Use Secure Electronic Messaging	
Objective	Use secure electronic messaging to communicate with patients on relevant health information.
Measure	A secure message was sent using the electronic messaging function of CEHRT by more than 5 percent of unique patients (or their authorized representatives) seen by the EP 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 3Mbps broadband availability according to the latest information available from the FCC on the first day of the EHR reporting period.

Table of Contents

- Definition of Terms
- Attestation Requirements
- Additional Information
- Certification and Standards Criteria

Definition 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.

Attestation Requirements

DENOMINATOR/NUMERATOR/ THRESHOLD/EXCLUSION

- DENOMINATOR: Number of unique patients seen by the EP during the EHR reporting period.
- NUMERATOR: The number of patients or patient-authorized representatives in the denominator who send a secure electronic message to the EP that is received using the electronic messaging function of CEHRT during the EHR reporting period.
- THRESHOLD: The resulting percentage must be more than 5 percent in order for an EP to meet this measure.
- 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 3Mbps broadband availability according to the latest information available from the FCC on the first day of the EHR reporting period.

Additional Information

- An EP or staff member could decide that a follow-up telephone call or office visit is more appropriate to address the concerns raised in the electronic message.
- There is not an expectation that the EP must personally respond to electronic messages to the patient.
- 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: (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.)