Increasing Compliance and Reducing Risk Through Information Governance Practices

Presented By:

Andi Bosshart, RHIA, CHC
Sr. VP Corporate Compliance & Privacy Officer
Community Health Systems

Lee Ann Chapman, RHIA, CHC
Corporate Compliance Director
Community Health Systems

Ann Meehan, RHIA
Sr. Consultant, Healthcare & Life Sciences
Iron Mountain
Session Objectives

- The Current Healthcare Landscape
- What is Information Governance (IG)?
- Case Study: Community Health Systems Records Retention - Risk Reduction and Defensible Disposition
  - Federal Rules of Civil Procedure
  - Challenges with Document and Record Retention
  - Plan of Action & Lessons Learned
- Next Steps
- Q&A
The Current Landscape: Key Focus Areas

STRATEGIC TARGETS
- Quality outcomes
- Reduced compliance & privacy risks
- Savings targets
- Achieve margin improvement
- Leverage technology

OPERATIONAL EFFICIENCY
- Enhance labor efficiency/ productivity
- Reduce redundancies/ rework
- Improve workflow

COMPLIANCE RISKS
- Advance proactive data and information management
- Improve defensible disposition
- Minimize breach & cybersecurity risks

MERGERS & ACQUISITIONS
- Integrate systems
- Address data discrepancies/ source of truth defined
- Integrate hospitals, physician practices, clinics, & other business units
- Manage cultural shifts

Polling Question: What Gives You a Headache?
- Changing regulations
- Advanced technologies
- Patient-generated health data
- Growing data volume
- Lack of focus on life cycle of paper and electronic data
- Data and information decisions made in silos
- Ongoing threats of cyber attacks and breaches
- Staff turnover
Let’s Talk About Paper…

Hospitals account for 1/3 of all healthcare breaches
Results varied by hospital type

Paper and films most often breached
- Theft
- Improper disposal
- Unauthorized access


69%

DID YOU KNOW?
Did you know that 69 percent of the information in most companies serves no regulatory, legal or business purpose?

70%

FAST FACT:
In a typical company, as much as 70 percent of paper documents and 60 percent of unneeded electronic information can be defensibly disposed of in a compliant manner.

What Is Information Governance?

An organization-wide framework for managing information throughout its lifecycle and for supporting an organization’s strategy, operations, regulatory, legal, risk, and environmental requirements.

Polling Question:
Where is your organization in its IG journey?

- A formalized IG program is in place with numerous metrics and successes
- A formalized IG program is in place but no metrics have been established
- We’ve started talking about an IG program but have not yet formalized a program
- Senior leadership has not yet embraced the need for an IG program
- I have no idea

Key IG Concept: Privacy & Cybersecurity

- Administrative Safeguards
  - Data and information inventories
  - Record retention policies and schedules
  - Defensible disposition practices
- Physical Safeguards
  - Buildings
  - Access
- Technical Safeguards
  - Systems
  - Appropriate access
  - Encryption, firewalls, cloud storage, data centers & redundancy

Health Care Industry Cybersecurity Task Force

“In health care, security and cyber risk has historically fallen to IT. **Information governance** is a relatively new concept in the industry and should include not just IT and security stakeholders, but also information stakeholders. Governance structures should also include clinical and non-clinical leaders. Governance of information shifts the focus from technology to people, processes, and the policies that generate, use, and manage the data and information required for care.”


Defensible Disposition – A Critical Component of IG and Risk Avoidance

“It is natural that information – data and records in all formats – will have an *end of life* at some point in time. Defensible disposition comes into play at this juncture and relates to making decisions about what can be disposed of based on an official policy, and that may mean either moving it to a secure archive or destroying it in a compliant way.”

Challenges with Defensible Disposition

1. Not knowing where to start
2. Ill-defined process or execution plan
3. Legal and operational considerations
4. Limited technology
5. Missing or inadequate controls


Community Health Systems
Case Study: Records Retention
What are Federal Rules of Civil Procedure ("FRCP")?

- Govern procedure for all civil suits in US District courts
- Established by the Supreme Court
- First adopted and made effective in 1938
- Several amendments with last one effective December 1, 2018
- Expected to set the tone for state and local courts over time
FRCP and Discovery

• The discovery process for electronically stored information ("ESI") is equal to that of paper records.
• Documents may be requested in native file format with metadata intact.
• Inability to produce e-documents could result in fines and sanctions.
• Sets the stage for comprehensive policies and procedures re: retention, retrieval, and destruction of records—including electronic records.

E-Discovery and Metadata Defined

• Electronic discovery or e-Discovery is the electronic aspect of identifying, collecting and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation. ESI includes, but is not limited to, emails, documents, presentations, databases, voicemail, audio and video files, social media, and web sites.

• Metadata is the electronic equivalent of DNA, ballistics and fingerprint evidence, with a comparable power to exonerate and incriminate. Metadata sheds light on the context, authenticity, reliability and dissemination of electronic evidence, as well as providing clues to human behavior. All sorts of metadata can be found in many locations. Some is crucial evidence; some is digital clutter.

  • Resource: Federal Judges Association Newsletter November 29, 2006
FRCP: What You Need to Know

- Metadata includes information about the content, context, location, version, and other characteristics of data
- Request a narrowed scope when "any and all" records are requested – this could actually include voicemails, text messages, emails, etc.
- Establish sources of info—back-up tapes, instant messages, voice mail, email, departmental computer systems (e.g., lab, imaging, pathology, and OR systems)
- Consider system access, data retention and destruction when IT is replaced or upgraded
- Legal Hold or Preservation Order applies to e-data under FRCP
- Spoliation is the intentional destruction, mutilation, alteration, or concealment of evidence
- State and local laws regarding e-discovery

FRCP and What You Need to Do

- Carefully and clearly define your records
- Employ data classification procedures
- Determine when the useful life of a document has ended
- Craft complete record retention policies, include e-records
- Develop an airtight record destruction policy and follow it—including e-records
- Inform vendors and contractors with entity records of your retention and destruction policies – ensure you have air tight BAAs – you should virtually never sign a vendor’s BAA if you are the covered entity
FRCP and What You Need to Do

- Develop a process to notify relevant parties of a legal hold when a subpoena or other concern re: litigation is received
- Implement electronic processes to preserve “hold” data
- Establish comprehensive disaster recovery plans and procedures
- Educate, educate, educate
- Summary: initiate Information Governance Practices!

FRCP Challenges: Admissibility

- Records will be admitted in court if one can demonstrate consistent application of policies, procedures, and methods that support the creation and maintenance of reliable, accurate records
- Printed data from information stored in a computer that accurately reflects the original, is an original (Federal Rules of Evidence)
Challenges: Data Maintenance & Disaster Planning

- Write policies and procedures to prevent alteration, tampering, and loss of data
- Include procedures to address technology obsolescence or loss during conversion processes
- Consider length of time to retain paper copies of imaged records—refer to state or other retention requirement
- Implement policies for maintaining, protecting, backing up, and recreating data when subject to natural disasters, fire, system downtime, or vandalism
  - Data back up – are your tapes stored in a ‘secure’ environment?
  - Disaster recovery plan
  - Emergency operations procedures
  - Testing and revision procedures
  - Data and applications analysis

Challenges: Destruction

- Purge and destroy records according to written retention and destruction schedules – stick to the guidelines – **if you have the records you must produce them**
- Electronic or imaged records and the accompanying structured and unstructured computer data (audit trails, metadata) should also be destroyed if state regulations allow
- Include destruction method and security of the destruction process in the destruction policy
Policy Check-Up

• Access and produce e-records pursuant to a legal request
  • Periodically review policies and technical capabilities to ensure a smooth discovery process
  • Stop destruction plans for documents upon which notice of potential litigation is received

• Storage and production of records, including the native file format and metadata maintenance
  • Plan for how business records will be retained and disclosed
  • If info is not necessary, it should not be retained
  • Implement an email retention policy including classification of emails

• Evaluation of compliance with the organization’s storage, retention, and destruction policies

Case Study: Records Retention

• Foreword

• Challenges
  • Size of organization
  • Resources
  • Turn-over

• Plan of Action
Case Study: Which of these boxes….

- Could have been destroyed more than 10 years ago but will likely generate storage fees for another 10 years?
- Could be harmful to your value and brand?
- Is highly valuable information and may be destroyed because of an incorrectly assigned destruction date?

Case Study: Plan of Action Initial Steps

- Creation/update of Policies and Procedures, including Retention Schedule
- Establish Document and Record Retention Committee
- Develop Survey Questions for Inventory!
- Communicate Plan of Action to Staff
  - Begin with Corporate departments first
  - Deploy to all hospitals and their affiliated entities
Case Study: Announcement to Staff

The Corporate Compliance Department has organized a Document Retention project including both paper and electronic storage of documents – including email. It is more important than ever to ensure documents and electronic media files are categorized, inventoried and destroyed according to schedule (insofar as no litigation hold exists), while continuing our effort to minimize the expense associated with maintaining our obligations for document retention.

Case Study: Phase One Inventory Questions

- Demographic data such as entity name, department name, contact information for person completing survey
- List all off-site storage vendors
- List all locations of on-site storage
- Estimate how many boxes stored with each vendor
- Are logs/manifest/indexes of each stored box maintained?
- Attach a copy of your document retention policy
Case Study: Project Goals

Primary goal: maintain secure, cost-effective storage of records and specifically to:

- Assess compliance with document retention and destruction guidelines
- Reduce liability of storing unnecessary documents
- Eliminate storage of documents in locations not meeting our security criteria
- Minimize off-site storage costs

Case Study: Phase Two Actions & Tools

- Project tools* were created to enable determinations regarding:
  - Physical security of current storage,
  - Whether documents continued to require storage, and
  - If records may be destroyed or moved
- Key terms defined: records, secure, unsecure, known & unknown
- A second, more detailed assignment Worksheet* was deployed
- Attestation of Completion*

*Refer to separate document or upcoming slide
Case Study: Project Tool

Case Study: Definitions

- **Secure**: Meets all requirements of physical security criteria
- **Unsecure**: One or more deficiencies of physical security criteria
- **Known**: Facility maintains an accurate log, manifest or inventory of stored material. Documents that are required for recall can be obtained in a timely manner without searching through multiple boxes.
- **Unknown**: Facility has boxes stored which lacks a log, manifest or accurate inventory of contents.
Case Study: Definitions – On-Site & Off-Site Physical Security Criteria

- **On-Site** Physical Security Criteria
  - Storage location is within the main facility
  - Secured behind locked door and access is limited to appropriate facility personnel

- **Off-Site** Physical Security Criteria
  - Perimeter Security (e.g. fence, proximity sensors, monitored cameras, 24/7 Guard)
  - All entry points are locked
  - Controlled access to facility via badge, guard, key or keypad
  - All employees must have background checks to screen out potential employees for arrests and/or convictions including: theft and/or identity theft
  - Access log maintained
  - 24/7 guard and/or video surveillance
  - Intrusion, fire protection and moisture alarm system
  - HVAC climate controlled to prevent freeze and exposure to extreme heat
  - Multi tenant storage segregation; affiliate storage is inaccessible to others
### Case Study: Worksheet

**Document Retention Project Tool Worksheet**

<table>
<thead>
<tr>
<th>Facility</th>
<th>State Name:</th>
<th>State Contact:</th>
<th>Document Retention On-Site Storage Worksheet</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Yes, go to question 2. If no, go to the Document Retention Project Tool Worksheet for Off-Site Storage.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Specific Reference</th>
<th>Page 2 Box A</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Storage location is within the main facility?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Storage location is locked and access is limited to appropriate facility personnel?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Are there additional locks and access is limited to appropriate facility personnel?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1. If not, go to question 2.</th>
<th>Specific Reference</th>
<th>Page 2 Box B</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Are there any doors that are not locked by key card?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1. Yes, go to question 3.</th>
<th>Specific Reference</th>
<th>Page 2 Box C</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the facility maintain an accurate log, manifest or inventory of all stored documents?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Case Study: Attestation

CHSPSC Compliance Department requires the FCO and CEO to complete a Document Retention Project Tool Worksheets & Attestation to certify complete and accurate review of each Document Retention Project Tool. A signature blank has been provided at the end of the document; typed names and signature are required. By signing this document, you are certifying the following:

I certify the Document Retention Project Tool has been completed for each survey response. All issues of concern or non-compliance have been reported to a CHSPSC Compliance Director.

<table>
<thead>
<tr>
<th>FCO Name (print)</th>
<th>FCO Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CEO Name (print)</th>
<th>CEO Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Case Study: Outcome Questions

- Is the Document Retention Project complete?
- Did the FCO & CEO sign the Attestation?
- Date the Attestation was presented to the Facility Compliance Committee
- Number of respondents who completed the Worksheets
- How many boxes were destroyed?
- How many boxes are eligible for destruction?
- How many boxes were sent to vendor storage?
- How many boxes are currently stored within the main hospital/entity?

Case Study: Lessons Learned & Best Practices

- Accountability: designate Executive Leadership & a Champion point person
- Team effort
- Education
- Oversight: use an existing Committee
- On-going monitoring:
  - Internal Audit
  - Vendor or internal tracking
Case Study: Don’t forget…

• Electronically stored information: email, voicemail, back-up tapes, cloud storage, etc.
• Records stored with contracted or outsourced vendors
  • Consider voice data, web-based applications or websites for Human Resources, Marketing, etc.
• New acquisitions
• Document scanning to EHR
Roadmap to Achieve Compliance & Enable Enterprise-Wide IG

I. Create a Governance Structure

II. Consistently Apply Policy

III. Get Control of Your Information

IV. Deliver Insight

V. Continuous Improvement: Ongoing Maintenance, Measures & Metrics

Polling Question:
Who should lead IG at your organization?

- CEO/COO
- CFO
- CIO/CITO/CISO
- Compliance
- Legal
- HIM
- It depends…
- None of the above
- I have no idea!
The Positive Impact of an IG Program

### Strategic Targets
- Quality outcomes
- Reduced compliance risks
- Savings targets
- Achieve margin improvement

### Operational Efficiency
- Enhance labor efficiency/ productivity
- Reduce redundancies/ rework
- Improve workflow

### Compliance Risks
- Advance proactive data and information management
- Improve defensible disposition
- Minimize breach & cybersecurity risks

### Mergers & Acquisitions
- Integrate systems
- Address data discrepancies/ source of truth defined
- Integrate hospitals, physician practices, clinics, & other business units
- Manage cultural shifts

---

A Multi-Phased Approach to Defensible Disposition

### A 3-Phased Approach

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess</td>
<td>Optimize</td>
<td>Transform</td>
</tr>
</tbody>
</table>

- **Assess**: Assess current state & design program
- **Optimize**: Optimize for risk and cost reduction
- **Transform**: Transform for enhanced business value

Defensible disposition is dependent on a solid policy around information/data/IT assets retention and disposition
Breaking It Down – Manageable Next Steps

Phase 1
Assess
- Develop a record retention policy & schedule or refresh your current one
- Ensure it is manageable
- Educate across the workforce, including location of policy/schedule & establish accountabilities

Phase 2
Optimize
- Look for a record retention policy & schedule
- Evaluate it for currency & thoroughness
- Ask staff if they are aware of a retention policy/schedule & where it is located

Phase 3
Transform
- Develop an enterprise-wide plan for defensible disposition
- Put policy into action
- Monitor & report metrics & continuously improve

Questions?