Massachusetts Health Data Consortium

18-Mar-2015

Healthcare Compliance in 2015

“Achieving seamless compliance with healthcare mandates.”
Agenda

I Introduction

II Legal – Issues in Compliance

III Provider(s) Challenges

IV Engagement Scenario

V Technology as a Tool

VI Summary / Q&A
I. Introductions

Matthew Fisher

Matt Fisher is the co-chair of Mirick O’Connell’s Health Law Group and a member of the firm’s Business Group. Matt focuses his health law practice on regulatory compliance, including HIPAA and fraud and abuse.

Paresh K. Shah

Paresh Shah is a founder and president of MindLeaf, with over 20 years of experience in healthcare. He is a Specialist in Healthcare Regulatory Compliance

* HIMSS – ICD10 Task Force member
* ICD10 Playbook: Co-Chair.


Don Gleason

Don Gleason is recognized for driving cross-organizational efforts that advance delivery excellence with a vision directly tied to customer satisfaction and compliance. Throughout his career he oversaw strategic client programs and operational improvements and provided strategic portfolio leadership and direction to over commercial payer, provider, and government healthcare / health information initiatives.
II. Achieving Compliance in 2015

12 Months

2015

<table>
<thead>
<tr>
<th>Jan</th>
<th>Feb</th>
<th>March</th>
<th>April</th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Privacy &amp; Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meaningful Use – Stage 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICD-10 (Meet compliance)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICD-10 Post compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Goal – Fear of not being compliant and the penalties associated.

www.mindleaf.com
Challenges

1. Establishing enterprise-wide understanding of the new compliance programs (MU-2, ICD-10, HIPAA Privacy/Security)
2. Assessing current vs. desired state for the enterprise. Developing a plan to close the gap
3. Reworking affected systems while not disturbing production during transition
4. Training
5. Attestation/Audit

*Budgeting the costs in a difficult economic environment*
Will you be able to achieve?

This presentation will offer a look into establishing a Compliance Program and potential areas of focus for you to consider, as your organization determines its approach to become a secure and compliant organization.

At the end of the presentation you will be able to discuss:

• How to prevent non-compliance
• How to protect from non-compliance
• Reduce tangible/non-tangible damage caused
I Assess/ Define to become a secure organization
II Develop documentation
III Train people and attest

MindLeaf model

Mission:
Secure & Compliant Organization

Assess

Time
Resource
Knowledge/Capacity
How to get started?

Privacy Monitoring

Monitor – Risk & Incident Mgmt

Internal Audit

Prevent Non-compliance

Protect from non-compliance

Reduce tangible/intangible damage caused

SAAS based platform
- Compliance Mgmt Platform
- (Documentation library)

www.mindleaf.com
II. Legal – Issues in Compliance

Start with an end in mind

1. Prevent Non-compliance
2. Protect from non-compliance
3. Reduce tangible/intangible damage caused

The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.
- Sun Tzu

Your company might get hacked, but 'you can't make it easy for them'
- Homeland Security Official Mar 11, 2015, 2:35pm EDT
Meaningful Use: Assignment of Incentives

Assignment a contractual issue

• CMS explicitly stated it does not want to play a role.
• Who gets the incentive?
  • Eligible Professionals (EP) and Eligible Hospitals
• How can incentive be assigned?
• What happens if EP leaves or retires?
Meaningful Use: Attestation

- Attestations and incentive payments being audited
- Essential to maintain documentation to support attestation
- What are biggest risks?
  - Risk assessment (similar to HIPAA)
- What are risks associated with attesting through proxy?
HIPAA: Lessons to Learn from Recent Breaches/Settlements

New York Presbyterian Hospital and Columbia University

- Settlement announced May 7, 2014
- Breach result of physician hooking personal computer server to system network
- System not secure, connecting server resulted in ePHI being accessible through internet search
- No prior efforts made to assess security of server
- No assessment of software protections available for server
- OCR found lack of adequate risk analysis
- Fined $4,800,000
HIPAA: 
*Lessons to Learn from Recent Breaches/Settlements*

**Parkview Health System**

- Retired physician filed complaint
- Parkview supposed to retain custody of medical records on behalf of physician
- Instead, Parkview employees delivered boxes of records to retired physician’s home
- Employees knew physician not at home
- Boxes of records left on driveway
- Fined $800,000
HIPAA: 
Lessons to Learn from Recent Breaches/Settlements

Concentra Health Services

• Laptop stolen from facility
• Laptop not encrypted
• Numerous prior risk analyses identified lack of encryption was a critical risk
• Some steps taken to encrypt, but efforts incomplete and inconsistent
• Fined $1,725,220
HIPAA: Lessons to Learn from Recent Breaches/Settlements

Anchorage Community Mental Health Services

- Self-notification of breach resulting from malware
- Malware compromised security of whole IT system
- ACMHS adopted Security Policies, but took form policies
- Policies, once adopted, not followed
- Software not updated with available patches and used outdated software
- Basic risks not identified nor addressed
- Fined $150,000
HIPAA: Lessons to Learn from Recent Breaches/Settlements

Nebraska Medical Center

- Treated first Ebola patient in the country
- 2 employees asked patient’s medical record
- Employees did not have purpose for access
- Employees terminated
- No fines, yet
HIPAA: 
*Lessons to Learn from Recent Breaches/Settlements*

Community Health System

- Data breached as a result of being hacked
- Not apparent whether controls and systems adequate or insufficient
- Offered warning to all other healthcare entities
- Demonstrates high value placed upon healthcare information
- No fines yet  **Lawsuits filed**

Anthem

- Hackers broke into system
- Up to 80 Million individuals impacted
- Result of cyber attack
- Need to analyze unusual activity
- Highlighted weaknesses in healthcare IT
- **Lawsuits coming**
HIPAA: How to Reduce Exposure?

HIPAA Security Risk Analysis (SRA)

• Common Findings of a HIPAA Security Risk Analysis
  • Lack of system activity review
  • Lack of encrypted offsite data backup
  • Lack of an implemented and tested disaster recovery plan
  • Lack of email encryption
  • Lack of laptop encryption
  • Lack of mobile encryption (smartphones / tablets / USB drives, etc.)
  • Lack of anti-virus on all endpoints and servers
  • Lack of security patching of servers and desktops
  • Lack of security penetration and vulnerability testing
  • Lack of security incident response procedures

Inventory, Access Risk, Recommend Additional Security
HIPAA: 
*How to Reduce Exposure?*

**Training**

- Training must create a culture of compliance (highlight sanctions)
- Consider different types of training for different categories of employees (e.g., special training for people with remote access or BYOD training)
- Training must extend to physicians
- Don’t forget about Security Reminders! (and Privacy Reminders!)
HIPAA:
How to protect patient information

• Inappropriate access to patient information

• What is inappropriate access?
  • Snooping (movie star/ex-girlfriend)
  • Stealing (gang member’s girlfriend)
  • Modifying/deleting (disgruntled employee)

• Ways to detect:
  • Auditing of Access
  • Employee education
HIPAA:  
How to reduce exposure?

- **Have a policy**
  - People, it's just Facebook. Not reality. Hello? Again ... it's just a name out of millions and millions of names. If some people can't appreciate my humor then tough. And if you don't like it, too bad, because it's my wall and I'll post what I want

- **Use of Encryption**
  - Safe harbor/get out of jail free card?
  - Inexpensive
  - Easy to implement

- **Increasing concern**
- **Protecting against hackers:**
  - Passwords – easy, but causes debate
  - Need to be complex, change often
- **Anti-Virus** – install & run
- **System Patching**
- **Penetration & vulnerability scans**

- **Do Not Send Unencrypted PHI**
- Constitutes 10% of breaches
- **Considerations for encrypting:**
  - Relatively inexpensive
  - Easy to implement
  - Patients want/expect to communicate by email
  - Omnibus Rule opens door
III. Providers Challenges

What is a bigger challenge for hospital CIOs and CISOs – selection of hardware and software for compliance or implementation of policies and procedures for security?

*Policies & Procedures* make you compliant, and *Tools* only assist in making your organization compliant.
Health Care Industry Oversight

- Congress
- Supreme Court
- Federal Circuit Courts
- Departmental Appeals

CMS

- RAC / Program Integrity
- PRRB Reviews
- Intermediaries
- Carriers

- CMS Regional Offices
- DME Regional Contractors
- Regional Home Health Intermediaries
- Drug Enforcement Administration
- Fed Aviation
- Security Exchange

- DME Regional Contractors
- Regional Home Health Intermediaries
- Drug Enforcement Administration
- Fed Aviation
- Security Exchange

Other Accreditation Agencies

- Office Inspector General
- Office of Inspector General

State-Level
- Oversight Departments
  - State-Level
    - Licensure
    - Surveys & Certifications
    - Courts
    - Attorneys General
    - Medicaid
    - Health Boards
    - Medical Boards

- Federal Trade Commission
- Food & Drug Administration
- OSHA
- Treasury
- FBI
- Labor
- Nuclear Regulatory Commission
- The Joint Commission
- Federal Emergency Management Agency
- Federal Trade Commission
- Federal Emergency Management Agency
- Federal Commission

- Federal Trade Commission
- Federal Emergency Management Agency
- Federal Commission

- Federal Trade Commission
- Federal Emergency Management Agency
- Federal Commission

GSA

- National Highway Traffic Safety Administration
- Nuclear Regulatory Commission
- Federal Emergency Management Agency
- Department of Transportation

IRS

- Environmental Protection Agency
- Department of Health and Human Services
- Department of Labor

- Environmental Protection Agency
- Department of Health and Human Services
- Department of Labor

- Environmental Protection Agency
- Department of Health and Human Services
- Department of Labor
A comprehensive Compliance Program

• Health care organizations face an increasingly complex regulatory environment with federal and state agencies enforcing laws and statutes and imposing significant penalties for non-compliance.

• Mitigating non-compliance requires a number of steps:
  – Assess compliance risks
  – Implement corrective-action plans and unify compliance activities
  – Monitor compliance risks and improve traceability for rapid response to audit inquiries
  – Manage incidents and complaints and third-party vendors

• Overall goal is to:
  – Establish a culture of ethical behavior and commitment to compliance with the applicable regulations, statutes and laws
  – Provide a safe mechanism for reporting and seeking help
  – Help raise awareness
  – Assist in creating a positive impact on our corporate reputation and public image
Compliance Factors

A recent report sponsored by the Association of Healthcare Internal Auditors revealed top compliance priorities. These include, but are not limited to:

- Health Information Exchanges (HIEs)
- Value-based Purchasing
- ICD-10 implementation, impact and readiness
- Payment Bundling
- Accountable Care Organizations (ACOs)
- Clinical Documentation
- Pay-for-Performance quality standards (CMS core measures and HCAHPS)
- HIPAA | ARRA (HITECH) | PPACA
- Meaningful Use
- Federal Information Security Management Act (FISMA)
- State-specific Privacy/Security laws
- CMS ACO Quality Measures
- CAHPS Survey for ACOs
- RAC / PI

There is no silver bullet to compliance; however, best practice suggests create a strong compliance program to:

- establish strong standards;
- communicate those standards to all levels of the organization; and,
- enforce those standards.

According to US Sentencing Commission Compliance guidelines state that if your organization is found in violation of the law but has a strong compliance program in place, the penalties incurred will be significantly reduced.
Compliance Strategic Planning

An effective Compliance Program is developed in the context of your organization’s mission. Some purposes of the program could be:

• Maintain and enhance quality of care
• Demonstrate sincere, ongoing efforts to comply with all applicable laws
• Revise and clarify current policies and procedures to enhance compliance
• Enhance communications internally and/or with BOD and governmental entities with respect to compliance activities
• Empower all responsible parties to prevent, detect, and resolve non-conformance with applicable laws, regulations and the program; and
• Establish mechanisms for employees to raise concerns about compliance and ensure concerns are appropriately addressed.
Approach

Change Management

People & Process
without Technology
- Frustration & inefficiency
- High cost of operation

People
(Resources)

Process
(Methods)

Technology
(Software, Hardware & Tools)

People & Technology
without Process
- Automated chaos & confusion
- Poor customer service

Process & Technology
without People
- Alienation & turnover
- Underutilized systems

Adapted from:
S. Bell, "Lean Enterprise Systems: Using IT for Continuous Improvement"
Compliance – Right Approach

The art and science of effective Change Management

People (Humanist)

Process (Mechanist)

Technology (Technologist)

People, Process & Technology
- Effective & Cost-Efficient Transformation
- Sustained Benefits

The “PEOPLE” aspect of successful business change or transformation is the most critical component of sustainable change and effective Organizational Change Management (successful business transformation.)

Technology and/or process changes are easier to prescribe and manage than are the effects on the people – sustainable solutions are people-inclusive.

Assuring this enables the transformation by allowing people to part of the evolution, rather than revolutionaries opposing change.

Adapted from:
S.Bell, "Lean Enterprise Systems: Using IT for Continuous Improvement"
IV. Engagement Scenario - Assessment

Representative Assessment / Discovery Life Cycle

Planning
- Management Synchronization
- Tailor Pre-Survey Materials
- Adjust Interview Q’s
- Project Kick-off
- Distribute Questionnaires

Data Gathering
- Prepare Site Reviews
- Collect Data from Support Team
- Conduct Reviews
- Conduct Response Reviews
- Prepare Clarifications

Analysis
- Conduct Analyses
- Document Findings
- Review Results & Findings
- Draft Corrective Action Plan / Implementation Roadmap

Reporting
- Prepare Report
- Finalize Corrective Action Plan / Implementation Roadmap
- Present Report
- Synchronize all stakeholders

Actions
- Set Priorities
- Perform Corrective Actions, including OCM, training, etc.
- Measure, Manage, Monitor & Maintain Transformations
- Plan Transitions

Estimated duration: 8-16 weeks
V. Technology as a tool – for compliance

Privacy Assessment
HIPAA Mgmt.

Install Software - Security Audit Manager residing on the EMR

IPA
Outpatient Clinic 1
Care Center

Internet

Web Services
Privacy Monitoring of PHI

*Provide Iatric/Security Audit Manager – Patient Privacy & Incident Risk Mgmt*

- Collect Logs from Electronic Health Records
- Monitor
- Security Audit Manager – Iatric Systems
- Monitor, identify and alert on privacy violations
- SAAS based/Hosted by HIPAA Compliant
- Provides a dashboard

www.mindleaf.com
Tools –
SAAS-based Platform to Assess, Mitigate, Monitor, Audit - HIPAA compliance

• Develops, initiates, maintains, and revises policies and procedures for Compliance Program and its related activities to prevent illegal, unethical, or improper conduct.
• Manages day-to-day operation of the Compliance program
## Marlborough Medical Associates, P.C.

<table>
<thead>
<tr>
<th>Element</th>
<th>Assess</th>
<th>Mitigate</th>
<th>Monitor</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>MODERATE</td>
<td>NONE</td>
<td>Active</td>
<td>NO-ISSUES</td>
</tr>
<tr>
<td>Privacy</td>
<td>LOW</td>
<td>NONE</td>
<td>Active</td>
<td>ISSUES</td>
</tr>
<tr>
<td>Security</td>
<td>LOW</td>
<td>NONE</td>
<td>Active</td>
<td>ISSUES</td>
</tr>
<tr>
<td>Software</td>
<td>MODERATE</td>
<td>HIGH</td>
<td>Active</td>
<td>NO-ISSUES</td>
</tr>
<tr>
<td>Hardware</td>
<td>MODERATE</td>
<td>HIGH</td>
<td>Active</td>
<td>NO-ISSUES</td>
</tr>
<tr>
<td>Business Associates</td>
<td>MODERATE</td>
<td>MEDIUM</td>
<td>Active</td>
<td>NO-ISSUES</td>
</tr>
<tr>
<td>Medical Records</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>Active</td>
<td>NO-ISSUES</td>
</tr>
<tr>
<td>Facilities</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>Active</td>
<td>NO-ISSUES</td>
</tr>
</tbody>
</table>
TRIGGER EVENT:
ICD-10 implementation deadline (01-OCT-2015)

PMO - Lite
- Capture status and progress of all ICD-10 initiatives across the enterprise.
- Implement well-defined risk assessment and risk mitigation.
- Conduct a comprehensive awareness and training program.

Post ICD-10 Compliance – 1st 90 Days
- Risk Analysis
- Mitigation Strategies
- Check list – Whom to contact

Issues
- Providers have little time left to prepare for compliance
- ICD-9 to ICD-10 transition is time and resource intensive.
- ICD-10 will have significant effect on the billing process.

Clinical Documentation
- Teamed with ICDLogic to provide SAAS based solution for CDI
- Cloud based / Educational/Fast
- Easy to Use
- Accurate
Cypher is like having a Clinical Documentation expert at your fingertips.

- **FEATURES**
  1. Search by condition or code
  2. Customize by specialty
  3. Navigation prompts
  4. Authoritative CDI guidance
  5. CDI Monograph library
  6. ICD-9, ICD-10 & SNOMED

- **BENEFITS**
  1. Clinically oriented
  2. Fast & easy
  3. Immediate dual coding & ICD-10 compliance
  4. Integrates with any EHR
  5. Affordable & cost effective

- **CDI Expertise Built Into System Logic**
- **Desktop Laptop & Tablet Responsive Design**
- **HIPAA Compliant**
- **INTELLECTUAL PROPERTY**
  - Copyrighted User Interface (Guided Navigation)
  - Copyrighted Proprietary Content
    - 380+ CDI Monographs (CM)
    - Custom Coding Indexes
    - Custom ICD-9 to ICD-10 conversion mapping

www.mindleaf.com
VI. Compliance Program(s) Status

- PREVENT NON-COMPLIANCE
- PROTECT FROM NON-COMPLIANCE
- REDUCE TANGIBLE / NON-TANGIBLE DAMAGE CAUSED

**How Does Your Organization Look?**

- Use compliance to Get Best Practices
- Will Meet Compliance
- Failure to meet Compliance
- Will Meet Compliance & be compliant.

To summarize – People, Policies & Procedures, Processes, and Tools (MindLeaf model) can help you achieve compliance at an affordable cost.
Your compliance program

Secure and Compliant Organization

- Legal Interpretation
- Process
- People
- Tools
- Attestation & Internal Audit
Point of Contact:

Paresh K. Shah
MindLeaf Technologies Inc.
781-275-1845
pshah@Mindleaf.com