MARYLAND
Department of Health

Maryland Medicaid EHR Incentive Program

Special Notice

November 2018

Security Risk Assessment Checklist

The Centers for Medicare and Medicaid Services (CMS) require Eligible Hospitals (EHs) and Eligible Professionals (EPs) who participate in the Electronic Health Records (EHR) Incentive Program to conduct a Security Risk Assessment (SRA) annually. In recent years, the Maryland Department of Health (MDH) has seen a number of providers fail a pre-payment or post-payment audit due to an incomplete SRA. To better assist providers with this measure, MDH has created a checklist[1] to help guide providers through the SRA process. The checklist below addresses criteria that cover many of the common reasons providers fail an audit.

- □ Is the SRA **completed and dated within the Program Year and before the attestation date** for Program Year 2018? For example, for Program Year 2018, the SRA must have been completed between Jan. 1, 2018 and Dec. 31, 2018.
- □ Does the SRA address threats/vulnerabilities to electronic Protected Health Information (e-PHI)?
- □ Does the SRA assign **likelihood ratings, impact ratings, and risk levels** for each threat?
- □ For each threat identified as a medium or high risk, does the SRA include a **remediation strategy** to minimize those risks?
- □ Does the SRA address the **encryption** requirement for e-PHI?
- □ Does the SRA **identify administrative, physical, and technical safeguards**?
- □ Is the SRA specific to **your** practice?
- □ Does the SRA include an **Asset Inventory**? For each asset (such as server, computer, etc.) the practice should have identified the type, location, responsible person, and whether it contains PHI.

Your SRA should have all of the elements listed above. Any deficiencies identified should be corrected before Dec. 31, 2018 to avoid a failed audit or loss of an incentive payment.

[1] Content adapted from OCR's Guidance on Risk Analysis Requirements under the HIPAA Security Rule, The HHS Office of the National Coordinator on Health Information Technology's Guide to Privacy and Security of Health Information, and CMS https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2016_SecurityRiskAnalysis.pdf

Please keep in mind that this checklist is to be used as a guide only, as there are numerous ways in which an SRA can be completed, and there is no single method that guarantees compliance with the HIPAA Security Rule. The checklist provided highlights the components of an SRA that are required, regardless of how the document is completed.

For the complete Program Year 2018 requirements, providers can access Modified Stage 2 and Stage 3 program requirements here.

For additional guidance, The Office of the National Coordinator (ONC) for Health Information Technology, in collaboration with the HHS Office of Civil Rights, created a new SRA Tool. Maryland Medicaid highly recommends using the ONC's SRA tool. The tool has been completely updated to be more user-friendly and provides a step by step process to complete an SRA.

Please note, a simple Yes/No checklist or simply stating that your PHI is stored on a cloud-based system, does not satisfy the SRA requirement.

If you have further questions about your SRA, Program Year 2018 requirements, or would like a preliminary review of your Program Year 2018 documentation, please contact the Maryland Medicaid EHR Incentive Team at mdh.marylandehr@maryland .gov.