2019 MEDICARE PROMOTING INTEROPERABILITY PROGRAM FOR ELIGIBLE HOSPITALS AND CRITICAL ACCESS HOSPITALS SECURITY RISK ANALYSIS FACT SHEET

Overview

On August 2, 2018, the Centers for Medicare & Medicaid Services (CMS) released the Fiscal Year 2019 Inpatient Prospective Payment System for Acute Care Hospitals and Longer-term Care Hospital Prospective Payment System Final Rule. In the rule, CMS continued its overhaul of the Medicare Promoting Interoperability Program to continue the following:

- Advancing certified electronic health record technology (CEHRT) utilization
- Reducing burden
- Improving interoperability and patient access to health information

The rule finalized a new performance-based scoring methodology with a smaller set of four objectives:

1. Electronic Prescribing
2. Health Information Exchange
3. Provider to Patient Exchange
4. Public Health and Clinical Data Exchange

Security Risk Analysis Requirement

In 2019, the **Security Risk Analysis** measure will remain a requirement of the Medicare Promoting Interoperability Program as it is imperative in ensuring the safe delivery of patient health data. This measure is not part of the new scoring methodology and does not contribute any points to the hospital's total score for the four objectives and measures.

Beginning in 2019, eligible hospitals and CAHs must attest that they completed the actions included in the Security Risk Analysis measure at some point during the calendar year in which the EHR reporting period occurs to successfully participate in the program.

Objective: Protect electronic protected health information (ePHI) 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 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 eligible hospital's or CAH's risk management process.

Additional Information

- Eligible hospitals and CAHs must conduct or review a security risk analysis of CEHRT including addressing encryption/security of data, and implement updates as necessary at least once each calendar year and attest to conducting the analysis or review.
- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each Promoting Interoperability reporting period. Any security updates and deficiencies that are identified should be included in the eligible hospital or CAHs risk management process and implemented or corrected as dictated by that process.
- It is acceptable for the security risk analysis to be conducted outside the Promoting Interoperability reporting period; however, the analysis must be unique for each Promoting Interoperability reporting period, the scope must include the full Promoting Interoperability reporting period and must be conducted within the calendar year of the Promoting Interoperability reporting period (January 1st – December 31st).
- 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.
- At a minimum, eligible hospitals or CAHs should be able to show a plan for correcting or mitigating deficiencies and that steps are being taken to implement that plan.
- The parameters of the security risk analysis are defined in 45 CFR 164.308(a)(1), which was created by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Meaningful use does not impose new or expanded requirements on the HIPAA Security Rule, nor does it require specific use of every certification and standard that is included in certification of EHR technology. More information on the HIPAA Security Rule can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.
- 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/for-professionals/security/guidance/guidance-risk-analysis/index.html.
- Additional free tools and resources available to assist eligible hospitals or CAHs include a Security Risk Assessment (SRA) Tool developed by the Office of National Coordinator for Health Information Technology (ONC) and OCR: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.

Additional Resources

For more information on Medicare Promoting Interoperability Program requirements for 2019, visit:

- Promoting Interoperability Programs Landing page
- 2019 Medicare Promoting Interoperability Program Requirements webpage
- FY 2019 IPPS and Medicare Promoting Interoperability Program Overview Fact Sheet
- 2019 Medicare Specification Sheets
- Medicare Promoting Interoperability Program Stage 3 Security Risk Analysis Specification Sheet for Eligible Hospitals, CAHs, and Dual-Eligible Hospitals