UK HealthCare
Kentucky Regional Extension Center

KY REC Tip for the Kentucky Medicaid EHR Incentive Program (Promoting Interoperability) 2021

Objective 1 - Protect Patient Health Information

<table>
<tr>
<td><b>Objective</b>: Protect electronic protected health information (ePHI) created or maintained by certified electronic health record technology (CEHRT) through the implementation of appropriate technical, administrative, and physical safeguards.</td>
<td><b>Measure</b>: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (including encryption) of data created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the provider’s risk management process.</td>
</tr>
<tr>
<td colspan="2"><b>Flexibility for Completing Your Security Risk Analysis in 2021</b>: 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 it must be conducted within the calendar year of the EHR reporting period.</td>
</tr>
</table>

What is different about conducting an SRA in 2021?

Medicaid Eligible Providers (EPs) will be allowed to conduct a security risk analysis (SRA) at any time during 2021, even if the EP conducts the analysis *after* attesting to meaningful use. Historically, the SRA had to be completed *prior* to attestation. An EP who has not completed an SRA for 2021 by the time he or she attests to meaningful use for 2021 will be required to attest that he or she will complete the required analysis by December 31, 2021.

Why was this change made?

Regulation requires all incentive payments for Program Year 2021 must be issued by December 31, 2021. To help facilitate this, the deadline for submitting 2021 attestations is August 31, 2021. CMS wants to allow for maximum flexibility for Medicaid EPs to attest before their state's 2021 deadline while maintaining their annual SRA schedule.

What are the requirements for attesting to Objective 1 in 2021?

An EP who has not completed an SRA for 2021 by the time he or she attests would be required to attest that he or she will complete the required analysis by December 31, 2021. The EP will be required to enter the date that the SRA is expected to be completed.

What if the SRA is not completed after the EP submits the attestation for 2021?

EPs could be required to submit evidence that the SRA has been completed even after the incentive payment has been issued. If an EP fails to conduct an SRA during calendar year 2021, and/or fails to provide evidence of the completion of the SRA upon request, the EP may have their incentive payment recouped.

Additional Information:

- EPs must conduct or review a security risk analysis of CEHRT, including addressing encryption/security of data, implement updates as necessary at least once each calendar year, and attest to conducting the analysis or review.
- 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 it must be conducted within the calendar year of the EHR reporting period.
- 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 EP's risk management process and implemented or corrected as dictated by that process.
- The security risk analysis requirement under 45 CFR 164.308(a)(1) must assess the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization creates, receives, maintains, or transmits. This includes ePHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media.
- At minimum, EPs should be able to show a plan for correcting or mitigating deficiencies and that steps are being taken to implement that plan.
- The parameters of the security risk analysis are defined 45 CFR 164.308(a)(1), which was created by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The PI Program does not impose new or expanded requirements on the HIPAA Security Rule nor does it require specific use of every certification and standard that is included in certification of EHR technology. More information on the HIPAA Security Rule can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

Common Errors:

- Not completing the security risk analysis
- Not developing a risk mitigation plan
- Not mitigating risks identified in your security risk analysis
- Failure to keep up with regulatory requirements
- Not reviewing HIPAA policies and procedures with workforce members
- Not safeguarding data on computers, laptops, and other media devices

- Not reviewing physical/environmental safeguards
- Not providing ongoing HIPAA Security training and security reminders to workforce
- Not conducting vulnerability scans on your network
- Assumptions regarding business associate agreements
- Assuming your IT vendor will take care of the security risk analysis
- Using a checkbox approach to compliance
- Completing a gap analysis in place of a complete, accurate and thorough security risk analysis
- Failure to review audit log procedures
- Failure to review breach notification process

Best Practices:

- Schedule and complete security risk analyses annually with a HIPAA Privacy and Security professional
- Implement a risk management process for mitigating and correcting identified risks
- Identify an internal resource to oversee the risk management process
- Implement a security and awareness training program for all workforce members
- Encrypt your electronic media storage devices and laptops
- Deliver ongoing HIPAA security reminders including how malware can infiltrate your network
- Document all security incidents and mitigation strategies relating to your ePHI
- Review and revise (if necessary) your HIPAA Security Policies and Procedures annually
- Identify the HIPAA Privacy and HIPAA Security Officials for your organization and communicate to workforce
- Review and update the SRA when changes are made to the environment of care or changes in EHRs utilized in providing care

CMS EP Specification Sheet – Protect Patient Health Information

For assistance with conducting a Security Risk Assessment, please contact the Kentucky REC at (859) 323-3090.

Website: www.KentuckyREC.com

Last Modified 01-20-21