

## Conducting Your Security Risk Assessment

The requirement for a security risk assessment (SRA) was created by the HIPAA Security Rule. Conducting a SRA is a requirement of the SC Medicaid EHR Incentive Program. Meaningful use 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.

The process should, at a minimum, require covered entities to:

- [Assess current security, risks, and gaps.](#)
- [Develop an implementation plan.](#)
- [Implement solutions.](#) A covered entity must implement security measures and solutions that are reasonable and appropriate for the organization.
- [Document decisions.](#) A covered entity must document its analysis, decisions and the rationale for its decisions.
- [Reassess periodically, documenting updates.](#)

### What is Risk Assessment?

The [Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule](#) requires that [covered entities](#) conduct a risk assessment of their healthcare organization. A risk assessment helps your organization:

- ensure it is compliant with HIPAA's [administrative, physical, and technical safeguards](#); and
- reveal areas where your organization's protected health information (PHI) could be at risk.

Watch the [Security Risk Analysis video](#) to learn more about the assessment process and how it benefits your organization or visit the [Office for Civil Rights' official guidance](#).

### Security Risk Assessment Tool (SRA)

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the Health & Human Services (HHS) Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable SRA Tool to help guide you through the process.

The SRA Tool takes you through each HIPAA requirement by presenting a question about your organization's activities. Your "yes" or "no" answer will show you if you need to take corrective action for that particular item. There are a total of 156 questions.

You can document your answers, comments, and risk remediation plans directly into the SRA Tool. Resources are included with each question to help you:

- Understand the context of the question
- Consider the potential impacts to your PHI if the requirement is not met
- See the actual safeguard language of the HIPAA Security Rule

**The tool serves as your local repository for the information and does not send your data anywhere else.**

Completing a risk assessment requires a time investment. At any time during the risk assessment process, you can pause to view your current results. The results are available in a color-coded graphic view (Windows version only) or in printable PDF and Excel formats. To download the SRA Tool as well as view details on how to use the tool, download the 24-page [SRA Tool User Guide \[PDF - 4.5 MB\]](#).

A paper-based version of the tool is also available:

- [Administrative Safeguards \[DOCX - 397 KB\]\\*](#)
- [Technical Safeguards \[DOCX - 312 KB\]\\*](#)
- [Physical Safeguards \[DOCX - 263 KB\]\\*](#)