2020 Medicare Promoting Interoperability Program for Eligible Hospitals and Critical Access Hospitals Security Risk Analysis Fact Sheet

Overview

On August 16, 2019 the Centers for Medicare & Medicaid Services (CMS) released the Fiscal Year 2020 Inpatient Prospective Payment System for Acute Care Hospitals and Longer-term Care Hospital Prospective Payment System Final Rule. In the rule, CMS continued its focus on the advancement of certified electronic health record technology (CEHRT) utilization, burden reduction, and improving interoperability and patient access to health information for the Medicare Promoting Interoperability Program for eligible hospitals and critical access hospitals (CAHs).

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 electronic health record (EHR) 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 EHR reporting period; however, the analysis must be unique for each EHR reporting period, the scope must include the full EHR reporting period and must be conducted within the calendar year of the EHR 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 CEHRT. 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 2020, visit:

- Promoting Interoperability Programs Landing page
- 2020 Medicare Promoting Interoperability Program Requirements webpage
- FY 2020 Medicare Promoting Interoperability Program Overview Fact Sheet
- 2020 Medicare Specification Sheets