

HIPAA Summit IV

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



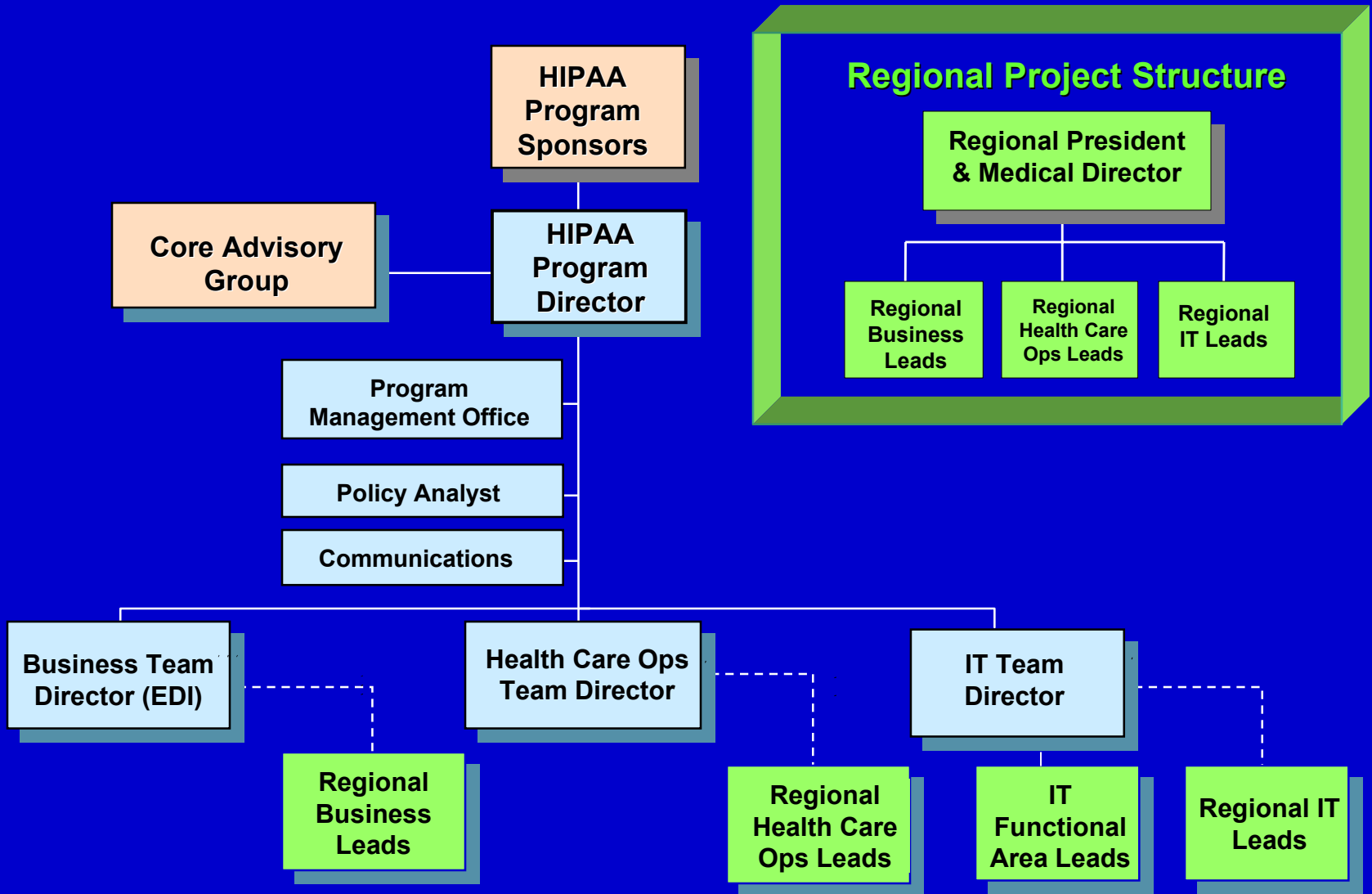
Kaiser Permanente: A Snapshot

- **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

National Team Organization



KP HIPAA Advocacy Efforts

- KP is working with a number of groups to better advocate for favorable interpretations/changes:
 - > DHHS > WEDI > AHHA > CMA/AMA
 - > Academic Medical Centers > Conferences
 - > Others
- We approached DHHS directly requesting “clarification” on several EDI issues. Resolved as we had requested. One response is pending.
- Testified before the National Committee on Vital Health Statistics, Subcommittee on Privacy, Aug. 21, 2001. (NCVHS advises DHHS.)

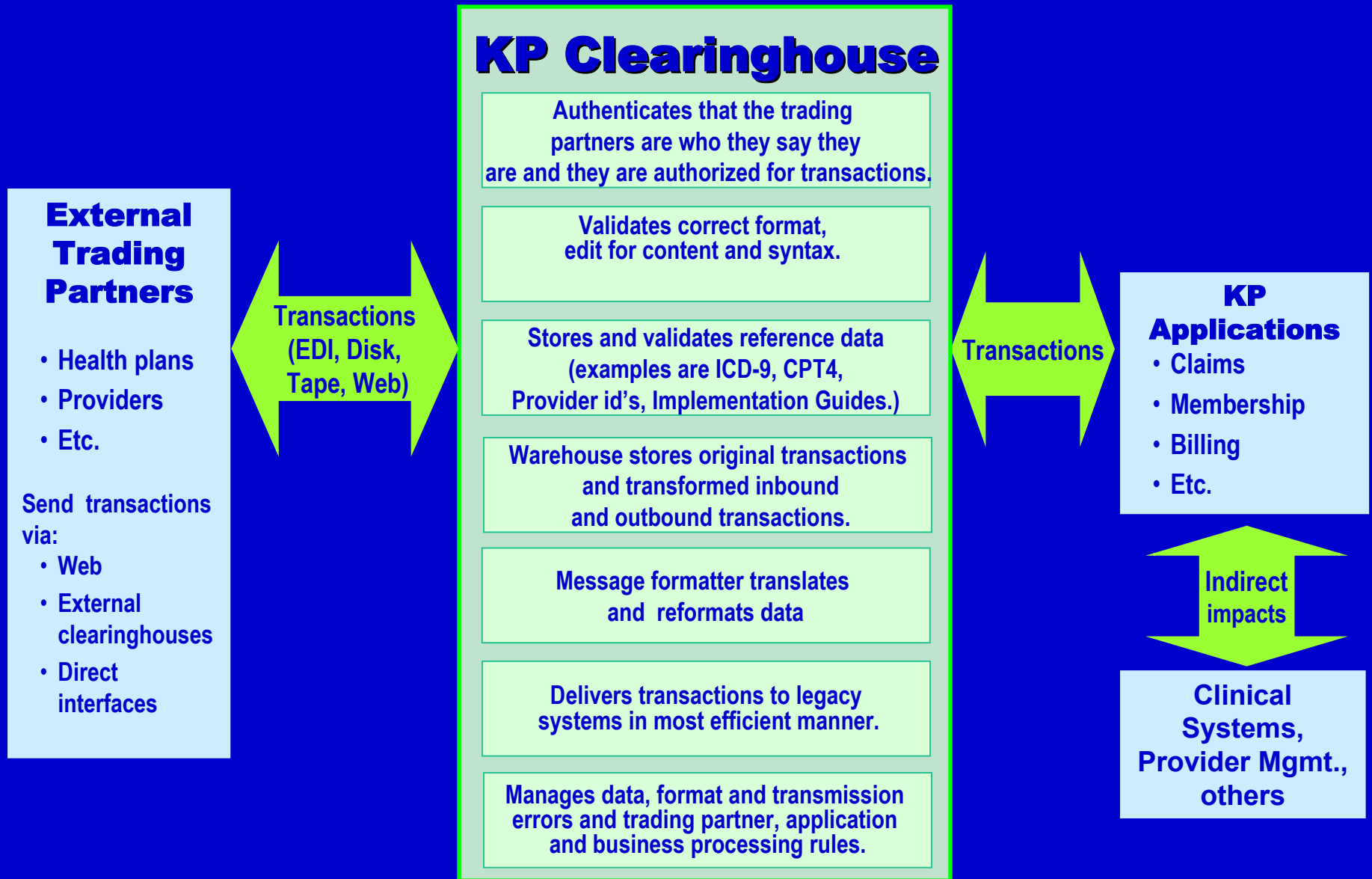
and more to come...

HIPAA EDI

Kaiser Permanente's EDI Approach

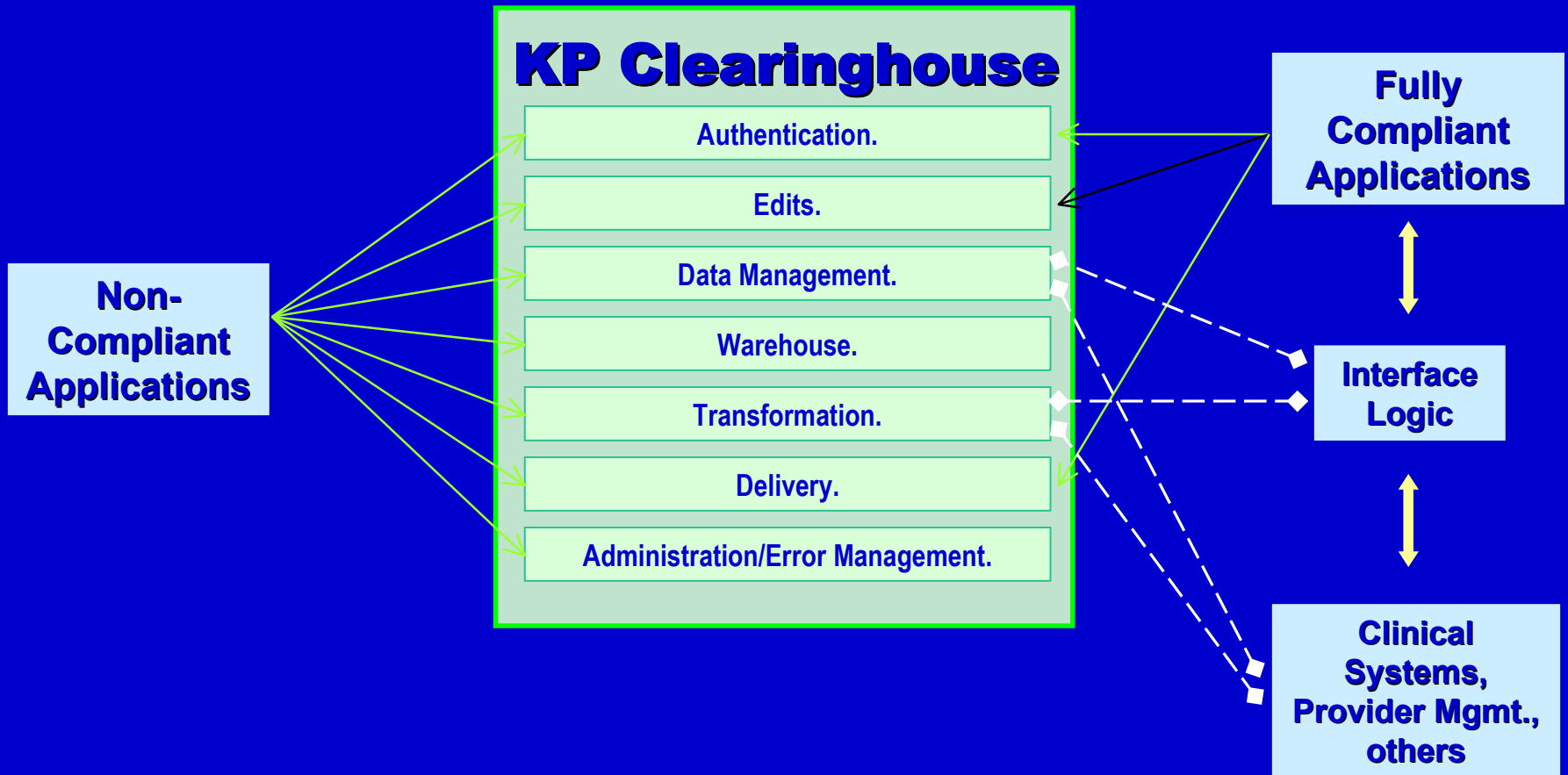
- **We are developing a “KP Clearinghouse” - a set of shared utilities - to translate specified information into HIPAA compliant format + modifying applications as needed.**
- **We chose the KPC approach because it is:**
 - ✓ significantly less expensive than modifying all applications affected,
 - ✓ 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.**

KP Approach: Clearinghouse Utility



KP Clearinghouse:

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



◆-----◆ Represents an example of re-use of KP Clearinghouse utilities

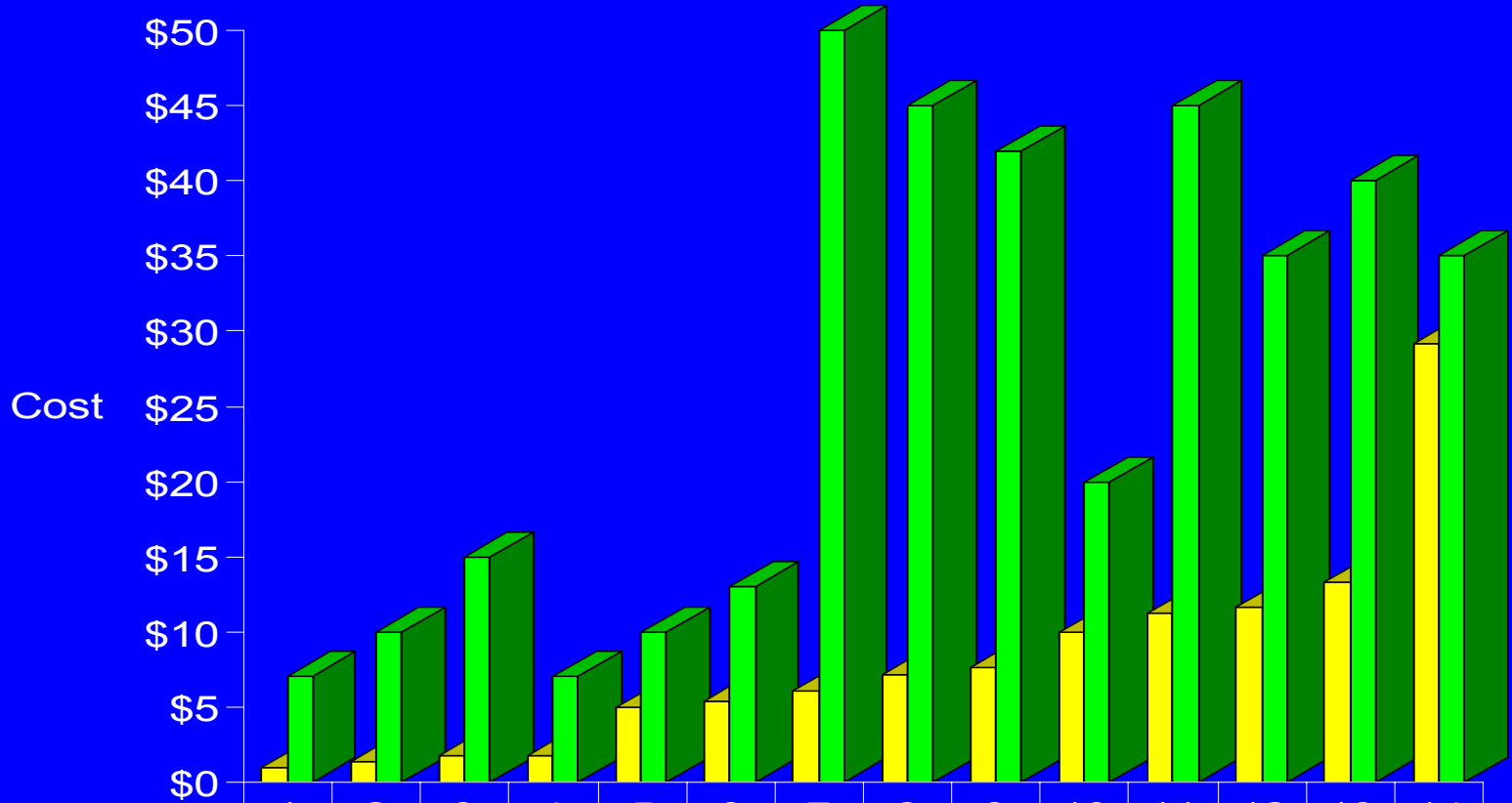
So What Are the Challenges of the EDI Extension for KP

- **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 EDI Compliance Cost Comparison



	1	2	3	4	5	6	7	8	9	10	11	12	13	14
■ Cost/ Member	\$1	\$1	\$2	\$2	\$5	\$5	\$6	\$7	\$8	\$10	\$11	\$12	\$13	\$29
■ Total Cost in \$M	\$7	\$10	\$15	\$7	\$10	\$13	\$50	\$45	\$42	\$20	\$45	\$35	\$40	\$35

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?

- Ready to take next steps after 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

HIPAA Privacy Rule...

What Just Happened???

- March 27 DHHS issued proposed revisions to HIPAA Privacy Rule
- Key message to our staff and physicians: “HIPAA is not going away”
- Key word: “Proposed”
- Advocacy takes the front seat in April

Biggest Challenge for KP

- Uncertainty - Where should we act?
Where should we wait?

Proposed HIPAA Privacy Revisions (the way they look to us)

- **Signed Consent:** Good news!
- **Privacy Notice:** Getting acknowledgement could be a challenge for health care systems
- **Disclosure tracking:** Some challenges
- **Marketing:** Still need to study
- **Minimum necessary:** More reasonable
- **Research:** De-identifying data still a concern
- **Privacy Officers:** No change
- **Training for Privacy and Security:** No change to the rule, but a huge task

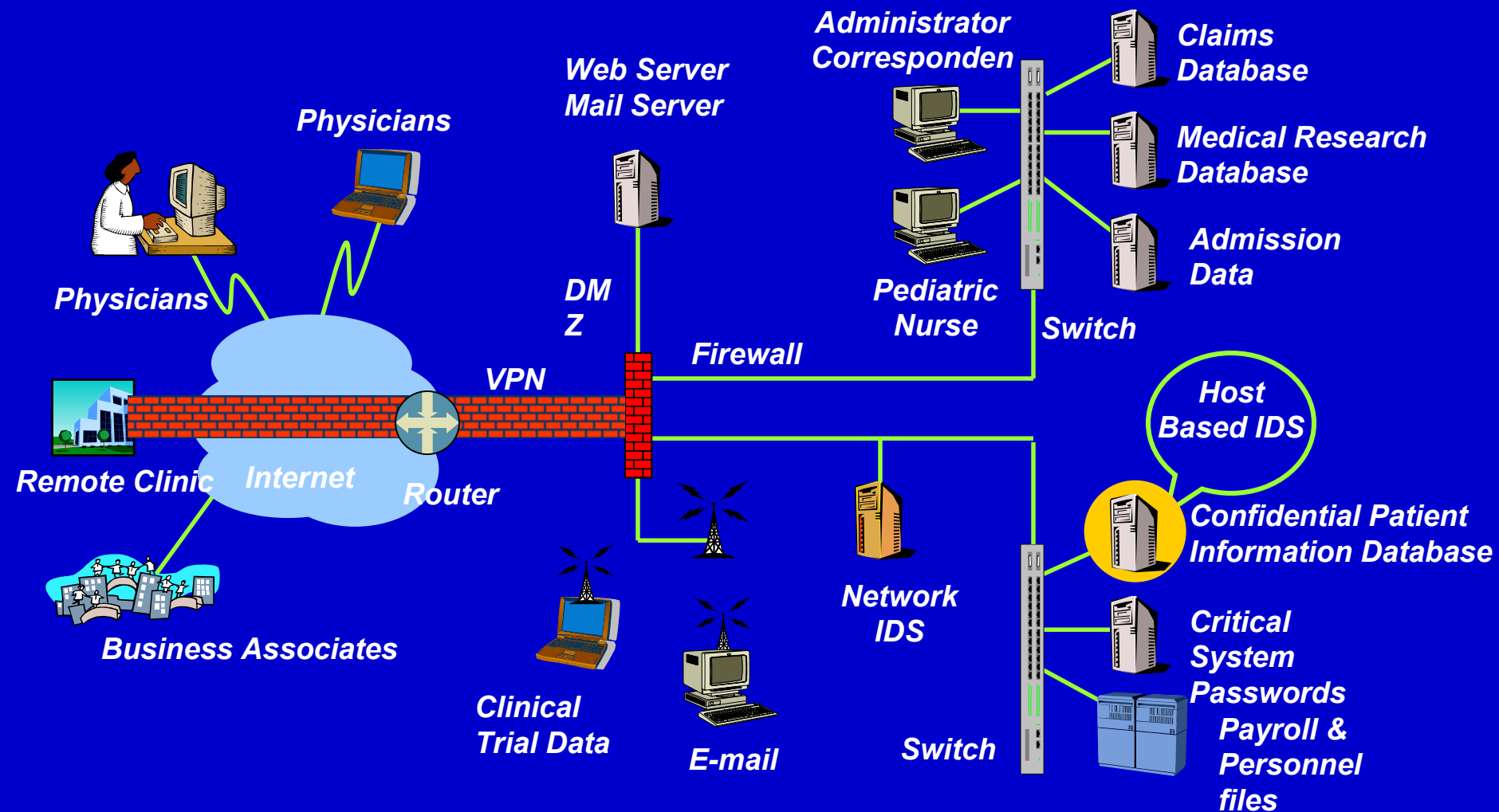
Challenges of Proposed Security Regulations for KP System

- 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

The KP Approach to HIPAA Privacy and Security

- Regional and national leads working together
- Baseline surveys used to establish where we are/what we do already
- Multi-disciplinary work groups develop approaches to key elements of HIPAA privacy and security
- Sub-work groups focus on specific issues

HIPAA 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

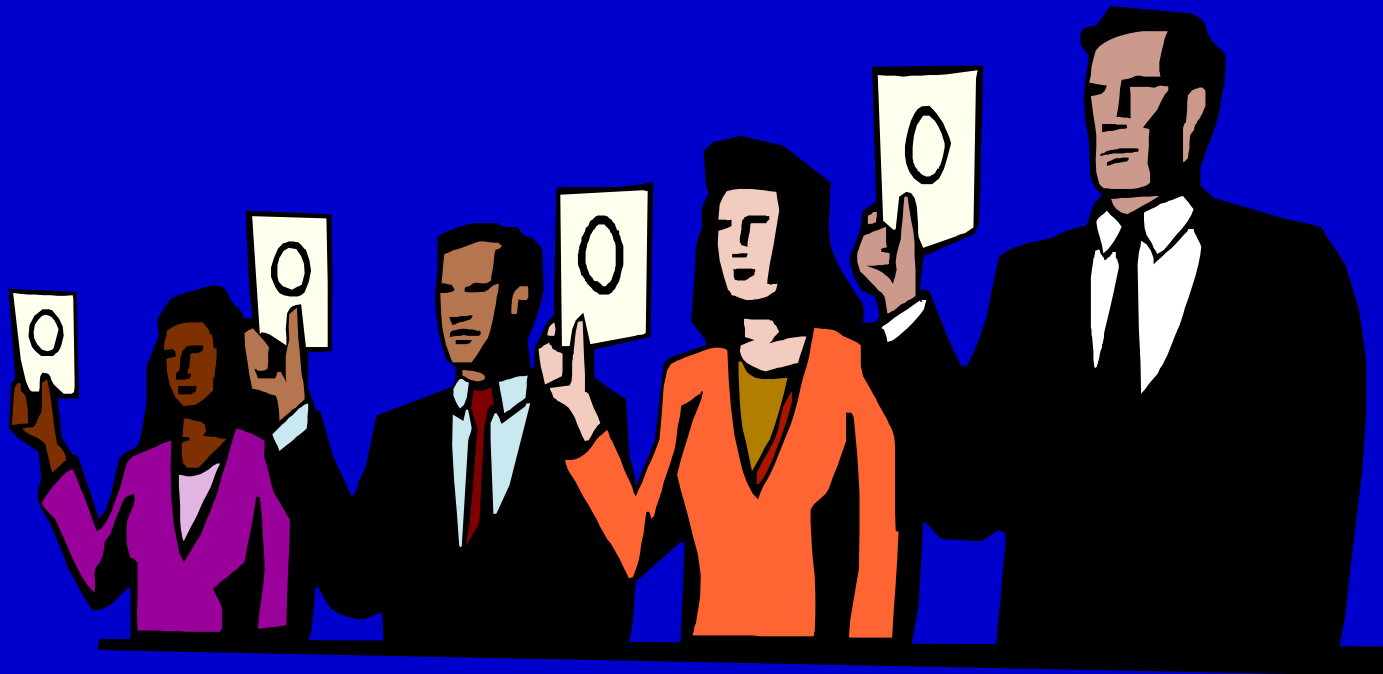


Steven—you are to begin therapy, as your blood test indicates 25% risk of teenage depression based on your genetic profile.

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!

Over The Top

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 rules¹**
- **Someone has to run the audits²**
- **Someone has to be accountable**

¹ the rules have to be meaningful

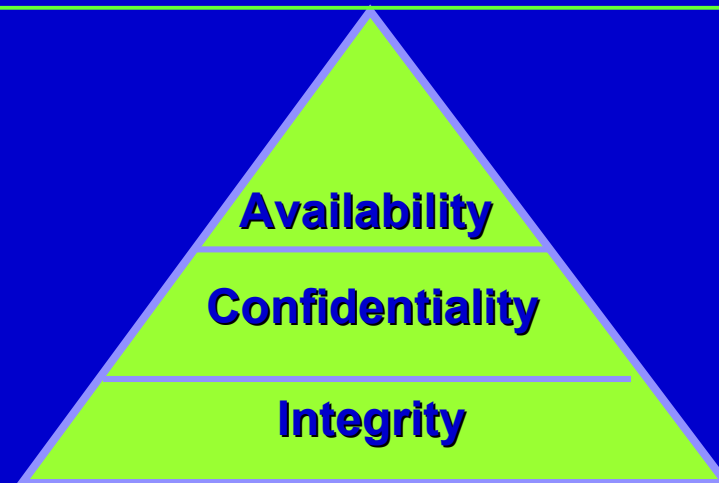
² the audits have to be meaningful

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

Security 'Vulnerabilities'

Item	Paper	Digital
Lack of policies and procedures	✓	✓
Incorrect policy implementation	✓	✓
No intrusion detection	✓	✓
Software bugs/ design flaws		✓
No firewall or poor implementation		✓
No virus protection/ poor implementation		✓

Information Security Hierarchy: Best Practices Approach

- **Administrative**
 - ✓ Policy & Procedure
 - ✓ Personnel Security
- **Technical**
 - ✓ Network Connectivity
 - ✓ Viruses
 - ✓ Authentication
 - ✓ Audit
 - ✓ Backup and Recovery
 - ✓ Encryption
 - ✓ Physical Security



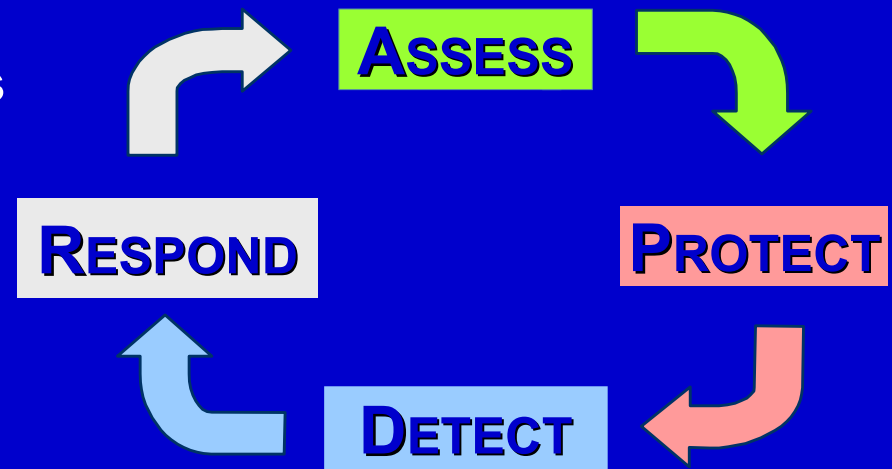
Top Ten 'Reasons' to Defer Security

“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 at time”

Security and Privacy Regulations: Risk Management Challenge

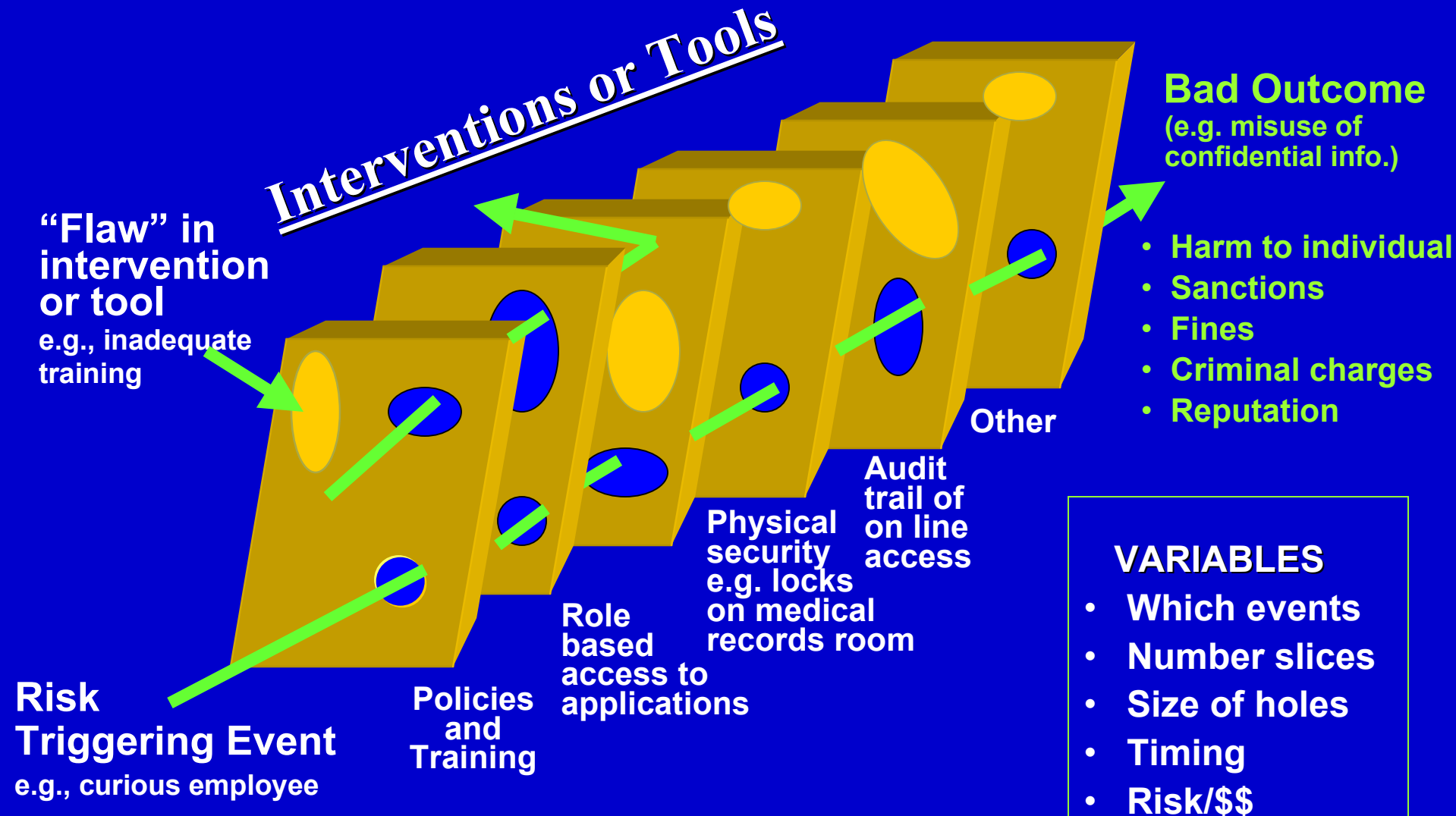


Diagram modified from James Reason's

“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