Does HIPAA Satisfy Meaningful Use Requirements?

Tod Ferran, CISSP, QSA
Help organizations comply with mandates, avoid security breaches, and prevent data theft since 2000.
Background
Meaningful Use Alphabet Soup

- CMS (Centers for Medicare & Medicaid Services)
- EHR (Electronic Health Record)
- CEHRT (Certified EHR Technology)
- CQMs (Clinical Quality Measures)
- EP & EH (Eligible Professional & Eligible Hospital)
- NQS Domains (National Quality Strategy)
Quick Overview of Meaningful Use

• Government incentives to implement and use CEHRT

• Core objectives
  – **Stage 1** – Conduct Risk Analysis (2011/2012 not necessarily HIPAA)
  – **Stage 2** – Protect ePHI (HIPAA)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>2012</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>2013</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>2014</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>2015</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>2016</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>3</td>
</tr>
</tbody>
</table>
Overview of MU Requirements (EP)

- Core measures
  - Stage 1 = 13
  - Stage 2 = 17

- Menu measures
  - Stage 1 = 5 of 10
  - Stage 2 = 3 of 6

- 64 clinical quality measures
  - Stage 1 and 2 = 9 of 64
<table>
<thead>
<tr>
<th>#</th>
<th>Measure Information</th>
<th>Measure Values</th>
</tr>
</thead>
</table>
| 11 | **Objective:** Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, or outreach.  
**Measure:** Generate at least one report listing patients of the EP with a specific condition.  
**Note:** This measure only requires a yes/no answer. |
|    | Numerator: N/A       | ☐ YES ☐ NO      |
|    | Denominator: N/A     |                |
| 12 | **Objective:** Use clinically relevant information to identify patients who should receive reminders for preventive/follow-up care and send these patients the reminders, per patient preference.  
**Measure:** More than 10 percent of all unique patients who have had 2 or more office visits with the EP within the 24 months before the beginning of the EHR reporting period were sent a reminder, per patient preference when available.  
**Exclusion:** Any EP who has had no office visits in the 24 months before the EHR reporting period. |
|    | Does this exclusion apply to you? | Yes ☐ No ☐ |
|    | Numerator: Number of patients in the denominator who were sent a reminder per patient preference when available during the EHR reporting period. |                |
|    | Denominator: Number of unique patients who have had two or more office visits with the EP in the 24 months prior to the beginning of the EHR reporting period. |                |
| 13 | **Objective:** Use clinically relevant information from Certified EHR Technology to identify patient-specific education resources and provide those resources to the patient.  
**Measure:** Patient-specific education resources identified by Certified EHR Technology are provided to patients for more than 10 percent of all unique patients with office visits seen by the EP during the EHR reporting period.  
**Exclusion:** Any EP who has no office visits during the EHR reporting period. |
|    | Does this exclusion apply to you? | Yes ☐ No ☐ |
|    | Numerator: Number of patients in the denominator who were |                |
• Medicare (run by CMS) payments if you start MU in
  – 2011 = $43,720
  – 2012 = $43,480
  – 2013 = $38,220
  – 2014 = $23,520

• Medicaid (individual states) payments
  – Year 1 = $21,250 (as late as 2016)
  – Max payout = $63,750
• Medicare (run by CMS)
  – Initial amount
    • < 1,150 discharges = base $2,000,000
    • Base $200 per discharge from 1,150
      up to a maximum payout of $6,370,400
  – Medicare share formula
    • # of IP Part A Bed Days + # of IP Part C Days
    Total IP Bed Days x [ Total Charges - Charges Attributable to
      Charity Care Total Charges ] IP=inpatient
  – Transition factor (from .25 to 1.0)
How Are You Doing?

- If you have a HIPAA compliance program, you’re already doing one core requirement for Meaningful Use.
- If not, this is a great time to start a HIPAA program
  - Kill two birds with one stone!
Does MU Make Sense For Me?

- Incentive payments
- Reduced Medicaid/Medicare payments
  - 1% to 5%
- 2011 to 2012
  - 17% reduction in MU participants
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional is not subject to the payment adjustment for the e-Rx in 2014</td>
<td>99%</td>
<td>98%</td>
<td>97%</td>
<td>96%</td>
<td>95%</td>
<td>95%</td>
</tr>
<tr>
<td>Professional is subject to the payment adjustment for the e-Rx in 2014</td>
<td>98%</td>
<td>98%</td>
<td>97%</td>
<td>96%</td>
<td>95%</td>
<td>95%</td>
</tr>
</tbody>
</table>
Overlap with HIPAA
Risk Analysis: M/U and HIPAA

- Concerned with identifying potential security risks
- Require Risk Management Plan
  - Risks to PHI are measured, ranked and prioritized
  - Show demonstrable progress on RMP
M/U Risk Analysis
• Only concerned with the risk of the EHR
• Only required for those participating in M/U
• Updated twice (Stage 1 and Stage 2 reporting)

HIPAA Risk Analysis
• Concerned with the entire PHI environment (e.g., EHR, email, etc.)
• Required of all CE’s & BA’s
• Reviewed and updated on a periodic basis (annually)
Common Questions

- Will M/U attestation count for HIPAA compliance?
- Will HIPAA compliance count for M/U attestation?
- Will my M/U risk analysis cover my HIPAA risk analysis?
- Will my HIPAA risk analysis cover my M/U risk analysis?
Risk Management Process

• Both M/U and HIPAA require you to correct security problems as part of your risk management process
  – What if this was your HIPAA Risk Management Plan?
M/U Stage 1 Requirements

• **2011-2012**
  “Conduct or review a security risk assessment of a certified EHR technology, and correct identified security deficiencies and provide security updates as part of an ongoing risk management process.”

• **2014**
  “Protect electronic health information created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical capabilities.”
M/U Stage 2 Requirements

• 2014

“Protect electronic health information created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical capabilities.”

“…including addressing the encryption/security of data stored in CEHRT…”
M/U Stage 3 Requirements

• 2016/2017
  – Final requirements unknown for now
Reporting Challenges

• Both Stage 1 and Stage 2 = Single check box – Yes / No
  – Tip of the iceberg is an understatement
Requirements to “Yes”

- HIPAA compliance
  - Assign Privacy and Security Officials
  - Conduct ‘complete and thorough’ Risk Analysis
    - Use outside resources
    - Apply industry best practices
  - Show demonstrable progress on Risk Management Plan
    - Prioritize RMP based on security and risk
  - Perform assessment of compliance with Security, Breach, and Privacy rules of HIPAA
    - OCR audit protocol – Consider outside resources
Understanding Security
Compliance vs. Security

- Compliant does not necessarily equal secure
- Understand what and why we are attacked
  - ID theft, Rx, and provision of health care
Importance of Securing PHI

- Bad PR
- Fines
- Loss of trust
- Patient health and patient safety
Recent Breaches

Horizon Blue Cross Blue Shield of New Jersey
Advocate Medical Group
Inspiring medicine. Changing lives.
AHMC Healthcare Inc
Adventist Health System
Anthem

Federal law enforcement says 1,000’s more
Bad PR

VA Healthcare Data Breach Exposes Info of 7000 Veterans
HealthITSecurity.com - Dec 29, 2014
The Department of Veterans Affairs (VA) experienced yet another healthcare breach, as it announced last week that approximately 7,000 veterans'...
Contractor's security flaw causes yet another VA breach
PierceHealthIT - Dec 29, 2014
Explore in depth (3 more articles)

UMass Memorial Medical Group announces potential insider breach
BY ADAM GREENBERG FEBRUARY 02, 2015
A former UMass Memorial Medical Group employee may have accessed patient information outside of normal job duties.

Anthem hack exposes data on 80 million; experts warn of identity theft

California dentist announces theft of server containing patient information

Boston Children's Hospital to Pay $40K Over Data Breach Allegations
December 19, 2014
Is HHS the only shark smelling blood in the water?
Civil Lawsuits

- Stanford, CA
  - BA passed 20k name/diagnosis codes to subcontractor to graph
  - Subcontractor posted online, looking for help
  - $4.1M civil lawsuit settlement

- AvMed, FL
  - Lost laptops
  - $3M class action settlement

- Bryne vs. Avery Center
  - Released her medical records without authorization
  - Negligence based on HIPAA as the ‘Standard of Care’
State Attorney Generals

• Kaiser Foundation
  – Delay of breach notification
  – $150K to California AG

• Triple-S Salud
  – Displayed Medicare numbers on mailings
  – $6.8M to Puerto Rico Health Insurance Administration
FTC

- GMR Transcription
  - Failed to adequately monitor compliance of BA
  - 20k records, $ unknown

- LabMD
  - Inadequate security
  - $ unknown, company shut down

- FTC fines up to $16,000/violation
- GMR fine could reach $320M
Loss of Trust

• 2013 – Average breach
  – $2.0M over two years (Ponemon)
  – >2k records compromised

• Patient loss if breached
  – 46% Insurance co
  – 42% Drug store
  – 40% Doctor/dentist
  – 35% Hospital
Patient Health/Safety

- $19k and 12 months to clean up identity theft
- Non-perishable data
  - SSN
  - DOB
  - Name
- Misdiagnosis or mistreatment
- $359/record
Summary

• MU and HIPAA – Distinctly separate
  – MU is optional (Sort of)
    • Reduced payments of 1% to 5%
  – HIPAA is not optional

• HIPAA compliance = ‘best practice’
  – Negligence and malpractice
Questions?

tod@securitymetrics.com
Thank you for your attendance!

Get your questions answered on PMI’s Discussion Forum: http://www.pmimd.com/pmiForums/rules.asp