NY Medicaid EHR Incentive Program,
A CMS Promoting Interoperability Program

Tip Sheet: Small Practices Using the SRA Tool

This Tip Sheet is designed to provide small practices with additional guidance about the ONC Security Risk Assessment (SRA) Tool as well as information to consider when hiring a security consultant. Providers participating in the NY Medicaid EHR Incentive Program must conduct an SRA each calendar year as part of the Meaningful Use requirements.

Getting Started with the SRA Tool

We know that each user of the tool has a varying degree of knowledge of information technology (IT) security. If you, or the professional that you are working with would like more assistance, these resources are available:

1. Start with this introductory document.

2. Read *Small Business Information Security: The Fundamentals*, which explains the how, what, and why of information security (32 pages). It was developed by the National Institute of Standards and Technology (NIST).

3. Review the instructions on how to download and run the SRA tool. Information is available on the NY Medicaid EHR Incentive Program website.

4. Finally, if you want even more information related to security, read *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (125 pages). This is very technical in nature and may include terms specific to an IT environment. The document contains a glossary of terms to assist in understanding the subject matter. The document is not geared specifically towards Protected Health Information (PHI) but is written for any organization that manages data that should not be in the public domain.

Items to Consider

What is the size of your office? Depending on the size, it may require multiple people to complete the assessment. The SRA Tool allows multiple users to complete a singular assessment. If you have multiple users of the assessment tool, the file where the assessment is being stored must reside in a location where all users have access.

What is the right answer? When completing the SRA Tool, remember there are no right or wrong answers. Use it for its intended purpose, which is to give you a listing of areas that should be investigated and remedied, so you are better protected from any negative incidents.

What is your timeline? If you have a deadline to complete all the questions, note that it will take more than a couple of hours to conduct the assessment. In many cases, you will need time to gather all the documentation required for the tool. For instance, one of the first items to fill out is a listing of all the technology assets you

have. This means all servers, laptops, cell phones and equipment that might contain PHI data and therefore pose a risk if anything should happen to it. This list should be as detailed as possible. The first assessment will be the most time consuming. When performing future assessments, you will be updating items that you have remedied or other information that has changed. Make sure you have enough time to accurately assess your security.

Security Risk Assessment Tool FAQs

Q: What do these questions have to do with security?

A: Each question is geared towards giving you a complete picture of your current security and the areas of improvement. Many questions will revolve around documentation. The best way to make sure everyone in your organization knows and follows the same processes and procedures is to document those processes and procedures. In many cases this also allows those around you to know what is expected of them when it comes to security. For example, if a person is unknown and attempts to enter an office area where PHI data is viewed and/or stored, you want that person intercepted and escorted elsewhere. If all employees learned that procedure from documentation and training, that is a security risk you are resolving. This only works if everyone on your team has consistent and shared documentation as well as training.

Q: Do I always need to have my data available?

A: Other topics in the SRA Tool have to do with availability. If some event of nature makes it impossible to enter your office, do you need to have a way to restore the information from your office? For some, this is not a concern and you can wait until the event has subsided.

Q: Who has access to your patients' PHI?

A: Are you appropriately vetting any office staff, such as background checks? Do you have others who have access to the office such as cleaning staff? Do you have any type of agreements with them related to secure data? Do you use some sort of service to repair hardware or use for software support? Those individuals could need access to the systems containing PHI data.

Q: How would someone access my information without authorization?

A: For those with harmful intentions towards you or your organization, they may attempt to gain access to some device in your office that doesn't have PHI data, but through it can attempt access to a device with PHI data. In some cases, security is an issue from such seemingly harmless things such as opening an email that contains some type of malware or virus which could impact your systems. This is another area where training and documentation are important, so all staff know what to do.

Q: I just got a new computer. What now?

A: Any computer or component of a computer that you are throwing away may have potentially sensitive information on it and needs to be electronically wiped before leaving your office.

With each question, there are follow-on questions that you want you think about in the likelihood of an event happening and then the impact if it does happen. When finished, the tool will show you the items which have a high likelihood of happening and a high impact to your organization. Your plan should start with those to reduce the risks you are currently exposed to.

Hiring a Security Consultant

Although the SRA Tool attempts to use language that may be easier to understand, especially for users unfamiliar with the information technology field, some organizations may choose to look for additional expertise to help answer the questions and work through the Tool.

If you choose to search for expert assistance you might want to consider the following:

- The individual or group should hold one or more of these standard certifications associated with security:
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information Security Manager (CISM)
  - Certified Authorization Professional (CAP)
  - Healthcare Information Security and Privacy Practitioner (HCISPP)
  - CompTIA Security+
- The security professional has experience in the field of healthcare.
- The security professional has practical, real-life experience in doing security risk assessments.
- Cooperation is key! If you decide to hire someone to work on the SRA Tool, you or your office staff should prepare to spend time with them! They won't know what documents exist or where to find them. They will, however, be able to look at those documents and give you feedback about their completeness and what other work might be required.

NY Medicaid EHR Incentive Program Resources

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 free 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.1 March 2019