Using Technology to Leverage your Compliance Program

April 18, 2018

Nicholas Merkin
Jeff Young

Introduction

Nicholas Merkin
Healthcare Compliance Expert

Jeff Young
Vice President - Product Development at Healthicity
## Agenda for Today

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction: The Uses of Data for Compliance Professionals</td>
</tr>
<tr>
<td>2</td>
<td>The Need for Adequate Data in Your Compliance Program</td>
</tr>
<tr>
<td>3</td>
<td>Examples of Using Technology</td>
</tr>
<tr>
<td></td>
<td>• Incidents</td>
</tr>
<tr>
<td></td>
<td>• Reporting/Ongoing monitoring</td>
</tr>
<tr>
<td></td>
<td>• Provider Audits</td>
</tr>
<tr>
<td></td>
<td>• Risk Assessments</td>
</tr>
<tr>
<td>4</td>
<td>Preparation for external audit</td>
</tr>
<tr>
<td>5</td>
<td>Key Takeaways</td>
</tr>
</tbody>
</table>

## The Importance of Using Data in Your Compliance Program

- Measure and assessing the effectiveness of compliance programs.
- Sword: Data provides a factual basis upon which to draw qualitative conclusions about the effectiveness of compliance programs.
- Shield: Data can be used to defend compliance activities in the wake of an incident.
The Importance of Using Data in Your Compliance Program

• To be effective, data must be meaningful and easy to understand.
• Compliance personnel should develop baseline metrics for comparative purposes.
• Presentation of data crucial to maximizing its use – especially to those outside the compliance function.

The Uses of Data for Compliance Professionals

• Gathering internal and external data regarding compliance matters

• Analyzing available data regarding compliance

• Reporting on the compliance function

• Developing compliance-related responses based on actionable data
Responding to a Compliance Incident: A Case Study

A Compliance Incident Hypothetical

Nurse X, a longtime hospital employee, was in a bind. That morning, he had needed to communicate a message about Patient A’s medical condition and treatment plan to Patient A’s daughter, who is Patient A’s primary caretaker. According to Patient A’s admissions records, such communications were to be made solely via the daughter’s cell phone number. Although Nurse X thought he had left a message for the daughter at what he thought was an appropriate number, Nurse X had misread the record and mistakenly left the message on the general voicemail box at the daughter’s place of work.
A Compliance Incident Hypothetical

Nurse X had encountered the daughter later that day and the daughter was clearly unhappy. The daughter berated Nurse X for his mistake and said that she was considering speaking with her uncle, who had been “pre-law” in college, before his acting career had taken off following a particularly well-regarded performance in a carbonated beverage commercial.

A Compliance Incident Hypothetical

Nurse X didn’t know what to do. On the one hand, she had always taught younger nurses that it was best to come forward early if they found that they had made a mistake concerning patient care. On the other hand, this really wasn’t a patient care issue. Nobody was hurt, right? Wasn’t it just an administrative error? Seems hardly worth getting anyone else involved. Nonetheless, later that night, unable to sleep, Nurse X decides to send an email to both the hospital’s legal department and compliance hotline explaining what had happened. Though a minor incident. The hospital’s GC and CCO decide that they’ll add the issue to their agenda for discussion at their weekly lunch meeting the next day.
The Hypothetical Continued

GC's POV: Nurse X violated the hospital’s confidential communications requirements. It’s a terminable offense. Let’s just end this issue today. I’ll call the daughter and tell her we’ll fire the staff member involved and offer her free food in the hospital’s cafeteria for life to sign a release and non-disclosure concerning the matter. We had an embarrassing HIPAA breach last year that was reported in the local press. I don’t want this getting out there even if it’s a minor matter.

The Hypothetical Continued

CCO's POV: I think there is a bigger problem that needs resolution here. The misread phone number was human error, but Nurse X violated the minimum necessary rule by leaving a message detailing both Patient A's medical condition and treatment plan for the daughter. Better to be transparent about this and use the incident as a teaching opportunity. The hospital needs to clarify this issue for all employees and possible to implement new procedures in this regard. Our employees need specific training as to what information may be left in a voicemail message. As you mentioned, we’ve had HIPAA breach issues recently. We need to commence an internal audit of HIPAA-related matters and modify our compliance program accordingly.
Responding to a Compliance Incident: Making a Plan

- Identify: Determine type of incident/case
- Preserve: Start Chain of Custody, secure data & document
- Collect: Image storage devices and recover data
- Analyze: Examine recovered data, search for potential evidence
- Report: Document facts & findings, summarize evidence, prepare testimony

Using Data to Answer the Pertinent Questions

- How did this happen?
- How often does it happen?
- How did we not know this was happening?
- What is the likelihood of it happening again?
- How do we keep it from happening again?
Commencing Your Investigation: Using Data to Answer Your Initial Questions

- Time period?
- Conflicts of interest?
- Related issues?
- Personnel involved (both for incident and to lead investigation)?
- Who should be walled-off from any investigation?
- Is there a privilege issue? Involving counsel?

The Nuts and Bolts: Using Technology For an Effective Incident Investigation

- Consult your policies and procedures
- Create a work plan
- Identify and secure pertinent documentation and information
- Lay a paper trail of your process and findings
Reporting and Correcting: The End Game and Beyond

- Reporting findings (internally and, maybe, externally)
- Making a corrective action plan
- Following it up with auditing and monitoring
- Litigation and settlement
- Avoiding an obstruction allegation

Different Members of the Organization Have Different Uses for the Data

- How does the General Counsel use it?
- How does the CCO use it?
- CEO?
- Head of HR?
- Clinicians?
Using Data for Proper Board Oversight

- Duty of care
- Boards duty to oversee the compliance function
- Business judgment rule
- The board’s role in decision making and ongoing compliance planning

Physician Audits

Challenges – Finite time and Resource:
  - Who to audit
  - What to audit
  - Trends (comparing past Audits)
  - Using data to influence audits

Benefits of focused audit with Data Analytics:
  - Identification of issues
  - Prevent or have data to support an external audit (Government or commercial payor)
Physician Audits

Who to Audit:
- Conduct Benchmarking/comparison to peers
  - Internal Data
    - Internal benchmarking
  - External Data
    - MGMA
    - Medicare
    - Third party data sources
    - Third Party Tools
    - AAPC – Free benchmarking tool
      (Medicare Data)

Physician Audits

What to look for in the data (based on comparison to benchmark):
- High level office visits
- Procedure patterns
- Diagnostic patterns
- Frequency of visits
- Use of Modifiers
Provider Audit: Data Examples

- Visually identify comparison to peer group
- Example shows higher submission of 99214 compared to peer group
Provider Audit: Data Examples

Provider Audit

Based on Data findings – Next steps:

• Audit
  • Focused audit based on patterns identified
    • Random selection of claims
    • Validation of services rendered
    • Action Plan: training on findings
  • Re-analyze in 90 Days
    • Are patterns still present?
    • Follow-up Audit
Assessing Risk

Challenges
• Where to start?
• Consistency
• Taking Action
• Re-assess

Risk Assessment: Where to Start?

What are the key areas of risk within your organization?
• Regulatory?
  • E.g. HIPAA
• Organization specific
• Prior identified risks
Risk Assessment: Consistency

Develop surveys based on identified risks
  • Send to key stakeholders

Develop scoring methodology
  • Scoring helps to normalize identified risks
  • Allows for prioritizing top risks to address

Risk Assessment: Taking Action

Prioritized Risks help to identify your annual work plan

Conduct Audit on identified/prioritized risks

Determine action plans based on Audit:
  • New Policies/Procedures
  • Training
Risk Assessment: Re-Assess

- Following year – Conduct survey’s on each risk area
- Score
- Identify if risk score has improved
- Re-prioritize – focus on:
  - New risks
  - Continued risks
- Utilize data from previous year(s) to trend and show improvement

Preparation for an External Audit

- Utilizing data and technology prepares an organization for an audit
- Ability to show the compliance health of an organization
- Demonstrates an organized compliance program
Preparation for an External Audit

Examples of data available from utilizing technology, data, tools:

- Known Incidents
  - Evidence of how an incident was investigated/corrective action take
- Evidence of individual(s) receiving training
- Evidence of provider audits
- Evidence of policies and procedures
- Evidence of assessing and taking action on identified risks

Some Other Key Takeaways

- Partner with other data owners in your organization
- Identify current data analytic activity
- Understand what external data analytics is being done by regulatory agencies and payers
- Work with internal and external auditors to do risk-based auditing/monitoring
Thank You.

Any Questions?