

Eligible Professional EHR Incentive Program Objectives and Measures for 2016 Objective 9 of 10

Date updated: February 4, 2016

| Secure Electronic Messaging | |
|-----------------------------|--|
| Objective | Use secure electronic messaging to communicate with patients on relevant health information. |
| Measures | For an EHR reporting period in 2016, for at least 1 patient seen by the EP during the EHR reporting period, a secure message was sent using the electronic messaging function of CEHRT to the patient (or the patient-authorized representative), or in response to a secure message sent by the patient (or the patient-authorized representative) during the EHR reporting period. |
| Exclusion | Any EP who has no office visits during the EHR reporting period; or any EP who conducts 50 percent or more of his or her patient encounters in a county that does not have 50 percent or more of its housing units with 4Mbps broadband availability according to the latest information available from the FCC on the first day of the EHR reporting period. |

Table of Contents

- Definitions of Terms
- Attestation Requirements
- Additional Information
- Regulatory References
- Certification and Standards Criteria

Definitions of Terms

Secure Message – Any electronic communication between a provider and patient that ensures only those parties can access the communication. This electronic message could be email or the electronic messaging function of a PHR, an online patient portal, or any other electronic means.

Fully Enabled - The function is fully installed, any security measures are fully enabled, and the function is readily available for patient use.

Attestation Requirements

NUMERATOR/DENOMINATOR/EXCLUSION

- DENOMINATOR: Number of unique patients seen by the EP during the EHR reporting period.
- NUMERATOR: The number of patients in the denominator for whom a secure electronic message is sent to the patient (or patient-authorized representative), or in response to a secure message sent by the patient (or patient-authorized representative).
- THRESHOLD: The numerator and denominator must be reported, and the numerator must be equal to or greater than 1.
- EXCLUSION: Any EP who has no office visits during the EHR reporting period; or any EP who conducts 50 percent or more of his or her patient encounters in a county that does not have 50



percent or more of its housing units with 4Mbps broadband availability according to the latest information available from the FCC on the first day of the EHR reporting period.

Additional Information

- The thresholds for this measure increase over time between to allow providers to work incrementally toward a high goal. This is consistent with our past policy in the program to establish incremental change from basic to advanced use and increased thresholds over time. The measure threshold for this objective was “fully enabled” for 2015, and is at least one patient for 2016, and a threshold of 5 percent for 2017 to build toward the Stage 3 threshold.
- Provider initiated action and interactions with a patient-authorized representative, are acceptable for the measure and are included in the numerator.
- A patient-initiated message would only count toward the numerator if the provider responds to the patient.
- The action for the numerator must occur within the calendar year but may occur before, during, or after the EHR reporting period if that period is less than one full calendar year.

Regulatory References

- This objective may be found in Section 42 of the code of the federal register at 495.22 (e)(9)(i). For further discussion please see [80 FR 62816](#).
- In order to meet this objective and measure, an EP must use the capabilities and standards of CEHRT at 45 CFR 170.314(e)(3).

Certification and Standards Criteria

Below is the corresponding certification and standards criteria for electronic health record technology that supports achieving the meaningful use of this objective.

| Certification Criteria* | |
|---|---|
| § 170.314(e)(3) Secure messaging | Enable a user to electronically send messages to, and receive messages from, a patient in a manner that ensures: <ul style="list-style-type: none"> (i) Both the patient (or authorized representative) and EHR technology user are authenticated; and (ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f). |

**Depending on the type of certification issued to the EHR technology, it will also have been certified to the certification criterion adopted at 45 CFR 170.314 (g)(1), (g)(2), or both, in order to assist in the calculation of this meaningful use measure.*

| Standards Criteria | |
|---|--|
| § 170.210(f) Encryption and hashing of electronic health information | Any encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the FIPS Publication 140-2 (incorporated by reference in § 170.299.) |