Developing & Maintaining an Effective Program for Data Integrity
June 28, 2016

Angel Hoffman (Advanced Partners in Health Care Compliance)
Adam Bennett (Cloudburst Security)
Maureen Saxon-Gioia (OSPTA Home Health Care)
SESSION GOALS

We will be focusing on:

• Importance of maintaining an effective data integrity program;
• Accuracy and consistency of stored data with use of standards and procedures;
• Ongoing consistent supervision and training of employees to mitigate risk;
• Prevention leads to a reduction in data-related integrity violations;
• Present some real world experiences
SESSION OBJECTIVES

- Explain opportunities which contribute to data compromise and leave an organization vulnerable.
- Describe program elements which contribute to risk mitigation.
- Identify a strategy for creating and maintaining a successful data integrity program.
- Discuss the impact to HIEs, patient safety and research.
Data Integrity: Security and Privacy

https://cdn2.hubspot.net/hubfs/530177/Compliance/14101009.jpg
SECURING THE DATA

Adam Bennett
Vice President
Cloudburst Security

www.cloudburstsecurity.com
Contributing Factors in Data Breaches

- #1 Most Successful Attack Vector: Spear Phishing email
- Lack of end user security awareness
- Lack of skilled cybersecurity personnel
Contributing Factors

- Lack of cohesive cybersecurity strategy/program
- Lack of budget/resources & management support
- Tools problem: “If I spend enough on tools I will be safe”
Recent Breach Examples

- Medstar – Ransomware
- Hollywood Presbyterian – Paid $17k ransom in Bitcoin
- KY Hospital – Ransomware
Hallmarks of a Successful Cybersecurity Program

- Strategic plan linked to policies, procedures, and relevant metrics
- 24x7 Continuous Security Monitoring
- Formal Incident Response Plans
- Enterprise-wide Advanced Endpoint Security solution
Hallmarks of a Successful Cybersecurity Program

- Network or cloud-based Anti-Malware solution (FireEye, Barracuda, Palo Alto, etc.)
- Other security tools – as appropriate
- Vulnerability Management program
Hallmarks (continued)

- **Regular testing/assessments**
  - Spear phishing exercises
  - Penetration Testing
  - Application Security
  - Efficacy Reviews (people, process, technology)
  - Risk Assessments & Program-wide reviews
Hallmarks (continued)

- **Focus on learning & improving**
  - Learn from data breaches (internal & external)
  - Stay abreast of current & breaking attacker techniques
  - Learn from peers (conferences, networking, friends, etc)
  - Audits & assessments are opportunities to improve
Mitigating Risks: Things to Remember

Maureen Saxon-Gioia, BSN, RN
Director of Quality Improvement and Compliance
mgioia@osptahome.com
Do Your Homework!

- Research and understand different standards and frameworks
- Inventory what your organization is already doing
- Seek support and help

10 Easy Steps to Implement Enterprise Risk Management

by Carol Fox | November 14, 2012 at 12:12 pm

http://www.rmmagazine.com/2012/11/14/10-easy-steps-to-implement-enterprise-risk-management
Start Small

- Focus on a specific area or single goal
- Identify achievable objectives
- Set parameters for success
- Manageable action plan
Go for the Quick Wins

- What can we fix now?
  - Prioritize action plans

*understanding which risk criteria are important to leadership creates an opportunity for frank discussions*

- Assign an owner for the mitigation
Keep People Informed!

- List what was accomplished to date
- Include the challenges in meeting goal
- Don’t forget Senior management updates
Personal Attributes for Success

- Understand your audience
- Efforts must be perceived as value added by others in the organization
- Demonstrate excellence in communication
- Develop your “soft skills”
Uses for Health Information

• Reportable data
• Core measures
• Meaningful Use
• Outcomes
• Value Based Purchasing

• Clinical Decision making
• Clinical Research
• Quality Improvement
• Public Health
Good News: EHRs Support Provider Decision Making

- Improved aggregation, analysis, and communication of patient information
- Clinical alerts and reminders
- Support for diagnostic and therapeutic decisions
- Built-in safeguards against potential adverse events

Good News: Clinical Decision Support (CDS)

- Increased quality of care and enhanced health outcomes
- Avoidance of errors and adverse events
- Improved efficiency, cost-benefit, and provider and patient satisfaction

https://www.healthit.gov/policy-researchers-implementers/clinical-decision-support-cds

Clinical Decision Support: AHRQ

<table>
<thead>
<tr>
<th>Target Area of Care</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive care</td>
<td>Immunization, screening, disease management guidelines for secondary prevention</td>
</tr>
<tr>
<td>Diagnosis</td>
<td>Suggestions for possible diagnoses that match a patient’s signs and symptoms</td>
</tr>
<tr>
<td>Planning or implementing treatment</td>
<td>Treatment guidelines for specific diagnoses, drug dosage recommendations, alerts for drug-drug interactions</td>
</tr>
<tr>
<td>Followup management</td>
<td>Corollary orders, reminders for drug adverse event monitoring</td>
</tr>
<tr>
<td>Hospital, provider efficiency</td>
<td>Care plans to minimize length of stay, order sets</td>
</tr>
<tr>
<td>Cost reductions and improved patient convenience</td>
<td>Duplicate testing alerts, drug formulary guidelines</td>
</tr>
</tbody>
</table>

https://healthit.ahrq.gov/sites/default/files/docs/page/09-0069-EF_1.pdf
# Benefits of Clinical Decision Support

<table>
<thead>
<tr>
<th>CDS Intent</th>
<th>Match to User’s Intention</th>
<th>Key Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reminder of actions user intends to do, but should not have to remember (automatic)</td>
<td>High</td>
<td>Timing</td>
</tr>
<tr>
<td>Provide information when user is unsure what to do (on demand)</td>
<td>High</td>
<td>Speed and ease of access</td>
</tr>
<tr>
<td>Correct user’s errors and/or recommend user change plans (automatic or on demand)</td>
<td>Low</td>
<td>Automatic: timing, autonomy and user control over response On demand: speed, ease of access, autonomy and user control over response</td>
</tr>
</tbody>
</table>
Factors That Impact Data Quality

**EMR Design Specifications**
- hardware or software platforms;
- presence of programming errors or bugs

**Documentation Accuracy**
- What does your quality assurance (QA) reveal about accuracy in documentation?

**Daily Workflow/Human Factor**
- Electronic documentation has changed the workflow of healthcare workers

http://www.dentalsoftwareadvisor.com/2012/04/01/dental-ehr-workflow-transition/
The Unintended Consequences

Review the integrity of the current system for inaccuracies caused by

- **Missing Data**
  - How the measure is calculated-
  - Are all data elements present?
- **Data integrity**
  - Documentation variation
  - Workflow variation

Documentation Integrity

• Template Documentation
• Cloning, Copy/Paste
• Dictation Validation
• Patient Identification
• Amendments to the Record

http://library.ahima.org/doc?oid=300257#.VxPucvkrLIU
Documentation Integrity

Healthcare Fraud and Abuse
• Fabrication of medical record for reimbursement from an overuse of copy and paste designed for efficiency
• May involve repeated billing and coding errors

Audit Integrity
• Individual User
• Workstation
• Document
• Date and time

http://library.ahima.org/doc?oid=300257#.VxPxfkrLIU
**Recommended Practices for Phase 1 — Safe Health IT**

1. Urgent clinical information is delivered to clinicians in a timely manner, and delivery is recorded in the EHR.
   - **Worksheet 1**
   - Implementation Status: Fully in all areas, Partially in some areas, Not implemented

2. Policies and training facilitate appropriate use of messaging systems and limit unnecessary messaging.
   - **Worksheet 2**
   - Implementation Status: Fully in all areas, Partially in some areas, Not implemented

3. The EHR includes the capability for clinicians to look up the status of their electronic communications (e.g., sent, delivered, opened, acknowledged).
   - **Worksheet 3**
   - Implementation Status: Fully in all areas, Partially in some areas, Not implemented

4. Messages clearly display the individual who initiated the message and the time and date it was sent.
   - **Worksheet 4**
   - Implementation Status: Fully in all areas, Partially in some areas, Not implemented

WHAT’S THE BIG DEAL?

Angel Hoffman
Owner/Principal
Advanced Partners in Health Care Compliance
ENSURING DATA INTEGRITY?

To ensure means to guarantee…
Can we guarantee the integrity of the data?

“Ideally, the health data in an electronic record should be accurate, up-to-date and complete, but unfortunately the real world is far from ideal.” - AHIMA
Inaccurate Health Information May...

Adversely affect the quality of an individual’s:

Health;
Insurance;
Employability;
Finances
CHECKLIST FOR DATA INTEGRITY

1. Start with physician engagement;
2. Technology and Clinical Documentation;
3. Importance of Finance and IT Teams understanding clinical workflows;
4. Relationship with enabling continuous process improvements;
5. Understanding and applying data to solve complex problems across an organization;
6. HIM professional's role and responsibility regarding clinical documentation integrity, leading the healthcare industry into the next generation of health informatics and data analytics.
HEALTH INFORMATION EXCHANGE

- Need to have standardized computable definitions

- These definitions of data form the basis for future safe decision making

- HIE special committees (under Board oversight) develop policy and procedures to govern health data, assuring that data is accurate, complete, relevant, and current

- Need high levels of data integrity, including data content standards and definitions to promote submission of quality data for which the HIE and participating organizations are responsible

- Data adjudication
IMPACT TO THE HIE COMMUNITY

- Trusting relationships
- Connecting all of an individual’s data throughout the HIE
- Medical decision making and treatment
- Reliability vs. Liability
- Provider concerns
- Ownership of the HIE data
STRATEGIES FOR SUCCESSFUL PROGRAMS

Manage patient identification systems from front end data capture to back end quality control

Patient identification integrity is a complex concept, which is often confusing to the healthcare industry.

The complexity is attributed to multiple factors including:

- Variability in practices of authentication
- Data collection
- Technology and ongoing monitoring
STRATEGIES FOR SUCCESSFUL PROGRAMS

Incorrect or incomplete data capture within the healthcare setting can create:

- Critical patient care issues
- Risk privacy breaches
- Negatively impacts consumer trust
- Fosters user concerns throughout the medical community related to data reliability

Health information organizations (HIOs) support, oversee, or govern the exchange of health-related information among the member organizations in accordance with nationally recognized standards.
As data exchange methods through Direct messaging, private exchange, or state HIOs continue to evolve, patient identification errors are expected to increase significantly.

In early 2011, the Office of the National Coordinator for Health IT (ONC) Health IT Policy Committee, hosted a hearing, regarding patient matching recommendations.

More recent ONC activities include: environmental scan of vendors, providers, and data exchange organizations are exploring current approaches, practices, and processes related to patient identification.
Today, health data exchange is working toward the overall goal of interoperability, by increasing information sharing across provider organizations using networks and internet-based technologies.

A fundamental and critical success factor is to create a model which provides a comprehensive view of a patient’s entire clinical record from multiple participating organizations.

Trust among the participating organizations remains a barrier and yet portability and interoperability are key factors and the foundation of HIPAA’s development.
WHAT IS MISSING?

We continue to struggle with the absence of a nationally recognized patient identifier.

In its absence, the HIO must rely on sophisticated matching technology and the quality and completeness of the demographic data collected and maintained by each participating healthcare provider to create its own unique patient identifier.

Therefore… once the HIO EMPI obtains demographic data from the participating organizations, it has the task of linking all of these individual demographic records for one patient into a single record.

One method is for the HIO to link these varying provider records for one patient into one record, assigning its own unique numeric identifier.
VERIFICATION AND VALIDITY

No matter what algorithm an organization uses to link records, the results should be verified by people, using record matching validity procedures (during the initial system deployment and periodically on an ongoing basis.

Failure to catch errors can result in data fragmentation due related to missing clinical information or overlaid medical records.

The result: subsequent negative outcomes, adverse events, serious privacy breaches, and legal ramifications.
RESPONSIBILITY

Organizations that fail to carry out their responsibilities:

**Willingness** to work with the other partner organizations;

Compromise patient care within their own organization;

Contaminate the HIO database causing administrative complications and/or compromise patient care at member organizations.

HIOs are responsible for the overall management of the data they store and need to develop data governance policies and practices to maintain the quality of their data.

The accuracy and completeness of the data is essential to the effective management of patient identity integrity and is required to promote trust among the HIO’s participating data trading partners.
With today’s emphasis on PATIENT QUALITY AND PATIENT SAFETY, this is a huge concern.

Data failures can lead to unintended consequences (e.g. incomplete, inaccurate, or outdated information).

Data integrity failures can result in delayed or missed diagnoses, incorrect treatment, and possible patient harm.
While similar wrong-entry or wrong-record errors previously occurred with paper medical records, errors in the electronic environment can have more far-reaching consequences if the faulty data is exchanged with other computerized systems and devices within the organization.

An electronic error can also be more difficult to eliminate. It’s not just a matter of crossing out a wrong entry in a record. It have been replicated elsewhere and it must be corrected wherever it has been copied. Communication of these record changes creates its own challenges.

Research results skewed by inaccurate data outcome, leading to unsafe medical practices and poor treatment regimes.
FINANCIAL RISKS

Risk management – quality issues and medical malpractice resulting in potential lawsuits resulting from:

Patient actual harm causing injury and/or death

Misdiagnosis has treatment and life threatening issues

Overall, poor care delivery, increased costs (more patient days), unnecessary medications and possible unforeseen surgeries, may result

WHY? Because the information available to the health care provider is inaccurate and unfortunately a medical decision was made based on the information available the practitioner.
REAL WORLD EXPERIENCES

LET’S TALK!

Feel free to share your insights, incidents and lessons learned