HALL RENDER
KILLIAN HEATH & LYMAN

Third-Party Tracking Tools in Healthcare

May 5, 2023

Agenda:

- Where did this all begin?
- What are tracking technologies and how do they work?
- Where are we now?
- What are the potential legal implications?
- Lessons learned
- What steps should health care organizations be taking?

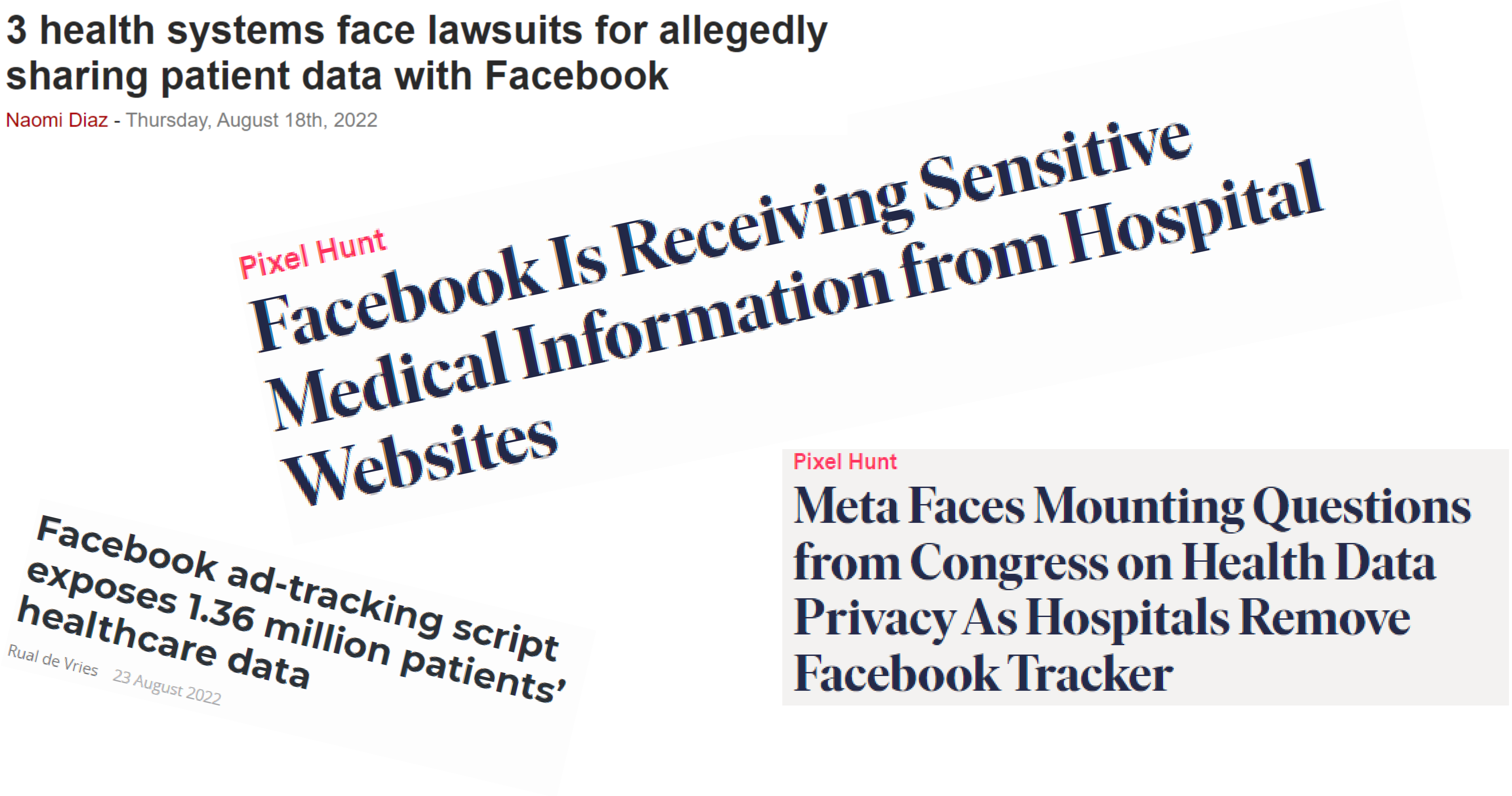
Where it all began

On June 16, 2022, *The Markup* published an article reporting that healthcare organizations across the country had installed the Meta (formerly, Facebook) Pixel within **authenticated patient portals** as well as public-facing portions of their websites.

The article concluded that, if not properly configured, the Pixel could send Facebook PHI, including, but not limited to the following elements:

- IP address
- First and last name
- Home address
- Email address
- Medication names
- Descriptions of allergic reactions
- Details about upcoming doctor's appointments.

The article named many healthcare organizations and offered screenshots as evidence.



3 health systems face lawsuits for allegedly sharing patient data with Facebook

Naomi Diaz - Thursday, August 18th, 2022

Pixel Hunt

Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Facebook ad-tracking script exposes 1.36 million patients' healthcare data

Rual de Vries 23 August 2022

Pixel Hunt

Meta Faces Mounting Questions from Congress on Health Data Privacy As Hospitals Remove Facebook Tracker

Where we are now

- Focus has expanded beyond just the Meta Pixel to the many other varieties of web trackers.

Google Analytics
Google Ads
Google Tag Manager
Adsense
YouTube
DoubleClick
Microsoft Clarity
LinkedIn
Facebook Pixel

Twitter
Pinterest
Reddit
SiteImprove
Acquia
Localytics
TVSquared
CallRail
AddThis

Craxy Egg
Adobe
LiveRamp
DemandBase
Nielsen Group
Salesforce
DataDog
HotJar
SiteScout

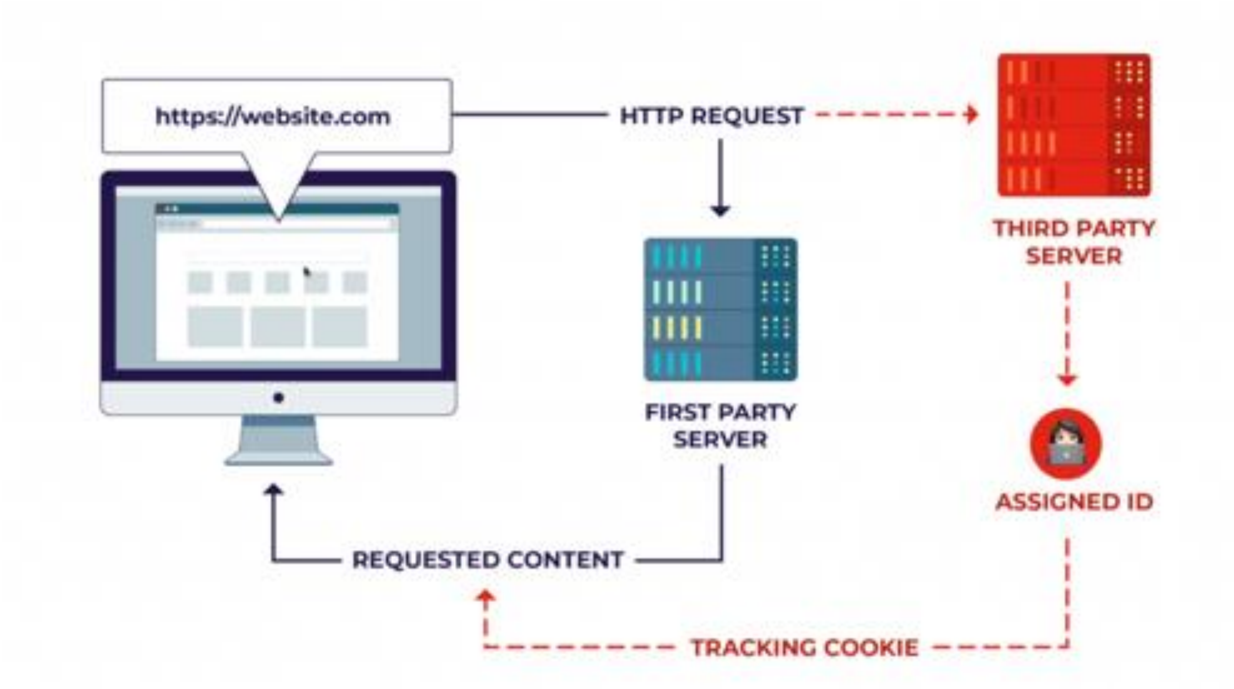
Medallia
InPowered
IponWeb
Oracle
LiveIntent
Dstillery
Rubicon
Bombora
Semasio

- **Timeout: Just what are web tracking technologies?**

What exactly are web trackers?

Third-Party Website Analytics

“One of the murkiest areas of Internet commerce is the trade of personal information gathered by certain companies who monitor our behavior online. This kind of third-party data gathering is ubiquitous on the web thanks to the humble ‘cookie’.” *MIT Technology Review*

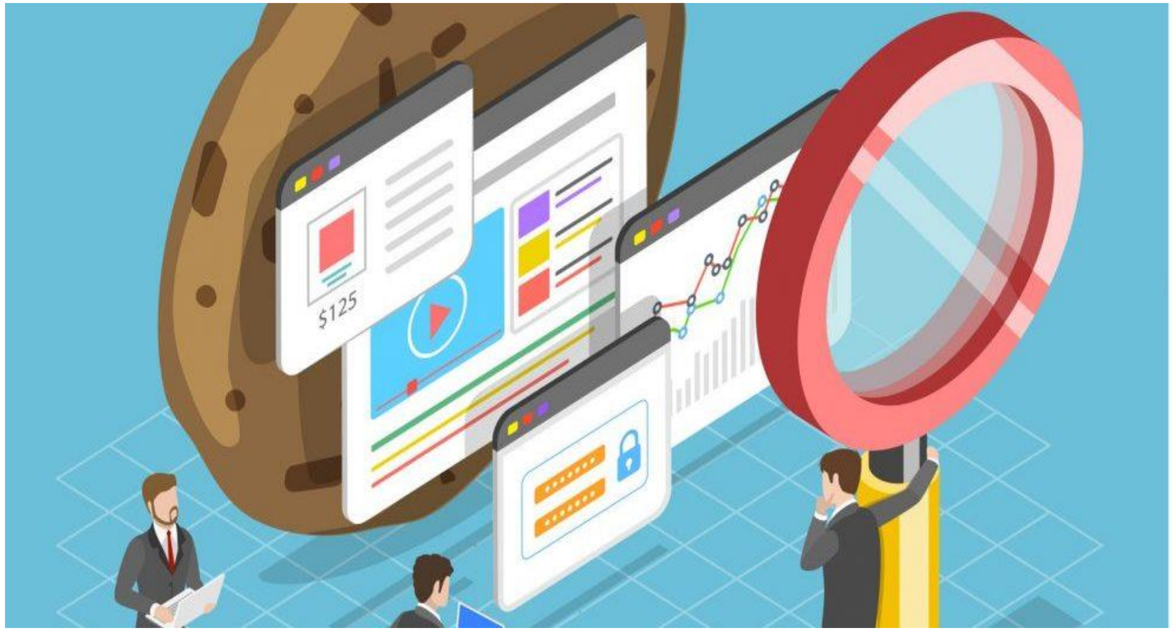


Cookie: Cookies are used to identify users online and provide a personalized browsing experience.

First party cookies are placed by the domain you are visiting. These are the cookie tracking options you agree to when you sign-in to a website or set up an account with a company. A first party cookie is saved to your device.

Third party cookies are placed by domains other than the one you are visiting and use information about your device, web browser, geographical location, operating system, etc. to identify your digital fingerprint.

Third-Party Website Analytics



Third party cookies include cross-site tracking cookies, tracking pixels, social trackers, and content trackers.

- Tracking pixels are single-pixel transparent images that exist within some websites but come from a third-party. While they are invisible to the user, this seemingly discrete connection allows third parties to glean useful information about your device such as your system hardware, browser configuration and **IP address**.

Where we are now

- 7 health systems have determined that their web tracker activities resulted in a breach of unsecured PHI under HIPAA.
  - Notifications to potentially affected individuals
  - Notifications to OCR and state AGs
  - Notifications to media
- Numerous health care organizations have been served with class action lawsuits.
  - Still too soon for any meaningful intelligence from these lawsuits.
- OCR has opened compliance reviews of numerous covered entities.
- State Attorneys General have opened investigations.
- The U.S. Senate Permanent Subcommittee on Investigations is investigating and holding hearings.

Where we are now

- OCR issued guidance on December 1, 2022.
  - Is it PHI? Information disclosed through tracking technologies placed on a regulated entity's website or mobile app is **likely PHI** when it includes any individually identifiable information because such information connects the individual to the regulated entity.
    - Patient relationship is not required
    - Specific treatment information (e.g., diagnosis or medical history) not required
  - Location Matters. Where the trackers are located on the website impacts whether or not the information is PHI. Tracking tools on authenticated pages of a regulated entity's website are more likely to collect PHI.
    - Authenticated pages, such as patient portals or telehealth platforms
    - Webpages that address specific symptoms or conditions (e.g., health assessments or symptom checkers)
    - Appointment scheduling or find-a-doctor pages

Where we are now

- OCR guidance (cont.)
  - Filtering Insufficient. Even if the tracking technology vendor claims to filter out or de-identify PHI, the initial disclosure of PHI must comply with HIPAA.
  - BAA or Authorization Required. If a tracking technology vendor is receiving PHI, they are a business associate and the regulated entity must ensure that a BAA is in place or that patient authorization is obtained.
  - Risk Analysis. The use of tracking technologies must be included in a regulated entity's risk analysis and risk management processes.
  - Breach Notification. Where PHI has been disclosed to a tracking technology vendor without a BAA or authorization, the presumption of breach applies and can only be overcome if the regulated entity can demonstrate that there is a low probability that the PHI has been compromised.
    - What does it mean to be compromised in these cases?

Potential Legal Implications

- Original allegation from *The Markup* was that the disclosures violate HIPAA.
- Potential HIPAA violations include:
  - Impermissible disclosure of PHI
  - Failure to conduct and maintain a breach risk assessment
  - Failure to conduct a risk analysis/develop a risk management plan
  - Failure to execute a Business Associate Agreement
  - Failure to timely notify of a breach

Potential Legal Implications

- Regulatory analysis has focused on HIPAA, but other claims have developed through class action lawsuits.
    - Invasion of Privacy
    - Unjust Enrichment
    - Breach of Implied Contract
    - Violations of the Electronic Communications Privacy Act (ECPA)
    - Violations of the Computer Fraud and Abuse Act (CFAA)
- State Attorneys General could also bring claims under state data protection and consumer protection laws.

Potential Legal Implications

- The current regulatory environment is very unclear.
  - Will OCR enforce potential violations as aggressively as they are investigating them?
  - Given how pervasive this issue is, will OCR take a prospective only enforcement stance?
  - Will OCR reward entities who voluntarily report with lenience or will they make an example of them?
  - Is OCR going to review websites and continue to open investigations of regulated entities prospectively?

Lessons Learned

Data Elements of Concern in June of 2022
IP Address
First and Last Name
Home Address
Email Address
Medication Names
Descriptions of Allergic Reactions
Details About Upcoming Doctor's Appointments

Data Elements of Concern in January of 2023	
June of 2022 Data Elements	Navigation Button Clicks
Site Search Terms	Interactive Tool Responses
Medical Record Number	Credit Card Information
Insurance Plan Type	Form Submissions
Proxy Access Request Details	Patient Portal Registration
Health Risk Assessment Data	URL Referral Source
Physician Searches	URL Page Paths
Zipcode/Geographic Location	Emergency Contact Details
Viewed and Downloaded Forms	Treatment Information

Lessons Learned

1. Web pages that include forms create a higher level of risk.
    - Many forms are found to be transmitting form field entries in plain text to tracking technology vendors
    - Patient portal access request forms, proxy access request forms, appointment scheduling forms, newsletter signup forms, foundation donation forms, bill pay forms, health risk assessment forms, etc.
2. Even if a certain third-party tracking technology is no longer in use by the organization or isn't tied to a specific ad campaign, if the tracking technology is still present on the site, it is likely still passively collecting information on individual users.
    - Tracking technologies are capable of passively collecting and transmitting information back to the tracking technology vendor – even if the organization is not seeing the results or reports from it. A third-party tracking technology must be completely removed or disabled to ensure it is no longer collecting user information.

Lessons Learned

3. Many third-party marketing firms, third-party web application vendors, and tracking technology vendors have stated that the information collected by and transmitted through the use of tracking technologies is not PHI.
    - Incorrect determinations by third-parties can create cause unnecessary delays between discovery and reporting.
4. Several organizations disabled the use of Facebook Pixel after it garnered media attention in July of this year. Previous use of the Pixel should be considered when performing a breach/risk analysis.
    - Will likely show in the history logs for the configuration of your website and applications.
5. Prior to disabling any tracking technologies, it is important to either record the configuration of the technology or ensure continued access to the tool/dashboard from where the technology is managed.
    - In the event a third-party is engaged to perform a forensic investigation, they will need to test each technology in its original form to determine what information was being collected and transmitted.

Next Steps

- Determine whether your organization is utilizing these third-party tracking technologies.
  - Assess the placement and configuration of the tracking tools – consider engaging a forensic firm to perform the investigation if internal findings are inconclusive.
  - Consider working with legal counsel to understand the scope and scale of the tracking technology implementation and whether a privacy violation may have occurred.
    - Carefully interpret what is PHI.
    - Carefully consider and document any HIPAA breach risk assessment that is performed.
- Expand the scope of technical evaluations performed on incoming technologies to include marketing tech and other similar tools which may fall beyond the purview of HIPAA.
  - Strengthen partnerships with marketing, security/compliance, and legal teams
- Enter into BAAs with all tracking technology vendors who will receive PHI.

Ask Yourself:

What third-party data tracking technologies or services are being used on your organization's website?

What applications or platforms are third-party data tracking technologies employed on? (EHR, telehealth platform, patient portal, appointment scheduling)

What data is transmitted to the third-party tracking technology vendor?

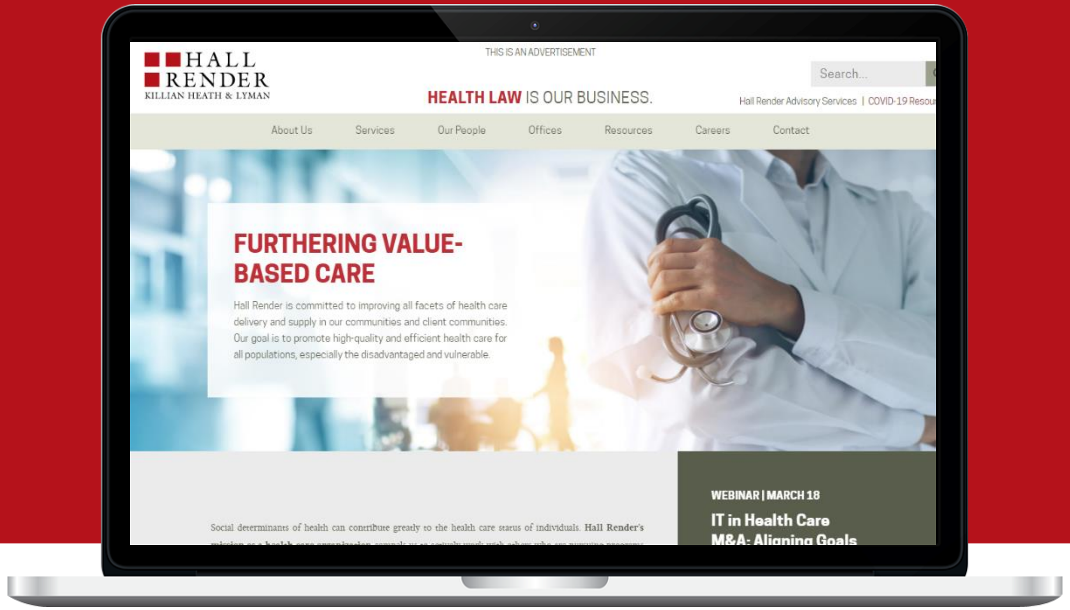
Is there a business associate agreement in place with third-party data tracking technology vendors?

Was a risk analysis or evaluation performed on third-party tracking technologies prior to or after implementation?

HEALTH LAW IS OUR BUSINESS.

HALL RENDER KILLIAN HEATH & LYMAN

For more information on these topics visit hallrender.com.


THIS IS AN ADVERTISEMENT
HALL RENDER KILLIAN HEATH & LYMAN
HEALTH LAW IS OUR BUSINESS.
Search...
Hall Render Advisory Services | COVID-19 Resou
About Us
Services
Our People
Offices
Resources
Careers
Contact

FURTHERING VALUE-BASED CARE

Hall Render is committed to improving all facets of health care delivery and supply in our communities and client communities. Our goal is to promote high-quality and efficient health care for all populations, especially the disadvantaged and vulnerable.

WEBINAR | MARCH 18

IT in Health Care M&A: Aligning Goals

Social determinants of health can contribute greatly to the health care status of individuals. Hall Render's

Mark Swearingen
mswearingen@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.