Meaningful Use Objective: Protect Health Information

Florida Medicaid Promoting Interoperability Program

Kim Davis-Allen,
Outreach Coordinator

May 10, 2019

Program Year 2019 – Basics

All providers have a minimum 90 day EHR reporting period

All providers attest to Stage 3 requirements

Providers must have 2015 certified technology

Clinical Quality Measures (CQMs): First time attesting to Meaningful Use (MU): 90 days

2nd or later years: Full year reporting

Must report one outcome or priority CQM

Stage 3 Meaningful Use Objectives

- Protect Electronic Protected Health Information (ePHI)
- Electronic Prescribing
- Clinical Decision Support (CDS)
- Computerized Provider Order Entry (CPOE)
- Patient Electronic Access to Health Information
- Coordination of Care through Patient Engagement
- Health Information Exchange
- Public Health and Clinical Data Registry Reporting

https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/TableofContents_EP_Medicaid_2019.pdf

Protect Patient Health Information

Objective:

Protect ePHI created or maintained by the certified electronic health record technology (CEHRT) through the implementation of appropriate technical, administrative, and physical safeguards.

Protect Patient Health Information

Measure:

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

Protect Patient Health Information

The security risk analysis requirement under 45 CFR 164.308(a)(1) must assess:

- The potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization creates, receives, maintains, or transmits.
- This includes ePHI in all forms of electronic media, such as:
  - ✓ Hard drives
  - ✓ Floppy disks
  - ✓ CDs
  - ✓ DVDs
  - ✓ Smart cards or other storage devices
  - ✓ Personal digital assistants
  - ✓ Transmission media, or
  - ✓ Portable electronic media

- HHS Office for Civil Rights (OCR) has issued guidance on conducting a security risk analysis in accordance with the HIPAA Security Rule: http://www.hhs.gov/hipaa/forprofessionals/security/guidance/guidance-risk-analysis/index.html.
- The Office of the National Coordinator for Health Information Technology (ONC) and OCR developed a free Security Risk Assessment (SRA) Tool to assist EPs: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.

Protect Patient Health Information

Additional Information:

- EPs must conduct or review a security risk analysis of CEHRT, including addressing encryption/security of data, implement updates as necessary at least once each calendar year, and attest to conducting the analysis or review
  - Can be done before, during or after the EHR reporting period but must be within the calendar year.

- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each EHR reporting period. Any security updates and deficiencies that are identified should be included in the EP's risk management process and implemented or corrected as dictated by that process.

No Exclusion

Contacts and Resources

Florida Medicaid Incentive Program
Promoting Interoperability

www.ahca.myflorida.com/medicaid/ehr

MedicaidHIT@AHCA.MyFlorida.com

Call Center 1.855.231.5472

FLORIDA
HIE SERVICES

www.Florida-HIE.net

FLHII@ahca.myflorida.com

E-FORCSE
Electronic-Florida Online Reporting of Controlled Substances Evaluation

Erika.Marshall@flhealth.gov
www.e-forcse.com

FloridaHealthFinder.gov
Connecting Florida with Health Care Information

http://www.floridahealthfinder.gov/index.html

Connect with us through Social Media:

https://www.facebook.com/AHCAFlorida

@AHCA_FL