NY Medicaid EHR Incentive Program,
A CMS Promoting Interoperability Program

Tip Sheet: Using the Security Risk Assessment (SRA) Tool

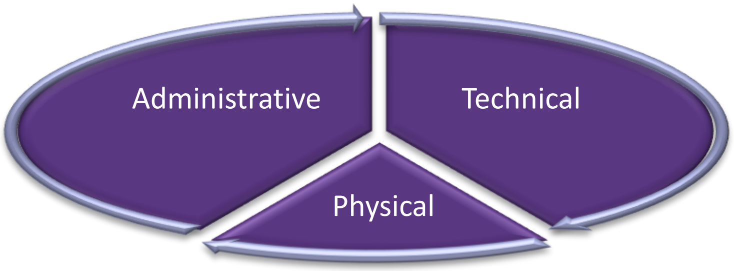
SRA Tool

This Tip Sheet provides additional guidance that may help you in using the ONC SRA Tool.

Who?	An Eligible Professional (EP) participating in the Medicaid EHR Incentive Program must conduct a security risk assessment.
What?	The SRA Tool was developed by the Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the Office for Civil Rights (OCR) and the Office of the General Counsel (OGC). The SRA Tool is designed to help providers and professionals perform a risk assessment.
Where?	The SRA tool is available as a Microsoft Word document and as an optional software application. Both are available online, at no cost. The Word documents and the software application provide similar capabilities. The documents, SRA application, and additional guidance are available at: https://www.healthit.gov/topic/privacy-security/security-risk-assessment-tool
When?	The SRA must be conducted within the same calendar year as the EHR reporting period and prior to the date of attestation.
Why?	Per 45 CFR 164.308(a)(1)(ii)(A), an EP must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the electronic protected health information held by that EP. An SRA must completed in order to meet the Meaningful Use Objective: Protect Patient Health Information.

Security Questions

The SRA Tool is divided into three documents: Administrative Security Questions, Technical Security Questions, and Physical Security Questions. There is a total of 156 questions. The SRA Tool walks through each Health Insurance Portability and Accountability Act (HIPAA) requirement by presenting a question about an organization’s activities. A “yes” or “no” answer will show if corrective actions are needed for that particular item.



Helpful Tips for the ONC SRA Tool

- ✓ Each document contains a section entitled “how to use this document” that provides information on completing the form. Complete all three forms, to complete the risk assessment for the EP.

- ✓ A risk assessment requires an understanding of technology and information security. While EPs may conduct the SRA themselves, they may also elect to engage a firm that possesses experience performing HIPAA Security Rule risk assessments.

- ✓ Answer each of the questions as accurately and completely as possible. If a question is unclear, or if the answer is unknown, additional research may be required. You may also refer to the SRA Glossary.

- ✓ Some questions list a choice for an “alternate solution”. In these cases, the alternate solution should meet the requirements for the question. Example: Windows are not permitted on the first floor; an alternate solution would be that the windows have the ability to lock.

- ✓ Some questions request a remediation plan. A remediation plan is a list of identified weaknesses, along with steps and planned dates that will be taken to correct. Each weakness should be assessed for risk and have that value provided in the remediation plan.

- ✓ Many questions provide help. Please see the “Things to Consider to Help Answer the Question” and “Possible Threats and Vulnerabilities” for additional help with answering the question.

- ✓ Each question is provided with a set of references to HIPAA and the associated control in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4. These references can be used to locate detailed and specific information for the requirements related to a particular question.

SRA Glossary

The following are useful definitions to common information security terms that are used throughout the SRA Tool.

Adverse Impact	Harm to the EP or its patients, following the accidental or deliberate loss of confidentiality, availability, or integrity of an EP program, the device on which it is installed, or the data it contains
Application	A software program that is installed and is used to store or query patient or other medical information. A software program (or app) can reside on mobile devices, laptops, desktops, medical equipment, and so forth
Availability	Ensuring timely and reliable access to and use of a program and the information it contains
Backup	A copy of data files and programs made to facilitate recovery, if necessary
Confidentiality	Ensuring that only the people who can use a program or view the information it contains are those persons who have been authorized to do so
Control	A measure that is put in place to protect against a threat to a program, office space, medical equipment, and so forth. Examples include: fire extinguishers, door locks, screen savers, and passwords.
Encryption	A method of protecting information that scrambles its contents to make it impossible for an unauthorized person to view or make changes
Firewall	A part of the device connecting an EP's office network to the Internet that protects against bad actors gaining access to the office network, from the Internet
Insider	A person who has legitimate permission to use or access the EP's office space, use of the network, an EP program, laptop, medical equipment, or other devices. Examples of an insider include an employee of the EP, a visiting authorized practitioner, maintenance persons, and so forth.
Integrity	The state of a program and the information it contains, where authenticity and completeness can be assured
Inventory	A listing of all equipment and programs at the EP, together with unique identification, location, and ownership of each
Likelihood	A measure based on the probability that an accidental or deliberate action (Threat) will occur and result in a loss of confidentiality, availability, or integrity of an EP program or information
Malware	A small software program that is designed to cause harm to the EP or equipment, with the intention to extort money, steal information, remotely control a computer for illicit purposes, perform unauthorized surveillance, disrupt EP business, etc.
Operating System	The base software that runs the laptop, desktop, mobile or medical device on which a program and its information resides. Windows, MacOS, iOS, Android, and Linux are examples.

Password	A string of characters that, together with a user name, is typed into a program or computer, to gain access or to unlock information protected with encryption
Phishing	A technique for illicitly acquiring sensitive data, such as bank account numbers, through a fraudulent solicitation in email or web site, in which the perpetrator masquerades as a legitimate business or reputable person
Policy	Documented statements, rules, or assertions that specify the correct or expected behavior of those accessing the EP’s office space, devices, programs and information
Ransomware	A disruptive form of malware that is designed to hold a system or its data hostage, to extort money, conduct blackmail, or disrupt EP operations
Risk	A measure that reflects the likelihood that an accidental or illicit action will occur and cause a loss of confidentiality, availability, or integrity of a program, device, or information, along with the impact that would result
Spam	Electronic junk mail or messages that are received through email, voicemail, text messaging, and so forth
Threat	Any circumstance or event (accidental or intentional) with the potential to adversely impact EP programs, information, or devices. A threat makes use of a vulnerability to cause harm.
User Name	The string of characters that identifies the person using an application or computer. Typical examples include an email address or person’s name.
Vulnerability	Weakness in a program, device, office space, or method of protection that could be used, either accidentally or intentionally, to cause harm

If you have additional questions...

Visit www.health.ny.gov/ehr

Our website contains up to date program information and resources, including:

- ✓ Webinars
- ✓ Email LISTSERV®
- ✓ Step-by-step attestation tutorials for MEIPASS
- ✓ Frequently Asked Questions (FAQs)

Contact a Regional Extension Center (REC)

New York State has two RECs that provide support services to healthcare providers as they navigate the EHR adoption process and achievement of meaningful use.

New York City	NYC Regional Electronic Adoption Center for Health (NYC REACH) Website: www.nycreach.org Email: pcip@health.nyc.gov Phone: 347-396-4888
Outside of New York City	New York eHealth Collaborative (NYeC) Website: www.nyehealth.org Email: hapsinfo@nyehealth.org Phone: 646-619-6400

Contact us at 877-646-5410 or hit@health.ny.gov

Questions? We have a dedicated support team that will guide you through the attestation process.

v.2 October 2018