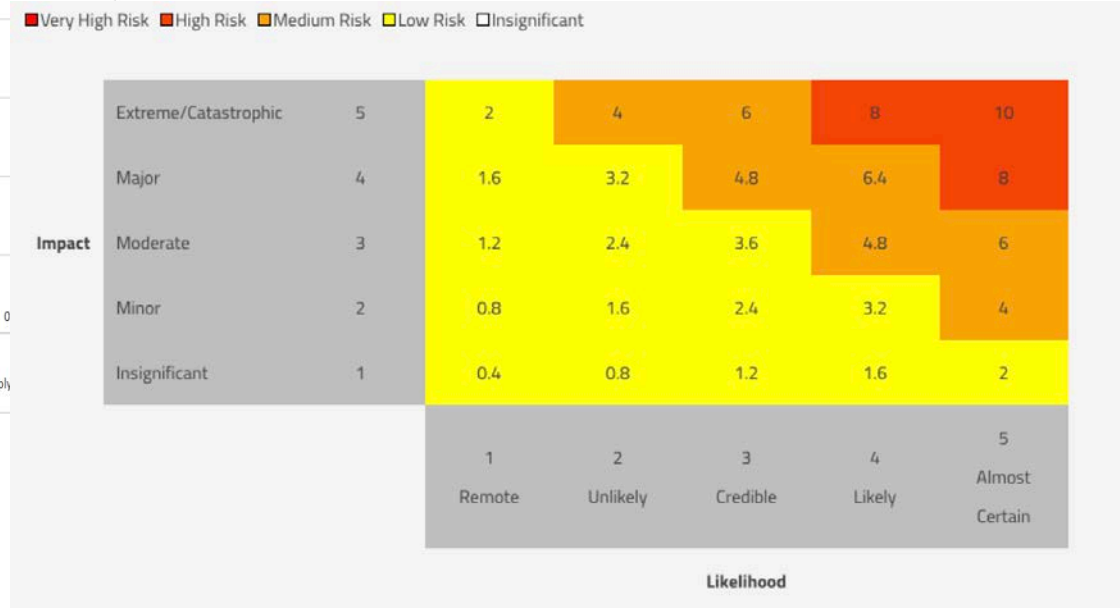
AHRMM
Advancing Health Care through
Supply Chain Excellence

Metrics

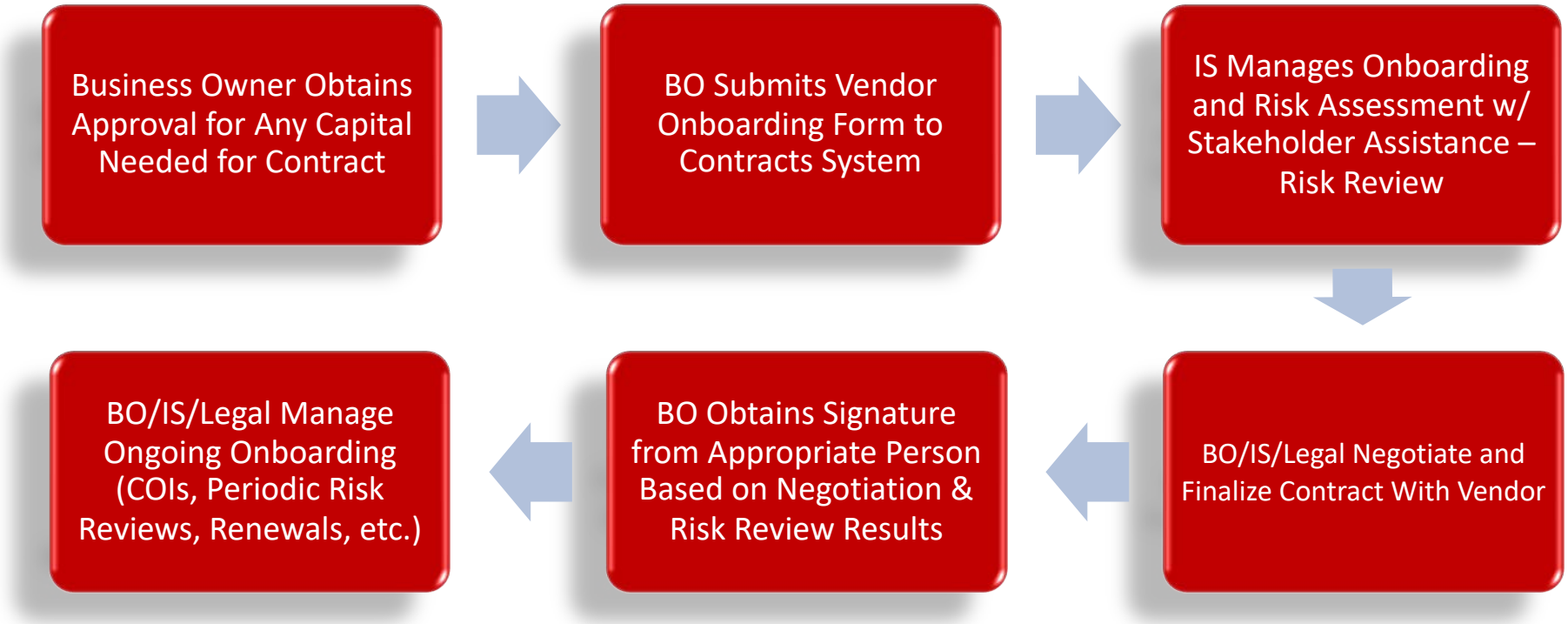


*The Legal tickets in process are captured on the last business day of the month.

**Tickets in process captures all open tickets.



Vendor Lifecycle Management Process



Loading... Supply Chain Efficiencies

Where to Begin?

- Meeting among Legal/Compliance, Supply Chain and Information Services to identify risks and begin developing processes to address them
- Contract Intake Process
  - Create a meaningful contract intake process to drive efficient contract review
  - Develop a Vendor/Contract Intake Form
    - Needs to capture information that will identify typical roadblocks (e.g., capital approval, regulatory red flags, security/privacy assessments)
    - Use as opportunity to identify issues needing collaboration between these and other departments at outset of vendor engagement
    - Address on the front-end issues that are likely to arise post-execution

Vendor/Contract Onboarding – Suggested Content

- Description of Goods and Services to be Provided
  - What is the scope of what the vendor is offering?
- Information Services Review
  - Will the vendor access any systems? What type of data will the vendor access? Will the vendor store any data? Will the vendor access or store data offshore? Is a technical or security assessment of vendor needed?
- Current issues with this vendor
  - Is this a problem vendor – invoicing and payment issues, contract compliance, vendor management concerns? In the news? Under CIA? Any pending litigation with the vendor?
- Vendor Relationship Termination
  - Can we terminate? Evergreen clause? Penalty language?

Please visit the Hall Render's blog at http://blogs.hallrender.com for more information on topics related to health care law.

Stephen C. Grothouse
317-977-1457
sgrothouse@hallrender.com

Erin M. Rozycki
248-457-7857
erozycki@hallrender.com

This presentation is solely for educational purposes and the matters presented herein do not constitute legal advice with respect to your particular situation.

HEALTH LAW
IS OUR BUSINESS.
Learn more at **hallrender.com**.

HALL RENDER
KILLIAN HEATH & LYMAN

100%

Loading