Modified Stage 2 Meaningful Use:
Objective #1 – Protect Electronic Health Information

July 5, 2016

Today's presenter:

Al Wroblewski, PCMH CCE, Client Services Relationship Manager

MeHI
MASSACHUSETTS eHEALTH INSTITUTE
at the MassTech Collaborative

Disclaimer

This presentation was current at the time it was presented, published or uploaded onto the web. This presentation was prepared as a service to the public and is not intended to grant rights or impose obligations. This presentation may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage attendees to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

Reminder

The attestation deadline for Program Year 2015 is

August 14, 2016

Agenda

- What is Meaningful Use (MU) Objective #1 all about?
- Steps to meet MU Objective #1

    1. Do the right thing
    2. Follow the process
    3. Conduct a thorough assessment or review
    4. Follow-up with appropriate actions
    5. Create and retain supporting documentation

- Attesting for MU Objective #1
- Common Issues
- Questions and Answers

What is MU Objective #1 all about?

MeHI
MASSACHUSETTS eHEALTH INSTITUTE
at the MassTech Collaborative

What is MU Objective #1 all about?

What is MU Objective #1 all about?

Protect Patient Health Information	
Objective	Protect electronic health information created or maintained by the CEHRT through the implementation of appropriate technical capabilities.
Measure	Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.
Exclusion	No exclusion.

What is MU Objective #1 all about?

Protect Patient Health Information - Additional Information

- Conduct or review a SRA
  - Encryption/security of data
  - Create mitigation plan
  - Implement updates
  - A minimum of once/year
  - Attest to conducting analysis

- Redo after upgrades
  - Cover entire EHR reporting period
  - Updates/deficiencies addressed demonstrating that corrections were made consistent with risk management process

What is MU Objective #1 all about?

Protect Patient Health Information - Additional Information

- Conduct during program year and before attestation
- Does not go beyond HIPAA Security Rule
- HHS Office for Civil Rights (OCR) has issued guidance on doing a SRA in accordance with HIPAA
- Free tools are available; no single required format

Steps to meet MU Objective #1

MeHI
MASSACHUSETTS eHEALTH INSTITUTE
at the MassTech Collaborative

Meeting MU Objective #1

1. Do the right thing

"Protect electronic health information created or maintained by the CEHRT through the implementation of appropriate technical capabilities."

- Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.

Meeting MU Objective #1

2. Follow the process

Meeting MU Objective #1

3. Conduct a thorough assessment or review covering all five of the key security areas for all locations identifying threats, vulnerabilities, risks and deficiencies:

    i. Physical safeguards
    ii. Administrative safeguard
    iii. Technical safeguards
    iv. Policies & procedures
    v. Organizational requirements

Meeting MU Objective #1

4. Follow-up and implement appropriate actions

    a) Assign responsibility for next steps
    b) Create and stick to timeline
    c) Document everything
    d) Demonstrate decision-maker commitment to and involvement in the process

Meeting MU Objective #1

5. Create and retain supporting documentation

    a) For attestation
    b) For audit purposes
    c) For internal use

Attesting for MU Objective #1

MeHI
MASSACHUSETTS eHEALTH INSTITUTE
at the MassTech Collaborative

Attesting for MU Objective #1

Objective:	Protect electronic health information created or maintained by the Certified EHR Technology (CEHRT) through the implementation of appropriate technical capabilities.
Measure:	Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by Certified EHR Technology in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306 (d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.

*Did you meet this measure?

○ Yes ○ No

If 'Yes', please enter the following information:

Date (MM/DD/YYYY): _____

Name and Title (Person who conducted or reviewed the security risk analysis): _____

Attesting for MU Objective #1

- Upload supporting documentation

1. SRA/R cover sheet attesting to the truthfulness and accuracy of the SRA/R

2. An SRA/R for every location where EP practiced
   a) Name of practice
   b) Location
   c) Date completed
   d) Signed
   e) List name and title of person who did SRA/R

Common Issues

Common Issues: Objective #1

Some common issues encountered with Objective #1

Common Issues: Objective #1

- Who should do it?
- Doesn't the EHR vendor already do this?
- There is no standardized format or set of questions
- Our system is totally secure --- we have no issues
- We can't afford to do an SRA/R
- We're a very small practice, why do we have to do this?
- We're a very large practice, why do we have to do this?
- Isn't this a duplication of HIPAA?
- When ePHI is shared electronically, who is liable for breaches?
- EP works for more than our organization and we cannot get the SRA from the other organization
- SRA not integrated into a risk management process

Questions

Questions?

Helpful Links

- CMS 2015 Program Requirements page
- MeHI Medicaid EHR Incentive Program page
- MeHI 2015 Supporting Documentation Requirements Guide
- HHS OCR HIPAA Guidance
- Risk Assessment Tool

Contact Us

MeHI
MASSACHUSETTS eHEALTH INSTITUTE

at the MassTech Collaborative

mehi.masstech.org

1.855.MassEHR

ehealth@masstech.org

Follow us @MassEHealth

Thomas Bennett
Client Services Relationship Manager
(508) 870-0312, ext. 403
tbennett@masstech.org

Brendan Gallagher
Client Services Relationship Manager
(508) 870-0312, ext. 387
gallagher@masstech.org

Al Wroblewski, PCMH CCE
Client Services Relationship Manager
(508) 870-0312, ext. 603
wroblewski@masstech.org

MeHI MASSACHUSETTS eHEALTH INSTITUTE at the MassTech Collaborative