Program Year 2017 Requirements
Protect Patient Health Information

(Security Risk Analysis)

Important Notice (Modified Stage 2 and Stage 3)

- ***Each provider must complete a Security Risk Analysis. There is no exclusion available for this measure.***
- It is acceptable for the security risk analysis to be conducted outside the EHR reporting period; however, the analysis must be unique for each EHR reporting period, the scope must include the full EHR reporting period, and must be conducted ***within*** the calendar year of the EHR reporting period (January 1st – December 31st).
    - In previous years, it has been acceptable to complete this after the reporting period but prior to submission. However, it now must be completed within the calendar year in which your reporting period falls. For example, if you are attesting to Program Year 2017, the security risk analysis must be completed within calendar year 2017 and not in 2018.
- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each EHR reporting period. 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 State's Security Risk Analysis Compliance Form will be an updated form for Program Year 2017. This form will be published on the website and sent via ListServ.

Modified Stage 2 & Stage 3 Requirements

Objective 1 – Protect Patient Health Information

Objective: Protect electronic protected health information (ePHI) created or maintained by the CEHRT through the implementation of appropriate technical capabilities.

Measure: Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT 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 EP's risk management process.

No exclusion available.