


Privacy and Security: Meaningful Use in Healthcare Organizations



Phyllis A. Patrick, MBA, FACHE, CHC

July 20, 2011

Webinar Essentials

1. Session is currently being recorded, and will be available on our website at <http://www.utsystem.edu/compliance/SWCAcademy.html>
2. Attendees are currently muted. If you wish to ask a question please click on the “Raise Hand” button . The webinar administrator will un-mute you at the appropriate time.
3. Be careful of turning down speaker volume to avoid feedback.
4. Questions may also be typed in the GoToWebinar *Question* panel.
5. CPE credit is available for this webinar for attendees who attend the live webinar. Please request credit by sending an email to the SWC Office at systemwidecomp@utsystem.edu.
6. Please provide your feedback in the post-session survey.

Agenda

- Overview of the Meaningful Use Program and Basic Requirements
- Meeting the MU Requirements for Privacy and Security Risk Analysis
- The Changing Role of the Privacy and Security Officer

The Vision for Health Care Reform

- Health Care will be:
 - Patient-centered
 - Evidence-based
 - Prevention-oriented
 - Efficient
 - Equitable
- Not “investments in technology, but efforts to improve health of Americans and performance of their health care system.”



Key Players

CMS – Centers for Medicare & Medicaid Services

- Responsible for establishing the EHR Incentive program through formal rule making
- The rule provides many of the parameters and requirements for the Medicare & Medicaid EHR Incentive Programs

ONC - The Office of the National Coordinator for HIT

- Resource for the entire health system to support the adoption of Health Information Technology (HIT) and the promotion of nationwide Health Information Exchange (HIE) to improve health care

OCR – Office for Civil Rights

- Responsible for HIPAA Enforcement (Privacy & Security)

Basics of Meaningful Use

- Defining Meaningful Use
- Benefits of Electronic Health Records (EHRs)
- Goals for Meaningful Use
- Incentive Programs (Medicare & Medicaid)
- Eligibility for MU Funds
- Certification of EHRs
- Application and Attestation Processes
- The Stages of Meaningful Use
- Criteria: Core and Menu Sets
- Timeline for Meaningful Use
- Financial Oversight/Combating Fraud and Abuse

Defining Meaningful Use

To be considered a meaningful user EHR user, the following requirements must be met:

- Use of certified EHR technology in a meaningful manner (e.g. e-prescribing)
- Use of certified EHR technology for electronic exchange of health information to improve the quality of healthcare, such as promoting care coordination
- Use of certified EHR technology to submit Clinical Quality Measures (CQM) and other measures in a form & manner specified by the Secretary of HHS

CMS Goals for Meaningful Use



1. Improve **quality, safety, and efficiency** of health care and reduce health disparities
2. **Engage patients and families**
3. Improve **care coordination**
4. Improve **population and public health**, and
5. Ensure **adequate privacy and security protections** for personal health information.

Incentive Money for Meaningful Use

Medicare EHR Program

- ✓ Began in FY 2011
- ✓ EPs may receive up to \$44,000 over 5 years, plus incentive if in HSPA
- ✓ Must begin by 2012 to get maximum
- ✓ Incentives for hospitals include \$2 million base payment
- ✓ Medicare EPs, hospitals and CAHs who do not show meaningful use have payment decreases beginning 2015

Medicaid EHR Program

- ✓ State Programs
- ✓ Begins in FY 2011
- ✓ EPs may receive up to \$63,750 over 6 years
- ✓ Incentives for hospitals may begin in 2011, depending on state
- ✓ No payment adjustment for providers who do not show meaningful use

Who is Eligible?

- Eligible professionals (EPs)
- Eligible hospitals
- Critical access hospitals
- Certain Medicare Advantage Organizations whose affiliated EPs and hospitals are meaningful users of certified EHR technology
- Eligible parties must be **meaningful users of certified EHR technology** (Medicare)
- Eligible parties must adopt, implement, upgrade or demonstrate meaningful use in first year of participation, and show meaningful use for up to 5 remaining years (Medicaid)

Certification of EHR: BASICS of the Process

1. Focus certification on Meaningful Use
2. Leverage the certification process to improve progress on privacy, security, and interoperability
3. Improve the objectivity and transparency of the certification process
4. Expand certification to include a range of software sources, e.g., open source, self-developed, etc.
5. Develop a certification transition (short-term to long-term)

Privacy and Security: Consistent themes throughout regulations and guidance.

Certification Criteria

- HIT Policy Committee determined areas where standards, implementation specifications, and certification criteria are needed
- Process and analysis likely to occur on a periodic basis
- Priority order of standards, implementation specifications, and certification criteria, communicated to the HIT Standards Committee to guide its work
- Work groups: MU, Certification/Adoption, Information Exchange, NHIN, Strategic Plan, Privacy & Security Policy, Enrollment, Governance, Quality Measures, Tiger Teams

Certification Priorities

- Technologies that protect the privacy of health information and promote security
- Nationwide health information technology infrastructure
- Utilization of individual certified electronic health record
- Technologies that, as a part of a qualified electronic health record, allow for accounting of disclosures

Certification Priorities (Cont'd)

- Use of certified electronic health records to improve the quality of health care
- Technologies that allow individually identifiable health information to be rendered unusable, unreadable, or indecipherable to unauthorized individuals
- Use of electronic systems to ensure the comprehensive collection of patient demographic data
- Technologies that address the needs of children and other vulnerable populations

How do I know if My System or EHR Module is Certified?

- Check healthit.hhs.gov, ONC or CCHIT web sites for certification status of vendors/systems
- Temporary certification program sunsets 12/31/11 or when permanent program is ready
- ONC approved the American National Standards Institute (ANSI) as the ONC-Approved Accreditor (AA) for the Permanent Certification Program (June, 2011)
- To date, more than 800 EHR products approved

Application Process: Registration and Attestation

- Requirements for Eligible Hospitals and Eligible Providers:
 - ✓ National Provider Identifier (NPI)
 - ✓ National Plan and Provider Enumeration System (NPPES)
 - ✓ Provider Enrollment, Chain and Ownership System (PECOS)
- Registration started January 3, 2011
- Attestation process started April 4, 2011
- **Attestation required:**
 - “... demonstrated meaningful use of certified EHR technology during the EHR reporting period”
 - “...**documented evidence of a recent risk analysis, findings of the analysis, and subsequent implementation of updates and corrections**”

Three Stages of Meaningful Use

Stage 1:

- ✓ Electronically capture information in a structured format
- ✓ Use information to track key clinical conditions
- ✓ Communicate information for care coordination
- ✓ Implement clinical decision support tools
- ✓ Use EHRs to engage patients and families
- ✓ Report clinical quality measures and public health information.

Three Stages of Meaningful Use

Stage 2:

- ✓ Use HIT for continuous quality improvement at the point of care
- ✓ Exchange information in the most structured format possible (HIE capabilities)
- ✓ Transmit patient care summaries across unaffiliated providers, settings, and EHR systems
- ✓ More requirements for e-prescribing and structured test results

Three Stages of Meaningful Use

Stage 3:

- ✓ Promote improvements in quality, safety, and efficiency
→ improved health outcomes
- ✓ Focus on decision support for national high priority conditions
- ✓ Provide patient access through self-management tools
- ✓ Provide access to comprehensive patient data (patient-centered information exchange)
- ✓ Improve population health

Stage 1 Measures

- Core Measures
 - Eligible Professionals
 - Eligible Hospitals
- Menu Set Objectives
 - Eligible Professionals
 - Eligible Hospitals

Menu Set Objectives: Eligible Hospitals

- Drug-formulary checks
- Record advanced directives for patients 65 years or older
- Incorporate clinical lab test results as structured data
- Generate lists of patients by specific conditions
- Use certified EHR technology to identify patient-specific education resources and provide to patient, if appropriate
- Medication reconciliation
- Summary of care record for each transition of care/referrals
- Capability to submit electronic data to immunization registries/systems*
- Capability to provide electronic submission of reportable lab results to public health agencies*
- Capability to provide electronic syndromic surveillance data to public health agencies*

* At least 1 public health objective must be selected

Menu Set Objectives: Eligible Professionals

- Drug-formulary checks
- Incorporate clinical lab test results as structured data
- Generate lists of patients by specific conditions
- Send reminders to patients per patient preference for preventive/follow up care
- Provide patients with timely electronic access to their health information
- Use certified EHR technology to identify patient-specific education resources and provide to patient, if appropriate
- Medication reconciliation
- Summary of care record for each transition of care/referrals
- Capability to submit electronic data to immunization registries/systems*
- Capability to provide electronic syndromic surveillance data to public health agencies*

* At least 1 public health objective must be selected

Meaningful Use Timeline

- October 1, 2010 - Reporting year begins for eligible hospitals and CAHs.
- January 1, 2011 – Reporting year begins for eligible professionals
- January 3, 2011 – Registration for the Medicare EHR Incentive Program begins
- January 3, 2011 – For Medicaid providers, states may launch their programs if they so choose
- April 2011 – Attestation for the Medicare EHR Incentive Program begins
- May 2011 – EHR Incentive Payments begin
- July 3, 2011 – Last day for eligible hospitals to begin their 90-day reporting period to demonstrate meaningful use for the Medicare EHR Incentive Program
- September 30, 2011 - Last day of the federal fiscal year. Reporting year ends for eligible hospitals and CAHs

Meaningful Use Timeline (Cont'd)

- October 1, 2011 – Last day for eligible professionals to begin their 90-day reporting period for calendar year 2011 for the Medicare EHR Incentive Program
- November 30, 2011 – Last day for eligible hospitals and critical access hospitals to register and attest to receive an Incentive Payment for Federal fiscal year (FY) 2011
- December 31, 2011 – Reporting year ends for eligible professionals.
- February 29, 2012 – Last day for eligible professionals to register and attest to receive an Incentive Payment for calendar year (CY) 2011

STAGE 2 Proposed MU Objectives

- In addition to taking Stage 1 objectives and measures further, Stage 2 (proposed) introduces the following new items:
 - 30% of visits have at least one electronic EP note
 - 30% of EH patient days have at least one electronic note by a physician, NP, or PA
 - 30% of EH medication orders automatically tracked via electronic medication administration recording

EP – Eligible Professional; EH – Eligible Hospital

STAGE 2 Proposed (Cont'd)

- Additional NEW measures:
 - 80% of patients offered ability to view and download via web-based portal, within 36 hrs of discharge, relevant information contained in the record about EH inpatient encounters. Data available in human-readable and structured forms
 - EPs – online secure patient messaging in use
 - Patient preferences for communication medium recorded for 20% of patients

EP – Eligible Professional; EH – Eligible Hospital

STAGE 2 Proposed (Cont'd)

- Additional NEW measures:
 - List of care team members (including PCP) available for 10% of patients in EHR
 - Record a longitudinal care plan for 20% of patients with high priority health conditions
- **NOTE: Stage 2 may be delayed until 2014, for providers registering and attesting in FY 2012.**

Source: HIT Policy Committee, January, 2011

Financial Oversight – Combating Fraud and Abuse

- Health care reform law includes 32 sections on program integrity and health care fraud, e.g.,
 - Improper hospital-physician relationships
 - CMS self-disclosure process for Stark-only violations
 - Enhanced protections for whistleblowers
 - Right of private action in HIPAA privacy cases

NCHICA White Paper

“Privacy and Security Implications of Meaningful Use for Health Care Providers”

October, 2010

<http://www.nchica.org/About/PressReleases.htm>

Recommendations for AMCs

1. Review existing governance of privacy and security programs.
2. Implement effective security and privacy governance processes.
3. Include security and privacy as primary components of the organization's strategic planning process.
4. Enhance internal controls for compliance with privacy and security requirements (federal and state).

Recommendations (Cont'd)

5. Conduct regular evaluations and audits of compliance with HIPAA/HITECH. Understand the gaps and prioritize improvement efforts.
6. Develop an ongoing and documented process for evaluating privacy and security programs.
7. Include privacy and security risk assessment in enterprise-wide risk assessment and management processes.
8. Develop new and enhanced training programs for all levels of the organization.

HITECH: Catalyst for Information Security Compliance



- Have you fully implemented the HIPAA Security Rule?
- How do HITECH and Meaningful Use impact this?
- What do you need to do to meet the Evaluation and Risk Assessment requirements?

HIPAA Security Rule effective since April, 2005; Privacy Rule since April, 2003.

HIPAA Security Rule

Evaluation Standard

Perform a periodic technical and non-technical evaluation, based initially upon the standards and implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.”
[§ 164.308(a)(8)]

Related Standards

- Security Management Process
§ 164.308(a)(1)(i)
- Risk Analysis
§ 164.308(a)(1)(ii)(A)
- Risk Management
§ 164.308(a)(1)(ii)(B)
- Information System Activity Review
§ 164.308(a)(1)(ii)(D)

Assessing Your Program

- Governance of the Privacy and Security Programs
- Privacy Rule and Security Rule Standards
- Policies and Procedures
- Risk Assessment and RA Management
- Program Infrastructure
 - Designation of Privacy and Security Officers
 - Reporting Relationships
 - Staffing and Resources
- Education and Training Programs
- Security Breach Notification Policy and Procedures
- Readiness to meet HITECH/HIPAA requirements and Meaningful Use criteria
- Impacts of Business Partner/Business Associate Relationships
- Auditing and Monitoring Processes

Hot Topics:

Information Security and Privacy

- Security Awareness Training for ALL levels of the organization (Ongoing, updated, interesting, engaging)
- Auditing and Monitoring Program (Account Management, Access)
- Risk Assessment integrated with organization-wide risk assessment processes
- Portable Media
- Encryption
- Physical Security
- Disclosure of sensitive information through Social Media
- Cyber-Insurance
- Vendor Management
- Cloud Computing
- Virtualization

Role of AMCs in Health Information Exchange



- ✓ Defining Health Information Exchange
- ✓ Goals of HIEs
- ✓ Hot Topics for HIEs
- ✓ Regional Extension Centers

Health Information Exchanges

- “. . . the mobilization of health care information electronically across organizations within a region, community or hospital system”, according to nationally recognized standards
- Goals: to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care
- Useful to Public Health authorities to assist in analyses of the health of the population

HIEs: Hot Topics

- Rules on access to PHI/Consenting Processes
- Rules on Accounting of Disclosures
- Security Issues
- New challenges emerging related to federal policy and governance of health information exchanges
- Secondary use of data
- Sustainability

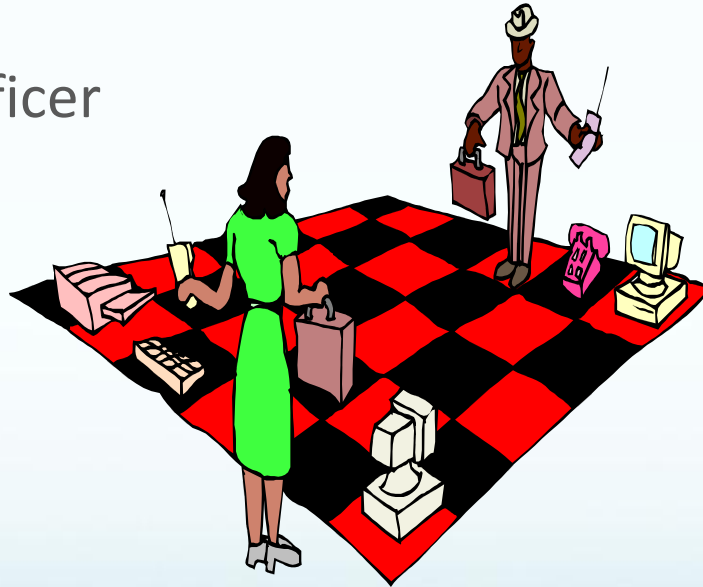


Regional Extension Centers

- Funded under HITECH
- Total of 60 RECs in US, based on state population
- Mandate to support primary care physicians in moving towards electronic health record adoption, and meaningful use of EHR
- Vendor selection process is key to RECs meeting community needs
- Receive assistance from the Health Information Technology Research Center
- To be evaluated every two years to determine if continued support is merited

New and Changing Roles

- Security Officer
- Privacy Officer
- Compliance Officer



The Early Days

- Roles generally created since 2003/2005, in response to HIPAA Privacy & Security Rules
- Responsibilities often combined with existing roles (HIM Director, Compliance Officer, CIO, IT Network Director, etc.)
- Security often viewed as IT function – information protection through technical controls
- Generally not senior positions
- Program developments, metrics, etc, often not reported to Board or B-level committee

Recommendations

- Re-evaluate roles and responsibilities of Privacy and Security Officers
- Elevate positions to senior leaders, with enhanced responsibility for strategic planning and participation in regional activities (HIEs)
- Officers should regularly report on status of programs to senior leaders and to Board, including B-level committee responsible for compliance, risk, audit oversight
- Establish formal, mandatory annual training in privacy and security risks for senior leaders and Board members

Recommendations (Cont'd)

- Consider establishing a B-level Risk Committee charged with enterprise-wide risk assessment and management, including privacy and security risks. Committee should be separate from Board Audit Committee
- Include privacy and security in job descriptions and evaluations of management at all levels



Recommendations (Cont'd)

- Conduct annual evaluations of privacy and security programs and ongoing compliance assessments (administrative, technical, physical safeguards, documentation practices)
- Seek to establish and provide concrete assurance of strategic and comprehensive privacy and security programs that incorporate managerial, operational, and technical controls
- View privacy and security as a patient satisfaction issue



Compliance and Privacy Implications of Meaningful Use

- Governance
- Role of Compliance and Privacy Officers in EHR selection and implementation
- Role of Compliance and Privacy Officers in Meaningful Use strategy and processes
- Data Exchange and Coordinated Care in the Context of Compliance, Privacy and Security
- Development and growth of Health Information Exchange (HIE) across regions, states, country

Integrating Meaningful Use with Your Compliance Program

- Fraud and Abuse potential – False Claims Act
- OCR Audit Program
- HIE Developments
 - Participation by Compliance, Privacy, and Security Officers
 - HIE Policies will affect organizational policies (e.g., consenting, notice of privacy practices, breach notification and remediation, patient and user access, patient portals, etc.)

Resources

- “Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis”, ONC White Paper
 - * *Paper includes Appendices on State laws and State models.*
- “Data Segmentation In Electronic Health Information Exchange: Policy Considerations and Analysis,” ONC White Paper
- North Carolina Health Information Communications Alliance, Inc. (NCHICA.org) web site and resources
- Health Information Security and Privacy Collaboration (HISPC) Reports on State Law, Business Practices, and Policy Variations

**PHYLLIS
PATRICK**
+ Associates

Culture | Security | Privacy

Phyllis A. Patrick, MBA, FACHE, CHC
Phyllis A. Patrick & Associates LLC

www.phyllispatrick.com
phyllis@phyllispatrick.com

914-696-3622