HIPAA Summit West II
A Case Study: Implementing HIPAA at Kaiser Permanente

Mary Henderson, MPH, MBA
National HIPAA Program Director

John DesMarteau, MD FACA
Kaiser Permanente Mid-Atlantic HIPAA Project
Kaiser Permanente: A Snapshot

- Kaiser Permanente has:
  - Regions in 9 states and Washington, DC
  - 8.3 million members
  - 29 Hospitals
  - 423 Medical Offices
  - 11,345 physicians
  - 122,473 employees
  - More than 3,000 applications that contain HIPAA relevant information
The KP HIPAA Approach

- **National sponsorship**: Health Plan, Hospitals, Medical Groups and IT
- **Regional sponsorship**: Regional Health Plan Presidents, Medical Directors
- **Multi-disciplinary core advisory group**: Legal and Government Relations, Internal Audit, Public Affairs, IT Security, Health care operations, Labor Relations, Others as needed
- **National and Regional Teams**: National directors for IT, Business, Health Care Operations; Regional leads for IT, Business, Health Care Operations; KP-IT Functional Leads
- **Legal expertise**: Internal and external
- **Advocacy**: To achieve favorable interpretations
HIPAA EDI
Kaiser Permanente’s EDI Approach

- We are developing a “KP Clearinghouse” - a set of shared utilities - to translate specified information into HIPAA compliant format and modifying applications as needed.

- We chose the KPC approach because it is:
  - significantly less expensive than modifying all applications affected,
  - achieves economies of scale in the short and long run,
  - allows for evolution of legacy systems and business processes, and
  - facilitates maintenance (e.g., the addition of new transactions and codes, changes to layouts)

- We believe that the KPC has a long term value even as applications are replaced.
Clearinghouse Utility for Achieving HIPAA Compliance:

**KP Clearinghouse**

- Authenticates that the trading partners are who they say they are and they are authorized for transactions.
- Validates correct format, edit for content and syntax.
- Stores and validates reference data (examples are ICD-9, CPT4, Provider id’s, Implementation Guides.)
- Warehouse stores original transactions and transformed inbound and outbound transactions.
- Message formatter translates and reformats data
- Delivers transactions to legacy systems in most efficient manner.
- Manages data, format and transmission errors and trading partner, application and business processing rules.

**External Trading Partners**

- Health plans
- Providers
- Etc.

Send transactions via:
- Web
- External clearinghouses
- Direct interfaces

**Transactions**

(EDI, Disk, Tape, Web)

**KP Applications**

- Claims
- Membership
- Billing
- Etc.

**Indirect impacts**

Clinical Systems, Provider Mgmt., others
KP Clearinghouse:

- Supports Compliant/Non-Compliant Applications
- Enables interface between applications

Non-Compliant Applications

KP Clearinghouse

- Authentication.
- Edits.
- Data Management.
- Warehouse.
- Transformation.
- Delivery.
- Administration/Error Management.

Fully Compliant Applications

Interface Logic

Clinical Systems, Provider Mgmt., others

Represents an example of re-use of KP Clearinghouse utilities
So What Are the Challenges of the EDI Extension for KP

- Applying for the extension
- Reminding executive leadership that HIPAA doesn’t go away
- Revising 2002 and 2003 budget plans
- Restructuring the work without losing momentum
- Redeploying staff
- Working with trading partners who want to send compliant transactions in Oct. 2002
And Benefits from the Extension

- Spreading EDI over an extra year = need for less $$ in 2002 budget
- More time to test our work
- Time to reevaluate our approach and identify opportunities the delay may provide (90-day study)
- With privacy deadline barreling our way, able to redeploy some staff to privacy work
HIPAA Compliance Cost Comparison

<table>
<thead>
<tr>
<th>Year</th>
<th>Cost/Member</th>
<th>Total Cost in $M</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1</td>
<td>$7</td>
</tr>
<tr>
<td>2</td>
<td>$1</td>
<td>$10</td>
</tr>
<tr>
<td>3</td>
<td>$2</td>
<td>$15</td>
</tr>
<tr>
<td>4</td>
<td>$2</td>
<td>$7</td>
</tr>
<tr>
<td>5</td>
<td>$5</td>
<td>$10</td>
</tr>
<tr>
<td>6</td>
<td>$5</td>
<td>$13</td>
</tr>
<tr>
<td>7</td>
<td>$6</td>
<td>$50</td>
</tr>
<tr>
<td>8</td>
<td>$7</td>
<td>$45</td>
</tr>
<tr>
<td>9</td>
<td>$8</td>
<td>$42</td>
</tr>
<tr>
<td>10</td>
<td>$10</td>
<td>$20</td>
</tr>
<tr>
<td>11</td>
<td>$11</td>
<td>$45</td>
</tr>
<tr>
<td>12</td>
<td>$12</td>
<td>$35</td>
</tr>
<tr>
<td>13</td>
<td>$13</td>
<td>$40</td>
</tr>
<tr>
<td>14</td>
<td>$29</td>
<td>$35</td>
</tr>
</tbody>
</table>
Value of Increased EDI Capabilities

- Potential cost reductions such as:
  - ✔ Reduced phone inquiries
  - ✔ Reduced processing of paper checks
  - ✔ Reduced manual keying of data and data verification
  - ✔ Reduction of other manual processes such as scanning, fax responses, mailroom handling, etc.

- Sets the technical environment which allows for broader benefits. Full benefit realization would require significant changes in business processes (e.g., linking contracts, referrals and claims to permit auto-adjudication of claims)
Where is KP Now on EDI?

- Almost finished with 90-day study
- Proceeding on the KPC - alpha build in May 2002; full build Sept. 2002
- Modifying some applications in 2002; delaying some to 2003
- Considering how to approach EDI extension request - one KP request or several (KP Regions)
- Planning for April 2003 test date
- Continuing to identify benefits
HIPAA Privacy and Security
Challenges of Privacy Regulations

- Getting consent for treatment, payment and healthcare operations from all 8.3 million current members and patients
- Tracking consent, effective date, revocation
- Effectively and efficiently tracking disclosures
- Minimum necessary - how to use subset of paper or electronic chart
- Finding privacy officers
- Training staff prior to April 14, 2003

National and regional multidisciplinary KP Work Groups developing approaches
Challenges of Security Regulations

- Estimating/securing resources prior to final regs (probably most costly area of HIPAA)
- Understanding current situation (i.e., multiple regions and varying policies)
- Assessing risk and making policy decisions
- Finding security officers
- Adding an audit trail
- Dealing with overlapping elements between HIPAA Privacy (deadline April 2003) and Security (no deadline yet) e.g., training and business associate agreements
Privacy and Security: Perspective from the Frontline
Privacy and Security A Matter of...

- People
- Systems
- Technology
- Regulations
- Evolution

... And the Clock is Ticking
Privacy - For almost 5000 years

The patient tells another person:
- no documentation
- no privacy

“My left foot is numb and I have this incredible thirst. I’ve been kind of depressed lately.”

Nevertheless...
Privacy Fears

Steven—you are to begin therapy, as your blood test indicates 25% risk of teenage depression based on your genetic profile.

Father just got a telemarketing call from a home blood sugar monitoring service. But I don’t think he ever followed up on that office visit to the doctor!
And now, Mr. Jones’ scores from our health insurance judges...
Elements of Privacy Management

- Admission
- Authentication
- Access controls
- Administration
- Accountability
- Audits (before not after)
- Apprehension

For example…
Audits

- Someone has to write the rules\(^1\)
- Someone has to run the audits\(^2\)
- Someone has to be accountable

\(^1\)the rules have to be meaningful
\(^2\)the audits have to be meaningful
Privacy Officer Needed

- Necessary for the practice to be HIPAA compliant
- Necessary as a good business practice
- Making certain that the practice remains HIPAA compliant
  - ✓ Risk assessment
  - ✓ Gathering consents
  - ✓ Proper disclosures
  - ✓ Proper security
- Interface with patients
- Can be the “office manager”
- HIPAA expertise abounds (print, internet, consultants)
Keeping Health Information Secure

- Information is a health industry asset
- Information can be critical and/or sensitive
- Loss of confidentiality, integrity, or availability can have financial implications
- Loss of Integrity or availability *can cost a life!*
How is Security Threatened?

- What is a threat?
  - Possibility, or likelihood, of an attack against your organization
  - Potential for damage to your organization

- Accidental vs. intentional threats

- Threat forms
  - Human Errors
  - Malicious Acts
  - System Failures
  - Natural Disasters
<table>
<thead>
<tr>
<th>Item</th>
<th>Paper</th>
<th>Digital</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of policies and procedures</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Incorrect policy implementation</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>No intrusion detection</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Software bugs/design flaws</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>No firewall or poor implementation</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>No virus protection/poor implementation</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
Information Security Hierarchy: Best Practices Approach

- **Administrative**
  - Policy & Procedure
  - Personnel Security

- **Technical**
  - Network Connectivity
  - Viruses
  - Authentication
  - Audit
  - Backup and Recovery
  - Encryption
  - Physical Security

Step 1: Information Security Policy and Standards
Step 2: Information Security Architecture and Processes
Step 3: Information Security Awareness and Training
Step 4: Information Security Technologies and Products
Step 5: Auditing, Monitoring and Investigating
Step 6: Validation
Top Ten ‘Reasons’ to Defer Security

“Compliance is in the eye of the beholder”

1. “We trust our staff and our physicians”
2. “Security expense cannot be cost-justified”
3. “Our software vendor is responsible for EDI security”
4. “We have a firewall!”
5. “Our IT Provider is handling our network security”
6. “Our information assets are not at risk”
7. “We can’t afford another Y2K of IT expenditures!”
8. “We have a solid consent and authorization process”
9. “If someone really wants to crack our system……”
10. “The HIPAA Security Standard is not finalized!”
Recommended Security Response... NOW!

- Assessment Gap
- Establish Roadmap
- Implement appropriate administrative measures
  - Security policy
  - Information Classification
  - Security Awareness Training
- Undertake appropriate technical remediation
  - Configurations
  - Physical security

“Little pieces at a time”
Risk Management Challenge

Risk Triggering Event
- e.g., curious employee

Interventions or Tools
- "Flaw" in intervention or tool e.g., inadequate training

Bad Outcome
- (e.g. misuse of confidential info.)
  - Harm to individual
  - Sanctions
  - Fines
  - Criminal charges
  - Reputation

VARIABLES
- Which events
- Number slices
- Size of holes
- Timing
- Risk/$$

Diagram modified from James Reason’s “Accident Causation Model”
HIPAA Risk Management Approach

- Provides a baseline of data and information for future initiatives
- Allows us to build a rational, replicable model for risk management
- Acknowledges that total elimination of risk may not be possible
Contributing to the Success of HIPAA at Kaiser Permanente

- HIPAA is in alignment with Kaiser Permanente values
- Active national and regional sponsorship
- Dedicated national and regional HIPAA Teams
- Multi-disciplinary approach
- KP is a “learning” organization
- Our 55-year history of providing high quality health care service to diverse populations
Questions?

- mary.henderson@kp.org
  (510) 271-5651

- john.desmarteau@kp.org
  (301) 625-4416