Proposed Meaningful Use Stage 2 Regulations and Security
From http://www.ofr.gov/OFRUpload/OFRData/2012-04443_PI.pdf
Posted to Office of the Federal Register February 23, 2012

42 CFR §495.6 Meaningful use objectives and measures for EPs, eligible hospitals, and CAHs.
(j)(16) and (17) EPs
(l)(15) hospitals & CAHs

(j)(16) and (l)15) on Risk Analysis

Proposed Objective: Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.

Protecting electronic health information is essential to all other aspects of meaningful use. Unintended and/or unlawful disclosures of personal health information could diminish consumers' confidence in EHRs and electronic health information exchange. Ensuring that health information is adequately protected and secured will assist in addressing the unique risks and challenges that may be presented by electronic health records.

Proposed Measure: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.

This measure is the same as in Stage 1 except that we specifically address the encryption/security of data is that is stored in Certified EHR Technology (data at rest). Due to the number of breaches reported to HHS involving lost or stolen devices, the HIT Policy Committee recommended specifically highlighting the importance of an entity's reviewing its encryption practices as part of its risk analysis. We agree that this is an area of security that appears to need specific focus. Recent HHS analysis of reported breaches indicates that almost 40 percent of large breaches involve lost or stolen devices.

Had these devices been encrypted, their data would have been secured. It is for these reasons that we specifically call out this element of the requirements under 45 CFR 164.308(a)(1) for the meaningful use measure. We do not propose to change the HIPAA Security Rule requirements, or require any more than would be required under HIPAA. We only emphasize the importance of an EP or hospital including in its security risk analysis an assessment of the reasonable and appropriateness of encrypting electronic protected health information as a means of securing it, and where it is not reasonable and appropriate, the adoption of an equivalent alternative measure.

We propose this measure because the implementation of Certified EHR Technology has privacy and security implications under 45 CFR 164.308(a)(1). A review must be conducted for each EHR reporting period and any security updates and deficiencies that are identified should be included in the provider's risk management process and implemented or corrected as dictated by that process.

We emphasize that our discussion of this measure and 45 CFR 164.308(a)(1) is only relevant for purposes of the meaningful use requirements and is not intended to supersede what is separately required under HIPAA and other rulemaking. Compliance with the HIPAA requirements is outside of the scope of this rulemaking. Compliance with 42 CFR Part 2 and State mental health privacy and confidentiality laws is also outside the scope of this rulemaking. EPs, eligible hospitals or CAH affected by 42 CFR Part 2 should consult with the Substance Abuse and Mental Health Services Administration (SAMHSA) or State authorities.

(j)(17) on Secure Messaging

Proposed EP Objective: Use secure electronic messaging to communicate with patients on relevant health information.

Electronic messaging (for example, e-mail) is one of the most widespread methods of communication for both businesses and individuals. The inability to communicate through electronic messaging may hinder the provider-patient relationship.

Electronic messaging is very inexpensive on a transactional basis and allows for communication even when the provider and patient are not available at the same moment in time. The use of common email services and the security measures that may be used when they are sent may not be appropriate for the exchange of protected health information. Therefore, the exchange of health information through electronic messaging requires additional security measures while maintaining its ease of use for communication. While e-mail with the necessary safeguards is probably the most widely used method of electronic messaging, for the purposes of meeting this objective, secure electronic messaging could also occur through functionalities of patient portals, PHRs, or other stand-alone secure messaging applications.

We are proposing this as a core objective for EPs for Stage 2. The additional time made available for Stage 2 implementation makes possible the inclusion of some new objectives in the core set. We chose to identify objectives that address critical priorities of the country's National Quality Strategy (NQS) (http://www.healthcare.gov/law/resources/reports/quality03212011a.html), with a focus on one for EPs and one for hospitals.
For EPs, secure electronic messaging is critically important to two NQS priorities--
- Ensuring that each person/family is engaged as partners in their care; and
- Promoting effective communication and coordination of care.

Secure messaging could make care more affordable by using more efficient communication vehicles when appropriate. Specifically, research demonstrates that secure messaging has been shown to improve patient adherence to treatment plans, which reduces readmission rates. Secure messaging has also been shown to increase patient satisfaction with their care. Secure messaging has been named as one of the top ranked features according to patients. Also, despite some trepidation, providers have seen a reduction in time responding to inquires and less time spent on the phone. We specifically seek comment on whether there may be special concerns with this objective in regards to behavioral health.

Proposed EP Measure: A secure message was sent using the electronic messaging function of Certified EHR Technology by more than 10 percent of unique patients seen by the EP during the EHR reporting period.
...