The Role of the Health Care Chief Compliance Officer in HIPAA and Privacy and Security Compliance

Gerry Zack, CCEP, CFE, CIA, CRMA

CEO

Society of Corporate Compliance and Ethics (SCCE) &

Health Care Compliance Association (HCCA)

Minneapolis, MN

HCCA™
Health Care Compliance Association

HIPAA, Privacy, and Security

- Aren't they just like any other category of compliance risks?
  - Yes and No

Different, Yet the Same

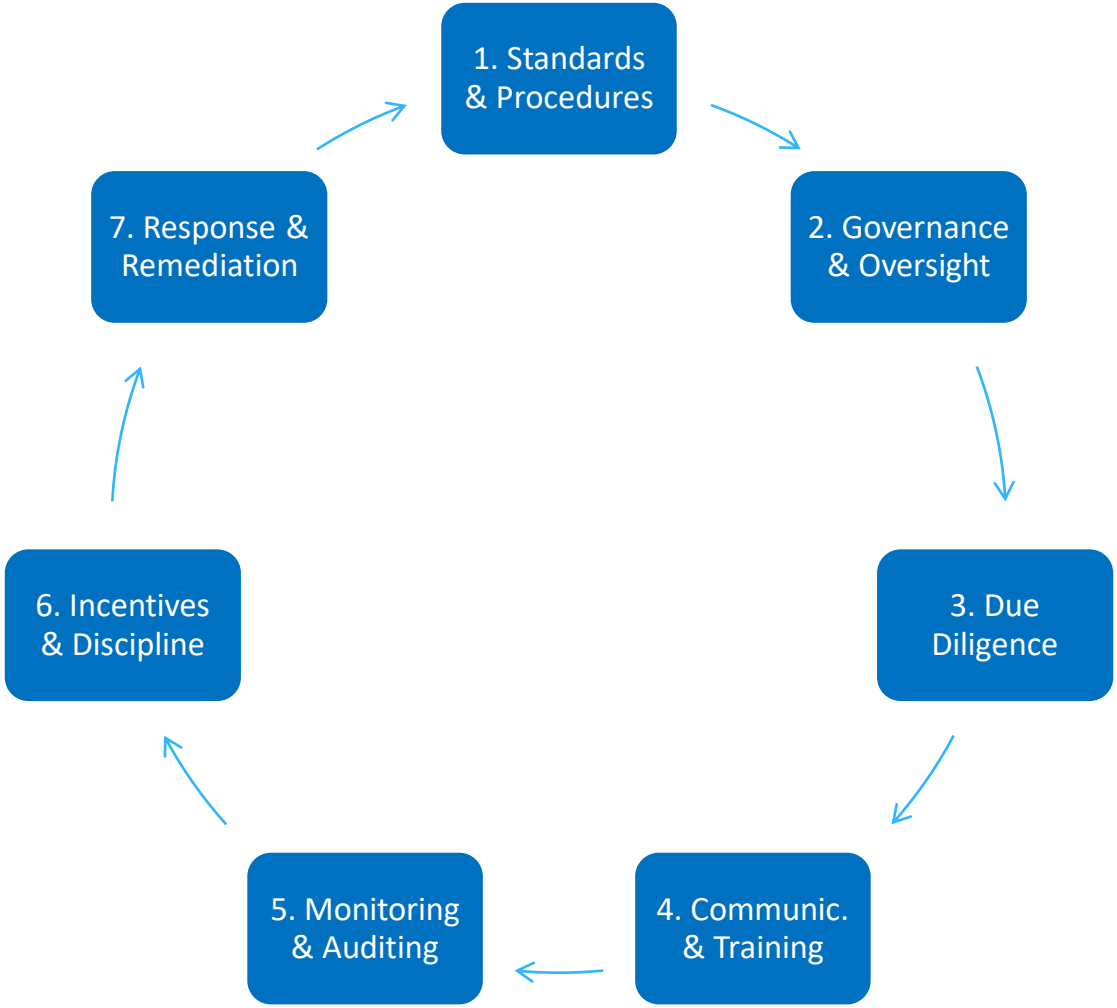
- How they are different
  - More technically complex than most compliance risks
  - Subject to more rapid change over time
  - More prone to intentional acts, in addition to unintentional
  - More prone to outsider threats than most compliance risks
- How they are the same
  - Approach to managing risk should follow the same framework as other compliance risks
  - Apply the seven elements of an effective compliance program

A Few Not-so-Random Ideas for Today

Improve Your Management of Risk

HCCA™
Health Care Compliance Association

Utilize ALL
7 Elements of a Compliance Program



HCCA™
Health Care Compliance Association

The 8th Element
Risk Assessments

- Greater need for continuous input than most other compliance risks
- Utilize process mapping to assist in identifying points of vulnerability
- Collaborate across departments

Collaboration is Key

- Management of HIPAA, Privacy and Security Risk crosses many departmental boundaries –in particular:
  - IT
  - Security
  - Accounting/finance (billing, etc)
  - Human Resources
  - Internal audit
  - Each service department

Focus on What Drives Risk

- Changes in laws and regulations (only part of it)
- Changes in methods of delivery and serving of patients
- Changes in technology
- Changes in people
- Changes in performance incentives
- Changes in organizational strategy
- Changes in processes
- Changes in utilization of third parties
- Mergers and acquisitions, integration

Data Analytics

- Focus on anomalies in digital evidence in six areas:
  1. Leading indicators (if any)
  2. Preventive controls
  3. The act (e.g. HIPAA violation, privacy/data breach, etc)
  4. Concealment of the act
  5. Detective controls
  6. Lagging indicators (effects of the act, if any)

Third-Party Management (U.S. DoJ)

- Risk-Based and Integrated Processes
  - How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company?
  - How has this process been integrated into the relevant procurement and vendor management processes?
- Appropriate Controls
  - What was the business rationale for the use of the third parties in question?
  - What mechanisms have existed to ensure that the contract terms specifically described the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

Third-Party Management (U.S. DoJ)

- Management of Relationships
  - How has the company considered and analyzed the third party's incentive model against compliance risks?
  - How does the company monitored third parties?
  - Does the company have, and has it exercised, audit rights?
  - How has the company trained the relationship managers about what the compliance risks are and how to manage them?
  - How has the company incentivized compliance and ethical behavior by third parties?
- Real Actions and Consequences
  - Were red flags identified from the due diligence of the third parties involved in the misconduct and how were they resolved?
  - Has a similar third party been suspended, terminated, or audited as a result of compliance issues?
  - How has the company monitored these actions (e.g. ensuring the vendor is not used again in case of termination)?

Audits of Third Parties

- Financial vs. Compliance
  - With financial, focus is on billing
  - Compliance focuses on contract provisions, compliance with laws
  - Either can address processes, policies, etc
- Surprise vs. With Notification
  - Surprise is more likely to detect fraud, noncompliance, etc, but creates other problems and inefficiencies
- Our Staff vs. Third Parties
  - Expertise, availability, cost considerations

Audit Clauses

- Establishes right to perform audits and have access to data of third parties
- Customized terms, not boilerplate, for each scenario
- Key issues:
  - Audit vs. inspect, review, examine, etc
  - Type of audit (financial, compliance, other)
  - Audit period – how far back
  - Record retention (which records and for how long)
  - Access to (or copies of) documents and records
    - Which ones? What format?
  - Planned (and notification) vs. surprise
  - Facilities, assistance, copying records, etc
  - Third party auditors? Who?
  - Application to subcontractors
  - Cost recovery, extrapolation, penalties, repayment, etc

3rd Party Auditing and Monitoring

- Risk-based plan customized for each third party
  - Many good techniques included in HCCA's *Health Care Auditing & Monitoring Tools*
  - Detailed plan describing:
    - Steps/techniques
    - Frequency
    - Approach to sample selection(s)
    - Responsibility
- Utilize forensic data analytics
  - Use multiple data sources to monitor for specific indicators
  - Multi-factor risk scoring vs. single-factor analytics
- Exercise audit rights clauses
  - When red flags arise
  - Periodically even when no red flags

Mergers and Acquisitions (U.S. DoJ)

- Due Diligence Process
  - Was the misconduct or the risk of misconduct identified during due diligence?
  - Who conducted the risk review for the acquired/merged entities and how was it done?
  - What has been the M&A due diligence process generally?
- Integration in the M&A Process
  - How has the compliance function been integrated into the merger, acquisition, and integration process?
- Process Connecting Due Diligence t Implementation
  - What has ben the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process?
  - What has been the company's process for implementing compliance policies and procedures at new entities?

QUESTIONS ??

Gerry.zack@corporatecompliance.org