Risk Assessing HIM’s Effectiveness in the Revenue Cycle

Elizabeth (Liz) Johnson, The Christ Hospital Health Network, Cincinnati, OH
Objectives

• Understand principles of risk assessment and importance in today’s risk environment
• Identify effective controls--and how to deploy
• Learn how to report on your control effectiveness and Key Risk Indicators
• Understand that HIM effectiveness is a Key Risk Indicator within the revenue cycle
Managing an organization’s risks in individual silos is like trying to pick up a six-pack without the little plastic thingy that holds them all together; you can do it, but it is far harder than it would be if the cans were connected to each other. --Andrew Bent
Risk and Risk Assessment
Principles and Procedures
Enterprise Risk Management*

“...a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

• This principle also applies to subunits: Revenue Cycle ➔ HIM


The Underlying Principle is Universal

- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise (or department) day-to-day.

- Risk Assessment and Mitigation of Risks supports value creation by assisting management to:
  - Deal effectively with potential future events that create uncertainty.
  - Respond in a manner that reduces the likelihood of downside outcomes and increase the upside.
  - Take a view of risk and risk mitigation within the business portfolio.

- Strategic
- Operations
- Financial (Reporting)
- Regulatory (Compliance)
- Reputation
Risk Defined

• Risk is the likelihood that a threat (or a threat agent) will exploit a given vulnerability, multiplied by the business impact of that exploit.
  • Inherent Risk is risk that exists before controls
  • Residual Risk is risk that exists after controls

• Risk can be:
  o Avoided (Do not Accept) or Transferred (Insurance)
  o Accepted and Mitigated –Managed (Controls), or Accepted and Not Mitigated (No Controls)
  o Or a combination of the above

• Impact is the implication to the organization in terms of materiality should the risk event occur

• Likelihood is the probability the risk may occur

• Sensitivity: implicating factors such as velocity, high priority, scrutiny

• Complexity: implicating factors such as interdependence, detectability, human behavior
## Sample HIM Portfolio Subject to Risk

**HIM Role in Revenue Cycle: Mission-Charter-Scope**

| Timely-Accurate Coding Hospital-Professional | Accurate, timely, complete records maintained efficiently-centrally | Controlled, secure and relevant ‘distribution of’ and ‘access to’ records |

### Functions subject to risk assessment - risk mitigation and monitors of effectiveness

| Oversight, Coder Competency, Resources, Education | IT, Software, Data Analytics, Security, Backup and Recovery, Storage | Coding capture, Provider competency, Provider records, CDI hospital and professional | Legal-Regulatory Compliance, Payor Rules, Downcodes-Denials, External Requests | Operations - Advisory Support, Indicator Reporting, Business Continuity, Change Management |

The COSO domains apply to all profile components.
How do I assess?

• Compile your portfolio subject to risk

• Survey the external and internal environments for risk factors and controls (are they present; are they effective).
  • External examples
    • State Medicaid Changes
      • New bundling for outpatient
    • Payor policy changes-federal, managed care, commercial
      • LCD-NCD coding and documentation changes
      • Payor down coding: ED E/M, DRG changes not in comportment with convention
  • Regulatory
    • Copy Paste, CDI, storage requirements, security, business continuity, CoP’s
  • Records requests and access to systems
    • Quantity, relevant content to defend claims, access with need to know
  • Internal Examples
    • Coder proficiency and concordance
    • Provider documentation completeness-timeliness
    • Monitors and reporting of key indicators – or lack of
<table>
<thead>
<tr>
<th>Risk</th>
<th>Survey Question Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Competency - Coding accuracy</td>
<td>Are competency reviews performed quarterly on 10% of work product? Is intervention effective? Education -resource program in place and comprehensive? Is coding validated every six months?</td>
</tr>
<tr>
<td>Data storage-back up</td>
<td>Are all medical records consolidated, including scanned documents? Are legacy systems tested periodically for retrieval? Is MR-transcription data backed up?</td>
</tr>
<tr>
<td>Performance Analytics and Monitor Reporting</td>
<td>Does information extraction and/or the utilization of information effectively facilitate performance improvement? Monitors in place for Key Risk controls? Does HIM deploy internal algorithm tools for monitoring?</td>
</tr>
<tr>
<td>Coding Capture and Clinical Documentation Improvement</td>
<td>Does the CDI program (Hospital and Physician effectively capture coding opportunity? Is documentation sufficient and reflective of services provided? Is there a structured education and review program to validate CDI effectives and assure providers receive standardized education?</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>Is coding reviewed for concordance with LCD-NCD-Payor policies before release from que? Is coding forced through the que when edit prevents processing-are monitors in place to evaluate daily? Are encoders and edits up to date for State Medicaid rules? Are external audit record requests abstracted for MN compliance prior to release-return to requestor? Are professional claims monitored for accurate coding levels and modifier use, signatures? Are Records timely authenticated?</td>
</tr>
<tr>
<td>Denials</td>
<td>Does HIM monitor coding denial rates by reason/ code, and report monthly on rates and actions? Does HIM Log and track all external audit requests, along with results? Report back to management for action planning? Are payors increasingly changing codes by down coding or using their internal standards in lieu of conventional stds?</td>
</tr>
</tbody>
</table>
## Rate the Risks and Controls

<table>
<thead>
<tr>
<th>#</th>
<th>Key Risk Domain 2018</th>
<th>Domain</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Inherent Risk</th>
<th>Goal Profile</th>
<th>Risk Tolerance</th>
<th>Improve</th>
<th>Assess</th>
<th>Monitor</th>
<th>Optimize</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Coder Competency</td>
<td>O,F,C</td>
<td>4.4</td>
<td>3.8</td>
<td>4.1</td>
<td>C, L</td>
<td>2.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a</td>
<td>Coding Accuracy</td>
<td>O,F,C</td>
<td>4.7</td>
<td>3.8</td>
<td>4.3</td>
<td>C, L</td>
<td>2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Data Storage-Backup</td>
<td>S,F,O</td>
<td>3.7</td>
<td>3.9</td>
<td>3.8</td>
<td>R, L</td>
<td>4.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Performance Analytics-Data Monitors</td>
<td>S,O,F,C</td>
<td>4.4</td>
<td>4.4</td>
<td>4.4</td>
<td>C, R, A</td>
<td>M, 4.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Coding Capture-CDI Hospital</td>
<td>F,C</td>
<td>4.0</td>
<td>4.0</td>
<td>4.0</td>
<td>C, R, L</td>
<td>3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4a</td>
<td>Coding Capture-CDI Professional-Other</td>
<td>F,C</td>
<td>4.5</td>
<td>4.5</td>
<td>4.5</td>
<td>C, R, M</td>
<td>4.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Regulatory Compliance</td>
<td>C,F</td>
<td>4.5</td>
<td>3.4</td>
<td>4.0</td>
<td>C, R, A, L</td>
<td>2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Denials</td>
<td>F,O,C</td>
<td>3.0</td>
<td>4.4</td>
<td>3.7</td>
<td>C, R, A, L</td>
<td>4.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Data Recovery Backup</td>
<td>O,C</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>R, M</td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Payors policies-downcoding</td>
<td>F,O,C</td>
<td>3.7</td>
<td>4.1</td>
<td>3.9</td>
<td>C, M</td>
<td>3.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Disaster Recovery Planning</td>
<td>O,C</td>
<td>4.0</td>
<td>3.7</td>
<td>3.9</td>
<td>R, L</td>
<td>3.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>External Records Requests-data bases</td>
<td>O,C,F</td>
<td>5.0</td>
<td>3.8</td>
<td>4.4</td>
<td>A, L</td>
<td>2.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>IT-Software Support-Utility</td>
<td>O,S</td>
<td>2.8</td>
<td>2.1</td>
<td>2.5</td>
<td>C, R, A, M</td>
<td>2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Risk Identification-Change Management*</td>
<td>O,F,C</td>
<td>4.0</td>
<td>4.0</td>
<td>4.0</td>
<td>C, R, A, M</td>
<td>3.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Talent Mngmnt -Recruitment-Retention</td>
<td>S,O</td>
<td>4.8</td>
<td>1.5</td>
<td>3.2</td>
<td>C, M</td>
<td>2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Impact Financial Key
- $500,000: 4 to 5
- $100,000 to $500,000: 3 to 4
- $10,000 to $100,000: 2 to 3

### Likelihood Key
- High Risk: 4 to 5
- Mod Risk: 3 to 4
- Low Risk: 2 to 3

### Goal Key
- C=Coding
- R=Records
- A=Growth

### Risk Domain Key
- Strategic-S; Operational-O; Financial-F
- Regulatory-R
- Growth-A

### Risk Tolerance Key: Low-L, Med.-M, High-H
- Controls: 5-ineffective
- 0-effective
**Heat Mat of Risks**

- **2018**

- **ASSESS**
  - High
    - Inherent Risk
      - 5
      - 4.5
      - 4
      - 3
      - 2.7
      - 2.5
      - 2
      - 1.5
      - 1
  - Low
    - Management effectiveness
      - 1
      - 1.5
      - 2.1
      - 2.4
      - 2.8
      - 3.2
      - 3.8
      - 4.1
      - 4.4
      - 4.7
      - 5

- **IMPROVE**
  - 3
  - 4a

- **OPTIMIZE**
  - 10
  - 1a
  - 12
  - 9, 8
  - 2
  - 6

- **MONITOR**
  - 5

**KEY:**

1. Coder Competency
2. Data Backup
3. Performance Analytics-Monitors
4. Coding Accuracy
4a. Coding Capture-CDI Hosp-Profess.
6. Denials
8. Payor policies-down coding
10. External Records Requests-Data Bases
12. Risk Identification-Change Management
Controls-Monitors and Case Study
A Case Study - External Records Request

MAC performs Medical Review of OP Belatacept Administration applying Ohio LCD*

MAC denies – no MN

Missing required diagnosis codes - coding codes from order

Dept/HIM not Aware of Denial Patterns

HIM fulfills records request using vendor who copies – timely sends hospital record to MAC

Admin stop time not on MAR; Waste not on MAR (in Pharm record)

Medical Necessity resides in Physician office notes - those notes not pulled over into hospital record

Records Processes

Claim Denial Missed timely 2\textsuperscript{nd} appeal $10,000/unit loss

*LCD requires select diagnosis codes; IV Start and Stop Times - Wasting should be in MAR. One dose Cost- $10,000; Reimbursement $13,000.
HIM Controls for the Risk in Case Study

• Report on denials patterns
  • Work with decision support to create reports
  • Select complex (error prone)-high volume-high cost services first.

• Initiate structured interdisciplinary reviews to scan the environment for patterns:
  • Monthly (weekly for high cost services monthly for high cost/vol. services)
  • New services-procedures, off label use, anomalies
  • Elect owner of the risk and request action plan and reporting

_HIM is the post office box and may receive letters without the stamp....to force an edit through, or code just the procedure without the why (MN), results in the dead letter syndrome (denials and rework). The risk is interconnected-so ‘return to sender’._
HIM Controls for the Risk in Case Study

• Inform Providers and Educate
  • Documentation
  • Templates and record formats
  • Front end diagnosis code edits for MN
  • CDI (Hospital and Physician Office-Other)

• Deploy LCD-NCD screening tools for coders-access personnel
  • Software support tools, edits, work que, supervisory review for edit bypass, Scheduling controls, review and abstracting of office records into hospital record (or alternative)

• Custom Checklists for records submission to external reviewers
  • Send RELEVANT INFORMATION-INCLUDE THE WHY
  • Abstract the record to call out key MN requirements, order, diagnosis, clinical need, start-stop time, orders, wasting, signatures, LCD-NCD
  • Perform query-as necessary to obtain required documentation, and attestations
Case Study: Backup Incident Response

• HIM engages an external transcription service (vendor) which is accessed via web or voice
  • The transcription is not backed-up

• The vendor is subject to a ransomware attack and the entire system is unavailable to all physicians for 2 weeks
  • The vendor is not sure whether the provider's PHI has been compromised
  • The provider cannot find a recent contract or BAA

• The backup system does not have enough devices and physicians do not know how to use

• Coding is delayed, billing is delayed because back-up transcriptionists not available, and there are not enough backup devices

• What are the risks? What controls would have prevented a crisis?
## Key Risk Indicators Report

<table>
<thead>
<tr>
<th>Key Risk Indicator</th>
<th>Measure</th>
<th>Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coding Accuracy-complex DRG's</td>
<td>&lt;2%</td>
<td>ABC review-error rate &lt;2% 5-2018</td>
</tr>
<tr>
<td>Work Que Failed MN Edits</td>
<td>25%</td>
<td>MN not captured at Registration</td>
</tr>
<tr>
<td>CDI Code Capture</td>
<td>80%</td>
<td>Query Capture</td>
</tr>
<tr>
<td>Denials</td>
<td>30%</td>
<td>Documentation supporting NCD-LCD; failure to send abstracted records w/MN to ext. reviewer</td>
</tr>
<tr>
<td>Modifier Application</td>
<td>10%</td>
<td>Error rate on watch list, certain providers need coder review of modifier app. TBD-review claims sample (refer to audit)</td>
</tr>
</tbody>
</table>
Approach for Value

Assess your processes for risk

Examine interventions, methods, process redesign, reporting that reveals trends, and optimize control effectiveness

Prioritize your next steps – strategy based on the goals of the enterprise
Thank You!
Questions?