Meaningful Use Audit Process: Focus on Outcomes and Security

Phyllis A. Patrick, MBA, FACHE, CHC

The 22nd National HIPAA Summit

February 6, 2014

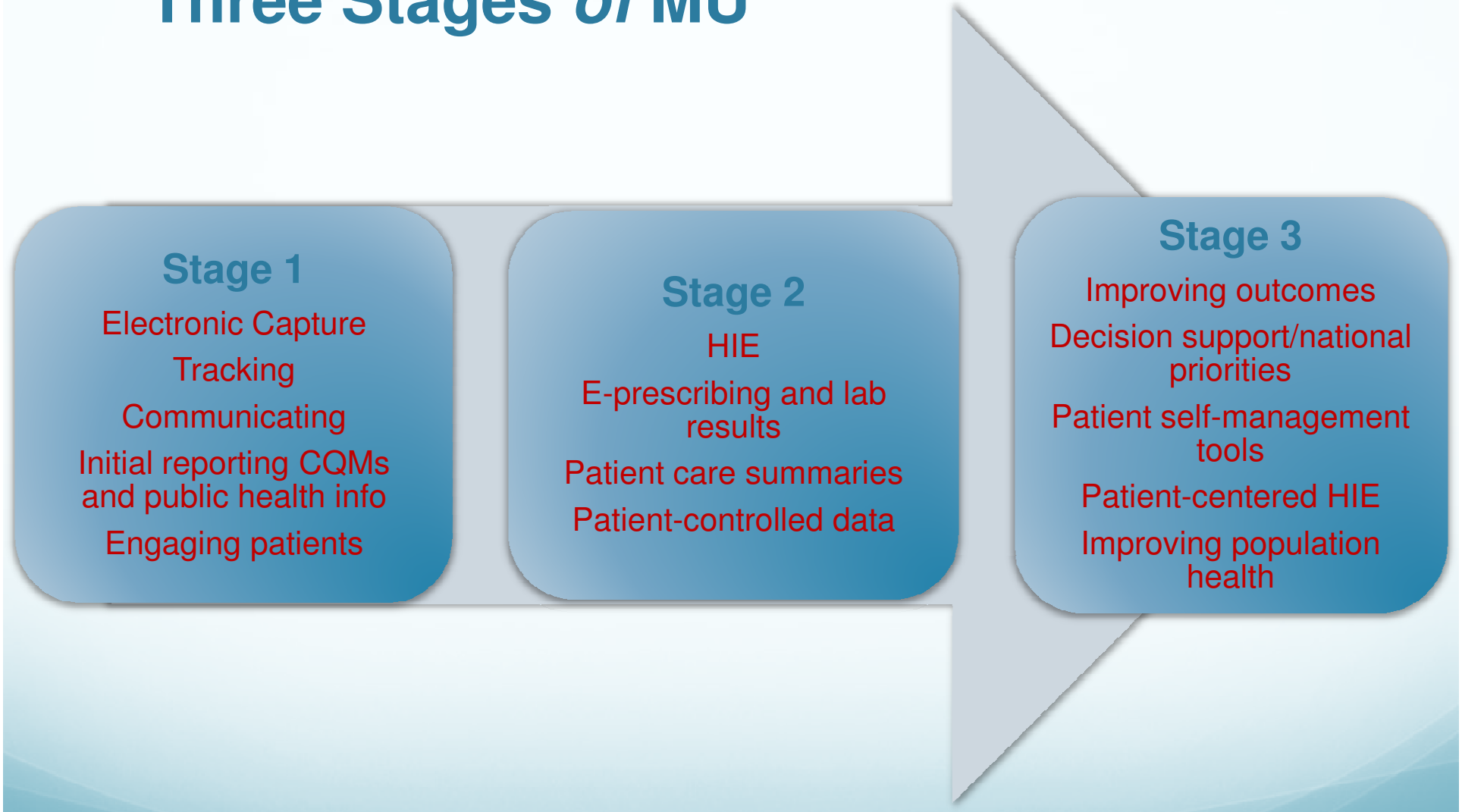
Topics

- Meaningful Use Refresher
- Meaningful Use and Outcomes Reporting: Alignment Initiatives
- Meaningful Use Stages 1, 2, and 3: Focus on Quality and Security
- Using Auditing to Improve Outcomes Reporting and Security Compliance

Meaningful Use Refresher

- CMS Goals
  - ✓ Improve Quality, Safety, Efficiency
  - ✓ Engage Patients & Families
  - ✓ Improve Care Coordination
  - ✓ Improve Public and Population Health
  - ✓ Ensure Privacy and Security for Personal Health Information
- Medicare and Medicaid (State) Incentive Programs
- MU is not a reimbursement program.
- MU was created to hasten adoption of EHR systems.
- Legislative Mandate: HITECH - 2009

Three Stages *of* MU



MU Refresher (Cont'd)

- Eligible Hospitals and Eligible Professionals must begin by 2014 (Medicare) and 2016 (Medicaid)
- Medicare payment adjustments/reductions, beginning 2015, for failing to demonstrate MU
- Core Set and Menu Set Objectives
  - ✓ CQMs required as core objective in Stage 1
  - ✓ CQMs must be reported in Stage 2 to meet MU
  - ✓ Security Risk Analysis required Stages 1, 2, 3
  - ✓ Security Risk Analysis, implementation of updates as necessary

EHR Implementation Life Cycle

National Learning Consortium

Clinical/Quality/IT Partnership

Clinical Quality Measures (CQMs)

- Tools that help CMS to measure and track quality of healthcare services provided by eligible professionals and eligible hospitals.
- Use data associated with a provider's ability to deliver high-quality care or relate to long term goals for health care quality.
- Include many aspects of patient care:
  - ✓ health outcomes
  - ✓ clinical processes
  - ✓ patient safety
  - ✓ efficient use of healthcare resources
  - ✓ care coordination
  - ✓ patient engagement
  - ✓ population and public health
  - ✓ clinical guidelines

PQRS EHR Incentive Pilot

- 2013 Physician Quality Reporting System (PQRS) Medicare Electronic Health Record (EHR) Incentive Pilot.
- Allows eligible professionals to meet clinical quality measure (CQM) reporting objective of meaningful use requirements for the Medicare EHR Incentive Program while also reporting for the PQRS program.
- EPs who wish to participate in the electronic reporting pilot must submit 12 months of CQM data, between January 1, 2014 and February 28, 2014.

Alignment Initiatives

- The clinical quality measures (CQMs) included in the EHR Incentive Program align with measures used in other Federal quality initiatives.
- CQMs are aggregated to measure and improve quality of providers, health plans, and state-funded medical program, e.g., Medicaid and Children's Health Insurance Program (CHIP).
- **CMS Goal: Harmonize all quality reporting programs with EHR electronic reporting.**

Alignment Initiatives (Cont'd)

- Clinical Quality Measures (CQMs) are an integral component of CMS' strategy to understand and improve quality of health care for beneficiaries.
- Quality initiatives are used by CMS in quality improvement, public reporting, and pay-for-reporting programs.
- CMS view is that "EHRs assist in collection of data that has direct correlation to the future of reimbursement and quality of healthcare processes". [HealthIT.gov]
- CMS objective is for providers to achieve MU with CQMs.

Example: Alignment Initiatives

- **Quality Reporting Alignment at CMS for Eligible Hospitals**
  - 2013:
    - ✓ Hospital Value-Based Purchasing (HVBP) aligned with Inpatient Quality Reporting (IQR) Program
    - ✓ CQMs reported *on Hospital Compare*
  - 2014:
    - ✓ EHR-based reporting by IQR
  - 2014 +:
    - ✓ EHR-based reporting in EHR Incentive Program and to IQR and other hospital reporting programs
- HIMSS Recommendation to Congress (9/13): Alignment of Healthcare Quality Reporting Requirements Across Federal Programs

Focus on Quality and Security

- Stage 2 goals focus on ensuring that the meaningful use of EHRs supports the priorities of the National Quality Strategy.
  - ✓ Use of Health IT for continuous quality improvement at point of care.
  - ✓ Exchange of information in a structured format.
- Health Information Exchange requirements:
  - ✓ E-prescribing becomes more demanding.
  - ✓ Structured lab results need to be incorporated.
  - ✓ Electronic transmission of patient care summaries to support transitions in care across unaffiliated providers settings and EHR systems.
- **INFORMATION FOLLOWS THE PATIENT.**

Review of Security Requirements

45 CFR 164.308(a)(1)

- MU Core Measure 15 (Eligible Professionals)
- **Objective** - Protect ePHI created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
- **Measure** - Conduct or review a security risk analysis in accordance with the Security Rule; implement security updates as necessary, and correct identified security deficiencies as part of a risk management process. The Entity must attest to this.
- **Exclusion** - None

Security Requirements (Cont'd)

- Must attest YES to having conducted **or** reviewed a security risk analysis in accordance with requirements under 45 CFR 164.308(a)(1).
- Must implement updates as necessary, at least once prior to end of the EHR reporting period, and attest to that conduct or review.
- Testing could occur prior to beginning of the first EHR reporting period.
- **But**, a new review would have to occur for each subsequent reporting period.

Security Requirements (Cont'd)

- Security update required if any security deficiencies were identified during the risk analysis, e.g.
  - ✓ Updated software for certified EHR technology to be implemented as soon as available
  - ✓ Changes in workflow processes or storage methods
  - ✓ Any other necessary corrective action that needs to be implemented in order to eliminate the security deficiency or deficiencies identified in the risk analysis
- Security risk analysis seems to cause trouble for professionals and hospitals.
- Requirement links to compliance with HIPAA Security Rule.

Auditing, Outcomes Reporting, and Security

Final Statement in Attestation

"I certify that the foregoing information is true, accurate and complete. I understand that the Medicare/Medicaid EHR incentive program payment I requested will be paid from Federal Funds, that by filing this … claim for Federal Funds, and the use of any false claims, statements, or documents, or the concealment of a material fact used to obtain Medicare/Medicaid EHR incentive program payment, may be prosecuted under Federal or State criminal laws and may also be subject to civil penalties."

Documentation

- EPs and EHs should print and retain every document they rely on when attesting to Meaningful Use after the close of each reporting period:
  - ✓ Often these documents cannot be reproduced by the EHR system
  - ✓ Time limits to respond to audits are very short
- Primary documentation requested in audits is **source document(s)** that provider/hospital used when attesting.
- Documentation should provide summary of data that supports information entered for attestation.

Documentation (Cont'd)

- Documentation must support each measure to which the EP/EH has attested, including any exclusions claimed.
- Types of documentation:
  - ✓ Screenshots
  - ✓ Letter/Email from receiving provider confirming exchange of key clinical information (date of exchange, names of providers, test successful YES/NO)
  - ✓ Security Risk Analysis/Risk Mitigation Plans
  - ✓ Immunization Registries data submission
  - ✓ Reportable Lab Results – e.g., to Public Health Agencies (Screenshots, Letter/Email from agency confirming receipt, data, names of parties, test successful YES/NO)

Documentation (Cont'd)

- Required for pre- and post-payment audits
- Must support meaningful use and clinical quality measure data that is submitted.
- All source material (paper and electronic) must be saved for at least 6 years from attestation.
- If using hospital cost report data, follow data retention policies and process.
- Documentation must support payment calculations (hospitals).
- Reports must come directly from the certified EHR system/modules.
- Don't rely on your vendor for documentation!

CMS Audits

- "This letter is to inform you that your practice has been selected by the CMS for an audit of your meaningful use of certified EHR technology for the attestation period. Attached to this letter is an information request list. Be aware that this list may not be all-inclusive and that we may request additional information necessary to complete the audit."

Audit Process

- Initial request letter (sample on CMS web site)
- Letter is sent electronically by Figliozzi and Company
- On-site review may occur
  - ✓ EP/EH may be required to demonstrate how the EHR system meets the meaningful use criteria
- Audit Determination Letter
  - ✓ Will document success in meeting the MU audit or
  - ✓ Recoupment of payment

Compliance Checklist

- Make sure that a Security Risk Analysis was conducted, a remediation plan developed, remediation occurred, remediation was **documented**. Plan of Action with administrative, physical, technical safeguards; organizational requirements and **documentation**.
- Document ongoing RA/RM processes and changes.
- Save all:
  - ✓ Attestation supporting **documentation**
  - ✓ CQM **documentation**
  - ✓ Payment calculation **documentation**
- Verify that incentive payments were accurate (possible over-payments or under-payments).

Compliance Checklist (Cont'd)

- Maintain all **documentation** for at least 6 years.
- Review all supporting **documentation** for attestations, reporting of CQMs, payment verification, etc. ***BEFORE*** any audit request.
- If contractor was used for Attestation process, review supporting **documentation** on a regular basis**. Ask questions**.
- Make sure you have all **documentation**.

Compliance Checklist - Vendors

- What is your vendor's EHR CHPL certification number?
- Can your vendor provide documentation for the EP/EH describing how to achieve each core measure, menu set measure, and clinical quality measures in the EHR?
- Has the vendor developed dashboard that you can use to show threshold status over time for each measure (core, menu set, CQMs)?
- How does the vendor support the EP/EH achieving MU?

Vendor Support: Security Compliance Checklist

- Auto logoff
- Authentication
- Passwords
- Data backup and storage
- Risk Analysis and Risk Mitigation
- Physical Security Safeguards
- Data Integrity
- Audit Trails

Vendor Security Compliance (Cont'd)

- Vendor security policies and procedures
- Access Control – EP/EH users, vendor access
- Automated Security Controls/Turn-on/Turn-off
- Technical Testing Schedule
- Emergency procedures
- Breach Notification Policy and Procedures
- SSAE16
- Other Assurances

MU Auditing Approaches

- **Documentation**: Is there an automated repository? Who is responsible? Is information easy to retrieve?
- **Process Testing**: How do you meet criteria over time, under different conditions, etc.? Have you found vulnerabilities in EHR? Have you tested data integrity?
- **Financial Reporting**: Can you trace the funds through the financial statements?
- **Governance Process for MU**: What is structure of team? How are decisions made, documented? Is process interdisciplinary?
- **Outcomes Reporting**: Have you reviewed for consistency with quality performance and outcomes reporting processes? How is the Quality Office involved?

MU Auditing Approaches (Cont'd)

- **Security Auditing of EHR Vendor(s)**: Do vendor security policies uphold compliance with Security Rule? Has vendor supplied certification documentation? Can you verify the security functionality of the EHR system? Are IT controls turned on and working properly? Have you tested key security provisions of the system?
- **Application Auditing and Testing**: How have upgrades affected compliance with MU, documentation requirements, security? Is training adequate? How are test plans deployed?
- The organization is responsible for assuring and documenting MU measures, not the vendor!
- Get all stakeholders involved (IT, Compliance, Privacy, Informatics, Quality/Performance Improvement, Clinical Staff, IT, Security, HIM, Finance, Internal Audit, etc).

Effective Auditing Adds Value

- MU is a dynamic, ongoing program and process!
- Conduct focused audits and use results to improve the MU Program
  - ✓ Preparation for Stages 2 and 3
  - ✓ Vendor preparedness/EHR Upgrade process/Vendor documentation
  - ✓ EHR Training Programs
  - ✓ Patient Volume Verification – MU documentation vs. patient census and billing data, other reporting requirements for same periods
  - ✓ Physician Practice documentation of MU funds, attestation process, security risk analysis, etc.
  - ✓ Risk analysis/risk mitigation → Security Program improvements

Resources

- EHR Meaningful Use Specification Sheet for Eligible Professionals – Clinical Quality Measures,
- OIG," CMS and Its Contractors Have Adopted Few Program Integrity Practices To Address Vulnerabilities in EHRs", OEI-01-00571, January 7, 2014. http://hhs.gov/oei/reorts/oei-01-11-00571.asp
- http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/EducationalMaterials.html - Educational Resources
- http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentivePrograms - EHR Incentive Program Information
- http://ushik.ahrq.gov/mdr/portals/mu - US Health Information Knowledge Base (USHIK) for Clinical Quality Measurement
- Phyllis Patrick, "The Meaningful Use Program: Auditing Challenges and Opportunities," New Perspectives, Association of Healthcare Auditors, Spring 2013.

PHYLLIS PATRICK + Associates

Security | Privacy | Culture

phyllis@phyllispatrick.com

914-696-3622

www.phyllispatrick.com