Health
Insurance
Portability and
Accountability
Act of 1996

Case Study in HIPAA Compliance for Health Plans

October 16, 2000

Mary Henderson
HIPAA Program Director
Kaiser Permanente

Presentation Summary

- How a complex organization prepares for HIPAA compliance
- Assessing HIPAA's potential impact
- Challenges for Health Plans re: Security & Privacy
- Challenges for Providers re: Security & Privacy
- Evaluating potential EDI solutions
- Communication and Change Management: Keys to success
- Lessons Learned So Far

Kaiser Permanente's Unique Situation

- 8 million members in 11 states and Washington, DC
- Includes health plans and providers
- Prepayment group practice
- Not claims-based
- Multiple Regions, multiple Medical Groups
- Variation among Regions/Medical Groups in systems and procedures
- Commonly owned systems and data

Comparing HIPPA with Y2K

Similar:

- Affects the entire organization
- Externally imposed
- Fixed compliance date(s)
- Risk to organization image
- Some collateral benefits
- Significant investment

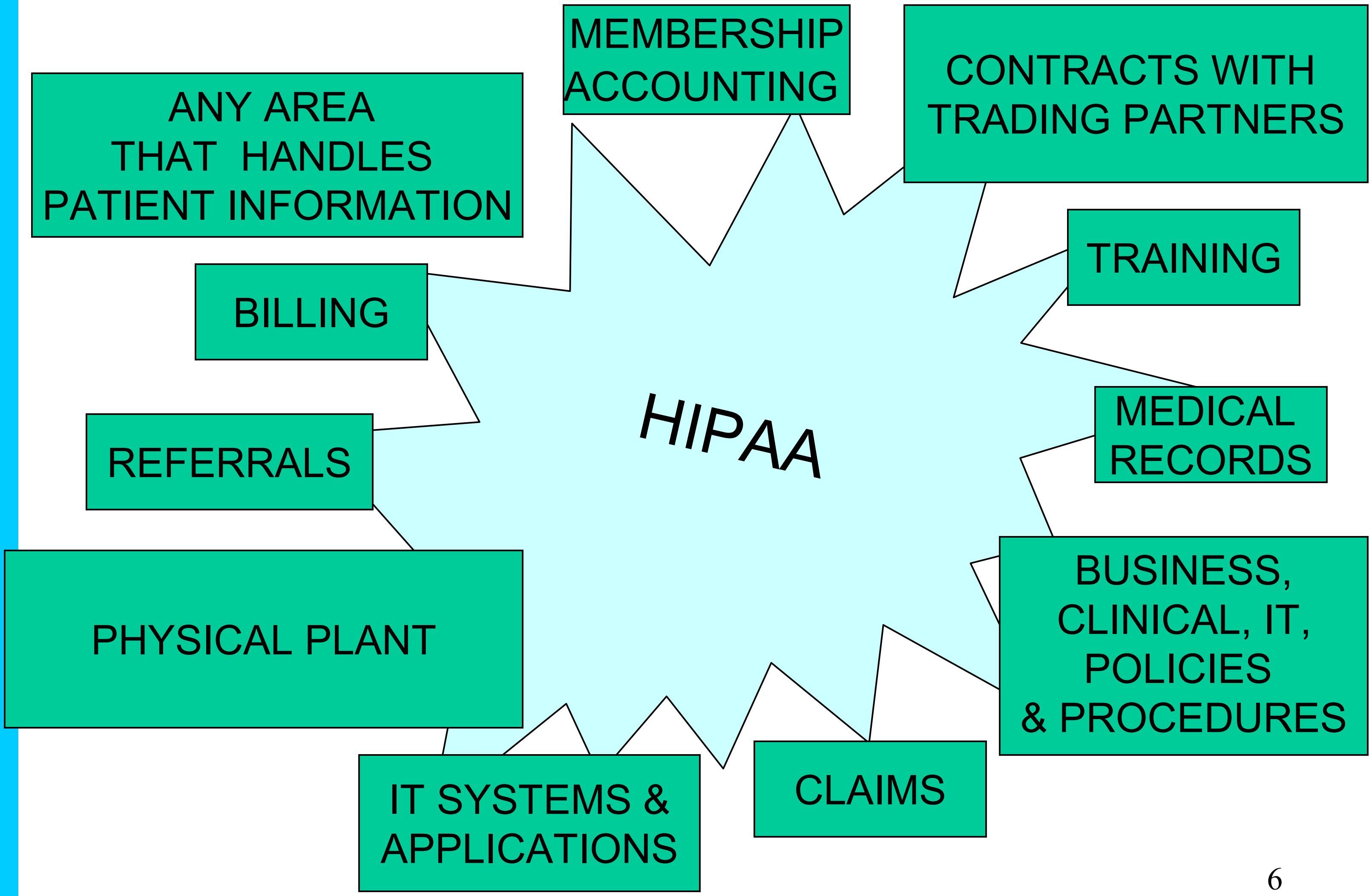
Different:

- More complex
- Greater business impact
- Multiple compliance dates
- Implementation can be phased prior to deadlines; no big bang
- More opportunities for significant collateral benefits
- Fines and sanctions

HIPAA Opportunities

- Sets stage for e-business
- Provides impetus for systems and process consolidation
- External deadlines impose structure
- Sets a baseline for security and privacy safeguards
- Promotes good business practices

HIPAA Impact at Kaiser Permanente



HIPAA

ANY AREA
THAT HANDLES
PATIENT INFORMATION

MEMBERSHIP
ACCOUNTING

CONTRACTS WITH
TRADING PARTNERS

TRAINING

BILLING

REFERRALS

MEDICAL
RECORDS

PHYSICAL PLANT

BUSINESS,
CLINICAL, IT,
POLICIES
& PROCEDURES

IT SYSTEMS &
APPLICATIONS

CLAIMS

Meeting the HIPAA Bar

- HIPAA compliance is mandatory
- Each Region is accountable for applications, policies, systems, practices
- Regions are in various stages of readiness
- Some national solutions; some local adaptations
- More than one path to compliance

Kaiser Permanente HIPAA Program

- National sponsorship from Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and the Permanente Medical Groups
- National Program Sponsors: President, KFHP, Inc., Executive Director of The Permanente Federation
- Regional Sponsors: Regional Health Plan Presidents, Medical Directors
- Multi-disciplinary core advisory group
  - Legal
  - Internal Audit
  - Public Affairs
  - Physician leadership
  - IT security
  - Health policy
  - Others as needed

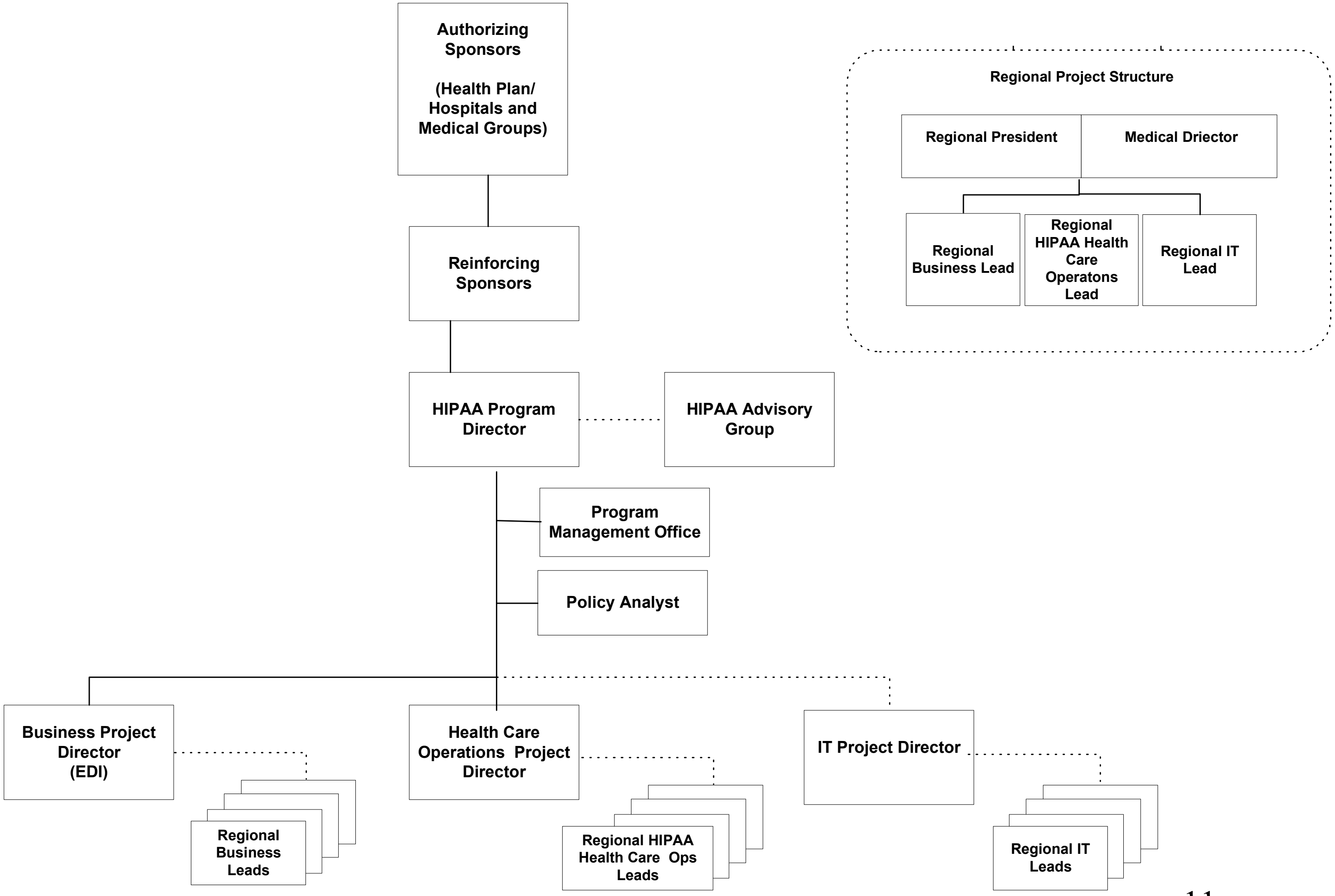
National HIPAA Program

- Provide coordination and project management
- Conduct assessment of HIPAA impact
- Develop national budgets and timelines
- Provide interpretation of HIPAA regulations
- Disseminate best practices and expertise
- Develop national solutions where possible
- Foster Regional implementation and local adaptations

National HIPAA Team Functional Areas

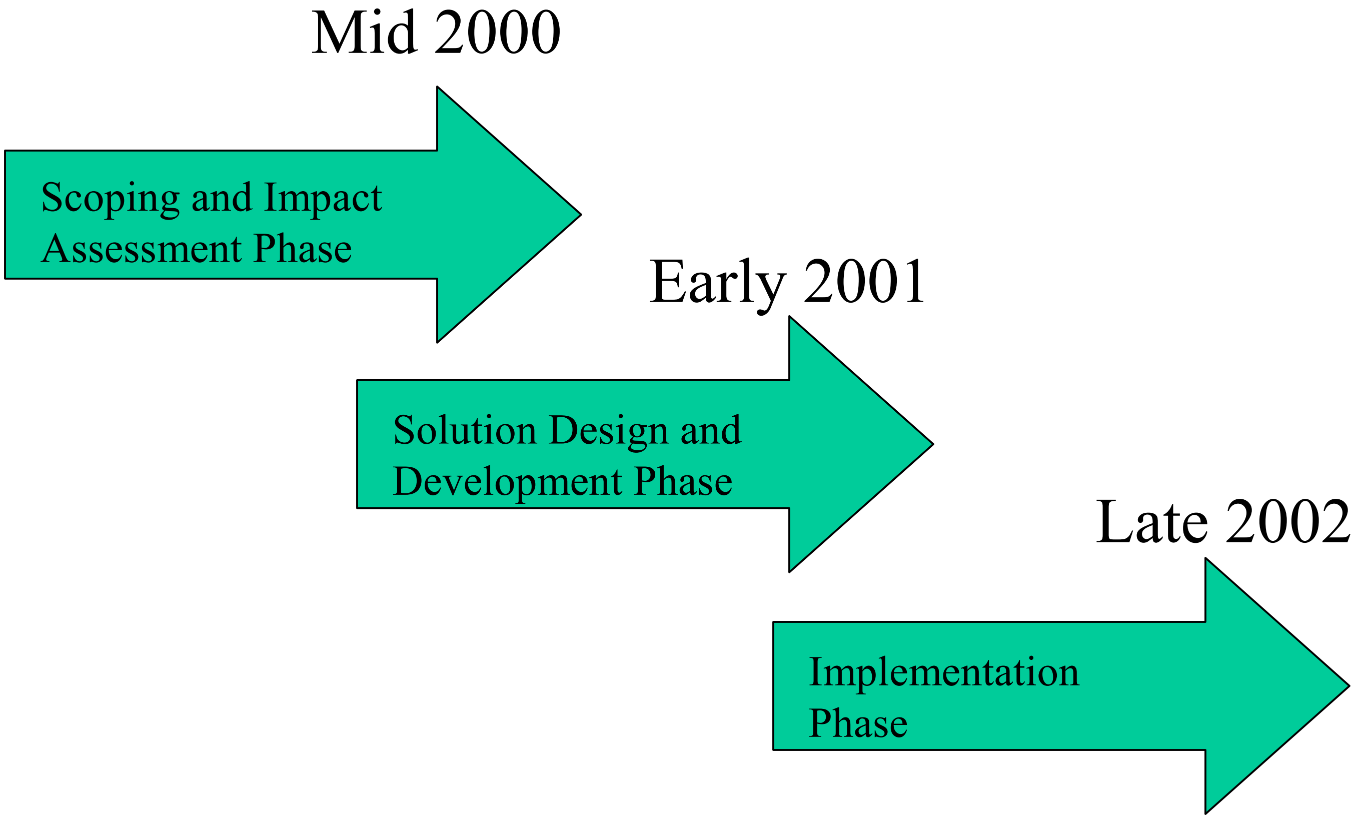
- Project management
- IT technical architecture/systems expertise
- Financial analysis
- Business process analysis
- Health care operations analysis
- Security and privacy analysis
- Communications
- Change management

National HIPAA Team Organizational Chart


Authorizing Sponsors
(Health Plan/ Hospitals and Medical Groups)
Reinforcing Sponsors
HIPAA Program Director
HIPAA Advisory Group
Program Management Office
Policy Analyst
Business Project Director (EDI)
Regional Business Leads
Health Care Operations Project Director
Regional HIPAA Health Care Ops Leads
IT Project Director
Regional IT Leads
Regional Project Structure
Regional President
Medical Director
Regional Business Lead
Regional HIPAA Health Care Operatons Lead
Regional IT Lead

KAISER PERMANENTE®

HIPAA Compliance: Big Picture



Mid 2000

Scoping and Impact Assessment Phase

Early 2001

Solution Design and Development Phase

Late 2002

Implementation Phase

KAISER PERMANENTE®

Scoping Effort Accomplishments

- Interpreted the proposed rules
- Clarified project scope and key impact areas
- Developed and launched awareness campaign
    - Focused on executive management
- Recruited key national positions
- Ensured Regional selection of leads for business, health care operations, IT
- Secured national and Regional sponsorship
- Studied related initiatives
- Developed proposed budget and timeline
- Conducted high level analysis
- Identified potential IT and business/health care operations solutions

Challenges for Health Plans re: Security & Privacy

- Gray areas in current regulations
- Conduct risk assessment, gap analysis, develop standardized policies and procedures
- De-identify patient information
- Provide HIPAA-compliant data to purchasers
- Provide HIPAA-compliant data to providers
- Ensure providers meet confidentiality requirements
- Specific areas of health plan business
  - e.g. claims and membership processes using patient identifiable data that has been in electronic format
- Standardize policies and practices re: privacy
  - Across state lines
  - Across provider groups
- *Note: Greatest security & privacy impact on providers*

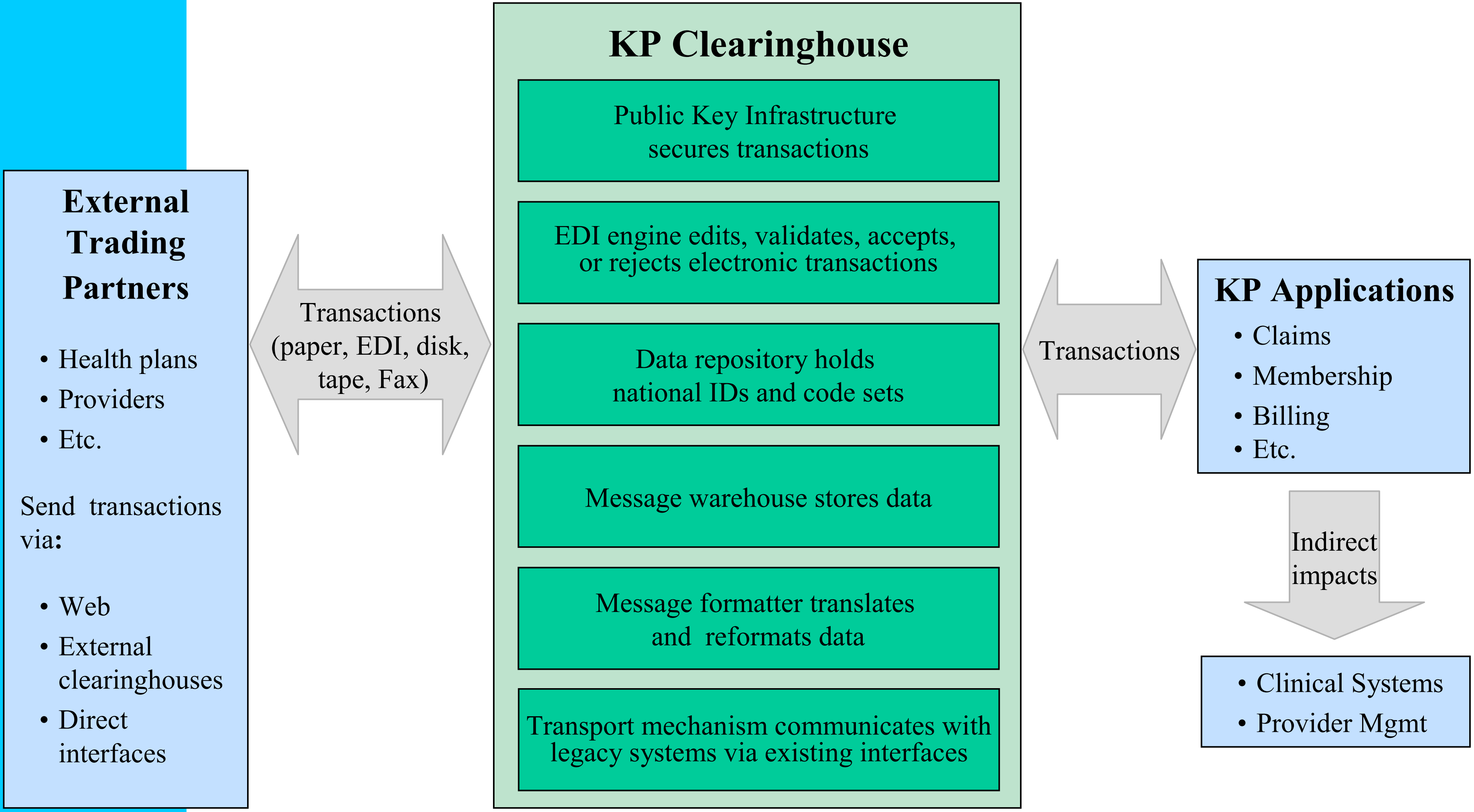
Challenges for Providers re: Security & Privacy

- Like health plans:
  - Many gray areas in regulations as currently written
  - Must conduct risk assessment, gap analysis, develop standardized policies and procedures
  - Must de-identify patient information
- Special challenges for providers:
  - Establish audit trails to show who has had access to patient records
  - Evaluate “minimum necessary” patient-identifiable information
  - Authentication and security for electronic medical record system, e.g. PKI

Possible Electronic Data Interchange Solution

- Some potential advantages:
  - Customized solutions for KP’s unique circumstances
  - Set of utilities developed nationally
  - Provides EDI, transaction translation, data mapping, and audit capabilities
  - Enables receipt and sending of HIPAA-compliant EDI transactions from new and legacy systems
  - Secures transactions
  - Flexible and evolutionary
  - Reduces redundant solutions

A Clearinghouse Utility to Achieve HIPAA Compliance - A Conceptual View



External Trading Partners

- Health plans
- Providers
- Etc.

Send transactions via:

- Web
- External clearinghouses
- Direct interfaces

Transactions (paper, EDI, disk, tape, Fax)

KP Clearinghouse

Public Key Infrastructure secures transactions

EDI engine edits, validates, accepts, or rejects electronic transactions

Data repository holds national IDs and code sets

Message warehouse stores data

Message formatter translates and reformats data

Transport mechanism communicates with legacy systems via existing interfaces

Transactions

KP Applications

- Claims
- Membership
- Billing
- Etc.

Indirect impacts

- Clinical Systems
- Provider Mgmt

Next Phase: Solution Design and Development

- Refine interpretation of regulations as they become finalized
- Complete comparison of HIPAA regulations with existing requirements
- Build Regional project teams and sponsorship
  - In-depth assessment in each Region (security, privacy, EDI, etc.)
  - Launch HIPAA leads summit meetings
  - Provide leads with tools for communication, project management, building sponsorship
- Develop communication plan and launch expanded campaign

Next Phase: Solution Design and Development (cont.)

- Complete design for EDI utility
  - Test preliminary design
  - Develop Regional rollout strategy
- Refine budgets as more information becomes available
- Plan security and privacy solutions (implement after regulations finalized)
- Link with other efforts already under way

HIPAA Lessons Learned

- Sponsorship is key to success
- Compliance depends on consistent interpretation of regulations
- Link with professional/trade associations
- Use energy of HIPAA to drive business decisions
- Integrate HIPAA activities (e.g. vendor upgrades, training) with ongoing activities
- Mantra: “This isn’t just about IT”