A Case Study: Implementing HIPAA at Kaiser Permanente

Mary Henderson
HIPAA Program Director
Kaiser Permanente
Kaiser Permanente: A Snapshot

- Kaiser Permanente has:
  - regions in 9 states and Washington, DC
  - 8.2 million members (6.1 million in Calif.)
  - 35 Hospitals/ Medical Centers
  - 423 Medical Offices
  - 11,345 physicians
  - 90,000 non-physician employees
  - More than 4,000 applications that may contain HIPAA relevant information
We need to move all of this forward into HIPAA compliance...
Leveraging HIPAA for Organizational Transformation

- HIPAA forces the industry to become electronically capable
- External imperative = internal leverage
- Momentum to transform an entire organization
- Identify the collateral benefits early
Strategic Questions for the KP HIPAA Transformation

- Who should be accountable for the transformation?
- How do we get this done on time?
- How do we handle the money?
- How do we get maximum value for resources invested?

We’re in a moving car. How do we change the tire?
KP’s Strategies for Making HIPAA Happen

- High level sponsorship
- Multi-disciplinary core advisory group
- Distribute ownership/ engage those affected
- Integrated national and regional teams
- One national budget with funding rules
- Defined responsibilities
- An orientation to the benefits
How Far Has This Taken Us?

- Assessed regulations and set strategy/timeline
- Secured sponsorship and funding
- Built systems, teams, funding model, awareness
- Conducted high-level analyses resulting in e.g., applications inventory, security matrix
- Developed an EDI approach
- Developed a multi-year funding forecast
- Developed intranet site for internal communication and document access
Where Are We Going Now?

- Implementing EDI solution
- Completing a baseline assessment: surveying our current practices and identifying gaps in security and privacy
- Designing a risk assessment process for determining security and privacy remediation approaches
- Establishing an internal review process
Challenges for KP:
EDI/Code Set Regulations

- Recognizing the benefits and planning broadly enough to achieve them
- Integrating with ongoing efforts (e.g., e-business)
- No easy answers for complex organizations with legacy systems:
  - replace legacy systems with HIPAA compliant
  - modify legacy systems to become HIPAA complaint
  - modify incoming and outgoing transactions to be compliant in a separate “application”
- Explaining the approach to sponsors and others in sound bites
- Identifier requirements still in draft form
Challenges for KP: Privacy Regulations

- Assessing risk and making policy decisions
- Getting consent as an “organized health care arrangement”
  - what about former members?
  - members who haven’t come in for care?
- Tracking consent, effective date, revocation
- Effectively and efficiently tracking disclosures
- Minimum necessary - how to use subset of paper or electronic chart
Challenges for KP: Security Regulations

- Estimating/ securing resources prior to final regs (probably most costly area of HIPAA)
- Understanding our current situation (i.e., multiple regions and varying policies)
- Developing a baseline assessment of what we already do and don’t do
- Assessing risk and making policy decisions
- Finding security officers
- Adding an audit trail
- We have:
  - a security matrix which provides a general framework
  - confidentiality measures in place
From Strategy to Tactics: A Risk Management Approach

- Conducting security and privacy baseline assessments (regional, functional)
- Establishing a Privacy Work Group
- Developing a Review Process
- Involving the people who are affected
Security and Privacy Regulations: Risk Management Challenge

Risk

Triggering Event
e.g., curious employee

“Flaw” in intervention or tool
e.g., inadequate training

Interventions or Tools

Policies and Training

Bad outcome
(e.g. misuse of confidential info.)

- Fines
- Sanctions
- Criminal charges
- Reputation
- Harm to individual

VARIABLES

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

Diagram modified from James Reason’s “Accident Causation Model”
Transformational Value of Our 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
KP HIPAA: Big Picture Benefits

- Builds evolutionary capacity
- A step toward common systems and processes
- Develops people who know how to do transformation
- Success disarms some of the fear around future transformation
What Supports Transformation at Kaiser Permanente?

- KP is a “learning” organization
- We have a national IT structure
- HIPAA is in alignment with Kaiser Permanente values
- We’re proud of our 55-year history of providing high quality health care service to diverse populations
Questions?

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