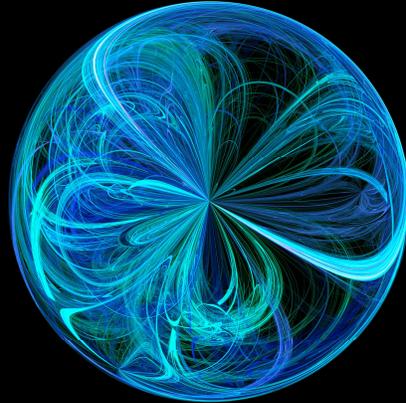


# HCCA Annual Compliance Institute



Session M3F: Addressing high-risk compliance areas and avoiding common pitfalls in risk assessment, monitoring & auditing

April 19, 2021

1

## Session Agenda

- 1 |  Learning objectives
- 2 |  Compliance work plans
  - ✓ Key considerations when conducting risk assessments
  - ✓ Compliance risk assessments: objectives, scope, and approach
- 3 |  Risk identification
  - ✓ Compliance risk universe
  - ✓ Risk assessment methodology
- 4 |  Risk prioritization
  - ✓ Risk ranking (impact & vulnerability) criteria
  - ✓ Heat map
  - ✓ Illustrative example
- 5 |  Development of compliance work plan
  - ✓ Prioritizing areas of compliance auditing and monitoring focus
  - ✓ Auditing/monitoring, training or “other activity” workplan
  - ✓ Approaching risks using different techniques

2

## Learning objectives

After this presentation you should be able to:



Build a **compliance work plan** to help proactively address known areas of risk



Learn how to approach risks using different assessment techniques: **training, analytics, auditing**



Demonstrate a **continuous improvement process** within your compliance program

3

## Polling question #1

**What industry sector do you represent?**

- A. Hospital
- B. Physician practice
- C. Post-acute
- D. Integrated health system
- E. Other

4

# Compliance work plans



5

## Setting the stage

Compliance professionals today are challenged with a multitude of competing priorities and limited resources to address complex, changing regulatory requirements. The universe of regulatory compliance risks within the health care organization spans well beyond traditional corporate compliance and includes risks related to managing protected health information (PHI), submitting claims for reimbursement, and managing contracted relationships, including vendors and clinicians, to name a few. Deploying a risk-based approach to help guide the compliance organization's focus may help prioritize efforts, justify resources and demonstrate value.

The importance of having a risk assessment in place is that it can help organizations to identify, quantify impact (when possible), and mitigate risk

### Key considerations

✓	Regulatory compliance risks exist throughout an organization
✓	Effective risk identification efforts consider both internal and external risk sources
✓	Enterprise-wide compliance risk assessments can help prioritize efforts and limited resources
✓	Impact, speed of onset, and vulnerability are common risk prioritization criteria
✓	Risk-based compliance plans can help demonstrate the compliance organization's value

6

## Compliance work plans

How can you build a compliance work plan to help proactively address known areas of risk?

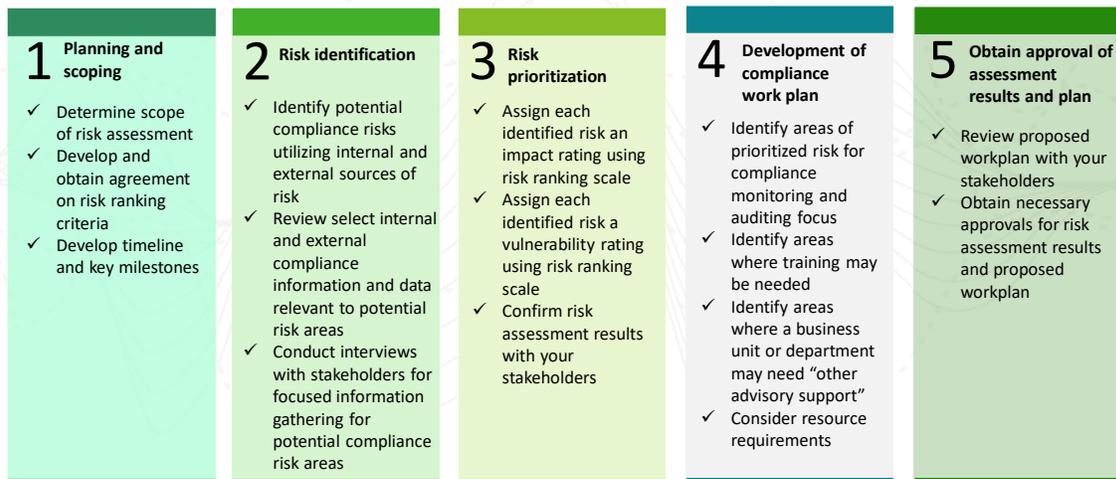
Key considerations	
✓	Consider first developing an “outside in” risk universe—Office of Inspector General (OIG), Centers for Medicare & Medicaid Services (CMS), U.S. Department of Justice (DOJ), the news
✓	What else is coming? Consider emerging risks/new regulatory requirements
✓	Use your own “inside data”—Do a multi-year lookback on refunds/self-disclosures, breaches, hotline issues; what are the patterns and trends?
✓	What has changed in your business (e.g., acquisitions, growth businesses/areas, new electronic medical record (EMR))?
✓	What is the universe of third parties and vendors your organization uses? Which ones may pose a higher risk?

HCCA 2021 Annual Compliance Institute 7

7

## Compliance risk assessment

The compliance risk assessment process should be used to identify and prioritize significant regulatory compliance risks using an efficient, structured approach. This can help inform a risk-based annual compliance work plan—which may include auditing and monitoring, training and education, and other “advisory” compliance support



HCCA 2021 Annual Compliance Institute 8

8

## Polling question #2

**How many years have you been a compliance professional?**

- A. Less than 2 years
- B. 3-5 years
- C. 5-7 years
- D. 7-9 years
- E. 10+ years

9

## Step 2: Risk identification



10

# Risk identification: Developing the compliance risk universe

Identifying relevant compliance risks

## Key compliance risk sources:

- Internal sources of regulatory information (e.g., policies, reports, contract requirements)
- External sources of regulatory information (e.g., OIG guidance, workplans, and activity, new regulations, Office of Civil Rights (OCR) activity)
- Past compliance risk universe
- Past experience (investigations, refunds, disclosures)
- Make sure you know what's happening in the industry

1. **Culture / Governance**
  - ◆ Culture / Tone at the Top
  - ◆ Policies and Procedures
  - ◆ Roles and Responsibilities
  - ◆ Compliance Function
  - ◆ Board Oversight for Compliance
  - ◆ Board Effectiveness / Knowledge Management
  - ◆ Executive Compensation / Performance Incentives / Alignment
  - ◆ Workforce & talent retention
2. **Institutional Compliance Program**
  - ◆ Code of Conduct
  - ◆ Training and Education
  - ◆ Communication
  - ◆ Disciplinary Action
  - ◆ Policies and Procedures
  - ◆ Auditing and Monitoring
  - ◆ Response and Prevention
  - ◆ Healthcare disparities / equity
  - ◆ Healthcare worker safety / mental health
3. **Departmental Compliance**
  - ◆ Pharmacy
  - ◆ Emergency Department (EMTALA)
  - ◆ Wound Care
  - ◆ Cancer Center
  - ◆ Laboratory
  - ◆ Radiology
  - ◆ PT/OT/ST
  - ◆ Operational Departments
4. **Contract Management/3<sup>rd</sup> Party Risk**
  - ◆ Physician Arrangements / Contracting
  - ◆ Joint Ventures
  - ◆ Vendor Agreements
  - ◆ Contract Repository
  - ◆ Third Party Vendor Management
5. **Conflict of Interest**
  - ◆ Board-level
  - ◆ Executive Leadership and Management
  - ◆ Non-employed Physicians
  - ◆ Foreign Support
6. **Clinical Research**
  - ◆ Research Compliance Program
  - ◆ Clinical Trials Billing
  - ◆ Human Subject Protection
  - ◆ Scientific Misconduct
  - ◆ Grant Management
  - ◆ Research Conflict of Interest
  - ◆ Institutional Review Board (IRB) Oversight
7. **Quality / Performance Improvement**
  - ◆ Patient Safety
  - ◆ Medical Errors
  - ◆ Patient Satisfaction
  - ◆ Value-Based Care
  - ◆ Quality Improvement / Benchmarking / Reporting
  - ◆ Joint Commission / Accreditation
  - ◆ HACs and Root Causes
  - ◆ Clinical related monitoring
  - ◆ Fraud, waste, and abuse prevention
8. **Hospital Coding and Billing**
  - ◆ Inpatient Coding ("compliance DRGs")
  - ◆ Short-Stay/Observation
  - ◆ Computer assisted coding
  - ◆ Admitting privileges/appropriate admission orders
  - ◆ Outlier payments/payments > charges
9. **Professional Coding and Billing**
  - ◆ Training and Education
  - ◆ Physician Documentation and Coding
  - ◆ Auditing and Monitoring
  - ◆ Computer assisted coding
  - ◆ Use of codes
  - ◆ Incident-to, split-shared, etc.
10. **Privacy and Security**
  - ◆ IT Security
  - ◆ Access and Permissions
  - ◆ Physical and Device Security
  - ◆ Privacy, Security, and Compliance readiness
  - ◆ Data with external, internal, or external intelligence
  - ◆ Data protection / data segmentation
11. **Assets Management / Procurement**
  - ◆ 340B Drug Pricing Program
  - ◆ Retail Pharmacy Pricing
  - ◆ Vendor background checks
  - ◆ Vendor vulnerability (single-source)
  - ◆ Vendors with PHI access / Business Associate Agreements
12. **Specific Compliance/Regulatory Risks**
  - ◆ Recovery Audit Contractor Readiness
  - ◆ Provider-based Status
  - ◆ Durable Medical Equipment
  - ◆ Cost reporting
  - ◆ Stark & Anti-Kickback
  - ◆ Medical Device Management
  - ◆ Manufacturer Credits for Medical Devices
  - ◆ Medical Necessity
  - ◆ Synchronized Providers
  - ◆ HIPAA Privacy & Security
  - ◆ Kick-Backs
  - ◆ Physician compliance / engagement
13. **Alternate Payment Models/Delivery**
  - ◆ Accountable Care Organization reporting
  - ◆ Telehealth and Virtual Care compliance
  - ◆ Price transparency
  - ◆ Population Health
14. **Other programs/services**
  - ◆ Inpatient Psychiatry
  - ◆ IP Rehabilitation
  - ◆ Ambulance Services
  - ◆ SNF, Hospice, Home Health (requirements for certification/payment)
15. **COVID-19 Regulatory and Financial Relief**
  - ◆ COVID-19 Relief Program Compliance
  - ◆ COVID-19 Waivers
  - ◆ COVID-19 Coding and Billing
  - ◆ Vaccine distribution
16. **Medical Education**
  - ◆ Program Quality & Accreditation
  - ◆ Affiliation Management
  - ◆ Faculty Recruiting & Retention
17. **Revenue Cycle**
  - ◆ Scheduling / Verifications
  - ◆ Registration / Admitting
  - ◆ Charge Description Master (CDM)
  - ◆ Charge Capture
  - ◆ Patient Billing / Collections
  - ◆ A/R Denials, Bad Debt
  - ◆ Credit Balances & Refunds
  - ◆ CMS PEPPER Monitoring
  - ◆ Payor Audits
  - ◆ In-house vs. Outsourced Functions

## Some questions to consider when developing the compliance risk universe:

- What regulatory compliance risk areas are applicable to us?
- What sources (both internal and external) should be included, given applicable compliance risk areas, for a comprehensive compliance risk universe?
- Where across the organization do key compliance risks reside (e.g., Revenue Cycle, Information Technology, Operations)?

11

# Risk assessment methodology | Conduct the assessment

Risks can be identified using a variety of methods

### Facilitated one-on-one interviews

- Interviews can be targeted to relevant and specific risks
- Provides opportunity to dig deeper into specific risk areas
- Participants are more willing to discuss risks/concerns
- Discussions are confidential and interviewees may feel more comfortable sharing information

### Facilitated group interviews

Provides opportunity to break down organizational/information silos

- Can provide end-to-end view of a process or risk impact
- Efficient for Internal Audit
- Voting technology can provide degree of confidentiality
- Need to be led by a skilled facilitator

### Facilitated polling session

### Survey

### Risk sensing

12

## Example risk assessment questions

### Risk identification

✓	Describe your areas of responsibility and your history with the organization
✓	What are the major objectives within your entity, function or department (as applicable)?
✓	Please describe the most significant regulatory compliance risks related to your function or department?
✓	Describe the regulatory compliance topics or issues you “worry” about – what are those items, whether within your span of control or not – that could be improved?
✓	Are there any historic or current compliance challenges or concerns that you feel are important for us to know about?
✓	What are your thoughts on the culture of the organization? Do individuals feel empowered to raise questions or concerns? Why or why not?
✓	Where would you allocate compliance resources if you were responsible for the compliance function and why?

13

## Polling question # 3

### What risk assessment method do you use the most?

- A. Interviews (group and/or individual)
- B. Surveys
- C. Risk sensing
- D. All of the above

14

## Step 3: Risk prioritization



15

### Risk ranking criteria

Risk prioritization

The criteria most commonly used for risk ranking during the assessment process are **impact and vulnerability**.

Impact is an estimate of the severity of adverse effects, the magnitude of a loss, or the potential opportunity cost should a risk be realized. Impact can be thought of as gross inherent risk.

Vulnerability is the extent to which the functional area may be exposed or unprotected in relation to various risk factors after existing controls have been considered. Vulnerability can be thought of as net residual risk.

You should work with your leadership team to customize and specifically define **High, Medium, and Low values for impact and vulnerability criteria** in a way that's relevant to your organization.

16

## Prioritizing risks: Impact criteria

Impact should be assessed based on both relevant financial and non-financial dimensions. Risk should not be defined solely based on financial impact, as other non-financial impacts (e.g., reputation) can be equally as important even though they may not be readily measured in financial terms. A risk rating (e.g., low, medium, high) will be assigned if the risk meets any of the criteria defined for that rating.

### ILLUSTRATIVE

Risk Criteria:		Low (1 - 3)	Medium (4 - 6)	High (7 - 9)
Impact	Importance or impact to the organization achieving their objectives.			
	<b>Financial</b>	<ul style="list-style-type: none"> <li>Minimal financial impact in terms of fines, penalties, cost of mitigation, lost revenue, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Moderate financial impact in terms of fines, penalties, cost of mitigation, lost revenue, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Significant financial impact in terms of fines, penalties, cost of mitigation, lost revenue, etc.</li> </ul>
	<b>Ability to operate</b>	<ul style="list-style-type: none"> <li>Minimal impact on ability to deliver highest quality, and innovative patient care (e.g., operations are minimally impacted)</li> </ul>	<ul style="list-style-type: none"> <li>Moderate impact on ability to deliver highest quality, and innovative patient care (e.g., operations are limited)</li> </ul>	<ul style="list-style-type: none"> <li>Significant impact on ability to deliver highest quality, and innovative patient care (e.g., significant interruptions of business operations for two or more key service lines; wide-spread impact on patient satisfaction: serious threat to future growth)</li> </ul>
	<b>Reputation</b>	<ul style="list-style-type: none"> <li>Minimal damage to public image and reputation</li> </ul>	<ul style="list-style-type: none"> <li>Moderate, limited term damage to public image and reputation (e.g., regional media attention)</li> </ul>	<ul style="list-style-type: none"> <li>Significant, sustained damage to public image and reputation (e.g., national media attention)</li> </ul>

HCCA 2021 Annual Compliance Institute 17

17

## Prioritizing risks: Vulnerability criteria

Vulnerability refers to the organization's susceptibility to a risk in terms of environmental factors related to the organization's preparedness, agility, and adaptability. Vulnerability component incorporates the concept of "management (or control) effectiveness"

### ILLUSTRATIVE

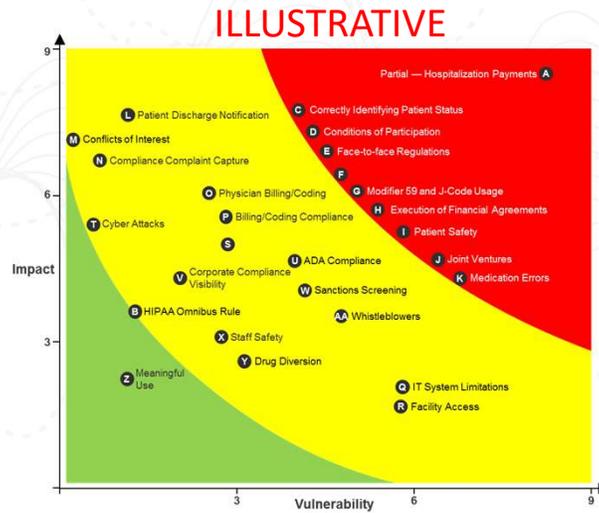
Risk Criteria:		Low (1 - 3)	Medium (4 - 6)	High (7 - 9)
Vulnerability	The extent to which the functional area may be exposed or unprotected in relation to various risk factors given the existing control environment.			
	<b>Process / Controls maturity</b>	<ul style="list-style-type: none"> <li>Process/controls are well-developed and have been in place for over a year</li> </ul>	<ul style="list-style-type: none"> <li>Process/controls are new (less than one year old)</li> </ul>	<ul style="list-style-type: none"> <li>Process/controls are still being developed</li> </ul>
	<b>Known previous compliance risk</b>	<ul style="list-style-type: none"> <li>No known previous compliance risks/incidents</li> </ul>	<ul style="list-style-type: none"> <li>Isolated previous compliance risks/incident</li> </ul>	<ul style="list-style-type: none"> <li>Multiple previous compliance risks/incidents</li> </ul>
	<b>Third party stakeholder (includes government) focus and/or enforcement activity</b>	<ul style="list-style-type: none"> <li>Minimal third party focus and/or enforcement activity.</li> </ul>	<ul style="list-style-type: none"> <li>Moderate, short-term third party focus and/or enforcement activity.</li> </ul>	<ul style="list-style-type: none"> <li>Significant, prolonged third party focus and/or enforcement activity.</li> </ul>
	<b>Existing compliance activity / resources</b>	<ul style="list-style-type: none"> <li>Adequate, proactive compliance activity / resource focus on risk area</li> </ul>	<ul style="list-style-type: none"> <li>Limited, reactive compliance activity / resource focus on risk area</li> </ul>	<ul style="list-style-type: none"> <li>Inadequate compliance activity / resource focus on risk area</li> </ul>

HCCA 2021 Annual Compliance Institute 18

18

## Prioritizing risks: Heat map view

The results of your assessment should be compiled and summarized. Organizations often present results on a “heat map” based on the agreed-upon ranking criteria. The following is an example of what a completed “heat map” might look like:



HCCA 2021 Annual Compliance Institute 19

19

## Learn how to approach risks using different techniques – not everything is an “audit”

Once you have this information and know your “higher risks” – then what?

✓	What falls to the audit workplan?
✓	What falls to monitoring? Can you incorporate analytics/continuous monitoring?
✓	What requires working with operations to improve policies? Where can/should compliance play the role of advisor?
✓	Are there areas that could benefit from specialized training?
✓	Consider the skills and knowledge of your team and where you may need outside help (don't limit your plan and how you address risks based on the resources on your team – that could be a fatal flaw)

HCCA 2021 Annual Compliance Institute 20

20

## Learn how to approach risks using different techniques – not everything is an “audit”

Improvement process

✓	Consider June 2020 DOJ guidance – How has the compliance program evolved over time to address existing and changing compliance risks?
✓	Consider – Can you show a 3-year “trend” in your top 10 risks, where items started off as high and you took mitigation steps?
✓	Has the company engaged in meaningful efforts to review its compliance program and confirm that it’s not stale?
✓	Consider – compliance culture surveys that are short and perhaps random? Do you conduct them 2-3 times/year to employee groups to get a “pulse” on the organization?
✓	Set annual goals for improving pieces of your program – for example, cleaning up your issues tracking system or log and then setting new standards, processes, etc. so that it’s more current and meaningful.
✓	Be able to “tell the story” when significant issues were identified during the year – what was the corrective action? How do you know it worked? Consider an annual report?

21

## Evaluation & Management Coding – Rolling Out the New Guidelines



Training vs. education

Proactive vs. reactive measures

- EMR coding algorithms/software
- E/M coding calculation tools
- Educational materials
- Create internal coding tools
- Lunch n’ learn sessions

Targeted education sessions – creating educational content specific to their job function

- Physicians
- Coder/billers
- Accounts receivable (A/R) – collectors
- Revenue integrity
- Clinical data management (CDM) team
- IT/Clinical IT teams
- C-Suite

22

## Exclusion and sanction screening

### Invest in an efficient and effective application that caters to the organization's need

- Avoid convoluted processes
- Contracting follow-up services for compliance teams who may lack the bandwidth to confirm all findings are resolved
- Internship opportunity
  - Healthcare administration programs – local universities
  - Sanction/exclusion screening procedure template

### Identify appropriate federal and state sources (examples):

- System for award management (SAM.gov)
- OIG exclusions database
- State Medicaid exclusion lists

### Communication plan

- Develop a formal rollout plan to communicate with affected departments

### Seamless process & symmetry between the key stakeholders:

- Medical staff office
- Human resources
- Compliance

23

## Polling question #4

**When my organization develops an annual compliance workplan, it includes more than an audit plan.**

- A. Yes
- B. No

24

## Step 4: Development of compliance work plan



25

### Development of compliance audit & monitoring work plan

Areas of identified compliance risk will be prioritized and used to develop a proposed workplan for compliance auditing and monitoring, including resource requirements

#### ILLUSTRATIVE



Significant risk consideration	Risk rating	Audit/Monitoring description	Frequency
Physician arrangements	High (Red)	Review, documentation and analysis of the design of controls over physician arrangement management including review of arrangements sample for compliance and control operating effectiveness.	Annual
Physician time reporting	Medium (Yellow)	Post-implementation assessment of the new physician time and effort process and system with selected control testing for operating effectiveness.	Annual
Records retention	Medium (Yellow)	Review of the records retention policy and processes / controls in place to assess adherence to the policy, including limited sample testing for control operating effectiveness.	Annual
Privacy and Security: User access to systems containing PHI	Medium (Yellow)	Periodic review of terminated employees to assess access to systems housing PHI has been removed	Monthly
Privacy and Security: Business Associate Agreement (BAAs)	Medium (Yellow)	Periodic reconciliation of business associate repository to make sure the list remains current and up to date, including BAAs for all vendors accessing PHI	Quarterly

HCCA 2021 Annual Compliance Institute 26

26

## Auditing and monitoring workplan

Audit or monitoring planning template

**ILLUSTRATIVE**

Risk Area	Audit Title	Audit or Monitoring Description	Process Owner	Timing (Quarter)	Budgeted Hours/Weeks
OIG High-Risk DRGs	Ongoing monitoring of selected high-risk DRGs identified by the OIG	Compliance will collaborate with HIM and CDI to identify the top 10 Medicare volume DRGs for the hospital and overlap with the OIG's list of DRGs that are high-risk/prone to coding error; an analytics dashboard will be developed with the help of the IT/business intelligence team	Compliance Analyst	Ongoing – start 1 <sup>st</sup> quarter 2021; roll out by 2 <sup>nd</sup> quarter and perform ongoing quarterly thereafter	5 hours/week through 2 <sup>nd</sup> quarter; 8 hours/month after/for remaining 2021

HCCA 2021 Annual Compliance Institute 27

27

## Compliance workplan for non-audit areas

Use this template when training or other “advisory support” is the appropriate risk response

**ILLUSTRATIVE**

Risk Area	Compliance Activity	Frequency/ Timing	Responsible Party	How will this be reported?	Resources Needed
New E&M coding guidelines for 2021	Support the organization's implementation of the new guidelines	4 <sup>th</sup> quarter 2020/1 <sup>st</sup> quarter 2021	Compliance E&M coding trainer	Training activities will be summarized and reported to the compliance committee	XXX hours of compliance support (E&M coder/training expert)
Exclusion/Sanction Screening	Assess external systems/vendors and contract with an external vendor for exclusion/sanction screening	1 <sup>st</sup> and 2 <sup>nd</sup> quarter 2021; goal to implement by end of 2021	Compliance Analyst	Results of the external vendor review/diligence and a recommendation will be presented to the compliance committee at the end of the 2 <sup>nd</sup> quarter	XXX hours of compliance analyst support
CARES Act/Provider Relief Fund funding	Continue to monitor organization's receipt of federal funds, ongoing attestation timeliness and advise on ongoing tracking of use of funds	Ongoing throughout 2021	Compliance Director	Ongoing agenda item at compliance committee meetings	XXX hours of compliance director support per quarter
CMS Waivers/Public Health Emergency	Monitor the organization's use and implementation of the various CMS waivers; track for waiver expiration/advise the business	Ongoing throughout 2021	Compliance Director	Ongoing agenda item at compliance committee meetings	XXX hours of compliance director support

HCCA 2021 Annual Compliance Institute 28

28

## Speaker bios



### Kelly J. Sauders

Partner  
Deloitte & Touche LLP  
[ksauders@deloitte.com](mailto:ksauders@deloitte.com)

#### RELEVANT EXPERIENCE

Kelly is a partner with Deloitte & Touche LLP with more than 25 years of experience providing risk, internal controls, compliance, and internal audit services to health care providers. She specializes in providing regulatory compliance, risk assessment, internal controls, and regulatory services to health care organizations. Kelly has assisted over a hundred companies with the development, implementation and assessment of their compliance programs over the course of her career. She has worked on numerous general and specialized regulatory compliance projects addressing topics such as hospital-physician contracting and financial relationships, coding, billing and clinical documentation, clinical research billing, off-label use of drugs/pharmacy billing, EMTALA, and medical necessity.

Kelly has also served as an interim compliance officer and as an interim director of internal audit for several clients, including AMCs and health systems. She has also supported organizations during OIG compliance reviews, government investigations and self-disclosures and in preparing for and operating under Corporate Integrity Agreements. Kelly is a Certified Public Accountant (CPA) licensed in the state of New York.



### Leslie V. Boles, BA, CCS, CPC, CPMA, CHC, CPC-I, CRC

Director of Compliance Audit  
Waud Capital Partners  
[lboles@waudcapital.com](mailto:lboles@waudcapital.com)

#### RELEVANT EXPERIENCE

Leslie Boles currently serves as the Director of Compliance Audit at Waud Capital Partners and a Coding Instructor at Rutgers University. She has more than 13 years of experience in healthcare, coding, auditing and compliance in the hospital inpatient/outpatient settings, and physician coding education.

Leslie has developed and implemented multiple training programs on physician coding and documentation, Medicare and Medicaid policy and compliance programs for certified coders. She is a subject matter expert in the areas of E/M, Radiology, OBGYN, General Surgery, Cardiology and Anesthesia coding.

She prides herself in presenting very complex coding and documentation regulations in a simplified manner to physicians and clinicians. She has the credentials of CCS, CPC, CPMA, CHC, CPC-I and CRC from the American Academy of Professional Coders, American Health Information Management Association and the Health Care Compliance Association. Leslie obtained her Bachelor's Degree in Healthcare Administration from The University of Arizona. She is member of the Board of Directors and the Compliance Committee Co-Chair of the Healthcare Financial Management Association (HFMA), NJ chapter. She is a coding mentor for the local AAPC and AHIMA chapters and enjoys mentoring young talent.