

Modified Stage 2 Objective 1: Protect Patient Health Information

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

Measure: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by Certified EHR Technology 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 EPs risk management process.

Exclusion: No exclusion.

There are no changes to this objective and measure regardless of when EPs attest to meaningful use.

[CMS Specification Sheet](#)

TennCare Notes - In Stage 2, EPs need to meet the security risk analysis requirements including addressing the encryption/security of data at rest. The security risk analysis must be completed **prior to attestation**. 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.

The attestation portal requires the EP to choose yes or no to having conducted or reviewed a security risk analysis as specified and report the person's name who conducted it with their title. Using the radio buttons providers will answer the following additional questions in PIPP:

- Was an inventory list prepared of all hardware and software that creates, receives, maintains or transmits Electronic Personal Health Information (EPHI) and
- Has a final report and/or corrective action plan been documented for all significant deficiencies noted during the SRA, including target dates for implementation?

Measure at a Glance

Type: task to be performed

Duration: a security risk analysis or review must be conducted during each EHR reporting year

If you are a provider participating in the EHR Incentive Program, conducting or reviewing a security risk analysis is required to meet Modified Stage 2 of meaningful use. This meaningful use objective complements but does not impose new or expanded requirements on the [HIPAA Security Rule](#).

The [NIST 800-66-Revision 1](#) has additional important information.

Appendix D of NIST 800-66 Revision1 provides a catalog of security standards to relevant NIST publications. It even gives the exact control mapping for 164.312(a)(2)(iv) Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information AC-3, SC-13 which are the specific control families explained in NIST 800-53.

Appendix E of NIST 800-66 Revision1 is another copy of the risk assessment guidelines straight from the *HIPAA Security Series: Basics of Risk Analysis and Risk Management* which list the 9 required steps of a risk assessment.

Relevant CMS FAQs:

[10092](#): finding answers to privacy and security questions regarding EHRs

[10754](#)- Security deficiencies

[13649](#)- Timing of analysis

Additional Resources

There are numerous methods of performing a security risk analysis and there is no single method or “best practice” that guarantees compliance with the Security Rule. While the required elements of a risk analysis are listed in the link, “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”, the method and format used to document the requirements are up to the individual practice. Some examples of items that should be considered in the security risk analysis process are outlined in the following tools:

[CMS Security Risk Analysis Tip Sheet](#)

Myths and Facts (Page 4)

[Guidance on Risk Analysis Requirements under the HIPAA Security Rule](#)

Elements of a Security Risk Analysis (Page 4)

[HIPAA Security Series 6: Basics of Risk Analysis and Risk Management](#)

[HIPAA Security Series 4: Security Standards: Technical Safeguards](#)

[NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems](#) Figure 3-1 Flowchart (Page 9)

[NIST Special Publication 800-30-rev1: Guide for Conducting Risk Assessments:](#)
Figure 3: Generic Risk Model with Key Risk Factors (Page 12)

[NIST Special Publication 800-66 rev1: An Introductory Resource Guide for Implementing the HIPAA Security Rule](#)
Activities, Descriptions and Sample Questions (Page 17)

[2013 NIST Training video, Pt 1 of 4](#) – all 4 videos would be helpful to view.

[Security Risk Analysis Tool](#)

[HealthIT.gov Security Risk Assessment Tool and Video](#)