Medicare Promoting Interoperability
PROGRAM

MEDICARE PROMOTING INTEROPERABILITY PROGRAM SECURITY RISK ANALYSIS MEASURE, SAFER GUIDES MEASURE, AND PREVENTION OF INFORMATION BLOCKING ATTESTATION FACT SHEET

Overview

The Centers for Medicare & Medicaid Services (CMS) is continuing its focus on the advancement of certified electronic health record (EHR) technology (CEHRT) utilization, and improving interoperability and patient access to health information for the Medicare Promoting Interoperability Program for eligible hospitals and critical access hospitals (CAHs).

For CY 2022, CMS is requiring Medicare Promoting Interoperability Program participants to attest to the following:

- **Security Risk Analysis** measure
- **Safety Assurance Factors for EHR Resilience (SAFER) Guides** measure
- **Actions to limit or restrict the compatibility or interoperability of CEHRT** attestation

Security Risk Analysis Measure

The Security Risk Analysis measure continues to remain a requirement of the Medicare Promoting Interoperability Program as it is imperative in ensuring the safe delivery of patient health data.

Eligible hospitals and CAHs must attest that they completed or reviewed 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.

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 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 Tool developed by the Office of National Coordinator for Health Information Technology and OCR: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

SAFER Guides Measure

As part of the FY 2022 Hospital Inpatient Prospective Payment Systems (IPPS) for Acute Care Hospital and Long-Term Care Hospital (LTCH) Prospective Payment System (PPS) Final Rule, CMS added the SAFER Guides measure to the Protect Patient Health Information objective, which will support the Medicare Promoting Interoperability Program's goals of improved EHR use and healthcare quality.

Eligible hospitals and CAHs will be required to submit one "yes/no" attestation statement for completing an annual self-assessment using all nine SAFER Guides (available at https://www.healthit.gov/topic/safety/safer-guides) during the calendar year in which their EHR reporting period occurs. Please see the below graphic from the *Journal of the American Medical Association* for additional guidance on completing the SAFER Guides assessment.[1]

Additional Information:

- To complete each self-assessment, participants are expected to fill out the checklist and practice worksheet at the beginning of each guide.
- For CY 2022, this attestation will be required, but the "yes" or "no" attestation response will not affect participants' total score for the Program. An organization does not have to confirm that it has implemented "fully in all areas" each practice described in a particular SAFER guide, nor will an organization be scored on how many of the practices the organization has fully implemented.
- For more information and direction on how to complete the SAFER Guides assessment, please see the following article from *JAMA Network*:
  - Guidelines for US Hospitals and Clinicians on Assessment of Electronic Health Record Safety Using SAFER Guides *(Note: This article can only be accessed via subscription)*

Actions to limit or restrict the compatibility or interoperability of CEHRT

To prevent actions that block the exchange of health information, the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) requires eligible hospitals and CAHs that participate in the Medicare Promoting Interoperability Program to show that they have not knowingly and willfully limited or restricted the compatibility or interoperability of their CEHRT.

Eligible hospitals and CAHs are required to show that they are meeting this requirement by attesting to the **Actions to limit or restrict the compatibility or interoperability of CEHRT** statement about how they implement and use CEHRT.

Additional Information:

- The **Actions to limit or restrict the compatibility or interoperability of CEHRT** has one statement based on section 106(b)(2) of MACRA about how health care providers implement and use CEHRT: *A health care provider must attest that they did not*

[1] https://jamanetwork.com/journals/jama/article-abstract/2788984#:~:text=The%20SAFER%20Guides%20are%20proactive,a%20safe%20and%20effective%20manner.

knowingly and willfully take action (such as to disable functionality) to limit or restrict the compatibility or interoperability of CEHRT.

- In order to submit an attestation, you have to act in good faith when you implement and use your CEHRT to exchange electronic health information. This includes working
- with technology developers and others who build CEHRT to make sure the technology is used correctly and is connected (and enabled) to meet applicable standards and laws.
- You must also ensure that your organizational policies and workflows are enabled and do not restrict the CEHRT's functionality in any way. For example, if your CEHRT gives patients access to their electronic health information or exchanges information with other health care providers, your practice must use these capabilities.
- You do not have to provide documentation to show you have acted in good faith to implement and use your CEHRT to support the appropriate exchange of electronic health information.

For More Information

- 2022 Medicare Promoting Interoperability Program Requirements
- ONC 21st Century Cures Act Final Rule
- 2022 CEHRT Requirements