PAUL HASTINGS

New to Healthcare Conference Compliance and Privacy Roundtable

Dhara Satija, Healthcare Consulting Leader, Paul Hastings LLP

Timothy C. Hogan, Senior Vice President and Chief Compliance Officer, Boston Children's Hospital

Kristen Eversole, Associate Vice President and Chief Privacy Officer, UMass Memorial Health

October 25, 2024

Healthcare Consulting

Presenter Bios

Dhara Satija, CHC, CFE, CRCR
Healthcare Consulting Leader,
Life Sciences and Healthcare Consulting Group,
Paul Hastings, LLP
978-604-9939 |
dharasatija@paulhastings.com

Dhara Satija is the Director of Healthcare Consulting in the Life Sciences Consulting Group of Paul Hastings. Dhara has nearly 15 years of consulting experience serving healthcare and life sciences clients across an array of issues, including projects ranging from strategy and operations to regulatory and corporate compliance, risk management, and investigation and litigation support. In particular, Dhara has led projects related to: development and implementation of compliance programs (i.e., written standards, training, and monitoring/auditing); design and delivery of internal compliance audits, investigations, and corrective action plans; support for provider self-disclosures/voluntary refunds; government-initiated audits; litigation support services; and Corporate Integrity Agreement (CIA) requirements.

Timothy C. Hogan, JD, FHFMA, CHC
Senior Vice President and Chief Compliance Officer
Boston Children's Hospital
857-218-4680 |
Timothy.Hogan@childrens.harvard.edu

Tim Hogan is Senior Vice President and Chief Compliance Officer for Boston Children's Hospital. He has previously served in compliance leadership roles at Beth Israel Deaconess Medical Center, Elliot Health System, and Harvard Vanguard Medical Associates / Atrius Health.

Tim recently served as New England regional executive for the Healthcare Financial Management Association and is a past president of the Massachusetts/Rhode Island Chapter. He is also a former chair of the Chapter's Compliance Committee.

Kristen Eversole, BS, RHIA, CHPC
Associate Vice President and Chief Privacy Officer
UMass Memorial Health
774-823-0093 |
Kristen.Eversole2@umassmemorial.org

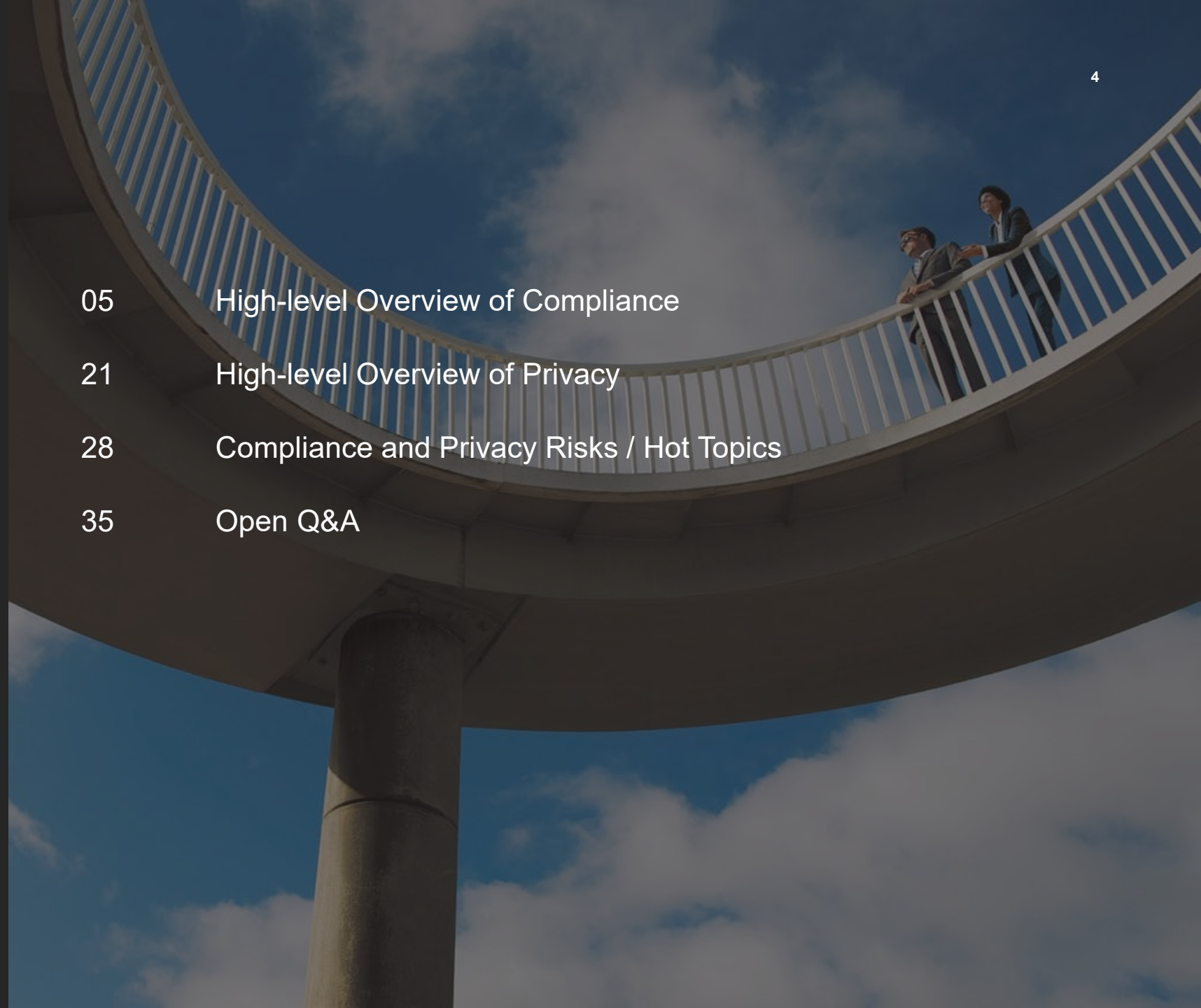
Kristen Eversole is currently the Associate Vice President and Chief Privacy Office for UMass Memorial Health. Prior to her position at UMass Memorial Health, she served in the Chief Privacy Officer role at Banner Health and has previous experience, not only in Privacy but also within the HIM (Health Information Management) field. Over the last 15 years, she has held Privacy and HIM positions within various healthcare systems, academic medical centers, and specialty hospitals. She is a former Director of AzHIMA, Arizona's chapter of AHIMA (American Health Information Management Association), as well as being awarded the "Rising Star" award.

Today's Objectives:

During this presentation, we will cover:

1. Overview of healthcare compliance and privacy and why it matters
2. Discuss hot topics / current risk trends in healthcare compliance and privacy
3. Understand the role, responsibilities and benefits of an effective compliance and privacy program

CONTENTS



PAUL
HASTINGS

HIGH-LEVEL OVERVIEW OF COMPLIANCE

Polling Question #1

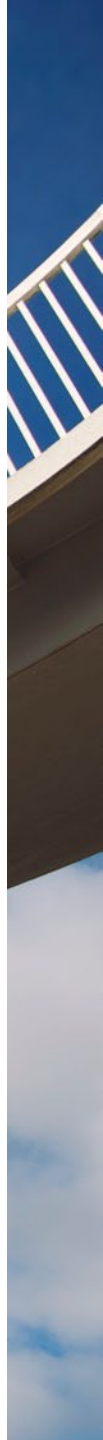
What is the most strictly regulated industry in the United States?

A. Nuclear Energy
B. Commercial Aviation
C. Banking and Investment Firms
D. Healthcare

Cost of Compliance Quick-Facts

Organizations that maintain a strong compliance program **save about 3 times** the cost administrating their compliance program compared to organizations that do not maintain a strong culture of compliance.

- The average cost of **compliance came in at $5.47 million**, while the average cost of **non-compliance was $14.82 million**
- The average cost of **non-compliance has risen more than 45%** in 10 years
- The cost of **regulatory risk averages $10,000 per employee**
- Since 2008, compliance-related operating costs have **increased 60%**
- Global compliance costs increased $33 billion from 2019 to 2020, totaling **$213.9 billion last year**
- Organizations **lose an average of $5.87 million** in revenue due to a **single** non-compliance event



Sources:
Non-Compliance Comes At Great Cost (colligo.com)
The Pandemic Drove Up Compliance Costs: Here's How To Get Back On Track (forbes.com)
Non-Compliance Comes At Great Cost (colligo.com)

Key Regulators

The Department of Justice (DOJ)

Office of the Inspector General (OIG) of Department of Health and Human Services (HHS)

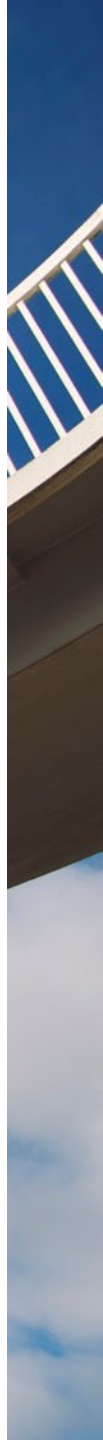
To identify and eliminate fraud, waste and abuse and to promote efficiency and economy in operations

Responsible for conducting audits, evaluations, and both criminal and civil investigations for all HHS agencies, including…

- Centers for Medicare and Medicaid Services (CMS)
- Public Health Service Agencies
  - Agency for Healthcare Research and Quality (AHRQ)
  - Centers for Disease Control (CDC)
  - Food and Drug Administration (FDA)
  - Health Resources and Services Administration (HRSA)
  - Indian Health Services (IHS)
  - National Institutes of Health (NIH)
  - Substance Abuse and Mental Health Services Administration (SAMHSA)
- Human Services
  - Administrations for Children & Families, Aging, and Community Living
- Department of Health and Human Services Office for Civil Rights (OCR)

Key Healthcare Regulations

- Anti-Kickback Statute (AKS)
- False Claims Act (FCA)
- Stark Law
- Health Insurance Portability & Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH)
- Medicare and Medicaid
- State and Local Laws (e.g., false claims, privacy)
- Civil Monetary Penalties Law
- Exclusion Provisions



Regulators Expect Compliance + Closely Scrutinize the Healthcare Industry

- Regulators continue to emphasize the **<u>importance of an effective, dynamic compliance program</u>** that is able to evolve with its organization. According to guidance material issued by the U.S. Department of Justice, ***"One hallmark of an effective compliance program is its capacity to improve and evolve"***
- Of the more than $2.68 billion in settlements and judgments recovered by the DOJ in 2023, **over $1.8 billion relates to matters that involved the healthcare industry**
  - Healthcare cases accounted for over 67% of the total recoveries for FCA enforcement in FY 2023
- **The DOJ recovered more that $2.2 billion in 2022 and $5.6 billion in 2021.**
  - 2021 was the 2nd highest False Claims Act (FCA) collection year in history with healthcare cases accounted for over 90% of the total recoveries

Source: https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-268-billion-fiscal-year-2023

Polling Question #2

When did many healthcare organizations begin to implement compliance programs?

A. After Medicare was enacted in 1965
B. After HHS-OIG was created in 1976
C. After Heath Insurance Accountability and Portability Act was passed in 1996
D. After Enron accounting fraud occurred in 2001

Compliance = Doing the Right Thing

- Compliance with Laws and Regulations

  Does it break the law?

- Compliance with Policies and Procedures

  Does it violate an organizational standard?

- Compliance with Ethical Guidelines

  Does it make you feel uneasy or nervous

What is a Compliance Program?

A Compliance Program is **a formalized effort to prevent, detect, and respond to business conduct that is inconsistent with federal laws, state laws, and/or an organization's values**.

Role of Compliance

- Provide guidance on the interplay between risk / standards and business strategy / need
- Provide input on business and company initiatives
- Provide information to Management and the Board to enable them to carry out their duties
- Conduct monitoring, auditing, investigations and risk assessments that could help identify areas for enhancements or efficiency

Everyone has an obligation to be aware of and abide by all polices, procedures that are relative to their respective job function.

PAUL HASTINGS

OIG Compliance Program Guidance

OIG has historically developed Compliance Program Guidance (CPG) as voluntary, nonbinding guidance documents to support healthcare industry stakeholders in their efforts to self-monitor compliance with applicable laws and program requirements.

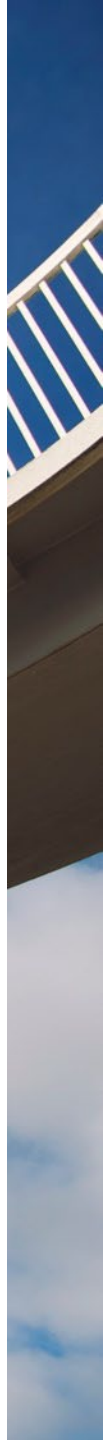
These CPGs have been directed at:

1) Hospitals
2) Home health agencies
3) Clinical laboratories
4) Third-party medical billing companies
5) The durable medical equipment, prosthetics, orthotics, and supply industry
6) Hospices
7) Medicare Advantage organizations
8) Nursing facilities
9) Physicians
10) Ambulance suppliers

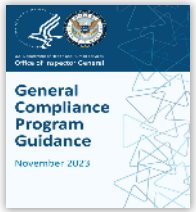
As part of the **OIG Modernization Initiative**, OIG has considered ways to improve and update existing CPGs and deliver new CPGs specific to segments of the healthcare industry. Key updates as part of this initiative include:

- More **user-friendly** and **accessible** guidelines
- Development of a **General CPG (GCPG)** applying to all individuals and entities involved in the healthcare industry ***(released Nov. 2023)***
- Development of updated **industry segment-specific CPGs (ICPGs)** for different participants and subsectors in the healthcare industry ***(coming in 2024)***

CPGs "are not intended to be one-size-fits-all, completely comprehensive, or all-inclusive of compliance considerations and fraud and abuse risks for every organization… the goal of these documents has been, and will continue to be, to set forth voluntary compliance guidelines and tips"



OIG Compliance Program Guidance (cont.)



On November 6, 2023, OIG published General Compliance Program Guidance ("GCPG") for the healthcare compliance community. The GCPG includes coverage of:

- Overview of Federal Healthcare Fraud and Abuse Laws
- The Seven Elements of an Effective Compliance Program
- Compliance Program Adaptations for Small and Large Entities
- General Compliance Considerations
- OIG Resources and Processes

The Seven Elements of an Effective Compliance Program

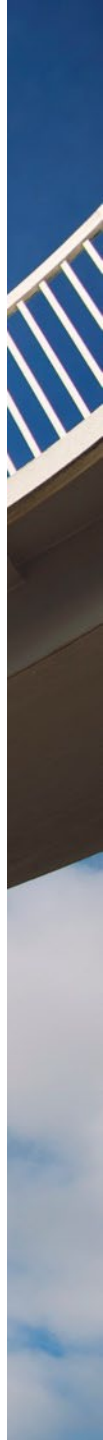
- Written Policies and Procedures
- Compliance Leadership and Oversight
- Training and Education
- Effective Lines of Communication with the Compliance Officer and Disclosure Programs
- Enforcing Standards: Consequences and Incentives
- Risk Assessment, Auditing, and Monitoring
- Responding to Detected Offenses and Developing Corrective Action Initiatives

OIG Compliance Program Guidance (cont.)

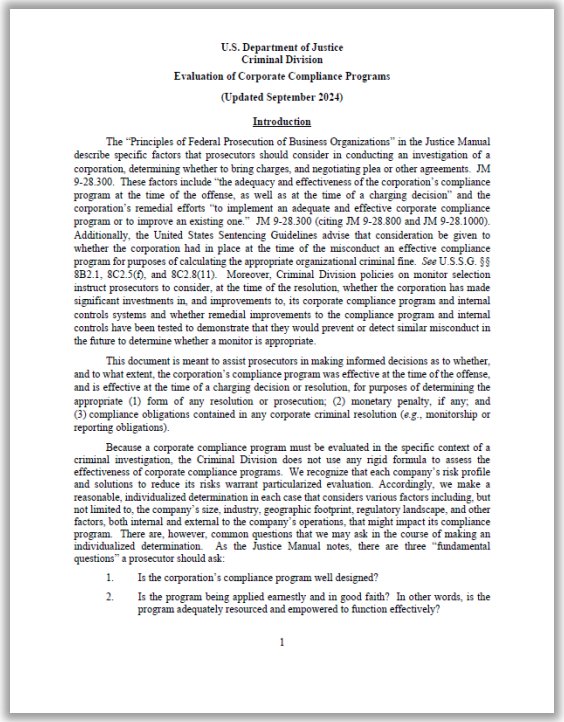
OIG has developed a series of voluntary compliance program guidance documents directed at various segments of the health care industry to encourage the development and use of internal controls to monitor adherence to applicable statutes, regulations, and program requirements.

- General Compliance Program Guidance
- Hospitals
  - Supplemental Guidance
- Nursing Facilities
  - Supplemental Guidance
- Individual and Small Group Physician Practices
- Home Health Agencies
- Hospices
- Clinical Laboratories
- DME, Prosthetics, Orthotics, and Supplies
- Ambulance Providers
- Third-Party Medical Billing Agencies
- Pharmaceutical Manufacturers
- Medicare + Choice Organizations
- Recipients of PHS Research Awards

Source: https://oig.hhs.gov/compliance/compliance-guidance/



DOJ Corporate Compliance Program Guidance



U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated September 2024)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (*e.g.*, monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

1

Click on the image to see the full document

On **September 23, 2024**, the DOJ announced updates to its Evaluation of Corporate Compliance Programs ("ECCP"), accompanied by remarks from Principal Deputy Assistant Attorney General Nicole M. Argentieri.

The remarks highlighted three key areas of update:

"Disruptive technologies"

In March, Deputy Attorney General Monaco announced that prosecutors would **consider how companies mitigate the risk of misusing AI**, directing the Criminal Division to consider "disruptive technology risks – including AI – in the ECCP."

Whistleblower / Speak up

On the heals of the recent whistleblower program announcement, this iteration of the ECCP includes questions "designed to evaluate whether companies are encouraging employees to speak up and report misconduct or whether companies employ practices that chill reporting." Specifically, under the updated ECCP, prosecutors will **consider how a company "assess[es] employees' willingness to report misconduct**."

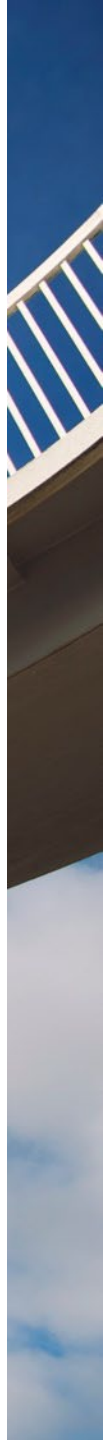
Compliance Program Access to Data

DAG Argentieri highlighted the ECCP's amendments emphasizing **prosecutor focus on "whether a compliance program has appropriate access to data, including to assess its own effectiveness."** Specifically, she noted, this assessment includes "whether compliance personnel have **adequate access to relevant data sources and the assets, resources, and technology that are available to compliance and risk personnel**."

PAUL HASTINGS

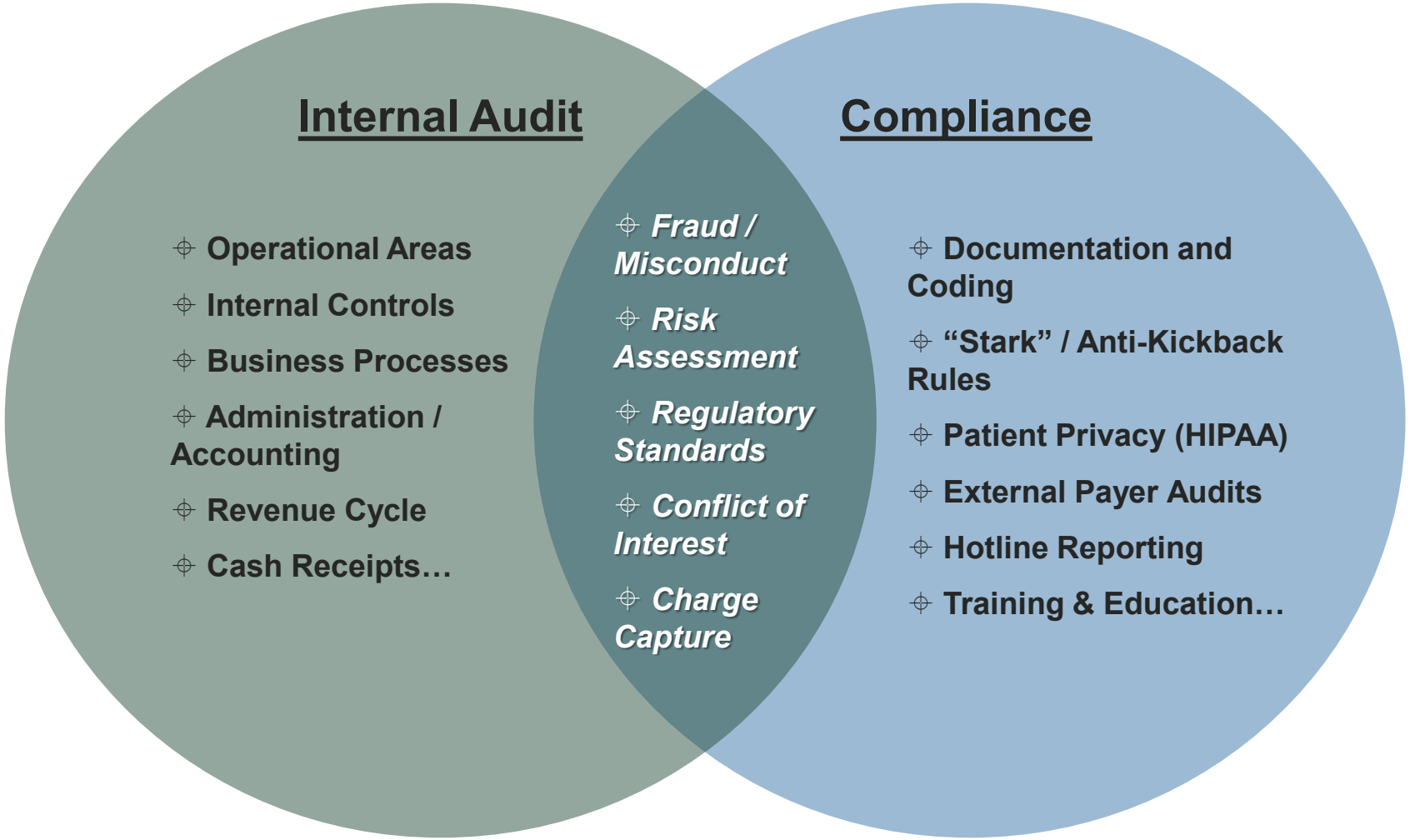
Benefits of Compliance within an Organization

- ✓ Maintain brand **reputation**, build customer **trust** and increase shareholder **value**
- ✓ Save **time, money, and resources** related to fines, penalties, and settlement costs, in the event of a regulatory inquiry
- ✓ Preserve **business operations**, increase **revenue** and limit disruptions that may result in loss of productivity
- ✓ Raise awareness of actual and perceived compliance **risk areas** to the organization
- ✓ Gain **comfort in pursuing greater risk** in certain areas if adequate control environment is in place
- ✓ Outline **tailored mitigations** to control for known risk areas, providing greater protection against possible regulator inquiries that may disrupt business operations and lead to loss of productivity and revenue



Internal Audit and Compliance

Internal Audit and Compliance can often assist in increasing overall collaboration, efficiency and evolving the capabilities of both teams



Polling Question #3

To which senior leadership role does Compliance report in most healthcare organizations?

A. Board of Directors
B. Chief Executive Officer
C. Chief Financial Officer
D. Legal Counsel

PAUL
HASTINGS

HIGH-LEVEL OVERVIEW OF PRIVACY

Polling Question #4

Which federal law safeguards your' protected health information?

A. HIPA
B. HIPAA
C. HIPPA
D. HIPPAA

Privacy and Electronic Security

Health

Insurance

Portability

Accountability

Act of 1996

PAUL HASTINGS

Applies to "Protected Health Information"

- PHI includes any individually identifiable information, in any form or media i.e., electronic, paper, or oral, relating to provision of healthcare including health, treatment, and payment information (past, present or future)

The Privacy Rule protects the privacy of individuals' health information and limits how it is shared

- Additionally, it gives individuals rights over their PHI including the right to access their health records, request corrections to their PHI, and more

The Security Rule establishes standards to protect the confidentiality, integrity, and security of electronic protected health information (ePHI)

The Breach Notification Rule requires organizations to notify affected individuals in the case of a data breach, as well as:

- The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)
- In addition, notice to prominent media outlet if more than 500 people affected

Notice required "without unreasonable delay"

- No later than 60 days of discovery (*note: state regulations may vary*)

What is a Privacy Program?

The primary role of a Privacy Program is **to ensure that PHI is securely handled and protected, while balancing the needs of patient care, business operations, organizational values, and regulatory compliance**.

Privacy Responsibilities

- Policy development
- Training and Education
- Providing Guidance and Input
- Monitoring Compliance
- Breach Management
- Reporting

Privacy Objectives

- Patient/Customer Trust
- Regulatory Compliance
- Operational Efficiency
- Risk Mitigation
- Ongoing Education

NOTE: Many Privacy Programs have started to expand their scope and roles to take on compliance related to not only PHI, but also PII/PI, AI, and data governance.

Benefits of an Effective Privacy Program within an Organization

- ✓ **Patient Protection & Trust –** Ensures patients' data is secure, maintaining confidence in the organization
- ✓ **Financial Protection –** Avoids costly fines, lawsuits, and breach remediation expenses
- ✓ **Operational Efficiency –** Improves processes and reduces administrative burdens
- ✓ **Reputation & Trust –** Strengthens patient and customer satisfaction and provides a competitive advantage
- ✓ **Proactive Risk Management –** Identifies vulnerabilities and ensures preparedness for any incidents
- ✓ **Regulatory Compliance –** Reduces legal and regulatory risks
- ✓ **Organizational Culture –** Encourages ethical behavior and accountability across the organization

Polling Question #5

According to IBM's Cost of a Data Breach Report, which country or region has the highest average data breach cost?

A. India
B. United States
C. Middle East
D. Germany
E. Canada

Quick Facts: Potential Costs of Privacy Non-Compliance

- According to IBM's Cost of a Data Breach Report 2024 the average total cost of a data breach globally is $4.88M; the US had the highest average cost at $9.36M; and healthcare still tops the list as the costliest industry for breaches
- Civil Monetary Penalties (CMPs), as of August 2024, range from $141-$2,134,831 depending on tier level of violation
- Highest amount paid as part of a resolution agreement $16M (highest in 2023 was $4.75M)
- Recent class action lawsuit settlements –
  - 23andMe $30M settlement stemming from a 2023 data breach
  - MCG Health $8.8M settlement stemming from a 2020 data breach
  - Mass General Brigham $18.4M related to tracking technologies (cookies, pixels, website analytics tools)
  - Advocate Aurora Health $12.2M related to Pixel/Facebook tracking technologies

Sources:
HHS Announces Civil Monetary Penalties (thomsonreuters.com)
Resolution Agreements (HHS.gov)
Cost of a Data Breach Report 2024 (ibm.com)
TopClassActions.com

PAUL
HASTINGS

COMPLIANCE AND PRIVACY RISKS / HOT TOPICS

Traditional and Emerging Healthcare Risks

Coding and Billing
Pharmacy
Cybersecurity
Price Transparency
Artificial Intelligence
Patient Care and Safety
Privacy & Security
False Claims Act
Changing Regulatory Landscape
ESG
Health Equity
Telehealth
Revenue Cycle Operations
Third-Party Management
Workplace Safety
Reputation
Conflict of Interest
Stark Law
Talent Retention and Success Planning
340B
Behavioral Health
Workforce Culture
No Surprises Act (NSA)
Anti-Kickback Statute
Clinical Research & Trials
Diversity, Equity and Inclusion
Drug Diversion
Tracking technologies

Compliance Risk Assessment

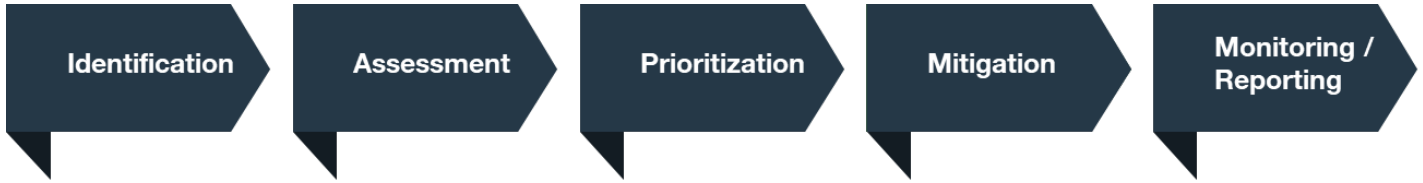
The Office of Inspector General ("OIG") and U.S. Department of Justice's ("DOJ") Evaluation of Corporate Compliance Programs ("ECCP") guide us in assessing the design, implementation and effectiveness of the risk management program and its activities.

Per OIG Supplemental Compliance Program Guidance for Hospitals:

Has the hospital developed a risk assessment tool, which is re-evaluated on a regular basis, to assess and identify weaknesses and risks in operations? And Does the risk assessment tool include an evaluation of Federal health care program requirements, as well as other publications, such as the OIG's CPGs, work plans, special advisory bulletins, and special fraud alerts?

Compliance Risk Assessment

Identify, prioritize, and assign accountability for managing existing or potential risks related to legal or policy non-compliance that could lead to fines or penalties, reputational damage, or the inability to operate in key markets



Effective risk assessment is the critical foundation for an effective compliance program tailored to the particular enterprise

HIPAA Risk Assessment

A comprehensive evaluation of **privacy** and **security** risks related to PHI that should identify vulnerabilities as well as improvement opportunities in the organization's policies, procedures, and technology systems. A HIPAA Risk Assessment will also assess compliance with the **HIPAA Privacy, Security,** and **Breach Notification Rules.**

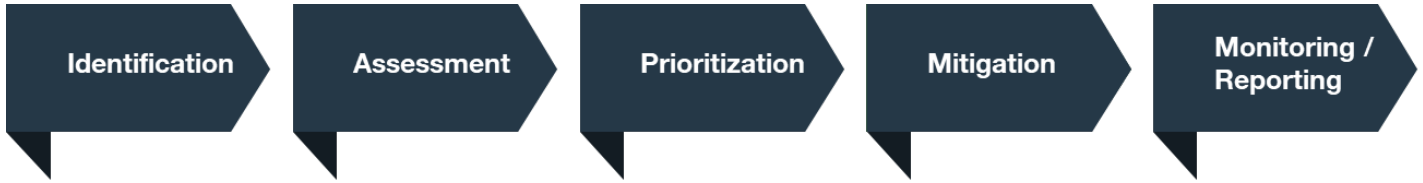
The HIPAA Security Rule requires annually conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI".

Beyond this, there is also risk to the confidentiality, integrity, and availability of PHI when it is not in electronic format. It is beneficial and may be necessary to conduct a HIPAA Privacy risk assessment into those areas as well, such as an individual's right to access, BAA compliance, and other requirements/rights provided under HIPAA.

Note: One additional type of "risk assessment" is referenced within the HIPAA Breach Notification Rule. When there has been an impermissible acquisition, access, use or disclosure of unsecured PHI (in any format), an individual HIPAA risk assessment of the specific incident, is necessary to determine whether the event is notifiable to HHS/OCR and the affected individual(s).

HIPAA Privacy and Security Risk Assessment

Best practice advises collaboration with Information Security to complete a comprehensive Privacy and Security Risk Assessment annually. Tools and methods could include manual review, automated tools, third-party audits, interview and surveys. The key components of a HIPAA Risk Assessment are similar to a Compliance Risk assessment:



A comprehensive HIPAA Risk Assessment is a critical part of maintaining HIPAA compliance and protecting PHI. Continuous monitoring and assessment are essential to address evolving privacy and security risks.

Polling Question #6

Which of these could lead to a potential Privacy violation?

A. Texting patient info via WhatsApp on your personal phone
B. Taking a selfie in a clinical space
C. Posting or replying to a comment about a patient on social media
D. Leaving your laptop open or unsecured in a public place
E. All of the above

Most Common Privacy Violations

- Hacking/Phishing
- Loss/Theft
- Unsecure transmission or storage of ePHI, for example:
  - Unencrypted data or devices
  - Improper disposal of PHI
  - Inadequate physical and technical safeguards
  - Use of non-approved business tools/platforms
- Inappropriate Access, Use and Disclosure, for example:
  - Employee “snooping”
  - Sharing/posting patient information or photos on social media
  - Inadequate access controls
  - Not following “Minimum Necessary” standard
- Lack of…
  - Training and education
  - Clear and consistent policies and procedures
  - Regular organization-wide risk analysis/risk assessments
  - Third-Party Risk Management
  - Oversight in entering HIPAA-Compliant BAAs

Causes of Billing Errors

Rehab. Ass'n of Va., Inc. v. Koslowski, 42 F.3d 1444, 1450 (4th Circuit), cert. denied, 516 US 811, 116 S.Ct. 60, 133 L.Ed.2d 23 (1995) Cited in Briggs v. Comm., 429 Mass. 241, 707 N.E.2d 355 (1999).

"[T]he statutes and provisions in question, involving the financing of Medicare and Medicaid, and among the most completely impenetrable texts within human experience. Indeed one approaches them at the level of specificity herein demanded with dread, for not only are they dense reading of the most tortuous kind, but Congress also revisits the area frequently, generously cutting and pruning in the process and making **any solid grasp of the matters addressed merely a passing phase."**

Billing and "False Claims":

- Federal and State law prohibits reimbursement for healthcare services that are not rendered appropriately or documented accurately
- Billing for an inappropriate or inaccurate level of service may be classified as **a false claim ***
- Violations can result in payment refunds, civil fines, imprisonment, and exclusion from government healthcare programs

PAUL
HASTINGS

OPEN Q&A

HFMA / NEHIA Joint:
2024 Compliance & Internal Audit Conference

Wed., December 4 - 7:15 AM to 5:00 PM
Thurs., December 5 - 7:30 AM to 6:30 PM
Fri., December 6 - 7:30 AM to 1:00 PM

Mystic Marriott Hotel & Spa
625 North Road (Route 117)
Groton, CT 06340

Register Now

The New England Healthcare Internal Auditors (NEHIA) and the Healthcare Financial Management Association (HFMA) MA-RI Chapter are excited to again host a 3-day educational conference bringing expert presenters from healthcare compliance, privacy, security, and of course, internal auditing. Each presentation is an opportunity for presenters to share their knowledge with all levels of conference attendees and for conference attendees to listen and learn best practices from some of the industry's best experts. In addition to providing low cost, high quality educational sessions, NEHIA and HFMA MA-RI will work diligently to connect conference members with each other to create a strong community of healthcare professionals in New England.

PAUL HASTINGS

UMass Memorial Health

Boston Children's Hospital
Until every child is well

Thank You!!!

hfma
ma-ri chapter