Uncle Sam HIT Me:
Compliance Risks in Implementation of Electronic Health Records
HCCA COMPLIANCE INSTITUTE, April 20, 2010
Bobbi Bonnet, RN, MPA
Senior Compliance Practice Leader, Kaiser Permanente

About Kaiser Permanente

- Nation's largest nonprofit health plan
- Integrated health care delivery system
- 8.7 million members
- 14,000 physicians
- 165,000 employees
- Serving 9 states and the District of Columbia
- 36 hospitals and medical centers
- 431 medical offices
- $40.3 billion annual revenues (2008)
Session Learning Objectives

- Provide an overview of the American Recovery and Reinvestment Act (ARRA) and its impact on Health Information Technology (HIT)
  - New regulatory impact for electronic health records (EHRs)
- Identify key risk areas in Electronic Health Record (EHR) implementation
- Provide a methodology for EHR compliance risk assessment

What today’s presentation will cover

- What is ARRA and HITECH Act / HIT
  - Definition of Electronic Health Record (EHR)
  - “Meaningful Use” (MU) requirements
  - Privacy Rule enhancements
- EHR Compliance Risk and Assessments
  - General and targeted risk areas
  - Assessment methodology and process
  - Sample tool for compliance assessment work
**What is ARRA?**

**American Recovery and Reinvestment Act (ARRA)**
- Signed by President Obama on February 17, 2009
- Multiple sections to the bill, not all related to HIT
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
  - Subtitle A: Promotion of Health Information Technology
  - Subtitle B: Testing of Health IT
  - Subtitle C: Grants and Loans Funding
  - Subtitle D: Privacy
  - Title IV: Medicare and Medicaid Incentives
- 19 Billion in funding for HIT in ARRA
- First round of draft EHR and MU regulations issued for comment 1/13/2010
  - Health and Human Service (HHS) Office of National Coordinator (ONC) Interim Final Rule (IFR)
  - HHS Centers for Medicare and Medicaid Services (CMS) Notice of Proposed Rule Making (NPRM)

---

**Qualified Electronic Health Record (EHR)**

...“an electronic record of health-related information on an individual that:

1. Includes patient demographic and clinical health information, such as medical history and problem lists; and
2. Has the capacity:
   i. To provide clinical decision support;
   ii. To support physician order entry;
   iii. To capture and query information relevant to health care quality; and
   iv. To exchange electronic health information with, and integrate such information from other sources.”

Source: Interim Final Rule, §170.102 Definitions.

**NOTE:** HHS has expanded the functional definition of an EHR from the clinical care record to include end-to-end system processes.
Standards Categories in EHR IFR

- **Content Exchange:** Standards used to exchange clinical information
  - Clinical summaries (HL7 CCD or ASTM CCR)
  - Prescriptions (NCPDP Script 5.0 or 8.1)
  - Structured electronic documents (CMS PQRI 2008 Registry XML) (HL7 2.5.1 or 2.3.1) (HIPAA EDI code set) (CPT-4) (HL7 CVX)

- **Vocabulary:** Standardized nomenclature and codes sets
  - Clinical problems (ICD-9-CM or SNOMED CT)
  - Medications (RxNorm)
  - Laboratory (LOIN-C)
  - Allergies (TBD, but considering UNII)

- **Privacy/Security:** Establishment of standards to support key security functions
  - Authentication (XUA and SAML)
  - Access control (TBD)
  - Transmission security (128 bit encryption, secure hashing algorithm [SHA-1] for transport of data)
  - Audit log and disclosure accounting data capture

- **Transport standards for HIE:** Establish communication protocols between systems
  - Common, predictable, secure (SOAP v2.1 or REST)

---

Timeline for EHR MU functionality

- **Stage 1:** Capture data in coded format; some functions and some reporting
- **Stage 2:** Expand exchange of information in the most structured format possible; population management; additional reporting requirements
- **Stage 3:** Focus on reporting quality for high priority conditions, patient self management, and access to comprehensive data
Meaningful Use (Federal Rule effective date TBD*, 2010)

- CMS and ONC have collaborated on the EHR standards and “use” criteria that will qualify providers and hospitals for reimbursement under ARRA EHR incentive program
- Hospitals and providers must use certified “EHR Systems” and/or “EHR Modules” to qualify for MU incentive funding
- To qualify for incentive funding, hospitals or providers must enter the program by 2014
- All hospitals and providers must comply by 2015 or have a percentage reduction in Medicare and Medicaid reimbursement
- Definitions for MU based on health outcome policy priorities
  - Improve quality, safety, and efficiency
  - Improve care coordination, population and public health
  - Engage patients and their families
  - Ensure privacy and security
- Reporting requirements and incentive criteria define discrete care goals in multiple areas
  - EHR objectives extend over four-year timeline to allow technology to be developed and users to adopt
  - Phased approach based on “initial use” date not calendar year
  - Measures identified to determine compliance for each objective
  - Separate goals and measures for providers and hospitals

* NPRM comments closure was 3/15/2010.
Tentative timeline for final rule publication is May 2010.

CMS Meaningful Use Overview

- Eligibility
  - Eligible hospitals can receive both Medicare and Medicaid incentives
  - Eligible professionals must choose between Medicare & Medicaid Incentives
  - Complex formulas for providers, some specialties and practice locations excluded from qualifying (e.g., hospital based specialties)
    - Incentive Calculations different for Fee-For-Service versus Medicare Advantage Organizations
  - Stage 1 criteria for being deemed “Meaningful User” of certified EHR
    - 25 objectives and measures for eligible professionals
    - 23 objectives and measures for eligible hospitals
    - Criteria for Stage 2 and Stage 3 to be defined through future rulemaking
- Reporting Mechanisms
  - Of the 25 objectives, 17 require attestation; 8 require data submission
  - In 2012, CMS expects eligible professionals and hospitals to report clinical quality metrics electronically while continuing to attest on measures tied to the MU requirements
EHR and MU Requirements and Issues

- ONC and CMS collaborated closely on proposed regulations
  - Ensure that EHR requirements would support CMS goals and measures
- Stage 1-3 EHR standards and MU qualifying criteria in tandem regarding system functionality, data exchange and reporting capabilities
- Proposed standards expand the definition of EHR (e.g., benefit eligibility checking and billing) beyond the clinical record to include practice management and operational functions.
- Stage 1 reporting over continuous 90 day period during 2011, but then must continue to use system ongoing from beginning of MU funding
- Must meet ALL objectives for Stage 1 to qualify for incentive funding
- Standards not defined in several areas yet (no standard defined for changes to clinical data, e.g., addenda or “summaries of care” documents for care transitions
- Some standards to be refined or revised based on Stage 1 experience
- Many questions about “Complete EHR” vs. “EHR Modules” and certification to meet MU
  - Certification of internally developed software (availability of certifying bodies and cost)

Privacy Enhancements that Impact the EHR

- New data breach rules and penalties now in effect
- New HIPAA enforcement penalties effective (2/17/11)
  - State Attorney General can now prosecute civilly under HIPAA (2/17/09)
- Changes to HIPAA disclosure accounting rules (1/1/11 or 1/1/14*)
  - “date dependent on EHR implementation date—before 1/1/09=1/2014; after 1/1/09=1/2011
  - Data collection for 3 year accounting requirement, including TPO
  - Required to disclose all Business Associate Agreements that access PHI
- Restrictions on certain disclosures and sale of PHI
  - Patient may request nondisclosure to health plan of any fully self paid treatment (2/17/10)
  - “Limited Data Sets” (minimum necessary) enhancements (8/17/10)
- Patient has right to obtain electronic copy of EHR (2/17/10)
  - Patient can direct provider to send directly to another person/entity
Compliance Life after EHR Implementation

Compliance Risks in Implementing an EHR...

**before you buy**

- Compliance risk profile based on type and complexity of systems
  - Clinical documentation and computerized physician order entry (CPOE) only versus integrated practice management system which includes clinical functions
  - Vendor needs to meet “meaningful use” criteria depending on application purpose and be certified to meet CMS expectations for functionality and interoperability

- Include compliance requirements in EHR vendor selection process
  - Partner with IT and business leadership at onset of project or initiative
  - Participate in software or system evaluation processes
  - Define requirements based on system functionality
    - Different risks for ambulatory or clinic settings versus hospitals or continuing care
  - Ask vendor for information on or validation of key application processes
    - Robustness and configurability of user and system security
    - Type of audit logs, information captured, system impact, ease of use
    - System support of cosignatures, e-signatures, authentication processes

  *“Bake compliance in, instead of brushing it on”*
Compliance Engagement for EHR...

*before you configure or install*

- All vendors have design sessions to craft workflows and make configuration decisions
  - Compliance personnel should be at the table from Day 1, providing compliance guidance on system design decisions
    - Consider a dedicated compliance resource for the EHR, at least through system implementation
  - Identify areas where there may be residual risk based on business decisions made
    - Example: No hard stop to require diagnosis association at time of ordering; what compensatory measures are in place to mitigate?
  - Request end-to-end workflow demonstrations of applications once configured to meet business needs
    - Review configuration testing output to ensure system outcomes are as expected and support compliance requirements

  “Bake compliance in, instead of brushing it on”

---

General Compliance Risk Areas for Evaluation of EHRs

The bigger the organization, the more complexity; the smaller the organization, the fewer the resources.

- Security settings/configuration; Security role classes/profile development; Change management
  - Too much access versus too restricted
  - Ease of monitoring system access (audit log volume)
  - Elevated access (programmers, application managers and coordinators)
  - Segregation of duties for organizations under Sarbanes-Oxley (SOX)
- Minimum necessary and scope of practice considerations
  - Dependent on system functions and security settings (user permissions and functionality)
  - Cross application security in integrated systems
- Source system feeds and interfaces (point-to-point or Simple Object Access Protocol [SOAP] for web services)
  - Ancillary systems (lab, imaging, pharmacy, dietary, respiratory)
  - Business process applications supporting key functions (finance, benefits, claims)
- Ongoing management of clinical content and system diagnosis and procedure files
- Change management processes for system changes
  - System upgrades, data loads, configuration, security settings or role based access permissions
- Hybrid records (paper and one or more electronic applications)
  - Interface and maintenance issues
  - Release of information (ROI)
  - “Legal Health Record”
Compliance Risks: Scheduling and Registration

- Patient identification validation
  - Master patient index
  - Search parameters and criteria
  - Who is permitted to create new charts?
- Forms and information
  - Key demographic information capture (required for MU)
  - Advance directives
  - Notice of privacy practices
  - "Important Information from Medicare"
- Coverage and benefits issues (required for MU)
  - Collect data on all insurers or responsible parties
  - Preauthorization
  - Advanced Beneficiary Notices (ABNs)
- Co-pays, deductibles, cost sharing collections
  - Many organizations collect this after the service is performed
- Physician supervision
  - MD onsite availability for midlevel practitioners scheduled to provide care

Compliance Risks: General Clinical Applications

- Security configuration and access monitoring
  - Role based provisioning
  - Access to functions is permissions driven and defined by business needs
  - Too much access = HIPAA risk
  - Too little access = potential patient safety or decreased operational efficiency
  - Access monitoring program (volume of transactions and resources to manage)
- Order entry (required for MU)
  - Medical necessity requirements
  - Scope of practice issues
  - Who orders what, sufficient documentation, authentication of orders
- Chart documentation (data integrity and authentication)
  - Who documents what
  - Cut and paste from previous encounter or different chart
  - Residents and midlevel practitioners proof of supervision
  - Encounter documentation and completion
    - Encounter closure logic (what data or information is required to close an encounter?)
    - Coding and billing for closed encounters only
    - Electronic Signatures and authentication of data
Compliance Risks: Ambulatory or Clinic Settings

- Computer assisted coding (Level of Service calculators, prospective mapping of ICD and CPT administrative codes)
- Order entry
  - Medical necessity
  - Who orders what (roles) and how documented in the system
- Encounter closure and completion of documentation
  - Timely encounter documentation completion
  - Diagnosis-order association
  - Electronic signatures
- EHR in-basket management
  - Patient data and info versus general communications
- Point of Care testing
  - Documentation requirements
- Configuration of non face-to-face encounters
  - E-mail or virtual encounters
    - Retaining patient centric communications
  - Telephone encounters
  - “Orders only” encounters

Compliance Risks: Inpatient settings

- Admission-Discharge-Transfer (ADT) (admission data required for MU)
  - Data capture, validation, synchronization processes
    - Ensure that all admissions have an order and admitting diagnosis
    - Emergency versus observation versus inpatient status
    - Reconciliation of discharge status between ADT and clinical documentation
- Specialty care modules
  - Emergency Department
    - Support EMTALA requirements
  - Intensive Care
    - Interfacing of monitoring and biomedical equipment
  - Surgical or anesthesia applications
    - Operative case scheduling
    - Procedure cards for surgical case setup
    - Documentation of time-out and key operative activities (sponge counts)
    - Pre-operative, intra-operative, and post-operative documentation
    - Medical device (implants) and surgical supplies information capture
  - Obstetrics
  - Oncology
    - Chemotherapy treatment plans and administration
- Hospital ancillary services integration (CPOE required for MU)
  - Lab, imaging, pharmacy, dietary, respiratory
Compliance Risks: Health Information Management

- Chart management tools sufficient to maintain chart and data integrity
  - Append
  - Amend
  - Redact
  - Misfile management, error correction, merge-unmerge of charts

- Release of Information (ROI)
  - Printing of legal EHR
  - Disclosure accounting (required for MU)
  - Patient requested and electronically available (required for MU)
  - Health Information Exchange (HIE)

- External document management
  - Health Information Exchange (HIE) (required for MU)
  - Outside medical records and correspondence

Compliance Risks: Administrative Coding

- Physician documentation and supervision of other practitioners
  - Coder-physician communications regarding diagnosis assignment
  - Appending or amending chart information once claims are submitted
  - “Incident to” services and physician supervision
  - Supervision of medical residents or midlevel practitioners (cosignatures and/or documentation)

- Charge capture and claims for services provided
  - Documentation complete and available to support coding of encounter and medical necessity
  - Feeds from all the clinical systems to ensure capture of all services to support downstream claims processes
  - Charges dropped with “results” not “orders”
  - Capture of “Never Events”, “Present on Admission” and “Hospital Acquired Conditions”
  - Bundling charges and/or global payments
    - Surgical services
    - Laboratory test panels
    - Dialysis (chronic renal failure)
  - Charge description master (CDM) current and validated
    - Often comprised of data from multiple system files
    - Provider information
    - Encounter information and place of service
    - Procedure and diagnosis files
  - Fee schedules
    - Linked to plans, groups, and/or benefits based on payor
Compliance Risks: Billing

- Synchronization of data across systems involved in end-to-end patient care and revenue cycle processes from registration through claims
  - Patient treatment and demographic data
  - Ancillary system data
  - Benefits information
  - Charge description master and fee schedules
  - Billing or claims data
- Site of Service appropriately identified *(impacts MU reporting for hospitals and providers)*
  - System facility and organization tables (“fac/org” for service location, department and/or specialty data)
- Claims scrubbers and charge routers
  - Ensure that rules are appropriately configured and data is synchronized
- Primacy of benefits
  - Coordination of benefits
  - Medicare Secondary Payer
- Denial management
  - Consider claims denial as a means to detect and mitigate upstream process failures
  - Root cause analysis and trending to improve performance and decrease risk
- Linkages to internal accounting systems and general ledgers

Compliance Risks: Support or Add-on Applications

- Reporting software or module *(extensive reporting required for MU)*
  - Access to reports with PHI should be role based
  - Ensure data can be classified by sensitivity
    - Chemical dependency
    - HIV or AIDS
    - Psychotherapy notes
  - Recommend report generation and access strategy be reviewed and/or approved by Privacy Officer.
- Utilization or case management *(CPOE for referrals for MU)*
- Access portals for patients, contract or affiliate providers
- Health Information Exchange (HIE) capability *(required for MU)*
Approaches to Evaluating Compliance

- **Audits** “Looking an inch wide and a mile deep”
  - Targeted scope
  - Structured
  - Methodical
  - Detailed and evidence driven
  - Desktop or on-site

- **Assessments** “Looking a mile wide and an inch deep”
  - Covers end-to-end review of application
  - Less formal
  - Ability to modify scope
  - Lower burden of proof (interviews and discussion/review of workflows)
  - Desktop review of documentation and policies, on-site interviews of key system and operational personnel

Methodology: Preparing for the Assessment

- **Know your target and do your homework**
  - What type of application?
  - What legal requirements are relevant?
  - What is the enforcement activity for prioritization of work?

- **Develop a tool to support your risk assessment work**
  - Create compliance objectives based on legal requirements
  - Include citations that support the objectives
  - Identify and document expected business practices necessary to meet compliance and monitor risk areas
Compliance Assessment Tool Sample

### Compliance Objective

- Medical record addenda (e.g., late entries, corrections of errors or clarifications in medical records) and physician queries and updates are appropriately documented.

### Expected Business Practices

- Documentation Standards policy should include legal addenda guidelines.
- System must be configured to maintain original medical record entry and show indication of addendum.
- Private orders use to query practitioners will be in accordance with legal guidance, and a contact documentation trail is captured.
- Process for updating medical records will reflect legal guidance on addenda to the medical record.
- Performance metrics and reporting guidelines should be developed to ensure addenda are documented appropriately.

### Observations and Findings

- Region has an addendum/release policy.
- Changes are reviewed to ensure that the addenda do not alter the coding and billing outcomes.
- HIM department will make corrections and add to the health record. HIM P&P documentation processes are available for downtime. HIM P&P for putting data back into the system post event.
- Coding Compliance, 2006, Inpatient Documentation and coding services training and guidance available to all staff in this area.
- Medical record documentation and coding queries form, Inpatient Documentation and coding services staff available for consultation.
- Reports available on key metrics and provided to leadership.

Resident physicians, non-physician practitioners and non-physician extended role providers are identified as such in the system. Regional policies related to audits and record retention are consistent with the National record retention and other policies.

- Each user must be identified by name and title when signing documentation.
- Security profiles should be created specific to resident physicians, nurse practitioners (NP), physician assistants (PA), certified nurse midwives (CNM), certified registered nurse anesthetists (CRNA) and other non-physician extended roles.
- The profiles should be consistent for all providers and practitioners in the same role with the same job functions.
- If appropriate (may vary by state) these profiles should require attending physician co-signature prior to closing an encounter or submitting a claim for services rendered.
- The system should provide the required audit and reporting functionality for audit and record retention.
- All medical records should be retained per policy and/or legal requirements.

### Methodology: Planning and Conducting an Assessment

- Engage appropriate leadership; provide background and purpose
  - Define date(s) for assessment activities with stakeholders input
- Engagement letter to leadership and stakeholders
  - Identify scope, process, timelines for onsite and desktop reviews
  - Request that operations and IT submit information requested in tool for desktop review
- Desktop review of documentation
  - Review of configuration, process, and workflow decisions
  - Review of pertinent policies and procedures around processes, legal, regulatory and documentation requirements
  - Review application level identity management, system configuration, and user role permissions
  - Partner with information security and other subject matter experts for technical expertise
- Onsite interviews
  - Include key IT, business, operational, clinical, and management personnel in interviews
  - Review tool objectives and validate information provided
  - Discuss areas where no information was provided
  - Discuss areas where controls are required and have not been identified
  - Discuss potential risks identified during desktop review
Methodology: Post-Assessment Activity and Follow-up

- Review preliminary findings and issues with leadership at end of on-site work
  - Exit conference
- Compile documentation to provide to leadership
  - Findings and observations draft document
    - Use tool to document findings in specific areas, and recommendations for mitigation of compliance risk
    - Includes information/analysis from desktop review and personnel and subject matter expert interviews
  - Executive summary and draft final report
    - Highlight of findings and compliance gaps
- Allow operations to input on findings/report accuracy before finalized
- Create corrective action plan (CAP) to mitigate identified risk areas
  - Define mitigation in collaboration with operations and leadership
  - Risk acceptance at right leadership level
  - Monitor CAP and close items as appropriate
  - Validate CAP completion through planned (future) audit activities
- Continue to monitor high-risk areas through establishment of ongoing measures and metrics reported to leadership

Compliance Risk Assessment: Summary

- Get involved from EHR project inception
- Identify legal requirements based on modules purchased or installed
  - Define controls and compliance requirements
- Partner with others where you do not have the subject matter expertise
- Get a seat at the table where decisions are made
  - Work with business and clinicians to ensure that configuration is done to ensure system workflows and output are compliant
  - Review data used to request any MU funding to ensure compliance with submission standards
- Perform assessments before implementation where possible
- Stay engaged and aware of enhancements post-implementation
- Target ongoing monitoring (metrics) and audit identified risk areas
- REMEMBER: The EHR is a tool to support the organization’s work, and is only as compliant as the configuration and workflows implemented
Conclusion: Links to Additional Information

EHR Interim Final Rule:

CMS Meaningful Use NPRM

Questions?? Thank you very much.
bobbi.bonnet@kp.org

Finally, a bit of nurse humor...