ELIGIBLE HOSPITALS AND CRITICAL ACCESS HOSPITALS OBJECTIVES AND MEASURES FOR THE 2024 EHR REPORTING PERIOD

The following information is for eligible hospitals and critical access hospitals (CAHs) attesting to CMS for their participation in the Medicare Promoting Interoperability Program in calendar year (CY) 2024.

Objective	Protect Patient Health Information
Measure	**Security Risk Analysis:** 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 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the provider's risk management process. Actions included in the security risk analysis measure may occur any time during the calendar year in which the EHR reporting period occurs.

Definition of Terms

N/A

Reporting Requirements

- YES/NO Attestation
    - To meet this measure, eligible hospitals and critical access hospitals participating in the Promoting Interoperability Program must attest YES to conducting or reviewing a security risk analysis at any point during CY 2024.

Scoring Information

- For CY 2024, this attestation is required, but the attestation response will not be scored.
    - Score: **N/A**

- *Reminder:* In order to earn a score greater than zero, an eligible hospital or CAH must complete the activities required by the Security Risk Analysis and SAFER Guides measures, submit their complete numerator and denominator or Yes/No data for all required measures, submit their level of

engagement for the Public Health and Clinical Exchange measures, attest to the Actions to limit or restrict the compatibility or interoperability of CEHRT statement, and the ONC Direct Review attestation, as well as report on the required electronic clinical quality measure data.

Additional 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.
- 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 eligible hospital or CAHs risk management process and implemented or corrected as dictated by that process.
- 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 https://www.hhs.gov/hipaa/for-professionals/security/index.html.

Regulatory References

- For further discussion, please see 83 FR 41634 through 41677.

Certification Criteria

Below are the corresponding certification criteria for EHR technology that support this measure.

Certification Criteria
No 2015 health IT certification criteria at this time.