Risk of the Electronic Health Record - Updates

Lori Laubach
Principal
Health Care Consulting

2014 AHIA Pacific Northwest Regional Seminar
The material appearing in this presentation is for informational purposes only and is not legal or accounting advice. Communication of this information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, or other professional advice is required, the services of a professional should be sought.
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>OIG Work Plan indicates target for claims</td>
</tr>
<tr>
<td>9/2012</td>
<td>NY Times - “Medicare Bills Rise as Records Turn Electronic” &amp; HHS/DOJ letter warning of EHR fraud risks</td>
</tr>
<tr>
<td>10/2012</td>
<td>ONC indicates it will look for upcoding</td>
</tr>
<tr>
<td>3/15/2013</td>
<td>CMS revises Program Integrity Manual (PIM)</td>
</tr>
<tr>
<td>4/16/2013</td>
<td>White paper, “REBOOT: Re-examining the Strategies Needed to Successfully Adopt Health IT” - “Cloned” or Copied Records Can Increase Medical Errors”</td>
</tr>
<tr>
<td>12/2013</td>
<td>OIG - Failure to implement hospital EHR fraud safeguards</td>
</tr>
<tr>
<td>1/2014</td>
<td>OIG - Failure to implement EHR fraud safeguards</td>
</tr>
</tbody>
</table>
OIG AUDIT REPORT ON HOSPITALS

• EHR technology can make it easier to commit fraud
• EHR documentation features, if poorly designed or used inappropriately, can result in poor data quality or fraud
• Examples:
  o Copy-pasting, AKA cloning;
  o Over documentation – inserting false or irrelevant documentation to support billing for higher level services – systems which auto-populate or generate extensive documentation with one single click of a checkbox

http://oig.hhs.gov/oei/reports/oei-01-11-00570.asp
OIG AUDIT REPORT ON HOSPITALS (CONT.)

• Recommendations:
  o Audit logs should be operational and not disabled
  o CMS should develop guidance on the use of the copy-paste function

Source: HHS Office of Inspector General, “Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology”, OEI-01-11-00570 (December 2013)

http://oig.hhs.gov/oei/reports/oei-01-11-00570.asp
OIG AUDIT REPORT ON MEDICARE CONTRACTORS

• Key Findings:
  o Few contractors reviewed EHRs differently from paper medical records
  o Not all contractors could determine if a provider had copied language or overdocumented in a medical record
  o CMS has provided limited guidance to its contractors on fraud vulnerabilities in EHRs

http://oig.hhs.gov/oei/reports/oei-09-11-00380.asp
• Key Recommendations
  o CMS should provide guidance on detecting fraud associated with EHRs (CMS said that it intends to develop guidance on the appropriate use of copy-paste functions, and will work on developing best practices for detecting fraud associated with EHRs)
  o Contractors should be directed to use providers’ audit logs (CMS said audit logs are helpful but may not be appropriate in every circumstance and that review of audit logs requires special training)

AHIMA AREAS OF CONCERN
AHIMA EMR/EHR AREAS OF CONCERN

1. • Authorship integrity risk
2. • Auditing integrity risk
3. • Documentation integrity risk
4. • Patient identification and demographic data risks

Guidelines for EHR Documentation to Prevent Fraud
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_033097.hcsp
# AUTHORSHIP INTEGRITY

<table>
<thead>
<tr>
<th>RTI</th>
<th>AHIMA</th>
</tr>
</thead>
</table>
| Methods (i.e., copy/paste, direct entry, import) for any update to an EHR be documented and tracked. | • Identification of the provider of record  
• Inability to accurately determine services and findings specific to a patient’s encounter |
| User ID of the original author be tracked when an EHR update is entered “on behalf” of another author | • Cut, copy and paste functionality  
• Ability to take over a record and become the author  
• Inaccurate representation of authorship of documentation |

# AUDITING INTEGRITY

<table>
<thead>
<tr>
<th>RTI</th>
<th>AHIMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of an audit log function and specifies audit log operation and</td>
<td>• Inadequate auditing functions</td>
</tr>
<tr>
<td>content for tracking EHR updates.</td>
<td>• EHR system preserve data produced in response to a specific request, or can it be recreated reliability</td>
</tr>
<tr>
<td>Use of user IDs and passwords to restrict unauthorized access to</td>
<td>• Does the EHR system provide access control functions?</td>
</tr>
<tr>
<td>EHRs.</td>
<td>• Access controls based on role of provider</td>
</tr>
<tr>
<td>Use of a provider’s National Provider Identifier to restrict EHR</td>
<td>• None</td>
</tr>
<tr>
<td>access and track updates to EHRs by author.</td>
<td></td>
</tr>
<tr>
<td>EHR technology support an “auditor” class of user to have read-only</td>
<td>• None</td>
</tr>
<tr>
<td>access to patient records.</td>
<td></td>
</tr>
</tbody>
</table>

# DOCUMENTATION INTEGRITY

<table>
<thead>
<tr>
<th>RTI</th>
<th>AHIMA</th>
</tr>
</thead>
</table>
| Methods (i.e., copy/paste, direct entry, import) for any update to an EHR be documented and tracked. * | • Automated insertion of data  
• Templates  
• Auto population of clinical data  
• Problem list maintenance |
| Original EHR documents be retained after they are signed off and modifications be tracked as amendments. | • Inaccurate representation of authorship of documentation  
• Amendment/correction issues |
| Requires that EHR technology not prompt an EHR user to add documentation but be able to alert a user to inconsistencies between documentation and coding. | • Inaccurate, automated code generation associated with documentation |

# PATIENT IDENTIFICATION INTEGRITY

<table>
<thead>
<tr>
<th>RTI</th>
<th>AHIMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>EHR technology be able to record and indicate the method used to confirm patient identity</td>
<td>• Automated demographic information</td>
</tr>
<tr>
<td></td>
<td>• Quality of Care</td>
</tr>
<tr>
<td></td>
<td>• Fraudulent activity</td>
</tr>
<tr>
<td>Requires that patients be able to access and comment within their EHRs. (4.2.10)</td>
<td>None</td>
</tr>
</tbody>
</table>

APPENDIX

RTI Recommendations
## RTI RECOMMENDATIONS

<table>
<thead>
<tr>
<th>Audit Functions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Requires the use of an audit log function and specifies audit log operation and content for tracking EHR updates. (4.2.1)</td>
<td></td>
</tr>
<tr>
<td>2) Requires that the methods (i.e., copy/paste, direct entry, import) for any update to an EHR be documented and tracked. (4.2.4)</td>
<td></td>
</tr>
<tr>
<td>3) Requires that the user ID of the original author be tracked when an EHR update is entered “on behalf” of another author (i.e., distinguish between entries made by an assistant and a provider). (4.2.6)</td>
<td></td>
</tr>
<tr>
<td>4) Requires that EHR technology be able to record and indicate the method used to confirm patient identity (i.e., photo identification, prior relationship). (4.2.11)</td>
<td></td>
</tr>
<tr>
<td>5) Requires that original EHR documents be retained after they are signed off and modifications be tracked as amendments. (4.2.7)</td>
<td></td>
</tr>
</tbody>
</table>
## User Authorization and Access Controls

6) Requires the use of user IDs and passwords to restrict unauthorized access to EHRs. (4.2.3)

7) Requires the use of a provider’s National Provider Identifier to restrict EHR access and track updates to EHRs by author. (4.2.2)

8) Requires that EHR technology support an “auditor” class of user to have read-only access to patient records. (4.2.8)

## Data Transfer Standards

9) Requires that a document ID tracking number be generated and attached to an EHR any time an EHR is exported (i.e., printed or electronically communicated). (4.2.9)

10) Requires that EHRs be exchanged using certain data standards (encryption) to ensure that data have not been altered during the transmission. (4.2.13)

11) Requires that EHR technology have the capacity to directly capture clinical information in structured and coded data and not impact EHR user productivity. (4.2.12)
## RTI RECOMMENDATIONS (CONT.)

<table>
<thead>
<tr>
<th>Patient Involvement in Anti-Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>12) Requires that patients be able to access and comment within their EHRs. (4.2.10)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>13) Requires that information transmitted for payment of claims be accurately linked and tracked to the appropriate EHR. (4.2.14)</td>
</tr>
<tr>
<td>14) Requires that EHR technology not prompt an EHR user to add documentation but be able to alert a user to inconsistencies between documentation and coding. (4.2.5)</td>
</tr>
</tbody>
</table>
QUESTIONS?

Thank you for your time!

Lori Laubach
Principal
Health Care Consulting
253-284-5208
Lori.Laubach@mossadams.com
Objectives

- Describe how two organizations have managed and responded to privacy matters using Epic tools
- Assess your organization’s ability to respond to privacy matters and patient requests to exercise privacy rights
- Prepare your organization to comply with requirements for participation with Epic’s national health information exchange
- Highlight emerging privacy risks
• How does an address error become a potential HIPAA violation
• Monitoring patient charts in Epic

MULTICARE HEALTH SYSTEM
How does an address error become a potential HIPAA violation?

- Patients linked incorrectly
  - Children of divorced patients linked to both parents
  - Children over 18 linked to parents
  - Husband may still be linked to ex-wife and new wife at the same time
  - Foster children linked to foster parents after the child moves on

- Employee updates wrong patient chart
  - Employee may pull up wrong patient chart
    - Same name – wrong middle initial
Investigating Address Errors in Epic

1. How to determine if the address was updated through AUTOLINK or manually
2. How to identify the employee who manually updated the address
3. Who in the organization can assist in correcting the problem
Investigation Process

• Review the patient’s Audit Trail under the encounter
  – From Patient Station select a patient encounter
  – Select Update
Audit Trail

• The Audit Trail tool can generate reports on demographic updates
  – Addresses
  – Insurance
  – Phone numbers
  – AUTOLINK vs. employee update
  – Etc.
Audit Trail Report Settings

• Select date range
• Select Run
Audit Trail Report

• The report will display updates made to the chart
• Look for **AUTOLINK** with address updates
Next Steps

• After confirming there has been an AUTOLINK update for the address
  – Confirm with the patient:
    • Who should they be linked to. For example: Spouse, children, etc.
    • Current address and phone number
  – Contact the Patient Accounts department to review the charges on the account
    • They will be able to separate the charges, if necessary; and add or remove links
• The Patient Accounts department will be an important player in resolving this concern
• Notify the patient you have corrected the issue and the appropriate family members are now linked to them
Future Prevention

- Many users have different views in Epic which can cause confusion
- Ask Patient Access and Patient Accounts to work together on streamlining guarantor linking
- Patient Access should confirm guarantor information with patients at each visit and work with Patient Accounts if there is a linking concern
Monitoring Patient Charts in Epic

- MultiCare does not allow employees (including physicians) to access their own chart or those of family members
  - MultiCare follows the American Medical Association guidance on treating family members
  - MultiCare monitors this type of access through a software tool called FairWarning
  - Two specific reports run daily Alerts to identify this type of access
    - Self Exam (same name match)
    - Family Snooping (same address match)
- Monitoring of High-Profile Patients
  - All patients in the news are monitored with daily Alerts
What can access reports tell you?

- The date and time the user entered the chart
  - Time Stamp
- How long the user was in each area of the chart
  - Time Stamp
- Where the user was in the chart
  - Access Description
    - Encounters
    - Labs
    - Medications
- Location of the user
  - Log-in Department Name
  - Job Description
  - Workstation ID
Access Issues That Can Evolve Into Compliance and Privacy Concerns

• Potential Drug Diversion
  – Authorizing medications for family members without physician approval
  – Printing a prescription from Epic and then using the option “Encounter Opened in Error” to void the transaction

• Accessing a minors chart with confidential information
  – Washington State law has specific rights of confidentiality for children over 13

• Accessing spouses chart and using the information in divorce proceedings

• Removing charges on your chart or a family members

• Accessing high-profile patient charts who are in the news
Challenges in Chart Monitoring

• There are challenges in monitoring 2.4 million patient charts
• MultiCare has the ability to review access on all charts
• MultiCare identifies high risk patients and will monitor that particular access routinely
• Otherwise, patient or employee concerns can drive an investigation
Preventative Education

• MultiCare requires several types of HIPAA education for all employees
  – New Employee Orientation
  – Annual Mandatory Education
  – Annual Compliance Training
  – Focus on Privacy articles
  – Department Staff Meetings
    • Focused on departments with specific HIPAA concerns
• How to assess compliance capability for expanding use of Epic’s health information exchange functionality to the National eHealth Exchange
• How to enhance privacy using Epic’s Break-the-Glass functionality
Access Methods

• People get access to medical information using a variety of methods
  – Verbal
  – Paper (fax, mail, etc.)
  – Scanned documents
  – Interfaces with other systems and other entities
  – Direct Epic provisioning
  – EpicCare Link
  – Epic In-basket
  – Epic ROI Inspector
  – Epic My Chart
  – Epic Care Everywhere/Elsewhere (MU2 – access to National eHealth Exchange)
National eHealth Exchange

The Internet

Common standards, specifications and policies enforced through Data Use & Reciprocal Support Agreement (DURSA)

Source: HealtheWay
DURSA - References

• Link to the latest version of the DURSA, focus on sections 15.04 and 15.05
  http://healthewayinc.org/index.php/exchange/dursa

• Overview from the June 19, 2013 HealtheWay webinar
What is DURSA?

- A comprehensive, multi-party trust agreement that is signed by all eligible entities who wish to exchange data among Participants
- Requires signatories to abide by common set of terms and conditions that establish Participants’ obligations, responsibilities and expectations
- The obligations, responsibilities and expectations create a framework for safe and secure health information exchange, and are designed to promote trust among Participants and protect the privacy, confidentiality and security of the health data that is shared

Source: HealtheWay June 19, 2013 Webinar
DURSA Flow Down Provisions

- Valid and enforceable agreements that require Participants to assure employees and non-employees:
  - Comply with the law
  - Reasonably cooperate with entity & HealtheWay Coordinating Committee on issues related to the DURSA
  - Transact message content only for a permitted purpose
  - Use message content in accordance with the DURSA
  - Report breaches to entity & HealtheWay
  - Refrain from disclosure of any passwords
DURSA Flow Down Provisions con’t

- Require user training on DURSA specific requirements
- Require user access monitoring
- Entity level policy addressing DURSA compliance with use for only a “permitted purpose” is sufficient for employees, but not non-employed user population
Emerging HIE Risk

Greater exposure to inappropriate access that results in a reportable breach, even if it is just access to a single HIE record

- DURSA requires breach notification to:
  - Other HealtheWay Participants involved in breach
  - HealtheWay Coordinating Committee

- Epic’s Rules of the Road for Care Everywhere – Care Epic

- HIPAA Privacy Rule requires breach notification to:
  - Individuals involved in breach
  - Department of Health & Human Services Office for Civil Rights

- State law and other contractual reporting requirements
Emerging HIE Risk

- Makes visible the best (and worst) practices in health information management within your organization for external parties
- Many organizations have unclear functional accountability for overall operational compliance with DURSA
- Some options for accountable areas
  - Health information management
  - Clinical informatics
  - Health information exchange management
  - Corporate compliance
  - Privacy office
  - Information security
  - Risk management
  - Legal
Assess Your Capabilities

• 5. Data integrity (correct data on wrong record)
• 4. Patient identification standard (duplicate records & 2 patients sharing one record)
• 3. User access monitoring (looking at adult step-daughter’s record)
• 2. User training (accessing records for non-business purpose)
• 1. User identity standard (policy, contract/agreements, demographic data requirements)
Assess Your Capabilities

• Does user training have specific CE and DURSA requirements for when a CE encounter can be initiated?

• What roles can initiate a Care Everywhere HIE encounter versus view the content once incorporated into the record?
  – Is there a policy that addresses this for employees?
  – Who is accountable and responsible for this?

• Do you have enforceable agreements with non-employees?

• Raising the level of awareness on gaps in your capabilities

• It is a process that takes time and resources to develop
Assess Your Capabilities

Other Participants are large multi-function entities with:

- Comprehensive access management processes
- Years of experience systematically monitoring access
- Automated systems to support identity and access management
- Dedicated resources for securing agreements, providing training and monitoring access for non-employees
- Clear lines of accountability for non-employees
Relevant Privacy Related Functions

- Investigate and respond to complaints
- Safeguard electronic health information
  - Manage user authentication, access and disclosure
  - Assure data integrity
  - Monitor user access proactively
  - Assure minimum necessary
- Support exercise of individual privacy rights
  - Manage requests for restrictions
  - Manage requests for amendments
- Privacy training
Examples of Epic Privacy Tools

1. Epic patient - clinician relationship demographic data
2. Epic patient location and user access log-in department data
3. Access security templates and periodic audit
4. Basic and conditional access log reports
5. Break-the-Glass functionality
6. Identity management and user access software or databases
7. Specialized log aggregation software
8. Infrastructure to support management of non-employee data and individual and entity agreements
Epic Privacy Safeguard

Break-the-Glass functionality
- Choose what you want to protect
- Select the frequency of the trigger
- Set exclusion criteria based on logical roles
- Configurable reasons for access

Reporting
- In-basket messages
- Clarity
Epic’s Break-the-Glass (BTG)
Epic’s BTG
Historic Encounter Level BTG

• Controlled visibility of record content
• Triggers based on user security template
• Daily presentation
• User complaints drove numerous exceptions to triggers
• Generated massive, detailed BTG in-basket report volume
Patient Level BTG

• Generic rather than population specific
• Triggered all users except for data driven relationships
• Annual presentation
• Systematic monitoring of BTG reports
• Drove privacy awareness and positive culture change through offering to employees as opt-in
BTG - Key Messages

- Staff offered the opportunity to put BTG on their Epic records
- Added for patients with legitimate concerns about their medical records (i.e. celebrities, ex-spouses)
- BTG is a deterrent to inappropriate access, it doesn’t prevent access
- BTG is set up at the patient’s request
- BTG will fire once a year per patient per user
- BTG triggers are monitored
Questions?

Cindy Ryals, CHPC
MultiCare Health System, Tacoma, WA
Email: cindy.ryals@multicare.org

Carolyn Barton, CHC, CHPC
Group Health Cooperative, Seattle, WA
Email: barton.cm@ghc.org
# Outline

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introductions</td>
<td>2</td>
</tr>
<tr>
<td>Interfaces – General</td>
<td>3</td>
</tr>
<tr>
<td>Overview of Epic interfaces</td>
<td></td>
</tr>
<tr>
<td>• Definitions</td>
<td>6</td>
</tr>
<tr>
<td>• Environment</td>
<td>7</td>
</tr>
<tr>
<td>• Risks</td>
<td>8</td>
</tr>
<tr>
<td>• Challenges</td>
<td>9</td>
</tr>
<tr>
<td>Elements of realization (Recipe)</td>
<td>11</td>
</tr>
<tr>
<td>Tools and controls</td>
<td>19</td>
</tr>
<tr>
<td>Practice case</td>
<td>25</td>
</tr>
<tr>
<td>Questions</td>
<td>29</td>
</tr>
</tbody>
</table>
Introduction

Who we are

Intended outcome
Interfaces - General

inter·face (ˈɪntərˌfɑːs/) noun
plural noun: interfaces

1. a point where two systems, subjects, organizations, etc., meet and interact.
"the interface between accountancy and the law"
Physics: a surface forming a common boundary between two portions of matter or space, e.g., between two immiscible liquids.
"the surface tension of a liquid at its air/liquid interface"

2. Computing: a device or program enabling a user to communicate with a computer.
Identify and Test System Interfaces

Our understanding of the flow of transactions includes an understanding of the interfaces between various relevant information systems. Our consideration of risks include those risks to the completeness and accuracy of data that moves from various source systems to destination systems.

• Understand the flow of transactions between systems and obtain or create a data flow diagram that depicts the handoffs between systems
• Relevant controls to address system interfaces should be. This could include manual reconciliation controls that may be tested.
• GITCs, such as job scheduling/monitoring, are usually not sufficient on their own to address completeness and accuracy of an interface.
Overview of Epic interfaces
Definitions, Environment, Risks, Challenges
Epic provides connectivity solutions for interactions with outside systems called Epic Bridges Toolkit.
Overview of Epic interfaces

**Bridges** is the name of Epic’s interface application, which is a **collection of tools, utilities, and background processes**. It provides the infrastructure to allow interfaces to operate and assist in interface configuration and maintenance. Bridges is the infrastructure that allows interface messages to be sent out of and accepted into Epic.

**HL7**, which is an abbreviation of **Health Level Seven**, is a standard for exchanging information between medical applications. This standard defines a format for the transmission of health-related information.

The **Interface Monitor** and **Hyperspace Dashboard** allow an interface administrator or a user in an operations center to view the status of a set of interfaces in real time. Interfaces can be started or stopped from the Interface Monitor activity and other Bridges activities are accessed from it.

The **Background Monitor** is a very important process in Bridges. It is usually configured to start running on system startup and should ordinarily be running. While it takes care of many tasks, its primary purpose is to confirm that interfaces are running; all other tasks are ancillary to this.
Sample Epic interface environment
Risks associated with Epic interfaces

Given the nature of health care services, the diversity of integrated systems, and the completeness of Epic modules, risks may arise from the implementation of interfaces in several areas:

• Patient Care: risks associated with the transmission, reception, and routing of patient data (e.g., lab orders, pharmacy prescriptions and radiology)
• Downstream Processing: risks associated with the transmission of data to sub-systems for further processing (e.g., provider credentials update and HIE platforms)
• Revenue Cycle: risks associated with the processing of charges and claims (e.g., professional charges, contract charges and patient insurance eligibility)
• Integration: risks associated with the integration of other department specific Electronic Medical Records (EMR) and exchange of patient information (e.g., wound care charting applications and dialysis clinic EMR)

These risks may be mitigated by the applicable controls for the data to be completely, accurately, and timely exchanged and processed.
Common challenges
Why is it difficult?

There are a number of common challenges that are encountered by Internal Audit (IA) departments when wanting to conduct an Epic interface assessment. However, these challenges do not come without alternatives:

• **Complex environment**: many interfaces, many systems, may be overwhelming
• **Not involved in implementation**: tight timelines usually prevent inclusion of IA during development
• **Lack of documentation**: poorly written/maintained interface documents increase difficulty
• **Points of contacts**: contractors or interface analyst with the expertise are gone
• **Time/Resource constraints**: time needed for Information Technology Auditors to complete assessment may be challenging with competing priorities
Elements of realization (Recipe)
Elements of realization

What may help?

In order to effectively assess Epic interfaces, a number of elements need to be present:

• **Getting involved early on**: what is future state like, how does it differ from previous state, how are risks affected, etc.

• **Good methodology for the assessment**: what is the approach, what documents are needed, what are the testing procedures, etc.

• **Good understanding of the processes**: why do we exchange data, what are the risks, what are the controls, etc.

• **Relevant documentation of the interface(s)**: what are the systems, what data is exchanged, how is it exchanged, etc.

• **Right tools for the assessment**: what is the framework, how is the assessment documented, etc.
Building your recipe
Get involved early

Being able to anticipate changes to the established methodologies and procedures and making sure that plans are documented are important factors for future interface assessments. Leading practices include:

• Getting involved early on in the implementation project, upgrade, or new module/interface implementation
• Participate in the assessment and scope finalization phase
• Understand the differences between current and future state
• Build relationship with the interface project team
• Review their deliverables for completeness and accuracy
## Getting involved pre-implementation (sample timeline)

<table>
<thead>
<tr>
<th>Month</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Planning</td>
<td></td>
<td></td>
<td></td>
<td></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>Assessment and Scope Finalization</td>
<td></td>
<td></td>
<td></td>
<td></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>Analysis</td>
<td></td>
<td></td>
<td></td>
<td></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>Development</td>
<td></td>
<td></td>
<td></td>
<td></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>Testing</td>
<td></td>
<td></td>
<td></td>
<td></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>Go-Live and Cutover</td>
<td></td>
<td></td>
<td></td>
<td></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>Post Go-Live</td>
<td></td>
<td></td>
<td></td>
<td></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>
Building your recipe
Developing a methodology

One of the first step in the assessment of interfaces is determining what the approach is going to be. Leading practices include:

- Determine an achievable scope
- Determine preliminary list of documents needed
- Identify points of contact, subject matter specialists
- Organize meetings with point of contacts to gather a solid understanding of the environment and existing interface problems if any (e.g., duplicates and errors)
- Request any missing documentation; draft documentation to materialize the understanding of processes when needed
- Develop testing steps to test interfaces are working as designed: completeness, accuracy, timeliness
- Conduct testing and document findings
Building your recipe
Understanding the processes

Besides understanding how the interfaces function or analyzing that they are implemented as designed, a broad understanding of the business processes is important to identify risks and potential controls. Leading practices include getting an understanding of:

• What is the need for an interface
• What type of data is exchanged
• What are the risks associated with the process
• What are the internal controls in place to mitigate the risks
• How are the internal controls changing with the implementation of interfaces
Building your recipe
Applicable documentation

Gathering the proper documentation is essential to an accurate assessment. For Epic Interface assessment, the list of documents typically requested are:

• Business requirements document
• Technical specifications document
• Functional requirements document
• Interface testing documents (Interface Testing Toolkit – Epic)
• Data conversion documents (if conversion is part of the assessment)
• Epic interface diagram
• Interface charter
• Data mapping

However, documents are not always readily available or do not capture the relevant elements. Leading practices encourage to:

• Prepare a data flow diagram by process is particularly valuable when multiple systems are involved and there is a highly complex IT environment
• Use corroborative inquiry to validate the understanding of the system
Building your recipe
The right tools

A solid framework goes a long way in the process of testing Epic interfaces and will often be the representation of the methodology. Leading practices include

<table>
<thead>
<tr>
<th>Significant Account or Disclosure</th>
<th>Source System</th>
<th>Destination System</th>
<th>Data Transferred</th>
<th>Method of Data Transfer</th>
<th>Frequency of Data Transfer</th>
<th>Description of Control to Validate Accuracy and Completeness of Data</th>
<th>Type of Control (Automated, Manual)</th>
</tr>
</thead>
</table>
Tools and controls

Monitoring, Dashboard, Typical controls
Leading practice controls
Completeness, accuracy, timeliness

<table>
<thead>
<tr>
<th>Interface type</th>
<th>Risk description</th>
<th>Control objective</th>
<th>Control activity description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Interface files are incomplete and/or inaccurate.</td>
<td>The transfer of data via an interface is complete and accurate.</td>
<td>The Interface generates control totals (i.e., total Dollar Values, Hash Values, Record Counts, or Checksums) from the source systems.</td>
</tr>
<tr>
<td>Inbound</td>
<td>Data in the target system is not complete or up to date, limiting the effectiveness of the system.</td>
<td>Interfaces are performed timely to meet scheduled requirements.</td>
<td>A job scheduler and error notification process ensures that the interface process runs timely and in the correct sequence.</td>
</tr>
<tr>
<td>Inbound</td>
<td>If exceptions are not properly tracked and managed they may not be resolved appropriately or in a timely manner.</td>
<td>Interface data-related errors are identified and tracked until resolution.</td>
<td>Interface programs contain exception report processing. The exception reports list verification errors (numeric/non-numeric), record count inconsistencies or invalid insertion/conversion attempts.</td>
</tr>
</tbody>
</table>
Practice case

The provider (SER) interface
Applying the recipe
Understanding the process

Inbound

Outbound

Credentialing

Epic

Lab

Pharmacy

Radiology

Name

Name, License, Specialty

Name, License, Specialty, NPI

Name, License, Specialty

Name, License, Specialty, NPI

• License

• Specialty

• SPI #, NPI #, DEA #
Applying the recipe
Developing a methodology

• Determine an achievable scope
  – Inbound and outbound interface for provider records

• Determine preliminary list of documents needed
  – Business requirements document for provider interface
  – Technical specifications document for provider interface
  – Functional requirements document for provider interface
  – Interface testing documents (Interface Testing Toolkit – Epic)
  – Epic interface diagram specific to the provider interface
  – Data mapping

• Identify points of contact, subject matter experts
  – Interface Manager
  – Schedulable Enterprise Resources (SER) Coordinator

• Conduct meetings
  – During the meeting with the SER Coordinator we learn that:
    • There is no reconciliation reports generated
    • There have been history of duplicates being created when the interface went live
    • There have been multiple ‘contacts’ created on some SER records
Applying the recipe (cont.)
Developing a methodology

• During the meeting with the interface manager we learn that:
  – There have been a lot of questions about what should be used for identification of the provider downstream (Credentialing ID vs. NPI vs. newly generated ID)

• Request additional documentation:
  – Extract of all provider (SER) records
  – Decision document concerning the external identifier for downstream systems
Applying the recipe
Test steps

• Testing the interface
  – Based on the evidence gathered so far, the auditor may:
    • Review the documentation and test that data is flowing according to design from the documented source system to the destination system(s)
    • Inquire about existing controls, work queues, monitoring capabilities, and document findings
    • Perform in-depth testing of issues brought up by subject matter specialists and points of contact:
      – Gather an extract of all SER records
      – Review for duplicates
      – Investigate if duplicates have been created through the interface
      – Document findings
Conclusion

Epic interfaces are complex

Elements of testing are no different than regular interfaces

Tailor your approach to your unique business and IT environments

Get involved early

Build a repeatable approach
Questions
Data analytics: your guide through healthcare’s shifting regulatory landscape

March 14, 2014
“The transformational change occurring in organizations today is dependent upon adopting insight from data ... **Everyone is now an analyst.** ”
*Data Science Central*

“Last year people stored enough data to fill 60,000 Libraries of Congress...”
*The Economist*

“...Data volume will double over the next two years”
*Gartner*

“90% of the worlds data was created in the past two years ”
*IBM*
Agenda

• Introductions
• Top issues confronting healthcare executives
• Responding to the challenge
• Leading practices – a closer look
  • Case study 1 – ICD-10
  • Case study 2 – Two-midnight Rule
  • Case study 3 – HIPAA/HITECH compliance
• Q&A
Top issues confronting healthcare executives
Constant evolution in the healthcare regulatory landscape...

- **Medicaid Bundled Payment Demonstration**
- **Insurance Exchanges Open Enrollment**
- **Medicare High Income Beneficiary Tax Increase**
- **Increased Medicaid Payments to Primary Care Physicians**
- **2.3% Medical Device Excise Tax**
- **Retiree Drug Subsidy Deduction Eliminated**

- **2012 and Earlier**
  - Patient’s Right to Electronic Access to Health Record
  - Flexible Spending Account Coverage Expanded
  - ADA Protection Access Expanded
  - 2010 Application Of Rules to Business Associates

- **2013**
  - Stage 1: Data Capture & Sharing
  - Stage 1: Data Capture & Sharing
  - Extended Deadline for Systems to Comply With Disclosure Rules
  - Health Information to Include 50 years

- **2014**
  - Standardized Format For Safety Data Sheets
  - Use Of New Labeling Elements Required
  - Increased Medicaid Payments to Primary Care Physicians
  - 2.3% Medical Device Excise Tax
  - Stage 2: Advance Clinical Processes
  - Stage 2: Advance Clinical Processes
  - Enhanced Wellness Incentives

- **2015**
  - Penalties for Failure to Comply With Meaningful Use of EHR Technology
  - Stage 3: Improved Outcomes
  - End Medicare Star Payment Demonstration

- **2020**
  - High Cost Plan Excise Tax
  - Medicare Donut Hole Closed

- ** HIPAA extended to Business Associates**
  - Omnibus Effective
  - HIPAA extended to Business Associates
  - Patient’s Right to Electronic Access to Health Record

- **2010 Application Of Rules to Business Associates**
- **2013 Application Of Rules to Business Associates**
- **2012 Application Of Rules to Business Associates**

- **2014 Application Of Rules to Business Associates**
- **2015 Application Of Rules to Business Associates**
- **2020 Application Of Rules to Business Associates**

- **2014 Application Of Rules to Business Associates**
- **2015 Application Of Rules to Business Associates**
- **2020 Application Of Rules to Business Associates**
...is keeping executives up at night

Top issues confronting hospitals (according to healthcare executives)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Rank (of 10)</th>
<th>Specific concern</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Challenges</td>
<td>1</td>
<td>Government funding cuts</td>
<td>85%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medicaid reimbursement</td>
<td>81%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medicare reimbursement</td>
<td>71%</td>
</tr>
<tr>
<td>Healthcare Reform Implementation</td>
<td>2</td>
<td>Reduce operating costs</td>
<td>72%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alignment of provider and payer incentives</td>
<td>66%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shift to value-based purchasing</td>
<td>60%</td>
</tr>
<tr>
<td>Governmental mandates</td>
<td>3</td>
<td>CMS audits (RAC, MAC, CERT)</td>
<td>83%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implementation of ICD-10</td>
<td>79%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CMS Regulations</td>
<td>65%</td>
</tr>
<tr>
<td>Patient safety and quality</td>
<td>4</td>
<td>Engaging physicians in improving the culture of quality</td>
<td>71%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Redesigning care processes</td>
<td>66%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pay for performance</td>
<td>54%</td>
</tr>
</tbody>
</table>

Source: American College of Healthcare Executives Announces Top Issues Confronting Hospitals: 2013
The challenges are significant...

People
- Lack of resources
- Inadequate analytical skills
- Competing priorities

Process
- Adapting to comply with regulatory expectations/changes
- Optimization of organizational structure

Technology
- Disparate information sources
- Financial data not linked with patient information
- Ineffective/obsolete Internal Audit processes
…and so are the penalties

**Leading health and hospital system**
Fined $1M for patient safety and quality-of-care deficiencies

**Regional teaching hospital**
Will refund $1.06M to Medicare for overbilling

**Medicare Recovery Audit Program**
Medicare RAC Overpayment Collections reach $4.5B

**Non-profit healthcare system**
Pays $275,000 to settle HIPAA violation accusations

Source: Department of Justice, 2014
What are our clients saying?

“My audit budget is finite, yet I am expected to increase coverage”

“Our auditors spend too much time on non value-add activities”

“We are missing the forest for the trees”

“We need to fundamentally improve audit quality and value”

“We can’t hire or keep the best people”

“We need to better align with compliance and risk”

“We need to better understand risk”
Responding to the challenge
The best offense is an effective compliance program...

Elements of an effective compliance framework

- **Business strategy**
  - Tone at the top
  - Risk assessment
  - Lines of communication

- **Business management**
  - Oversight and responsibility
  - Policies and procedures
  - Training
  - Monitoring

- **Business assurance**
  - Auditing
  - Enforcement and discipline
  - Response and prevention
...where oversight and responsibility for compliance is shared...

<table>
<thead>
<tr>
<th>Tone and Oversight</th>
<th>Risk Assessment</th>
<th>Monitoring</th>
<th>Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management</strong></td>
<td><strong>Compliance</strong></td>
<td><strong>Internal Audit</strong></td>
<td></td>
</tr>
</tbody>
</table>
| • Owns and manages risks  
• Responsible for maintaining effective internal controls | • Oversees / monitors risks  
• Helps to translate legal interpretation of laws into actionable standards | • Provides independent assurance  
• Scope of assurance is broad - from strategic to compliance risks |
...and an analytics-driven approach provides greater risk assurance

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulators utilizing data-mining to target risk areas and noncompliance</td>
<td>Better understanding of risks using the same techniques as the regulators</td>
</tr>
<tr>
<td>Healthcare has heavily invested in technology but lacks the skill sets for effective use</td>
<td>Advanced analytical techniques can be more cost efficient than traditional methods</td>
</tr>
<tr>
<td>Need for visibility into compliance risk</td>
<td>Analytics can identify issues missed by traditional testing</td>
</tr>
<tr>
<td>Competitive pressures forcing innovation</td>
<td>Visibility to mistakes in logic or processing errors vs. hypothetical risks – accelerates root cause analysis</td>
</tr>
</tbody>
</table>
Implementing a Successful Program
Why are analytics so important today?

**Company expectations:** Maximizing the use of technology to increase coverage, quality and business impact, while managing a finite audit budget

**Competitive landscape:** Competitors continue to strengthen their capabilities and seek new talent

**Value/Relationship:** Insights open the door for deeper discussion on issues and develop/strengthen relationships

**Talent development and appeal:** Effective integration of analytics will strengthen the business skills of auditors

**Audit/Business Partnership:** Innovation and resulting methods could be ultimately transitioned into the business

**Regulatory Expectations:** Audit need to get stronger assurance and quantifiable results
**Biggest Challenges with Analytics**

- Developing a sustainable methodology and process: 41.2%
- Acquiring deep analytical skills and capabilities: 31.2%
- Adopting an effective structure: 14.8%
- Selecting the right tools and technologies: 12.8%

**Additional Challenges**
- Vision, Strategy & Roadmap
- Managing Data
- Business Buy-in
- ROI

*The Data Conundrum Global Webcast Survey Results*  
PwC
What are the major benefits?

What are the benefits?

1. Increase coverage, quality, and business impact
2. Establish competitive advantage in industry
3. Create deeper discussion on issues and develop/strengthen relationships
4. Strengthen the business and technical skills of auditors
5. Cultivate an audit/business partnership

Quantifiable:

- Development saved compared to traditional BI
- Audit hours saved (fieldwork review)
- Expenses minimized
- Revenue found

Quantifiable but not Always Tracked to Amounts:

- Audit coverage
- New policies enacted
- Audit user base adoption and expansion
- Audit procedures refined

Qualitative:

- Higher quality management conversations
- Risk focused testing
- Visual focus on trends and outliers
- Adoption by broader IA dept
Effective Data Analytics Strategy

- Consistent
- Sustainable
- Efficient

Financial, Operational
Structured, Unstructured
Internal, External

Ownership
Accountability
Talent Development

Collaborative
Timely
Relevant

Maintainable
Intuitive
Adaptable

Vision
Acceptance
Mandate
Funding
Relationships

Change

Business Value

Data

Process

Infrastructure & Tools

Vision
Acceptance
Mandate
Funding
Relationships

Consistent
Sustainable
Efficient
**Level 0**
*Initial / Developing*
- Capability limited to very few individuals
- Inconsistent effectiveness
- Limited audit or business value

**Level 1**
*Consistent*
- Limited but growing capabilities
- Ad hoc activities resulting in unpredictable and inefficient performance
- Success based on individual

**Level 2**
*Relevant*
- Capabilities developed and adopted
- Capabilities used to drive audits
- Defined goals and standardized processes and tools

**Level 3**
*Integrated*
- Capabilities are well developed and practiced with appropriate governance
- Data sources are readily available
- Activities begin to become repeatable and CM metrics are developed
- Core analytics skillsets within 5-10% of department

**Level 4**
*Embedded*
- Scale is achieved for department specific teams
- Improvement methodologies are implemented
- Monitoring occurring for metrics and controls

**Level 5**
*Transformational*
- Analytics risk models being adopted by the business
- Analytics changing auditor behaviors
- New value propositions
- Alignment and cross-leverageable platform across lines of defense
- Game changing to audit delivery and value

*Industry current state*
Characteristics of analytics today

**Analytics;** discovery and communication of meaningful patterns in data

**Big data;** collection of large and complex data sets

- Visualization
- Trending & comparisons
- Dashboarding

**Data**
- Financial, Operational
- Structured, Unstructured, Internal, External

**Speed and portability;** available anytime, anywhere
Leading practices – a closer look
Case study 1 – ICD-10
Top ICD-10 preparation concerns facing providers

- Revenue Neutrality
- Medical necessity: dependence on professional providers for diagnosis
- Technology requirements and vendor readiness
- Overall ICD-10 implementation costs
- Managed care contracting and reimbursement implications
- “Initiative Overload”
- Clinical documentation requirements for specificity
- Productivity and staffing: short-term and long-term
- Cash flow implications
ICD-10 compliance risk roadmap

1. ICD-10 requirement announced
2. Awareness, planning, risk and impact analysis
3. System implementation, data conversion, testing, reporting redesign
4. Training and configuration management
5. HIPAA ICD10 conversion complete
6. Post-conversion KPI reporting

2009 - Fall 2014 deadline
ICD-10 “Know your number” demonstration

**KYN: Overview**

The Know Your Numbers (KYN) Claim Analytics tool helps an organization tell a story. Traditional testing and reporting approaches often consist of static queries and reports which take time to adjust and refresh. Visual analytics reduce the time spent creating analysis, enabling faster and more informed decision making. By organizing and exploring data through stunning interactive visualization, the tool offers the ability to better manage, examine, evaluate, and present information.

KYN allows drill down into the claims data in a meaningful way. By highlighting the highly impacted areas, users can narrow the focus on places that have significant influence to the organization. Dynamic filtering and drilldown capabilities allow focus by key data elements, bringing to light trends, outliers, and anomalies.

**Version**

KYN Claim Analytics - Provider
Version 2.1 (2/6/2014)

**Contact Information**

Matthew Higgins
Director
matthew.higgins@us.pwc.com

Dayi (Miriam) Shou
Manager
dayi.m.shou@us.pwc.com

Fran Grabowski
Senior Associate
fran.grabowski@us.pwc.com
Case study 2 – Two-midnight rule
**New regulatory pressure for providers: Two-midnight Rule**

- CMS revised guidance: inpatient admission = duration of minimum two midnights
- Long-stay observation cases increased from 3% of all observation cases in 2006 to 8% in 2011
- Goal is to reduce financial burden on Medicare beneficiaries
  - Observation stays result in greater out-of-pocket beneficiary expenses
- Probe and educate period
- October 1, 2013 through September 2014
- Providers can retrospectively rebill inappropriate and denied inpatient claims as outpatient
Recommended data analytics roadmap

Actionable Insight:
• Training of Clinicians
• Optimization of Admission and Rebilling Processes
• Documentation Review and Improvement
Two-midnight Rule demonstration

Inpatient Summary

Claims: 564
(7.35% of total IP Medicare claims)

Reimbursement: $55,087,458
(2.57% of total IP Medicare reimbursement)

Charges: $190,084,815
(1.47% of total IP Medicare charges)

IP Claims Breakdown by LoS

At-Risk Inpatient Claims

Inpatient claims with Length of Stay (LoS) less than 2 days. These claims would not comply with two-midnight rule inpatient admission guidelines and would be denied.

Outpatient Summary

Claims: 9,667
(24.34% of total OP Medicare claims)

Reimbursement: $119,879,897
(50.34% of total OP Medicare Reimbursement)

Charges: $707,434,299
(47.29% of total OP Medicare charges)

OP Claims Breakdown by LoS

At-Risk Outpatient Claims

Outpatient claims with Length of Stay (LoS) of 2 or more days. These claims would need to be billed as inpatient in order to secure reimbursement under new regulations.
Case study 3 – HIPAA/HITECH compliance
**HIPAA/HITECH issues are not going away...**

- Data breach costs have risen over the past 5 years (average cost ~$13.2M\(^1\)) and is now a key industry focus at hacker conferences.
- 452 large breaches and 50,000 small breaches over last 3 years. \(^2\)
- 58% of healthcare data breaches are due to business associates/3rd parties. \(^2\)
- Regulators (OCR, state attorneys, etc.) have stepped up auditing and enforcement activities
- Audits focus on privacy and security costs ~$100,000 per review and is up to 6 weeks in duration.
- Non-compliance has resulted in heavy fines and increased monitoring.

---

1: Ponemon Institute Study 2012  
2: HHS  
PwC  
February 2014
...and require continuous monitoring of compliance

Advanced Analytics Approach

- OCR Protocol
- NIST 800-66
- NIST 800-53
- HITECH
- HITRUST CSF Framework
- ISO27xxx
- PCT DSS1.2
- Red Flag
- MA Data Protection Act

- Deep healthcare IT industry experience
- Relationship with regulators
- Recognized services leader

- Practical & cost effective assessments
- Utilization of an integrated framework
- Recommendations for a sustainable compliance program
- Experienced professionals provide project acceleration
- Knowledge transfer to our clients
HIPAA/HITECH demonstration
Questions?
Integrated Risk Management: Doing the Right Risk Management Work Efficiently

Tammi Keating, Vice President, Compliance Strategy and Operations
Learning Objectives

• Discuss integrated risk management as a way to build capacity for addressing the rapidly evolving risk and regulatory landscape.

• Explain the creation of Kaiser Permanente’s plan to address this landscape – design, elements, partners, and target focus areas.

• Compare before and after scenarios, including the role of Internal Audit Services and other risk management units.
Why Integrated Risk Management?

Challenges Facing Kaiser Permanente

• Managing risk is increasingly complex.
• Competition is intensifying.
• Risk management capacity is critical.
Impact on Operations

Risk Management Units:

- Internal Audit Services Department
- National Compliance, Ethics & Integrity Office
- Technology Risk Office
- Sarbanes-Oxley Program Management Office

Unit #1 Wants…
Unit #2 Needs…
Unit #3 Asked for…
Unit #4 Expects…
Risk Management Complexities

- There are evolving federal, state, and local regulations that are impacting known risks and there are emerging vulnerabilities.
- There are multiple ways risk management units understand, communicate, assess, prioritize, and mitigate risk.
- There are business, operations, and information technology teams that have access to different information and tools.
Addressing the Challenges

Solution

• Develop and adopt a framework, models, and tools that increase risk management effectiveness and efficiency.

• Build and operationalize a coordinated approach to assess, prioritize, plan and conduct risk management.

Foundational Principles

• Create capacity.

• Coordinate, team, and rely.
Objectives

Prioritize effective work through:

- Common risk language and framework.
- Common understanding of process objectives, business risks, and risk ownership.
- Integration of complete prioritized compliance, Sarbanes-Oxley, and technology risk requirements into processes.
- Responsive management action plans.
Perform efficient risk management activities through:

- Coordinated coverage of risks.
- Common approaches to risk activities.
- Right level of assurance activity.
- Consideration of risks in business planning reviews and budgets.
- Common tools, including Kaiser Permanente Governance, Risk, & Compliance.
- Measurement and continuous improvement.
Governance Model

Executive Sponsors

- Integrated Risk Management Executive Steering Committee
- Integrated Risk Management Strategy Team
- Integrated Risk Management / Kaiser Permanente Governance, Risk, & Compliance Advisory Committee

2014 Integrated Risk Management Projects

- Commercial Membership Administration
- Pharmacy
- Clinical Technology
- Facility Administration
- Information Technology Operations
- Risk Adjustment Reporting
- Ongoing: Health Insurance Exchanges, Revenue Cycle, Hospitals, Medicare Membership Administration

Integrate
Adopt & Operationalize
Expand
Integrated risk management aligns people, process and technology.

- Understand Business Objectives
- Assess & Prioritize Risk
- Develop a Joint Plan

Enterprise Process Directory
Common Risk Framework
Assurance Activities

Kaiser Permanente Governance, Risk & Compliance Tools, Processes, and Reporting

Do the Right Risk Management Work Efficiently
The enterprise process directory provides a tiered way of seeing the work of the business.

- A comprehensive, end-to-end process view that helps to identify where risk occurs and helps to organize risk management activities.
Assess and Prioritize Risk

The common risk framework helps place risk management units and operations on the same page about the most important risks to manage.
Develop a Joint Plan

A joint plan clarifies the appropriate level of assurance activity across operations and risk management units.

- Describe the current state, key challenges, assessment of management preparedness
- Identify a business process area
- Business process owner
- Assign the risk #
- Describe the risk
- Enter the risk rating

1st Line of Defense
- Operations

2nd Line of Defense
- Risk management units

3rd Line of Defense
- Independent review

List current risk assurance activities by line of defense

Describe planned and/or recommended activities by line of defense
Each Kaiser Permanente Governance, Risk & Compliance module adds value on its own, but the greatest value is in integrating our risk management work into one platform of processes, tools, and reports.

- **RuleTrack**
  - Policy
  - Controls
  - Regulations

- **RiskTrack**
  - Risk grouping
  - Risk linkage to processes and work efforts
  - Joint plans

- **AuditTrack**
  - Documentation
  - Planning
  - Execution

- **CaseTrack**
  - Hotline
  - Cases
  - Issues
Integrated Risk Management Projects

Risk management units and their business partners have applied integrated risk management in the following key areas:

• Health Insurance Exchanges
• Provider and Member/Patient Billing
• Hospitals
• Medicare Membership Administration
Focus Areas for 2014

Integrated risk management is expanding to other areas this year:

- Commercial Membership Administration
- Pharmacy
- Clinical Technology
- Facility Administration
- Information Technology Operations
- Risk Adjustment Reporting
Benefits of Integrated Risk Management

Through greater coordination, teaming, and relying, the integrated risk management project characterizes risk in consistent terms, provides common tools, and reduces operational burden.
Benefits to Internal Audit Functions

Internal audit functions realize many benefits from integrated risk management.

• The enterprise process directory informs and/or becomes the audit universe.
• The risk rating matrix informs the timing and/or selection of audits and assessments.
• The first and second lines of defense inform the scope of audits, and the collection of such activities becomes a risk assurance map.
Realizing the benefits of integrated risk management requires leadership engagement and commitment.

- Risk management unit leaders are committed to using the foundational elements and measuring results.
- Operational leaders sponsored and championed integrated risk management projects in their areas.
- Stakeholders were educated on definitions and how to apply the foundational elements.
- Stakeholders participated throughout the project lifecycle.
A Look Ahead

Integrated risk management at Kaiser Permanente is becoming a way of life.

• The enterprise process directory will be an organizing principle for work we will identify within a business process and relate to risk.

• Project leaders are reporting risk mitigation status regularly to accountable executives.

• Use of joint plans is proliferating.

• Hospital leaders are sponsoring continued efforts within their hospital as well as spreading across hospitals within their regions.
APPENDIX
Risk Management Units are:

- Departments that support operations in identifying and acting on business requirements stemming from laws and internal policies.
- Departments that also assist operations with programs to meet those requirements including testing, or auditing as needed.
Consolidation/Competition in the Health Care & Insurance Industries

2014 NW AHIA Seminar

Teri Long, Executive Director, Internal Audit Services
# Agenda

<table>
<thead>
<tr>
<th>Learning Objectives</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Pace of Change</td>
<td>4</td>
</tr>
<tr>
<td>- Developments in the U.S. 1900 – 2000</td>
<td>6</td>
</tr>
<tr>
<td>Today’s Health Care and Insurance Environment</td>
<td>9</td>
</tr>
<tr>
<td>- The Affordable Care Act</td>
<td>10</td>
</tr>
<tr>
<td>Impact on Health Care and Insurance</td>
<td>12</td>
</tr>
<tr>
<td>- Affordability</td>
<td>13</td>
</tr>
<tr>
<td>- Rise of consumerism</td>
<td></td>
</tr>
<tr>
<td>- Changes in the way stakeholders conduct business</td>
<td></td>
</tr>
<tr>
<td>- Technology</td>
<td></td>
</tr>
<tr>
<td>Competition in Oregon and Washington</td>
<td>20</td>
</tr>
<tr>
<td>What’s Next</td>
<td>25</td>
</tr>
<tr>
<td>Questions</td>
<td>28</td>
</tr>
</tbody>
</table>
Learning Objectives

1. Obtain an overview of the existing and on-going changes and related impact.

2. Explain how some stakeholders are responding to the changes.

3. Discuss the impact of the changes to the future of health care and insurance.
The Pace of Change
The Pace of Change

Are we living in a time of unprecedented change for the health care and insurance industries?
<table>
<thead>
<tr>
<th>Decade</th>
<th>Developments</th>
</tr>
</thead>
</table>
| 1900s  | • AMA becomes a powerful force  
        • Surgery is now common for removing tumors, tonsils and appendectomies.  
        • The US lags behind European countries in finding value insuring against the cost of illness  
        • Railroads are the leading industry to develop extensive employee medical programs |
| 1910s  | • Hospitals are modern scientific institutions, antiseptics and cleanliness are valued, and medications are used for pain  
        • Progressive reformers argue for health insurance, support is growing  
        • Opposition from physicians and other interest groups, and our entry to the war in 1917 slow the reform efforts for health insurance |
| 1920s  | • Penicillin is discovered, but it will be 20 years before it’s used to combat infection and disease  
        • Dramatic Increases in the cost of medical care shift the focus from lost wages to illness  
        • Physician incomes are higher and the profession has more prestige  
        • Rural health care facilities are inadequate  
        • General Motors signs a contract with Metropolitan Life to insur 180,000 workers |
| 1930s  | • The Depression changes priorities placing greater emphasis on unemployment and “old age” benefits  
        • Social Security Act is passed without health insurance  
        • The Roosevelt Administration pushes for health insurance but the effort is derailed by conflicts over priorities  
        • Blue Cross begins offering private coverage for hospital care in several states, despite the advise of numerous insurance professionals |
## Developments in Health Care and Insurance in the U.S.

<table>
<thead>
<tr>
<th>Decade</th>
<th>Developments</th>
</tr>
</thead>
</table>
| **1940s** | - Penicillin comes into use  
- Prepaid group healthcare begins  
- Roosevelt asks Congress for “economic bill of rights,” including the right to adequate medical care  
- Truman offers national health program plan, proposing a single system that would include all Americans. The AMA denounces the plan and a House subcommittee calls it a Communist plot |
| **1950s** | - More medications are available to treat diseases such as infections, glaucoma and arthritis, and new vaccines are available to prevent childhood diseases like polio  
- The first successful organ transplant is performed  
- Early in the decade, national health care expenditures are 4.5% of the Gross National Product  
- Private insurance is available for those who can afford it and welfare services are in place for the poor. Federal responsibility for the sick poor is firmly established  
- Legislative proposals for hospital insurance are made but none are successful  
- The price of hospital care doubled from previous decades |
| **1960s** | - Physician specialists grow from 55% to 69% of the profession  
- Over 700 companies are selling health insurance  
- Concerns about doctor shortages and the need for more physicians results in federal measures to expand education programs  
- Medicare and Medicaid are signed into law  
- Individuals, especially the elderly are having difficulty affording insurance |
## Developments in Health Care and Insurance in the U.S.

<table>
<thead>
<tr>
<th>Decade</th>
<th>Developments</th>
</tr>
</thead>
</table>
| 1970s  | - World Health Organization declares smallpox eradicated  
- “War on Cancer” centralizes research at the National Institute of Health  
- Medical care includes a greater use of technology and medications  
- Nixon’s plan for national health insurance is rejected by liberals and labor unions  
- Healthcare costs are escalating rapidly, in part because of unexpectedly high Medicare expenditures, rapid inflation, expansion of hospital expenses and profits and changes in medical care. American medicine is now viewed as being in crisis |
| 1980s  | - Medicare shifts payment by diagnosis (DRG) instead of treatment. Private plans quickly follow suit  
- Corporations begin to integrate hospital systems, enter many healthcare-related businesses, and consolidate control. There is a shift towards privatization and corporatization of healthcare  
- Complaints by insurance companies that the traditional fee-for-service method of payment to doctors is being exploited. Capitation payments to doctors becomes more common |
| 1990s  | - June 1990, about 140,000 Americans have HIV/AIDS, with a 60% mortality rate  
- Health care costs rise at double the rate of inflation  
- Expansion of managed care helps to moderate increases in health care costs  
- Federal health care reform fails to pass in the Congress  
- There are 44 million Americans, 16% of the nation, with no health insurance |
| 2000s  | - Health care costs continue to rise  
- Medicare is viewed by some as unsustainable and must be rescued  
- Changing demographics in the workplace lead many to believe that the employer-based system of insurance can’t last  
- Consumer advertising for pharmaceuticals is on the rise |
Today’s Health Care and Insurance Environment

What are some of the changes impacting us today?

- Regulation - Increases in the complexity and amount of new regulation, Health Care Reform, Focus on fraud, waste and abuse
- Economics - Rising costs for health care, Decreasing reimbursement rates from Medicare, Decreases in profit margins, Increases in malpractice cases
- American Health - Aging population, Longevity and better end of life care, Increases in chronic conditions
- Delivery of Care – Shortages in certain medical specialties, Delivery of primary care, Patient access and network adequacy, Changes in Scope of Practice
- Consumer Expectations – Focus on health and prevention, Changes in how people want care delivered, Increasing consumer demands and expectations
- Technology - Improvements in medical care and related technology, Electronic Medical Records, Advances in pharmaceuticals
Health Care Reform – The Affordable Care Act

Key Goals of the ACA

- Everyone has Coverage
- Consumer have Choice
- Health Care Providers Compete Quality
- Care Delivery is Rewarded for Performance

Millions of people now have access to high quality affordable health care
2014 ACA Challenges

- Federal and state exchange website issues
- Delays in state exchange go-live dates
- Application deadline changes
- Payment deadlines shifted
- Premium shock
- Keep your plan
- Very high initial volume
- Delays in some aspects of the Act
Impact on the Health Care/Insurance Environment

Providers and insurers are seeing the impact of change in several key areas, including:

- Focus on affordability
- Rise of consumerism
- Changes in the way stakeholders conduct business
- Technology needs
Stakeholder Response to Change - Affordability

The focus on affordability is not new, but has become a way of doing business. Consumers, employers, and tax payers are all demanding more value for the dollars spent. Perception is that rising health care costs bear little relationship to improvements in access or quality.

Several studies have found that more than 50% of health care spending in the U.S. is wasted or actually harmful to the patient.

Some of the responses to the focus on affordability include:

- Cost containment efforts – Focus on costs not directly related to patient care, centralization, or a move to shared services.
- Mergers, acquisitions and affiliations – Benefits to affiliations may include group purchasing arrangements, shared services, and staff training/development.
- Insurance companies are getting more involved in delivering care, and some care providers are getting into the insurance business.
- Some insurers are exiting some markets and lines of business.
Stakeholder Response to Change - Consumerism

Consumers are demanding accountability from both health care providers and insurers. Public demands have grown for more transparency related to the costs for specific services and linkage to quality measures.

Some of the responses to the focus on consumerism include:

- New focus on individual health, wellness programs, and preventative care.
- Providers are leveraging new technology and existing behavioral tools to personalize care for patients. Examples include use of interactive web-sites, skype, remote monitoring of patient vitals, etc.
- Insurance product development is focused on products that are more standardized, easier to understand and driven by what people need.
- Efforts by providers to reduce avoidable hospital readmissions, improve transitions between health and long-term care settings, increase patient safety, and help patients make informed and evidence-based decisions about the treatments that are right for them.
- Some states now require pricing transparency and require providers to give estimates of what specific procedures will cost.
Stakeholder Response to Change – Approach

Stakeholders have changed the way they do business in response to the myriad of changes in the environment.

Stakeholder responses have included:
• Employer groups – To address rising health care costs have shifted the costs of health care to employees by offering insurance plans that are not as comprehensive as in the past or by increasing the individual employee contribution to monthly premiums. Employers may also offer wellness discounts to employees to encourage healthy habits. Some groups have moved to fully funded insurance products to help offset costs.
• Pharmaceutical industry – The industry has been highly criticized for having higher drug prices than in other nations and there has been pressure to contain spending on drugs. The focus on the linkage between benefits, risks, and the cost of products has increased. The industry has become more fragmented with more companies competing for the same profit pool. The increase in competition has resulted in specialization within organizations, lower funding levels for research and development, more focus on sales and marketing, and outsourcing of some activities.
Stakeholder Response to Change – Approach

Stakeholders have changed the way they do business in response to the myriad of changes in the environment.

Stakeholder responses have included:

• Small Medical Practices – Small or single physician practices are facing some significant challenges which have resulted in some consolidation. Medical practices are being challenged by reductions in reimbursement rates, increased financial risk, implementation of electronic medical records, rising operating costs, an uncertain medical legal climate, and new reporting requirements.

Small practices will be difficult to maintain because reimbursement rates are dropping and physicians will not be able to make up the differences in volume. Increases in volume compromise the physicians ability to conduct home or hospital visits, shortens the time spent with each patient, doesn’t allow for preventative care, and makes it very difficult to coordinate care for chronic illnesses.
Stakeholder Response to Change – Approach

Stakeholders have changed the way they do business in response to the myriad of changes in the environment.

Stakeholder responses have included:
- Medical Providers have:
  - Developed and implemented cross-specialty teams and networks of providers that are accountable for the full range of services used by their patients for care.
  - Affiliated with other providers and networks.
  - Begun to use e-Health (tools that can aggregate information from multiple sources to give an overall understanding of clinical modalities) and the Internet to get information on clinical practice guidelines for new technology.
  - Implemented electronic medical records.
  - Leveraged tools to conduct self assessments and risk management to help improve value and increase profitability.
Stakeholder Response to Change – Approach

Stakeholders have changed the way they do business in response to the myriad of changes in the environment.

Stakeholder responses have included:

- Insurers have:
  - Implemented significant changes in the way they administer insurance products to comply with the ACA.
  - Brought a wider variety of new products to market including those that feature higher deductibles and co-payments, and cost sharing.
  - Brought more private exchanges to the workplace, providing purchasers with new options.
  - Consolidated through mergers and acquisitions to gain market share or a competitive advantage.
Stakeholder Response to Change – Technology

Technology offers some opportunities to provide better health care at more affordable prices.

Some of the responses to the focus on technology include:
• Identification of new ways to deliver care.
• Implementation of electronic medical records.
• Focus on privacy and security concerns.
• Making health care information available to the consumer using the Internet.
• Facilitating care integration.
Competition in Oregon and Washington

The Herfindahl-Hirschman Index is by many as a measure of market competitiveness based on market share and number of firms in the market. The score is calculated by squaring the market share of each company, then adding the resulting numbers, with a maximum score of 10,000 indicating a monopoly-controlled market.

In 2012, the AMA argued that “anti-competitive conditions exist” in 83% of the 368 metropolitan areas studied, and that in half of them, one insurer had a commercial market share of 50% or more. The AMA contends that a lack of competition “threatens health care delivery across the country, leading to access to care being compromised and lower payment rates for physicians.”

America’s Health Insurance Plans, contend that provider consolidation has been the driving force behind rising healthcare costs, and in turn, rising insurance premiums.

Where are Oregon and Washington in the Herfindahl-Hirschman Index?
Competition in Oregon and Washington

Oregon
• Ranked first as the most competitive insurance market in the country, with an HHI score of 1272.
• Regence Blue Cross Blue Shield of Oregon (HMO and PPO plans) has the largest market share, with 20%, followed by Kaiser Permanente, with 19%.
• Oregon has annual per capita healthcare spending of $6,580, slightly less than the national average of $6,815.

Washington
• Ranked tenth with an HH score of 2578. Premera Blue Cross controls 42% of the state’s HMO and PPO market, followed by Regence Blue Shield of Washington, with 22%.
• In a few of Washington’s smaller markets, Group Health Cooperative and Kaiser Permanente have the largest market share.
• Washington has annual per capita healthcare costs of $6,782, slightly below the national average.

Note: The information quoted dates to 2012.
## Competition in Oregon and Washington

### Washington State Hospital Closures, Openings, Mergers, and Acquisitions

<table>
<thead>
<tr>
<th>Year</th>
<th>Closures</th>
<th>Openings</th>
<th>Mergers</th>
<th>Acquisitions</th>
<th>Affiliations</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>2009</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2010</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2011</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>2012</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>
Competition in Oregon and Washington

Oregon Market Facts:

- Oregon is the only state with more than one not-for-profit, consumer operated and oriented plan (Co-OP). These co-op plans were authorized and funded by the Patient Protection and Affordable Care Act to enhance competition and consumer value in the insurance market.
- Oregon’s exchange has attracted 11 insurers to the individual market and 9 for the small business market. The first set of rate filings show that some insurers are engaging in aggressive pricing to attract customers.
- Between 2006 and 2013, the fastest growing segments of the population are those 60 to 65 years of age (26%) and those 70 to 74 (45%).
- Oregon has 58 hospitals. Operating margins have remained stable over the 5-year period 2008 to 2012, ranging from a low of 3.58% in 2008 to a high of 4.63% in 2009. The overall rate for 2012 was 4.59%. Inpatient days have decreased by 5.24% in the period 2008 to 2012 because of decreases in patient admissions and reductions in length of stay. ED visits during the same period increased by 5.38% and outpatient visits increased by 11.59%.
- In 2008, Medicare and Medicaid accounted for 53% of patient revenue in Oregon hospitals. The rate rose to 61% in 2012. The rise in government payments is matched by a decrease in commercial insurance revenue from 39% in 2008 to 32% in 2012.
- In 2012, 6 of the 32 cost-based Medicaid hospitals had negative margins. 12% (4) had margins of negative 5% or worse.
Competition in Oregon and Washington

Washington Market Facts:
• Washington has 97 community general, 3 private specialized services, 2 state-owned psychiatric, 4 military, and 4 U.S. Veteran Affairs hospitals.
• Most hospitals have fewer than 100 beds. 16 have 100 to 199, 11 have 200 to 299, 6 have 300 to 399, and 4 have more than 400 beds.
• Hospital ownership is 42 public district, 44 private Not for Profit, 9 For Profit, and 2 are State/County.
• Private Not for Profit hospitals account for 65% of all community beds.
• The Seattle Times published a story on February 5, 2014 and said, “Washington has been able to do little to shed light on health-care costs, and the state last year earned an “F” for its cost-transparency laws, according to groups promoting health-care reform.”
• Washington imposed ACA-like reforms in 1993 and instituted guaranteed issue, community rating, premium price controls, and planned to phase in employer and individual mandates to purchase health insurance. Most of the reforms were repealed the next year.
• The State of Health Care in Washington State published in 2012 identified the following issues as the top areas of concern for the industry: Overregulation, out-of-control costs, prevention, and workforce needs. The report also noted significant shortages of health care professionals including registered nurses, radiation technicians, physician assistants and dentists.
What’s Next

What will the future look like for the health care and insurance industries?

The evolution of both industries will continue as they have in the past, but the current environment will help shape the course they take. Some possibilities include:

Regulatory Environment:
• Regulators will not approve affiliations that don’t create benefit for the public.
• States will drive change. Medicaid will have impact on local pricing structures which will impact individual states.

Pharmaceutical Industry:
• Limits on market entry, market access, price increases unless there is proof of incremental clinical benefits.
What’s Next

What will the future look like for the health care and insurance industries?

Care Delivery
• More primary care will be delivered in retailers like Walmart and Walgreens.
• Continued focus on delivery system reform that will result in more consolidation and may create more complex models than we have today.
• Fewer stand alone community hospitals.
• More nurses with advanced education and expertise will provide care. The traditional scope of practice will change.
• Health care will be personalized and will be provided in a variety of venues (mobile services, employer clinics, tele-medicine, Web, medical homes, micro-clinics).
• Payment for health care related services will be value based and focused on quality and outcomes.
• Precision tools will be leveraged to identify the right treatment for the patient.
• New devices and services will be used in patient care.
• The quality and effectiveness of patient care will be measured, monitored and reported to provide transparency to patients and purchasers. This same data will be used to identify treatment options with the best outcomes.
What’s Next

What will the future look like for the health care and insurance industries?

Technology:
• More investment in health care IT solutions.
• Use of technology will continue to increase.
Question or comments
Finding Value in Sarbanes-Oxley & Model Audit Rule Compliance

Karen Rasmussen, CPA, CHC
NW Region Director, Internal Controls Services
Learning Objectives

- Understand the landscape and evolution of Sarbanes–Oxley & Model Audit Rule Compliance
- Learn how the new COSO requirements affect SOX & Model Rule programs
- Highlight opportunities for efficiencies and effectiveness
- Identify ways to leverage value and align with enterprise risk management objectives
- Share best practices
Sarbanes-Oxley – History & Maturity Continuum
The Sarbanes- Oxley Act of 2002 required all public companies to comply with new regulations on Internal Controls over Financial Reporting.

To ensure compliance, many companies went overboard in their efforts to assess their internal control environment.

As programs became more mature and regulations/auditors more reasonable, SOX became embedded in the culture of many companies.

Instead of hiring outside resources to assess internal controls, many companies moved to internalize resources.

SOX Compliance increased awareness about the importance of knowing risks and maintaining a sound control environment.

Many non-profits and private companies not required to comply with SOX embraced it voluntarily.
The Entrée of Model Audit Rule

- The Annual Financial Reporting Model Regulation (known as the Model Audit Rule) was adopted by the National Association of Insurance Commissioners (NAIC) in 2010.

- The requirement to comply varies by state. All insurance plans in Oregon & Washington are required to comply if annual premium revenue exceeds $500 million.

- MAR requires annual certification by the plan’s CEO and CFO for Management’s Report of Internal Control over Financial Reporting.

- The audit must be filed by June 1 following the preceding December 31 year end.

- The objectives and guidelines of Section 404 of the Sarbanes-Oxley Act apply to MAR.

- External audit attestation is not required for Model Audit Rule unless the insurance plan is public.

- Subject to audits by the Insurance Commission.
Management’s Report of Internal Controls over Financial Reporting

Letter A
Completed by: Program Level Executives: CEO, CFO

State the following:

Management of (the Company) is responsible for establishing and maintaining adequate internal control over statutory financial reporting. The Company has established an internal control system designed to provide reasonable assurance regarding the fair presentation of statutory financial reporting. Management conducted an assessment of the effectiveness, as of December 31, 2013, of the Company’s internal control over statutory financial reporting, based on the framework established in the Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Based on our assessment under that framework, and to the best of management’s knowledge and belief, after diligent inquiry, management has concluded that the Company’s internal control over statutory financial reporting is effective to provide reasonable assurance regarding the reliability of financial reporting and the preparation of statutory financial statements as of December 31, 2013.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Projections of any evaluation of effectiveness to future periods are also subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Based on management review of internal controls, there were no unremediated material weaknesses as of December 31, 2013 identified as part of the Company’s internal control structure over the statutory financial statements for the year ended December 31, 2013.

___________________________  Date: ___________________
Chief Executive Officer

___________________________  Date: ___________________
Chief Financial Officer
New COSO Requirements & SOX/MAR Compliance
COSO Framework Changes

1992 COSO Cube

- Operations
- Financial Reporting
- Compliance
- Monitoring
- Information and Communication
- Control Activities
- Risk Assessment
- Control Environment

2013 COSO Cube

- Operations
- Reporting
- Compliance
- Entity
- Division
- Operating Unit
- Function
- Monitoring Activities
- Information & Communication
- Control Activities
- Risk Assessment
- Control Environment
New COSO Framework – What hasn’t changed

- SOX/MAR requires a framework be used
- Use a top-down, risk-based approach
- Basic definitions of internal controls
- Criteria to assess control effectiveness & deficiencies
- Evaluating all five components of the internal control system
- Applying judgment and assessing effectiveness of the internal controls systems
New COSO Framework –
What has changed

- Codifies 17 principles supporting the 5 required components of internal control
- Clarifies role of objective-setting coming first
- Reflects the increased relevance of technology
- Adds enhanced discussion of governance concepts
Expands the reporting category of objectives to include non-financial and internal objectives

Enhances consideration of anti-fraud expectations in its own principle

Increases focus on non-financial components to broaden use

Must convert documentation to the principles-based approach of the new COSO standards by 12/15/14.
Opportunities to increase Effectiveness & Efficiency
Work to integrate and leverage all audit efforts (external, internal & SOX)

Establish common risk framework

Implement self assessment and monitoring processes

Key controls and testing
  - Eliminate redundant controls
  - Make sure you have the right key controls
  - Don’t test too often or too much
Effectiveness & Efficiency Opportunities

- Create sustainability
- Improve processes upstream to eliminate sources of defects
- Focus on preventive controls
- Create a strong entity-level control foundation
- Strengthen financial reporting controls – high return area for efforts
Efficiency + Effectiveness = Excellence!
Great organizations learn from their mistakes – always opportunities for improvement.

Be vigilant about quality control execution and oversight.

Change is constant and we must be aware of potential control implications.

**Strength, maturity and learnings are key!!**
Strength @ Kaiser

- Fewer deficiencies & material weaknesses
- Understanding increased – compliance process locked and loaded
- Staff experienced
- Accountability and knowledge across the organization ingrained
Maturity @ Kaiser

- Checks and balances are working
- Self-assessment and Self-reporting are becoming part of our DNA
- Costs decreasing as we internalize and become more efficient
- IT and Access performance improved and sustained
Learnings @ Kaiser

- Keep your eye on the ball – complacency is not our friend
- Any environment is dynamic – stay on top of changes & their impact on processes, risks and controls
- Remain inquisitive – ask a question if something doesn’t look right
- Small things can make a big difference – and become significant
Leverage Value and Align with Enterprise Risk Management Practices
Establish a common risk framework and definitions across your organization

Build more value added internal audit plans from SOX/MAR learnings

Use the risk assessment and process maps as a tool for continuous improvement and enterprise risk management.

Communicate improved results through SOX maturity to demonstrate value

Coordinate with auditors to avoid duplication
Share Best Practices
Share Best Practices

- Share program improvements & best practices
- Do you use self-assessment?
- What has made the most difference in your program?
- How do you use technology?
- What is your biggest challenge?
- If your work has been audited by the Insurance Commission or SEC, share your experience
What do health systems need to do?

- Dramatically improve efficiency and reduce costs while improving quality and service
- Deploy technology that will enhance consumer engagement in health
- Enable industry-wide transformation
- Secure health care provider capacity
- Change models of care
What can we do?

- Position ourselves as trusted advisors to leadership
- Help improve efficiency and reduce costs while improving quality and service
- Deploy technology that will enhance efficiencies & the control environment
- Provide support for industry-wide transformation
Comments or Questions?
Applying the COSO Framework to Healthcare
A presentation to AHIA’s Regional Conference – Seattle, WA
March 14, 2014

Presenters:
Michael MacBryde, Partner
Frank Martens, Director

---

**Agenda**

Introductions
COSO – What’s Changing? What’s Not?
Healthcare Mapping Example
Recommended Actions
Questions
Why update 1992 Framework?

Changes in the business environment
Changes inside the business
Lack of clarity
Lack of understanding

Do stakeholders understand requirements of effective internal control?

Only 50% thought it was generally easy to interpret
- Difficult to interpret
- Somewhat difficult to interpret
- Moderately easy to interpret

Source - COSO’s survey of users and stakeholders, worldwide – January to September 2011
**2013 Framework preserves core strengths embedded in 1992 Framework**

**Updated COSO Cube**

What is NOT fundamentally changing...

- Core definition of internal control
- Three categories of objectives and five components of internal control
- Each of the five components of internal control are required for effective internal control
- Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness

**2013 Framework increases ease of use**


- Consider changes in business & operating environments
- Articulate principles to facilitate effective internal control
- Expand operations and reporting objectives

**Refresh Objectives**

**Updates**

- Update Context
- Clarify Requirements
- Broaden Application

2013 Framework articulates principles and points of focus

2013 COSO Cube

Legend
- Components and Principles are requirements for an effective system of internal control
- Points of Focus and Controls are subject to management judgment

2013 Framework articulates seventeen principles for effective internal control

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>1. Demonstrates commitment to integrity and ethical values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Exercises oversight responsibility</td>
</tr>
<tr>
<td></td>
<td>3. Establishes structure, authority and responsibility</td>
</tr>
<tr>
<td></td>
<td>4. Demonstrates commitment to competence</td>
</tr>
<tr>
<td></td>
<td>5. Enforces accountability</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>6. Specifies suitable objectives</td>
</tr>
<tr>
<td></td>
<td>7. Identifies and analyzes risk</td>
</tr>
<tr>
<td></td>
<td>8. Assesses fraud risk</td>
</tr>
<tr>
<td></td>
<td>9. Identifies and analyzes significant change</td>
</tr>
<tr>
<td>Control Activities</td>
<td>10. Selects and develops control activities</td>
</tr>
<tr>
<td></td>
<td>11. Selects and develops general controls over technology</td>
</tr>
<tr>
<td></td>
<td>12. Deploys through policies and procedures</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>13. Uses relevant information</td>
</tr>
<tr>
<td></td>
<td>14. Communicates internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicates externally</td>
</tr>
<tr>
<td>Monitoring Activities</td>
<td>16. Conducts ongoing and/or separate evaluations</td>
</tr>
<tr>
<td></td>
<td>17. Evaluates and communicates deficiencies</td>
</tr>
</tbody>
</table>
2013 Framework clarifies requirements for an effective system of internal control

An effective system of internal control requires:
- Each of the five components of internal control and relevant principles is present and functioning
- The five components are operating together in an integrated manner

Components are present and functioning if each relevant principle is determined to be present and functioning (e.g., no material weakness exists)

Relevant principles are present and functioning if persuasive evidence exists that controls are selected, developed and deployed to effect them

Components operate together when:
- Components are present and functioning
- Internal control deficiencies aggregated across components do not result in the determination that one or more material weakness exist

COSO principles – A deeper dive
### 2013 Framework describes points of focus for each principle, for example...

<table>
<thead>
<tr>
<th>Component</th>
<th>Control Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principles</strong></td>
<td></td>
</tr>
<tr>
<td>Principle 1</td>
<td>Demonstrates Commitment to Integrity...</td>
</tr>
<tr>
<td>Principle 2</td>
<td>Exercises Oversight Responsibility</td>
</tr>
<tr>
<td>Principle 3</td>
<td>Establishes Structures Authority,...</td>
</tr>
<tr>
<td>Principle 4</td>
<td>Demonstrates Commitment to Competence</td>
</tr>
</tbody>
</table>

**Points of Focus**
- Sets the tone at the top
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely manner
- Establishes oversight responsibility
- Applies relevant expertise
- Operate independently
- Provides oversight for the system of internal control
- Considers all structures of the entity
- Establishes reporting lines
- Defines, assigns and limits authorities and responsibilities
- Establishes policies and practices
- Evaluates competence and addresses shortcomings
- Attracts, develops, and retains individuals
- Plans and prepares for succession

### Points of focus describe important characteristics of the principles, for example...

<table>
<thead>
<tr>
<th>Component</th>
<th>Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principles</strong></td>
<td></td>
</tr>
<tr>
<td>Principle 6</td>
<td>Specifies suitable objectives</td>
</tr>
<tr>
<td>Principle 7</td>
<td>Identifies and analyzes risk</td>
</tr>
<tr>
<td>Principle 8</td>
<td>Assesses fraud risk</td>
</tr>
<tr>
<td>Principle 9</td>
<td>Identifies and analyzes significant change</td>
</tr>
</tbody>
</table>

**Points of Focus**
- Complies with applicable accounting standards
- Considers materiality
- Reflects entity activities
- Includes entity, division, operating unit, and functions
- Analyzes internal / external factors
- Involves appropriate level of management
- Estimates significance of risks identified
- Determines how to respond to risks
- Considers various types of fraud
- Assesses incentive and pressures
- Assesses opportunities
- Assesses attitudes and rationalizations
- Assesses changes in external environment
- Assesses changes in business model
- Assesses changes in leadership
### COSO Mapping – Principle 14

<table>
<thead>
<tr>
<th>Principle</th>
<th>Points of Focus</th>
<th>Controls to support the Principle (Note 1)</th>
</tr>
</thead>
</table>
| **Principle 14: Communicates Internally** | - Communicates Internal Control Information — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.  
- Communicates with the Board of Directors — Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity’s objectives.  
- Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.  
- Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.  
[Other Management identified points of focus, if any] | Describe controls that support the Principle |

#### INFORMATION AND COMMUNICATION

- CMS Medicare Managed Care Manual  
  Element IV – Effective Lines of Communication  
- HIPAA  
  Privacy Rule

---

Principle 15 - Are the controls developed across the entity to demonstrate the Principle is present?

**Yes or No**  
If No, describe the gap and action plan (Note 2)
## COSO Mapping – Principle 14

<table>
<thead>
<tr>
<th>Principle</th>
<th>Points of Focus</th>
<th>Controls to support the Principle (Note 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INFORMATION AND COMMUNICATION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 14: Communicates Internally — The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicates Internal Control Information — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicates with the Board of Directors — Communication exists between management and the board of directors so that both have information needed to fulfill their roles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provides Separate Communication Channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Other Management identified points of focus, if any]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Consider documenting rationale for additional relevant PoF identified by management or for any PoF set out in the Framework that were not deemed relevant.

**In the gap and action plan (Note 2)**

**Principle 15 - Are the controls developed across the entity to demonstrate the Principle is present?**

**CMS Medicare Managed Care Manual**

**Element IV – Effective Lines of Communication**

- Written Standards of Conduct and/or policies and procedures must require all employees, members of the governing body, and FDRs to report compliance concerns and suspected or actual violations related to the Medicare program to the sponsor.

**HIPAA**

- Privacy Rule

  - Notice of Privacy Practices

- Standard agenda templates for audit committee meetings.
- CMS audit results are disseminated to the BoD
- Reporting and tracking of issues with non compliance
- Publicized processes for reporting non compliance

**HIPAA**

- Privacy Rule - Notice of Privacy Practices

  - Posted and available for patients (e.g. include effective dates, use and disclosure etc.)
COSO Mapping – Principle 14

<table>
<thead>
<tr>
<th>Principle 14: Communicates Internally — The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Internal Control Information — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.</td>
</tr>
<tr>
<td>Communicates with the Board of Directors — Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity’s objectives.</td>
</tr>
<tr>
<td>Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.</td>
</tr>
<tr>
<td>Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.</td>
</tr>
<tr>
<td>Other Management identified points of focus, if any</td>
</tr>
</tbody>
</table>

Describe controls that support the Principle

Principle 15 - Are the controls developed across the entity to demonstrate the Principle is present?

Table: Controls to support the Principle

<table>
<thead>
<tr>
<th>Principle Points of Focus</th>
<th>Controls to support the Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMATION AND COMMUNICATION</td>
<td></td>
</tr>
<tr>
<td>CMS Medicare Managed Care Manual</td>
<td></td>
</tr>
<tr>
<td>HIPAA Privacy Rule - Notice of Privacy Practices</td>
<td></td>
</tr>
</tbody>
</table>

| 1. Do these controls exist? |
| 2. Are you comfortable with its level of mitigation? |

Recommended Actions

- **Step #1** – Read COSO’s updated IC Framework (and illustrative documents) and communicate and educate the Board of Directors, C-Suite, operating unit and functional managers
- **Step #2** – Determine application to your specific compliance efforts
- **Step #3** – Conduct a preliminary assessment of what is covered and missing by mapping the principles to existing controls
- **Step #4** – Complete a comprehensive assessment and take action to implement necessary changes in controls and related documentation
- **Step #5** – Develop and execute plan timely ensuring necessary changes are implemented in time to achieve your objective(s)
- **Ongoing** - Consider opportunities to (i) apply internal control to additional operational, reporting and compliance objectives, (ii) optimize the design of controls to mitigate risk to acceptable level, and (ii) converge processes and controls within the five components that support multiple, overlapping objectives
Thank you...