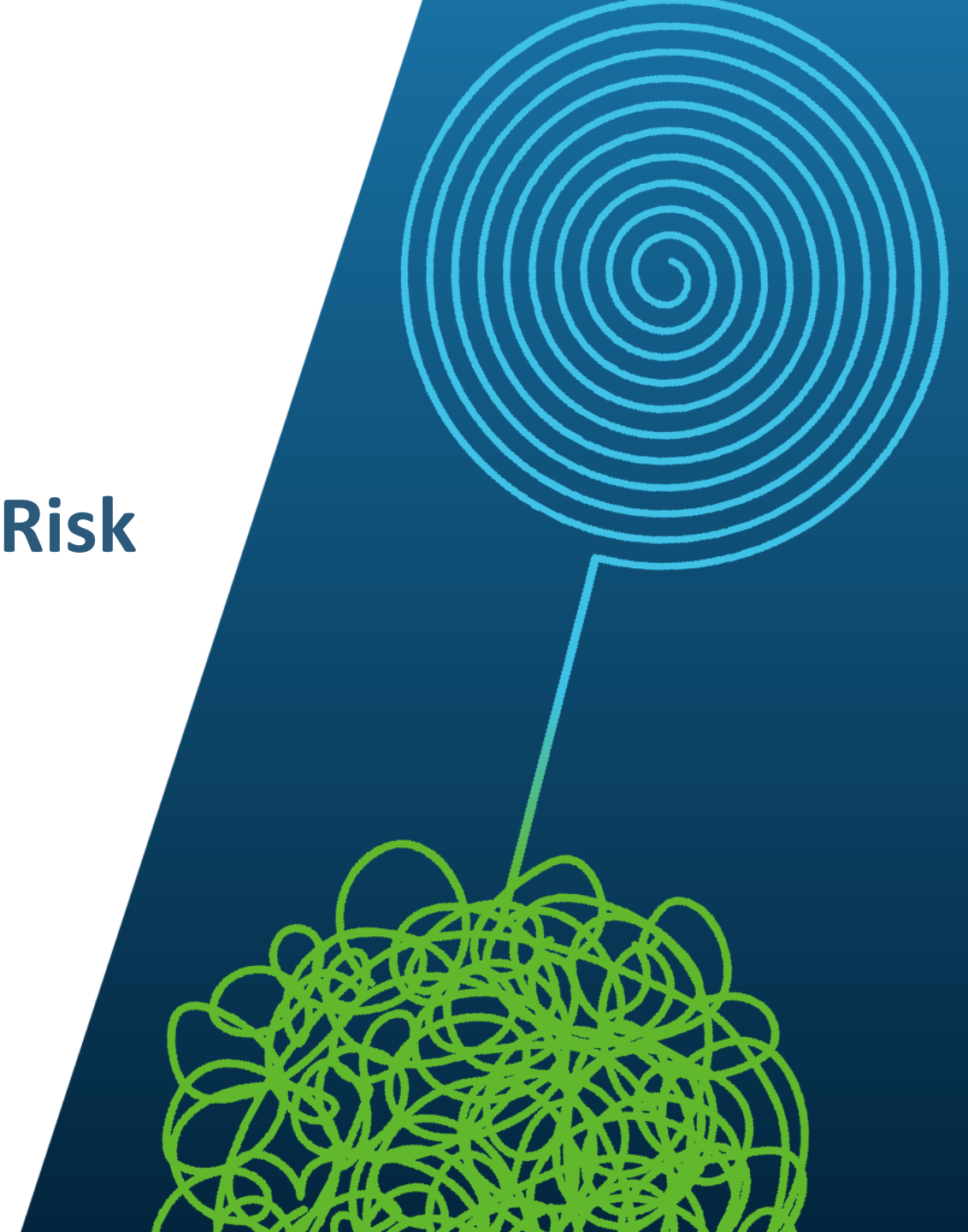
Healthcare Regulatory Roundup #109

Top 10 Healthcare Compliance Risk Areas Managers Need to Know

February 18, 2026



© 2026 PYA, P.C.
WE ARE AN INDEPENDENT MEMBER OF HLB—THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

Housekeeping

- Slides, handouts, and forms available in **Resources Panel**
- Enter questions in **Q&A Panel** – questions will be responded to via e-mail after the webinar
- Enlarge, rearrange, or close panels as you prefer
- For technical difficulties, try refreshing your browser

Introductions



Shannon Sumner
Principal, CCO
ssumner@pyapc.com



Miriam Murray
Senior Manager
mmurray@pyapc.com



Katie Croswell
Manager
kcroswell@pyapc.com

PYA
pyapc.com
865.673.0844

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

Today's Agenda

Top 10 Compliance Risks:

1. Outsourced Arrangements
2. Vendor Oversight
3. Administrative Compensation and Compensation Stacking
4. Cybersecurity and Data Breaches
5. Artificial Intelligence (AI)
6. Digital Transformation and Digital Care
7. Healthcare Real Estate
8. Emergency Medical Treatment and Labor Act (EMTALA)
9. Exclusion Screenings
10. Reimbursement Pressures

1. Outsourced Arrangements

Common Outsourced Arrangements

- Clinical services and staffing
- Medical directors
- Technology and software including EHR systems
- Recruitment
- Coding
- Billing

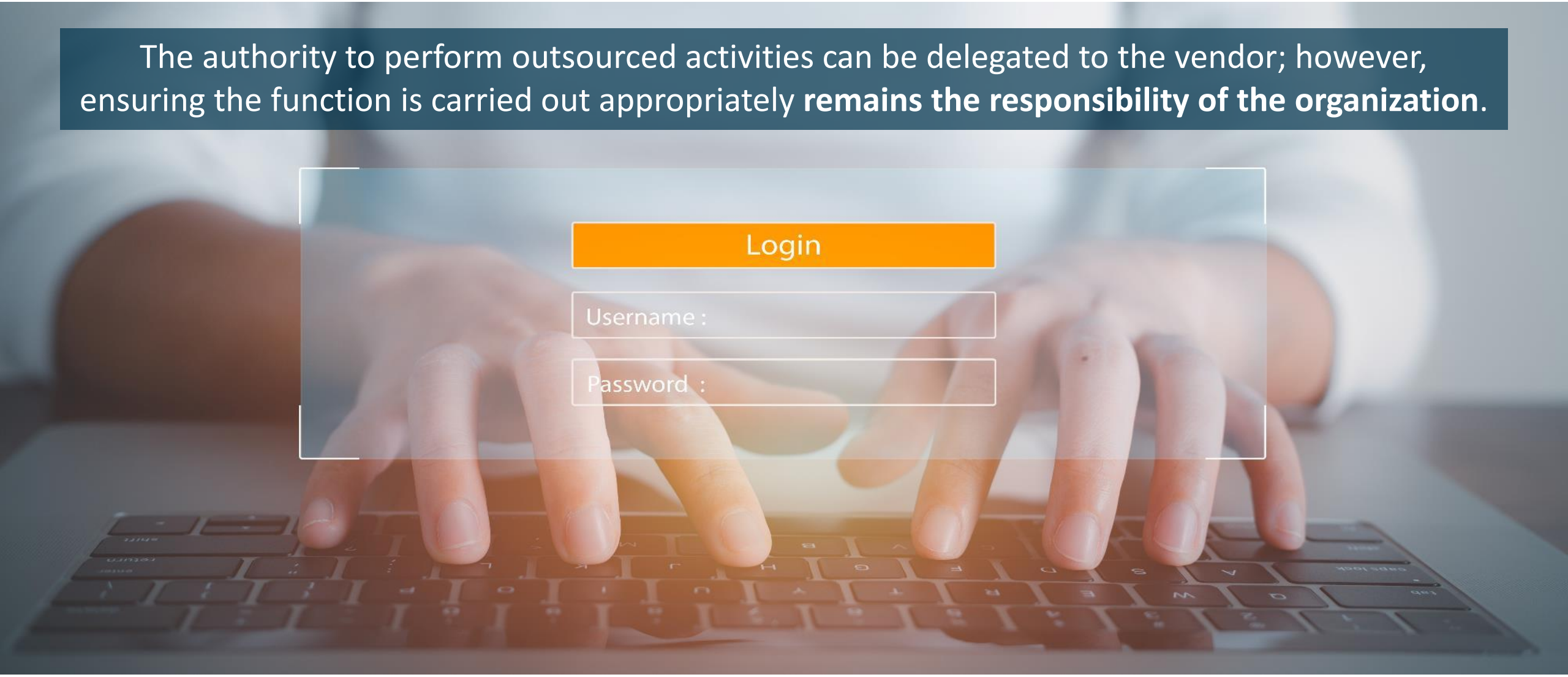


Common Outsourcing Risks

- Medical record documentation
- Medical necessity
- Medicare and Medicaid supervision requirements
- HIPAA, privacy, cybersecurity
- Conditions of participation
- Conditions payment
- Fraud by vendor or partner

Responsibility *Doesn't* Transfer

The authority to perform outsourced activities can be delegated to the vendor; however, ensuring the function is carried out appropriately **remains the responsibility of the organization**.



Best Practices – Outsourced Vendor Arrangements

- **Due diligence**
  - Understand the arrangement; research the service and the vendor/partner
- **The agreement**
  - Emphasize performance guarantees and performance monitoring
  - Expectations should be documented regarding confidentiality, audit rights and contract termination if the vendor's performance is unacceptable and consistently does not meet organizational expectations
  - Indemnification and Insurance
  - Compliance with laws (be specific)
  - Certification process
- **Policy and procedure**
  - Contracting policy
  - Vendor Management policy
- **Auditing and monitoring**
  - Business departments who utilize outsourced activities must ensure appropriate oversight and monitoring of the vendor's performance is occurring

2. Vendor Oversight

Examples of Third-Party Vendors

Medical Device Manufacturers	IT Service Providers (*IT support, network management, cybersecurity services*)	Telehealth Platforms	Electronic Health Record (EHR) Providers
Cloud Service Providers	Third-Party Administrators	Billing and Coding Firms	Laboratory Services
Supply Chain Vendors	Data Analytic Companies	Consultant and Advisors	Marketing and Website Services

Third-Party Risk Management (TPRM) Lifecycle



Vendor Risk Assessment: Due Diligence Considerations

Do your homework!

- Data Privacy & Security Breaches
- Regulatory Non-Compliance/Settlement Agreements (CIAs)
- Cybersecurity Incidents and Security Ratings
- Conflicts of Interest
- Compliance Program Maturity
- Financial and Operational Stability
- Excluded Providers

DOJ's Evaluation of Corporate Compliance Programs (September 2024)

- Third-party risk management expectations:
  - **Risk-based and integrated processes**
    - Integrated with the entity's procurement and vendor management processes
  - **Appropriate controls**
    - Ensuring appropriate business rationale for the use of third parties
    - Do contract terms specifically identify the services to be performed?
  - **Management of relationships**
    - How does the company monitor performance? Audit rights?
  - **Real actions and consequences**
    - Mitigation of due diligence identified risks

3. Administrative Compensation and Compensation Stacking

Administrative Compensation for Physicians and Physician Practices – Common Challenges

- Work is not performed at all, not documented properly or took less time than the physician was paid for
- Payment is made without supporting documentation
- Services are not commercially reasonable (CR)
  - For example, paying two physicians in the same system administrative pay to develop the same set of protocols
- Administrative compensation needs to be stacked with other elements of compensation to ensure the totality of the compensation package remains consistent with Fair Market Value (FMV)

Compensation “Stacking” – Common Challenges

- The individual elements (e.g., base compensation, call pay, and medical director) appear consistent with FMV in isolation, but the total package is too high or does not make sense from a CR perspective because a single physician could not provide all of those services.
  - This is harder to evaluate for community physicians where the hospital does not have sight lines into the total compensation level or the clinical productivity level for services outside of the hospital setting.
    - We saw an instance where physician leaders had very busy private practices (75th percentile level of activity) but when all administrative agreements were totaled, they had more than 2,000 hours of obligation over and above their private practice.
  - This can get very tricky for value-based payments that come from commercial payers for physicians employed by the hospital.
    - It will take a while for value-based payment data to make its way into the benchmark survey data which lags by a year at least.

4. Cybersecurity and Data Breaches

Healthcare Cyber Risks on the Rise

Ransomware attacks including removing system backups and encryption of electronic health records

Greater reliance on cloud-based services due to remote (non-clinical) workforce

Medical device software vulnerabilities

Third-party software vulnerabilities

Human error

Phishing attacks

(Common entry point and becoming more sophisticated, bypassing multifactor authentication and business email compromise attacks)

2025 Cyber Crime Targets

- Healthcare systems, including specialty clinics and physician groups, continue to be a top target for cyberattacks
- Hackers have pivoted their focus to third-party vendors, software services, business associates, non-hospital providers, and health plans
- **As of December 2025, there were 697 data breaches reported to HHS-OCR affecting over 60,976,942 individuals.***
- Over 80% of stolen PHI records in 2025 were taken from third-party vendors, IT service providers, and non-hospital partners…not hospitals themselves, according to the American Hospital Association.*

*Sources:
https://www.hipaajournal.com/december-2025-healthcare-data-breach-report/
https://www.aha.org/news/aha-cyber-intel/2025-10-07-2025-cybersecurity-year-review-part-one-breaches-and-defensive-measures

Cyber-Fraud and Data Breach Mitigation: What Healthcare Managers Need to Know

- Recommendations:
  - **Human error is still the #1 cause**
    - Build a security-aware culture
    - Ensure team members are aware of company policies and reporting requirements
  - **Compliance**
    - Proactively update cybersecurity and information systems security policies.
    - Conduct documented risk analyses and remediation plans
    - Ensure BAAs are updated and enforced
  - **Strong access controls**
    - Require Multi-Factor Authentication (MFA) across all systems
    - Enforce “minimum necessary” access
    - Conduct access reviews (quarterly) and remove dormant accounts immediately

5. AI

AI and Privacy Risk

- AI in healthcare offers transformative benefits for efficiency, improved care, and patient experiences across diagnostics, administration, and patient engagement, but also introduces significant risks, especially when sourced from third-party vendors.
  - System security
  - Cybersecurity threats
  - Improper use of AI tools
- HIPAA regulates how PHI is collected, used, disclosed, and secured. In addition, AI tools utilizing PHI must comply with the same HIPAA standards as all other technologies.
- Healthcare organizations must understand how AI platforms use PHI—whether internal or provided by business associates.

AI and Risk-Mitigating Strategies

- Healthcare organizations must build AI-specific privacy programs, including:

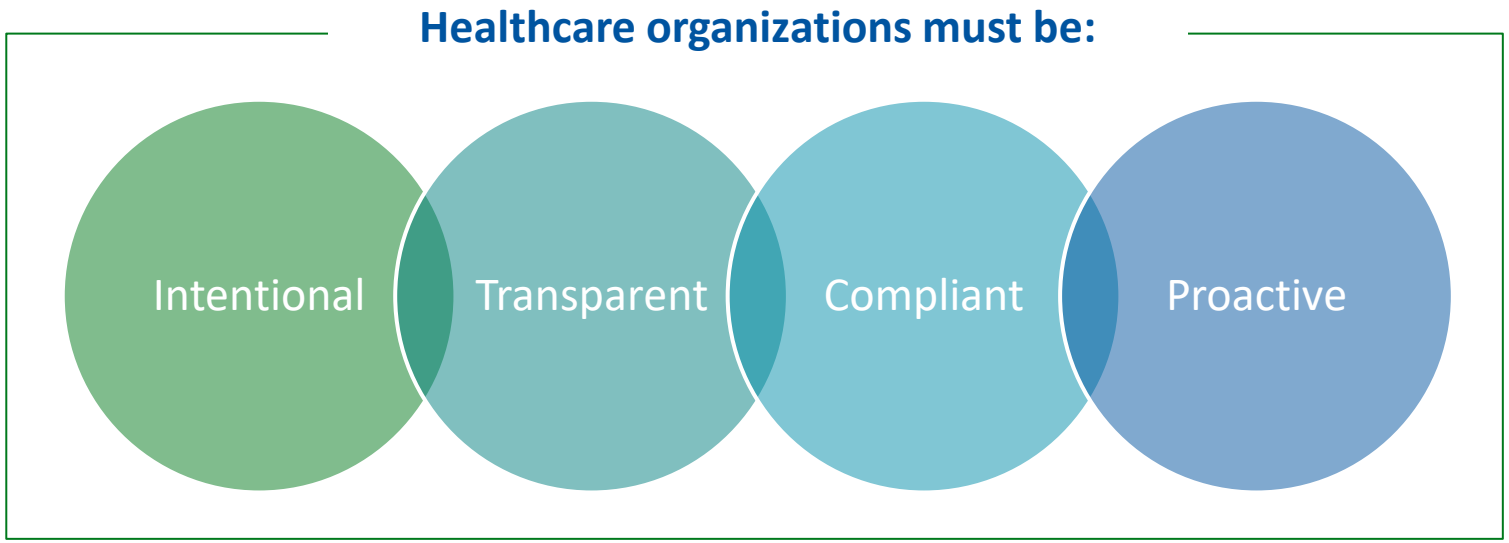
1. Comprehensive AI inventory
2. AI-specific risk assessments



3. Minimum-necessary configuration
4. Strong technical safeguards
5. Establishing AI specific policies and workforce training
6. Continuous monitoring & auditing
7. Incident response protocols
8. Business associate oversight
9. Vendor due diligence

Key Takeaways

1. Maintain an organization-wide AI inventory.
2. Monitor evolving AI-related privacy laws.
3. Continuously adapt privacy/security programs.
4. Balance AI benefits with heightened privacy risks.
5. Embed compliance and privacy protections into every stage of AI adoption.



6. Digital Transformation and Digital Care

Digital Transformation and Digital Care

- **What is Digital Transformation?**
  - It is an organization-wide shift from traditional/manual process to technology-enabled workflows to improve efficiency, quality, decision-making, and patient outcomes.
  - In healthcare, Digital Transformation includes:
    - Implementing unified EHR systems
    - Automating revenue cycle functions
    - AI-assisted clinical documentation
    - Digital onboarding and patient intake
    - Virtual patient care
    - Predictive analytics for quality and safety
    - Advanced cybersecurity modernization

Digital Care

- **Digital Care** refers specifically to the clinical delivery of healthcare through digital tools and virtual modalities
  - Forms of Digital Care include:
    - Telehealth/telemedicine
    - Remote Patient Monitoring/digital devices (RPM/RTM)
    - Digital therapeutics
    - Mobile health apps and patient portals
    - AI-enabled care assistants



How Healthcare Managers Can Help with Digital Care Compliance

- Healthcare managers play a central role in ensuring privacy, security, proper documentation, billing compliance, and staff adherence to federal and state regulations.
  - Understand how digital care is being used by team members and vendors in your company/department
  - Update policies, procedures, and staff training for digital care services
  - Monitor/review telehealth-specific and RPM services and workflows for compliance with government regulations
  - Document all patient digital care encounters properly including patient identity and patient consent
  - Integrate compliance into daily digital care operations
  - Support ongoing monitoring, quality improvement, and reporting

https://telehealth.hhs.gov/providers/best-practice-guides

7. Healthcare Real Estate

Risks to Watch for in Real Estate

Ascension Sacred Heart Pensacola agreed to pay **$2.4 million** for allegedly violating the civil monetary penalties law by paying remuneration in the form of free or below fair market value space, equipment, and personnel – *February 28, 2023*

https://oig.hhs.gov/fraud/enforcement/ascension-sacred-heart-pensacola-agreed-to-pay-24-million-for-allegedly-violating-the-civil-monetary-penalties-law-by-paying-remuneration-in-the-form-of-free-or-below-fair-market-value-space-equipment-and-personnel/



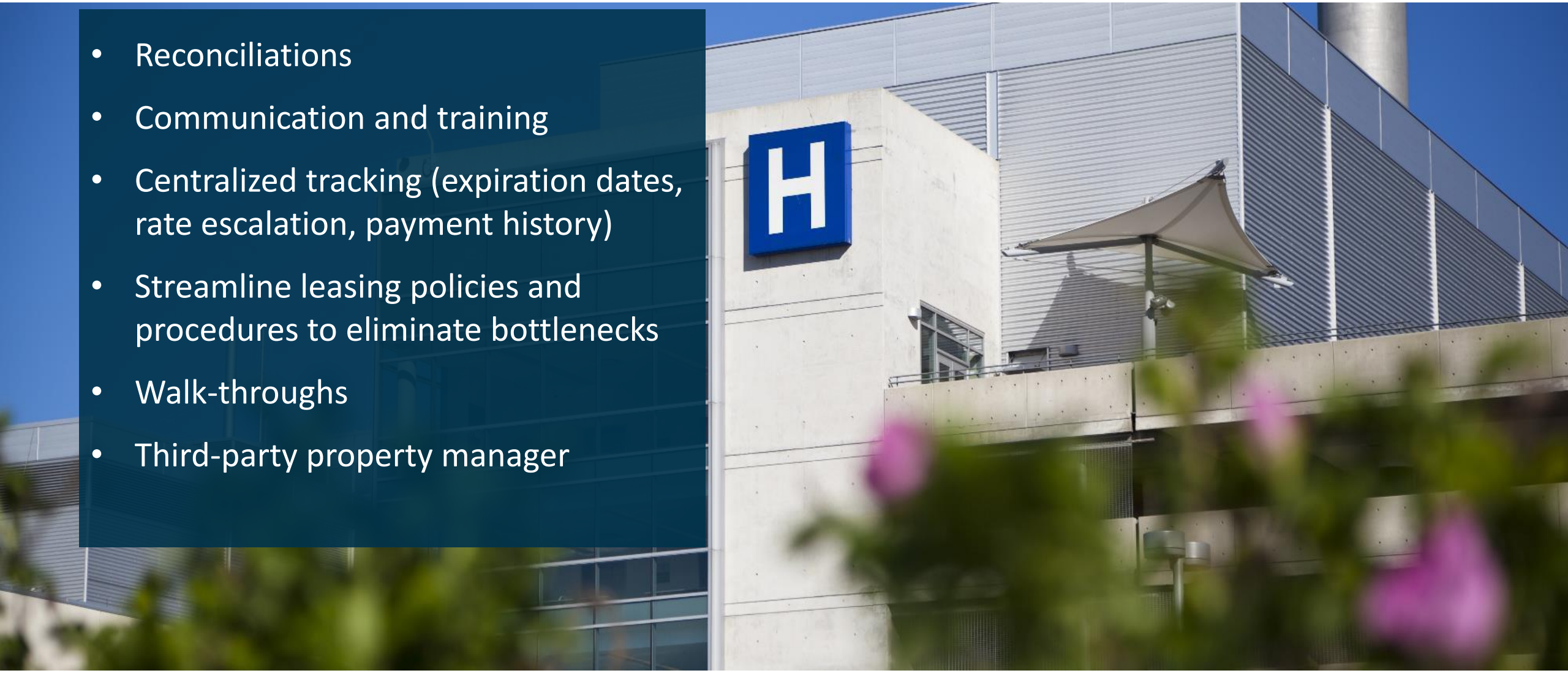
Healthcare Real Estate Common Challenges

- Hospital leases to physicians at rates that are below or above FMV or under terms that are not Commercially Reasonable
- Terms are extremely long and don’t give the parties the ability to adjust for changing market conditions (no annual escalators)
- Physician tenants fail to pay
- Lease expires but space continues to be occupied
- Space creep
- Hospital staff supporting physician
- Emergency Department used “after office hours” for treatment



Real Estate Best Practices

- Reconciliations
- Communication and training
- Centralized tracking (expiration dates, rate escalation, payment history)
- Streamline leasing policies and procedures to eliminate bottlenecks
- Walk-throughs
- Third-party property manager



8. EMTALA

EMTALA Overview

- Section 1867 of the Social Security Act imposes requires Medicare-participating hospitals that offer emergency services to provide medical screening examination (MSE) furnished by qualified medical personnel (QMP) when request is made for examination or treatment for emergency medical condition (EMC) (including active labor) regardless of individual's ability to pay.
  - When a patient:
    - **Presents at dedicated emergency department (DED) requesting examination or treatment of any medical condition**
    - **Presents on hospital property requesting examination or treatment of what may be an EMC**
    - **Is in hospital-owned/operated ambulance**
    - **Is in a non-hospital owned ambulance on hospital property (e.g., 250 yards of main building) for presentation at the DED**

EMTALA Overview

- Hospitals required to provide stabilizing treatment for patients with EMCs.
- If a hospital is unable to stabilize a patient within its capability, or if the patient requests, appropriate transfer should be implemented.



https://www.cms.gov/Regulations-and-Guidance/Legislation/EMTALA

Stabilizing Treatment – Evidence of Treatment

- Is it performed **within the capability of facility and staff**?
- Confirm that **all physicians are presenting to the facility when called** and in compliance with timeframe set forth in facility policy.
- Is there **a communication process between the clinical staff and registration staff** so that any required prior authorization can be sought once stabilizing treatment has been initiated?
- **Continued care** could be reasonably performed as an outpatient or later as an inpatient?
- Are patients **discharged with appropriate instructions** for follow-up care?
- Has **follow-up care availability** been identified?

Stabilizing Treatment

- Providing treatment within hospital's capabilities to stabilize for discharge or transfer:
  - If physician believes pregnant patient presenting at ED is experiencing EMC, and that abortion is stabilizing treatment necessary to resolve that condition, physician must provide that treatment.
  - When state law prohibits abortion and does not include exception for the life of pregnant person — or draws exception more narrowly than EMTALA's EMC definition — state law is preempted.
  - When direct conflict exists between EMTALA and state law, EMTALA must be followed.
  - EMTALA's whistleblower provision prevents retaliation by hospital against any employee or physician who refuses to transfer patient with EMC whose has not been stabilized by initial hospital, e.g., patient with emergent ectopic pregnancy, patient with incomplete medical abortion.

https://www.cms.gov/files/document/qso-22-22-hospitals.pdf

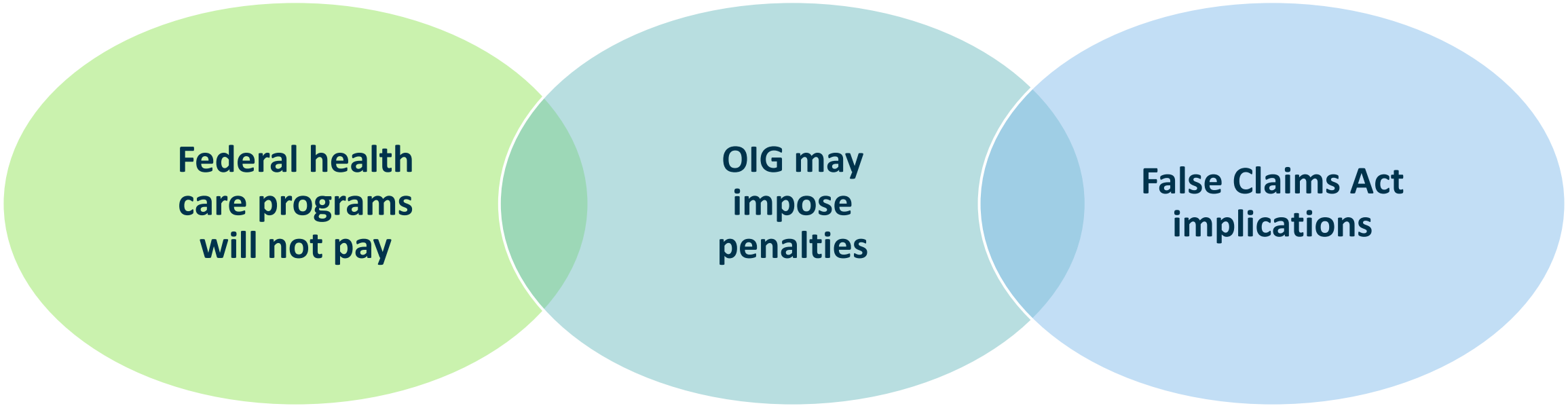
9. Exclusion Screenings

What is an Exclusion?

- Final administrative act that prohibits participation in any federal health care program (Medicare, Medicaid, and Tricare)
- Imposed on an individual or entity
- Posing unacceptable risk to patient safety and/or program fraud



Consequences to OIG Exclusion



2025 Settlement Cases

- **Center at Lowry Agreed to Pay $292,000**
  - Lowry employed an individual who was excluded from participating in any Federal health care program. OIG alleged that the excluded individual, a registered nurse, provided items or services that were billed to Federal health care programs.
- **Center at Northridge Agreed to Pay $227,000**
  - Northridge employed an individual who was excluded from participating in any Federal health care program. OIG alleged that the excluded individual, a registered nurse, provided items or services that were billed to Federal health care programs.
- **Kidspeace National Centers of New England Agreed to Pay $44,000**
  - Kidspeace, through a contractor, employed an individual who was excluded from participating in any Federal health care program. OIG alleged that the excluded individual, a speech pathologist, provided items or services that were billed to Federal health care programs.

Point of Care – Providers



Credentialed

Medical Staff Department



Non-Credentialed

Point of Care

Risks and Courses of Action

- **Risks**
  - What to watch for…
    - Employee turnover
    - Decentralization
    - Error reports
- **Excluded…now what?**
  - Contact Compliance Officer and CEO immediately.
    - Refer to policy and procedure
    - Suspend/revoke privileges
    - Investigate for self-disclosure



10. Reimbursement Pressures

Reimbursement Pressures

- Declining reimbursement rates across Medicare, Medicaid, and commercial payers that are not keeping up with inflation.
- Increased administrative burden (e.g., prior authorization requirement, complex billing rules, denial management, technology costs)
- Growth in value-based care expectations without matching infrastructure funding
  - Investment in care coordination, analytics, and reporting
  - Financial penalties if benchmarks aren't met
  - Savings are not guaranteed
- Rising labor, drug, and supply costs outpacing reimbursements
- Heightened payer scrutiny leading to more audits and recoupments (medical necessity, coding accuracy, bundled payments)

Best Offense



Thank you for attending!

PYA's subject matter experts untangle the latest industry developments each month in our popular Healthcare Regulatory Roundup webinar series.

For on-demand recordings of this and all previous HCRR webinars, and information on upcoming topics and dates, please follow the link below.

https://www.pyapc.com/healthcare-regulatory-roundup-webinars/

PYA

pyapc.com | 865.673.0844

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA



A national healthcare advisory services firm providing consulting, audit, and tax services