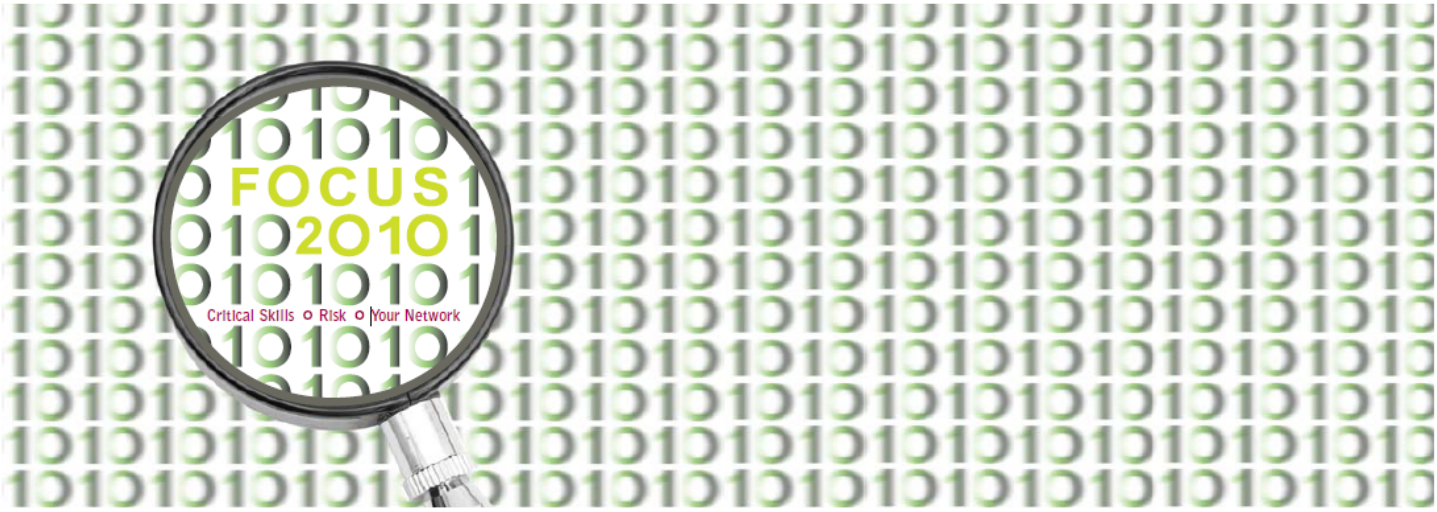
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



G21: HIPAA, HITECH, and Latest Trends

Scott Morgan and Roy Masatani,
Kaiser Permanente

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

HIPAA, HITECH, and Latest Trends

Scott Morgan: Executive Director, National Compliance Privacy and Security Officer Kaiser Permanente

Roy Masatani: Director, National Compliance Audit Kaiser Permanente

Topics

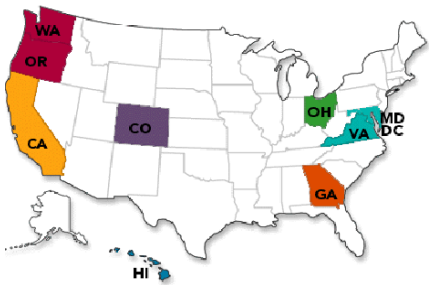
- Objectives
- What is Kaiser Permanente and Compliance?
- What is PHI vs. PII?
- Regulations
- Risk Landscape, Assessment, Metrics, and Monitoring
- IT Auditing at Kaiser Permanente
- Auditing for HIPAA Compliance
- NCO HIPAA Audit Program -- Example
- Closing Comments
- Appendices

Objectives

- Provide overview of health care regulations that impact privacy and security
- Discuss the impact that assessments and audits have on security programs
- Provide example of Kaiser Permanente's audit program for HIPAA compliance

What is Kaiser Permanente?

- One of nation's largest not for profit health plans
- 8.6 million members
- 179,000 employees and physicians
- 35 Hospitals, 454 Medical Office buildings
- 8 Regions, serving 9 states and the District of Columbia
- $42.1 billion annual revenues
- 3 organizations
  - Kaiser Foundation Health Plan, Inc
  - Kaiser Foundation Hospitals and subsidiaries
  - The Permanente Medical Groups



(As of December 31, 2009)

What is PHI? (Defined in HIPAA)

- **Protected Health Information (PHI)**
  - information related to an individual's past, present and future health care and health care payment information
  - containing identifiers – such as name, medical record number, address, e-mail, social security number, driver's license number, etc.

What is Personal Information?

- California State Law (Civil Code 1798) on Personal Information Disclosure and other similar state laws
- Personal Identifiable Information (PII)
  - An individual's first name or initial and last name in combination with any of the following data elements when they are not encrypted:
    - Social Security Number
    - Driver's License or ID Card number
    - Account number with access code to financial account
    - Medical information
    - Health insurance information

Regulations That Affect Privacy and Security Protection of PII

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Implemented by the Privacy Rule and the Security Rule (45 CFR Sections 160 and 164)
    - defines protected health information (PHI)
    - establishes safeguards
    - limits disclosure of PHI
- American Recovery and Reinvestment Act of 2009 (ARRA)
  - Incorporates Health Information Technology for Economic and Clinical Health (HITECH)
  - Interim Final Rule, Breach Notification for Unsecured PHI, August 24, 2009
  - Forthcoming modifications to HIPAA Privacy and Security Rules
- Genetic Information Non-Discrimination Act of 2008 (GINA)
  - Interim Final Rules, 74 Fed Reg 51664 (October 7, 2009)
  - Proposed Rule amending HIPAA Privacy Rule to incorporate GINA, 74 Fed Reg. 51698 (Oct 7, 2009)
- State Laws and Regulations
  - Protecting health information and information technology/exchange

HIPAA

- The HIPAA Privacy Rule covers the uses and disclosures of protected health information (PHI) where such use or disclosure concerns any of the following formats: written (hard copy), electronic, or spoken (oral).
- The HIPAA Security Rule covers the requirements for which electronic PHI must be safeguarded, whether physically locked away or otherwise protected from unauthorized access or use.

ARRA: HITECH

- American Recovery and Reinvestment Act (ARRA) Title XIII-Health Information Technology (HITECH)
  - Promotes industry-wide adoption of electronic health records (EHR)/systems & health information exchange
    - Financial incentives (grants/loans/Medicare & Medicaid incentive payments) to hospitals and physicians for EHR "meaningful use"
    - Integration of quality and outcomes measures as part of electronic health records/systems (still under development)
  - Creates structure/governance for Health Information Technology adoption
    - Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) provides oversight
    - Standards & policy development
    - Certification process for electronic health records/systems
    - Distribution of incentives
    - Monitoring and enforcement
  - Research and testing
    - National Institute of Standards and Technology (NIST) standards and technology leadership
    - Research and development programs

Privacy Changes ARRA Will Bring

- New patient privacy rights
  - Access to PHI in electronic format
  - Restrictions on use or disclosure of PHI
  - Disclosure accounting for treatment, payment, health care operations disclosures made through EHRs
- Regulations for Business Associates
  - New direct requirements to protect PHI
  - Fines for breaches
- Breach reporting requirements
  - Harm assessment
  - Reporting requirements to HHS
- Increased enforcement and penalties
  - Prosecution by State Attorney
  - Fines and penalties increased
- De-identification subject to new guidance

HIPAA Modifications
Notice of Proposed Rulemaking (NPRM)

- Published 7/14/10
- The majority of the changes in the Proposed Rule implement HITECH
- Provides individuals with the right to obtain electronic PHI in an electronic format
- Provides a right to restrict disclosures to health plans under certain circumstances
- Strengthens the rules governing enforcement
- New requirements are applicable to marketing, the sale of PHI, and fundraising
- Relaxes the rules applicable to Authorizations for research
- Permits disclosure of vaccination records to schools without all inclusive authorization
- Expands access to PHI of decedents
- Requires changes in Notice of Privacy Practices (NPP) reflecting several of these modifications

Breach Notification

- Interim Final Rule effective 9/23/09
- Definition of what constitutes a breach
- Office for Civil Rights (OCR) has indicated it will investigate all breaches of >500 records
- Applicability to Business Associates
- Enforcement and penalties
- Notification requirements
  - Timing
  - To whom
  - Contents of the notification

Business Associates

- ARRA added new obligations for business associates, requiring an update for all Business Associate Agreements (BAAs)
- Expands definition of Business Associates
- Requirements were effective immediately and applied to all valid BAAs
- Kaiser Permanente notified existing business associates about the new obligations through unilateral amendments
- Kaiser Permanente has revised the BAA template for *new* business associates and for those contracts that require extensive revisions to comply with the new requirements

Access to PHI in Electronic Format

- Currently, a patient has a right to receive a copy of his/her PHI in the form requested, if readily available
- HITECH requires
  - if PHI is contained in an electronic health record (EHR), the individual is entitled to PHI in an electronic format
  - if PHI is maintained electronically, regardless of whether it is part of an EHR, the covered entity must provide the individual with access in the electronic form requested, if it is producible in such form
  - if PHI is not in electronic format, information must be provided in a form agreed upon by the parties
  - individual may request health information be sent to a third party, provided that the request is clear, conspicuous, and specific

Restrictions on Use and Disclosure

- Under current HIPAA requirements, a patient has a right to request to restrict the use and disclosure of his/her PHI for treatment, payment, and health care operations, but the covered entity may refuse such requests.
- HITECH and the HIPAA NPRM requires that health care providers must agree to restrict disclosure of PHI:
  - when the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for carrying out treatment), and
  - the PHI pertains to items or services for which the health care provider has been paid by the patient in full

GINA Protects Genetic Information

- Genetic information must not be used for underwriting for health insurance purposes
- New definitions apply for genetic tests, genetic information, genetic services, family member, and other terms that apply to the use of genetic information for underwriting for health insurance purposes
- Genetic information may not be shared with or sold to third parties (for marketing purposes or for underwriting for health insurance purposes)

State Rules and Regulations

- Many state regulations based on California Breach Notification law
- States vary on reporting requirements
- Reporting disclosures of personal information to state agencies
- Notification of disclosures to individuals
- Medical and Identity fraud

Risk Landscape

- Risk Landscape
  - Lost and stolen ePHI
    - Unencrypted devices of all types
    - Unintended disclosures
  - Inappropriate access to PHI
- Health Information Exchanges (HIE) becoming more prevalent
- Greater fines and penalties

Risk Assessment

- Risk Assessment
  - Identify threats and vulnerability
    - Review previous risk assessment documentation
    - Review adverse occurrences
    - Review recent audits or reports
  - Likelihood + Impact = Risk Rating
- Support for program needed from the senior leader level to front-line employees
- Determine frequency of assessments
- Determine plan and timeline to remediate risk
- Leadership sign-off for both accepting and mitigating risk

Metrics

- Develop metrics to monitor compliance with regulations, policies and procedures
- Map HIPAA specifications against NIST security documents to develop metrics (see Appendix A)
- Build new metrics to monitor as new rules and regulations are instituted (new regulation related metrics)
  - Number of breaches identified by Business Associate
  - % of Privacy and Security notifications to state agencies that were reported within the regulatory timeframe
  - % of Privacy and Security notifications to CMS reported within 24 hours of the incident date
  - % of Privacy and Security notifications to HHS reported within 60 days of the discovery date, for any incidents affecting 500 or more
- Develop a “Scorecard”

Monitoring and Reporting

- Monthly regional and national department metrics review
- Annual regional compliance review
- Hospital assessments
- Partner with IT to obtain IT based measures, especially as new technology becomes available
- Reporting of key measures to leadership, including Boards of Directors

IT Auditing at Kaiser Permanente

Different But Collaborative IT Audit Functions

- National Compliance Office
  - IT Audits – HIPAA Security Focused
  - Revenue Cycle Audits – Billing & Claims Processing (HIPAA and Government Payer Focused)
- Internal Audit Services
  - IT Audits -- IT Applications and Operations
  - Sarbanes-Oxley -- IT Audit Testing
- Information Technology Organization
  - IT Compliance Audits -- Policies & Standards Remediation
  - Payment Card Industry (PCI) – IT Audit Validation
- Sarbanes-Oxley (SOX) Mega Process
  - IT Audits -- SOX Key Controls Testing

National Compliance Office (NCO) - Audit

2010 Reviews Include Compliance to Government Regulations (Center for Medicare and Medicaid Services) and HIPAA

Examples:

- Hospital Services Billing (HB) (Claims UB-04)
- Professional Services Fee Billing (Pro Fee) (Claims CMS-1500)
- Revenue Cycle and Medicare Compliance
  - Facilities On Site Validations
  - Claims Coding Validations (e.g., ICD-9 Codes, CPT Codes, etc.)
  - Build HIPAA Requirements Testing into Revenue Cycle Compliance Review (RCCR) Checklists
  - Map RCCR Tests to Key SOX Controls
- Information Security Policies (ISP)
  - "Mini ISP Audit Program"-- Mapped Policies and Tests to HIPAA Requirements

Auditing for HIPAA Compliance (1 of 2)

- Understand the new HIPAA/HITECH ("HIPAA") regulations and impact of changes
- Identify key/critical (risk-based) HIPAA requirements for the organization
- Map organization's existing Information Technology (IT) / Information Security (IS) Policies and Standards to HIPAA requirements
- Identify gaps related to policies and standards
- Develop new policies, standards, and procedures for HIPAA compliance gaps

Auditing for HIPAA Compliance (2 of 2)

- Develop new and/or revised compliance objectives and audit tests
- Build HIPAA compliance objectives into applicable audits
- Perform HIPAA compliance tests, document results, report to Management and Regulators, summarize trends, and address deficiencies as needed
- Retain audit workpapers and other compliance evidence for external auditors and government regulatory examiners

NCO HIPAA Audit Program

Management Objective: Establish Consistent and Objective Metrics Relating to Kaiser Permanente's Compliance with HIPAA and Information Security Policies

Background

- NCO Audit work is recognized as the source for accurate and objective information that is used by National Compliance Office's Senior Leadership and others to make critical decisions.
- NCO Audit work encompasses all regions and functional areas including Health Plan, Care Delivery, Revenue Cycle, Information Technology, etc.
- NCO Audit needs to evaluate Kaiser's compliance with HIPAA and Information Security (IS) policies in all work that we do.

NCO HIPAA Audit Program

Standardization is Critical

- How do we determine which HIPAA requirements to evaluate?
- How do we incorporate the evaluation of HIPAA requirements and IS policies, leading to reliable and consistent compliance measures, into all NCO Audit work?
- Create a "mini audit program" that…
  - Consists of seven control objectives
  - Focuses on evaluating business operational processes
  - Follows the Office of Inspector General (OIG) compliance elements (e.g., Policies & Procedures, Training, and Monitoring)
  - Is "Plug and Play" -- designed to be incorporated and integrated into the 2010 NCO auditing activities (e.g., Hospital Billing Reviews, Claims Reviews)

NCO HIPAA Audit Program

HIPAA Requirements Mapped to Kaiser Permanente Information Technology/Information Security Policies

NCO Management selected six key/critical policies to audit, plus one extra objective for other HIPAA related observations:

1. Information Security Governance
2. Secure Electronic Storage of PHI/MPII Data
3. User Access Management
4. Business Continuity
5. Security Breach Incident Management
6. Business Associate Agreements (BAAs)
7. Other HIPAA Related Compliance Requirements

NCO HIPAA Audit Program

For Each Compliance Objective

- **Mini Audit Program Guidance…**
  - Define Compliance Objective
  - Cite HIPAA and Kaiser Permanente Compliance Sources, and COBIT References
  - Describe Validation Test – Regional vs. Local Facility (e.g., Hospital, Medical Center)
  - Specify Validation Procedural Steps – Regional vs. Local Facility
  - Define Scoring Methodology
  - Identify Information To Be Requested (e.g., Interviews/ Interviewees, Systems/Processes Walkthroughs, Controls Evidence, Compliance Demonstrations, and Relevant Documentation)
  - Perform Audit Validation Testing
  - Document and Summarize Results

NCO HIPAA Audit Program

Compliance Objective 1: Information Security Governance

- What: Is there an effective organizational infrastructure in place defining Information Security strategy and governing activities, policies, standards, and outcomes, etc.?
- Why: All organizations, especially those the size and complexity of Kaiser Permanente, need a consistent long-term governance infrastructure, and policies and standards upon which to rely. (Besides, HIPAA, ARRA, SOX, and OIG all say we **must** have it).
- How: Follow Mini Audit Program which provides guidance.

NCO HIPAA Audit Program

Control Objective 1:

Information Security Governance

- HIPAA
  - 164.308(a)(1)(i) - Security Management Process
  - 164.308(a)(i)(ii)(A) - Risk Analysis
  - 164.308(a)(i)(ii)(B) - Risk Management
- Information Security Policy
  - NATL.IS.001: 01.0 Information Security Governance and Organization
- COBIT
  - PO1 Plan and Organize – Define a Strategic IT Plan
  - PO6 Communicate Management Aims and Direction
  - PO9 Assess and Manage IT Risks
  - DS5 Ensure Systems Security
  - ME3 Ensure Compliance with External Requirements
  - ME4 Report on IT Governance Status

NCO HIPAA Audit Program

Compliance Objective 2:
Secure Electronic Storage of Member/Patient Data

- What: Are adequate and effective policies, standards, and procedures in place to define, train, implement, and monitor electronic member/ patient data, to ensure that the data is securely stored and safeguarded from unauthorized access, theft, damage, or destruction?
- Why: Electronic member/patient data is considered private and confidential, and must be stored on Kaiser network servers, shared drives, or servers that otherwise meet Kaiser security standards (e.g., physically secured, automatic encryption capability, etc.).
- How: Follow Mini Audit Program which provides guidance.

NCO HIPAA Audit Program

Control Objective 2:
Secure Electronic Storage of Member/Patient Data

- HIPAA
  - 164.308(a)(1)(i) - Security Management Process
  - 164.308(a)(i)(ii)(A) - Risk Analysis
  - 164.308(a)(i)(ii)(B) - Risk Management
- Information Security Policy
  - NATL.IS.001: 04.0 Secure Electronic Storage of Member Patient Data
- COBIT
  - PO3 Technology Standards
  - PO9 Assess and Manage IT Risks
  - AI2 Application Security Controls
  - DS4 Backup Storage and Protection Plan
  - DS5 Ensure Systems Security
  - D11 Manage Data
  - DS12 Manage the Physical Environment
  - DS13 Manage Operations
  - ME3 Ensure Compliance with External Requirements

NCO HIPAA Audit Program

Compliance Objective 3:
User Access Management

- What: Are adequate and effective policies, standards, and procedures in place to define, train, implement, and monitor user access rights?
- Why: We need to take all reasonable and necessary actions to limit unauthorized access to information assets. Adherence to principles such as “minimum necessary” and “segregation of duties” is critical to a compliant Information Security environment.
- How: Follow Mini Audit Program which provides guidance.

NCO HIPAA Audit Program

Control Objective 3:
User Access Management

- HIPAA
  - 164.308(a)(1)(i) -Security Management Process
  - 164.308(a)(i)(ii)(A) -Risk Analysis
  - 164.308(a)(i)(ii)(B) -Risk Management
- Information Security Policy
  - NATL.IS.001: 12.0 User Access Management
  - NATL.IS.001: 02.0 Acceptable Use of Information Systems and Assets
  - Minimum Necessary NATL.NCO.PRIV.14
- COBIT
  - PO4 Define the IT Processes, Organization, and Relationships
  - PO9 Assess and Manage IT Risks
  - AI2 Application Security Controls
  - AI4 Enable Operation and Use
  - DS5 Ensure Systems Security
  - DS7 Educate and Train Users
  - ME3 Ensure Compliance with External Requirements

NCO HIPAA Audit Program

Compliance Objective 4:
Business Continuity

- What: Are adequate Business Continuity Plans in place? Are they periodically tested and updated?
- Why: Business Continuity is about having viable plans ready to support the continued operations of critical processes in the event of any unexpected/unplanned business interruption. Patient care delivery and safety concerns are affected; potential fraud, waste, and abuse should also be considered.
- How: Follow Mini Audit Program which provides guidance.

NCO HIPAA Audit Program

Control Objective 4:
Business Continuity

- HIPAA
  - § 164.308(a)(7)) -- Contingency Plan
- Information Security Policy
  - NATL.IS.001: 14.0 Business Continuity and Disaster Recovery
- COBIT
  - PO9 Assess and Manage IT Risks
  - DS3 Manage Performance and Capacity
  - DS4 Ensure Continuous Service
  - DS8 Manage Service Desk and Incidents
  - DS9 Manage the Configuration
  - DS10 Manage Problems
  - DS11 Manage Data
  - DS13 Manage Operations
  - ME2 Monitor and Evaluate Internal Control
  - ME3 Ensure Compliance with External Requirements

NCO HIPAA Audit Program

Compliance Objective 5:
Security Breach Incident Management

- What: Do we have adequate and effective processes and procedures in place to address breach notification and reporting requirements?
- Why: We operate in a highly regulated environment with very extensive requirements on breach notification and reporting. We must adhere to these requirements or risk potential heavy fines, and the loss of good faith and reputation.
- How: Follow Mini Audit Program which provides guidance.

NCO HIPAA Audit Program

Control Objective 5:
Security Breach Incident Management

- HIPAA
  - (§ 164.308(a)(6)) -- Security Incident Procedures, Response and Reporting
- Information Security and Privacy Incident Management
  - NATL.NCO.PS.130
- COBIT
  - PO9 Assess and Manage IT Risks
  - DS5 Ensure Systems Security
  - DS7 Educate and Train Users
  - DS8 Manage Service Desk and Incidents
  - D11 Manage Data
  - DS12 Manage the Physical Environment
  - DS13 Manage Operations
  - ME2 Monitor and Evaluate Internal Control
  - ME3 Ensure Compliance with External Requirements

NCO HIPAA Audit Program

Compliance Objective 6:
Business Associate Agreements

- What: Are policies, standards, and procedures implemented for ensuring Business Associate Agreements (BAAs) are established?
- Why: Kaiser Permanente is a "Covered Entity" and we therefore have an obligation to ensure that BAAs defining roles/responsibilities between us and our "Business Associates" (vendors with access to PHI) relating to Information Security exist. Business Associates must have a framework in place to comply with HIPAA minimum security requirements.
- How: Follow Mini Audit Program which provides guidance.

NCO HIPAA Audit Program

Control Objective 6:
Business Associate Agreements

- HIPAA
  - § 164.308(b)(1) and 164.314(a)(1)) -- Business Associate Contracts or Other Arrangements
- Business Associate Contract Requirements to Safeguard Protected Health Information
  - NATL.NCO.PS.003
- COBIT
  - PO6 Communicate Management Aims and Direction
  - PO9 Assess and Manage IT Risks
  - AI5 Procure IT Resources
  - DS1 Define and Manage Service Levels
  - DS2 Manage Third Party Services
  - DS4 Ensure Continuous Service
  - DS5 Ensure Systems Security
  - D11 Manage Data
  - ME2 Monitor and Evaluate Internal Control
  - ME3 Ensure Compliance with External Requirements

NCO HIPAA Audit Program

Compliance Objective 7:
Other HIPAA Related Requirements

- What: Are information security policies, standards, and practices established, compliant with, and aligned with the Kaiser Permanente Information Security Program addressing the HIPAA Security Rule, to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity?
- Why: The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
- How: Follow Mini Audit Program which provides guidance.

NCO HIPAA Audit Program

Control Objective 7:
Other HIPAA Related Compliance Requirements

- HIPAA
  - §164.310 (a)(2)(ii) -- Facility Security Plan
  - §164.310(a)(1) -- Facility Access Controls
  - §164.314(b)(2) -- Implementation Specifications
  - §164.310(c) -- Workstation Security
  - Others
- Information Security Policy
  - NATL.IS.001: 05.0 Facilities Information Security and Privacy
- COBIT
  - PO7 Manage the IT Human Resources
  - AI6 Manage Changes
  - DS5 Ensure Systems Security
  - DS9 Manage the Configuration
  - DS11 Manage Data
  - DS12 Manage the Physical Environment
  - DS13 Manage Operations
  - ME2 Monitor and Evaluate Internal Control
  - ME3 Ensure Compliance with External Requirements

Closing Comments

- Federal and State health care regulations are changing rapidly
- Organizations must be able to react to changes quickly and comply with new requirements to stay in business
- Health care is highly regulated (e.g., CLIA, CMS, DEA, DOL, EPA, ERISA, FCC, FTC, HHS, JCAHO, NRC, OCR, OIG, OSHA, PCI, RAC, etc.)
- At Kaiser Permanente, the various auditing organizations must work together and collaborate to:
  - Reduce government regulatory risks and ensure compliance
  - Optimize resources, effort, and time
  - Minimize audit impact upon the business and operations
  - Evaluate and enforce uniformity in the implementation of policies and procedures, communications and training, and monitoring across the enterprise

QUESTIONS?

Contact Information

- Scott Morgan
  - Scott.Morgan@kp.org
- Roy Masatani
  - Roy.Masatani@kp.org

Appendix A: Example of NIST Mapping to HIPAA Security Specification

Access Controls

- References: NIST 800-12, NIST 800-14, NIST 800-21, NIST 800-34, NIST 800-53, NIST 800-63, FIPS140-2, NIST 800-66
- Does the organization's IT systems have the capacity to set access controls? (NIST 800-66)
- What method of access control is used (i.e. identity based, role based, or a combination of both)? (NIST 800-66)
- Have rules of behavior been established and communicated to system users? (NIST 800-66)
- How will rules of behavior be enforced? (NIST 800-66)
- Who will manage access control procedures? (NIST 800-66)
- Are current users trained in access control management? (NIST 800-66)
- Will user training be needed to implement access control procedures? (NIST 800-66)
- Are the organization's types of access controls divided into read, write, delete, execute and create? (NIST 800-12)

Appendix A (cont.): Example of NIST Mapping to HIPAA Security Specification

Access Controls (cont.)

- Is there a centralized administration, decentralized administration or a hybrid approach that approves, modifies, terminates, and monitors access control? (NIST 800-12)
- Is there a separation of duties for those who administer access controls and those who administer the audit trail? (NIST 800-14)
- Does the organization employ automated mechanisms to support the management of information system accounts? (NIST 800-53)
- Does the information system automatically terminate temporary and emergency accounts after a specified period of time? (Indicate the time period) (NIST 800-53)
- Does the information system automatically disable inactive accounts after a specified period of time? (Indicate the time period) (NIST 800-53)
- Does the organization employ automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals? (NIST 800-53)

47

ISACA San Francisco Chapter

Appendix B: Regulatory Agencies Acronyms and Links

- CLIA – Clinical Laboratory Improvement Amendments
  - http://www.cms.gov/clia/
- CMS – Centers for Medicare & Medicaid Services
  - http://www.cms.gov/
- DEA – Drug Enforcement Administration
  - http://www.justice.gov/dea/index.htm
- DOL – Department of Labor
  - http://www.dol.gov/
- EPA – Environmental Protection Agency
  - http://www.epa.gov/
- ERISA – Employee Retirement Income Security Act
  - http://www.dol.gov/dol/topic/health-plans/erisa.htm
- FCC – Federal Communications Commission
  - http://www.fcc.gov/
- FTC – Federal Trade Commission
  - http://www.ftc.gov/

48

ISACA San Francisco Chapter

Appendix B: Regulatory Agencies Acronyms and Links (cont.)

- HHS – Health and Human Services
  - http://www.hhs.gov/
- JCAHO – The Joint Commission
  - http://www.jointcommission.org/
- NRC – Nuclear Regulatory Commission
  - http://www.nrc.gov/
- OCR – Office for Civil Rights
  - http://www.hhs.gov/ocr/
- OIG – Office of Inspector General
  - http://oig.hhs.gov/
- OSHA – Occupational Safety & Health Administration
  - http://www.osha.gov/
- PCI – Payment Card Industry Security Standards Council
  - https://www.pcisecuritystandards.org/index.shtml
- RAC – Recovery Audit Contractor
  - https://www.cms.gov/RAC/