Secure Electronic Messaging	
Objective	Use secure electronic messaging to communicate with patients on relevant health information.
Measure	For a Promoting Interoperability (PI) reporting period in 2018, for more than 5 percent of unique patients seen by the eligible professional (EP) during the PI reporting period, a secure message was sent using the electronic messaging function of certified electronic health record technology (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 PI reporting period.
Exclusion	Any EP who has no office visits during the PI 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 Federal Communications Commission (FCC) on the first day of the PI reporting period.

Table of Contents

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 public health record, 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

YES/NO/EXCLUSION

- DENOMINATOR: Number of unique patients seen by the EP during the PI 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 resulting percentage must be more than 5 percent in order for an EP to meet this measure.
- EXCLUSIONS: Any EP who has no office visits during the PI 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 PI reporting period.

Additional Information

- The thresholds for this measure have increased over time 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, was at least one patient for 2016, and is 5 percent for 2017 and 2018 to build toward the Stage 3 threshold.
- This measure includes provider-initiated communications (when a provider sends a message to a patient or the patient's authorized representatives), and provider-to-provider communications if the patient is included. A provider can only count messages in the numerator when the provider participates in the communication (e.g. any patient-initiated communication only if the provider responds to the patient.) Note: Providers are not required to respond to every message received if no response is necessary.
- The EP action may occur before, during, or after the PI reporting period. However, in order to count in the numerator, it must occur within the PI reporting period if that period is a full calendar year, or if it is less than a full calendar year, within the calendar year in which the PI reporting period occurs.

Regulatory References

- This objective may be found in Section 42 of the code of the federal register at 495.22 (e)(9)(i) and (ii). 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 Standards and Criteria

Below is the corresponding certification and standards criteria for EHR 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).

Note: 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 PI 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.)