MS-ISAC®
Multi-State Information Sharing & Analysis Center®

CIS Center for Internet Security®

The NCSR and Your HIPAA Security Rule Assessment Requirement

This guide will show how to leverage the Nationwide Cybersecurity Review (NCSR) to accomplish a self-assessment of your HIPAA security protections, saving your organization time and resources.

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

What is the HIPAA Security Rule?

"The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."

This information is available courtesy of the U.S Department of Health and Human Services (https://www.hhs.gov/)

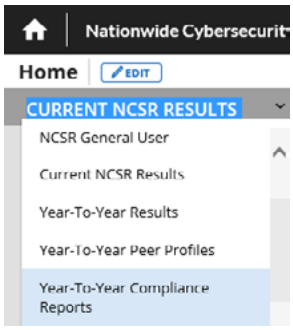
Overview

Use the Nationwide Cybersecurity Review (NCSR) provided by the MS-ISAC as your HIPAA Assessment by leveraging the HIPAA Crosswalk Report:

1. Complete the Nationwide Cybersecurity Review (NCSR) Assessment
   - NCSR Information and Registration Form Located Here: **https://www.cisecurity.org/ms-isac/services/ncsr/**
2. Print the report named "2019 HIPAA Compliance Regulation Report", located within the "Year-To-Year Compliance Reports" Dashboard of the NCSR Portal.
3. Download the free Security Risk Assessment tool provided by The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR)
   - **https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool**
   - Please note, the MS-ISAC does not endorse any one assessment resource. If an organization would prefer to utilize an alternative risk assessment resource, this step can be completed using the alternative resource.
4. Take each line item on HIPAA Compliance Regulation Report and fill in the appropriate line item from Security Risk Assessment Tool

NCSR Portal and Report Description

The following dropdown is listed in the upper left-hand side of the NCSR Portal home screen. The dropdown shows dashboard options, which display NCSR results when selected.



After selecting the dashboard named "Year-To-Year Compliance Reports," the following report will appear:

2019 HIPAA Compliance Regulation Report

HIPAA ID	Organization
480340	Test 2019

After selecting the "HIPAA ID", there will be a listing of HIPAA Security Rules, along with the NIST CSF subcategory/NCSR question and your submitted answer.

Below is an example of the correlation from the HIPAA Security Rule line item, to the submitted answer within your NCSR:

HIPAA Security Rule 45 C.F.R. 164.310(a)(2)(ii)_ID.AM-1:	Cross-walked to NIST CSF (ID.AM-1)	I scored: Implementation in Process
HIPAA Security Rule 45 C.F.R. 164.310(d)_ID.AM-1:	Cross-walked to NIST CSF (ID.AM-1)	I scored: Implementation in Process
HIPAA Security Rule 45 C.F.R. 164.308(a)(1)(ii)(A)_ID.AM-:	Cross-walked to NIST CSF (ID.AM-2)	I scored: Implementation in Process
HIPAA Security Rule 45 C.F.R. 164.308(a)(7)(ii)(E)_ID.AM-2:	Cross-walked to NIST CSF (ID.AM-2)	I scored: Implementation in Process
HIPAA Security Rule 45 C.F.R. 164.308(a)(1)(ii)(A)_ID.AM-3:	Cross-walked to NIST CSF (ID.AM-3)	I scored: Partially Documented Standards and/or Procedures
HIPAA Security Rule 45 C.F.R. 164.308(a)(3)(ii)(A)_ID.AM-3:	Cross-walked to NIST CSF (ID.AM-3)	I scored: Partially Documented Standards and/or Procedures
HIPAA Security Rule 45 C.F.R. 164.308(a)(8)_ID.AM-3:	Cross-walked to NIST CSF (ID.AM-3)	I scored: Implementation in Process
HIPAA Security Rule 45 C.F.R. 164.310(d)_ID.AM-3:	Cross-walked to NIST CSF (ID.AM-3)	I scored: Partially Documented Standards and/or Procedures
HIPAA Security Rule 45 C.F.R. 164.308(a)(4)(ii)(A)_ID.AM-4:	Cross-walked to NIST CSF (ID.AM-4)	I scored: Tested and Verified

If you match the HIPAA 'reference' (in red) to the downloaded HHS self-assessment tool (or other "tool" that you may be utilizing) HIPAA 'reference' section, you can take your results and respond to the pertinent HIPAA question. Please see the below example. The following section is from the HHS Security Risk Assessment Tool referenced above. This specific example is applicable to the Administration, Physical, or Technical section.

A3 - §164.308(a)(1)(ii)(A) Required Does your practice categorize its information systems based on the potential impact to your practice should they become unavailable?

- (X) Yes
- ( ) No

Note: This specific assessment will include additional questions and analysis.

Consider whether your practice's risk analysis is designed to protect its information systems and ePHI that it processes, stores, and transmits from unauthorized access, use, disclosure, disruption, change, or damage.

Consider whether your practice's risk analysis:

- Identifies threats
- Identifies vulnerabilities inherent in its technology, processes, workforce, and vendors
- Contemplates the likelihood of occurrence
- Estimates the potential magnitude of harm

Possible Threats and Vulnerabilities:

You may not be able to identify which information systems and applications are most critical to your practice's operations if they are not categorized based on the potential impacts to your practice should they become unavailable.

This failure to categorize your information systems could impact your practice in that timely and accurate ePHI may not be available, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.

Examples of Safeguards:

Below are some potential safeguards to use against possible threats/vulnerabilities. NOTE: The safeguards you choose will depend on the degree of risk and the potential harm that the threat/vulnerability poses to you and the individuals who are the subjects of the ePHI.

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

[45 CFR §164.308(a)(1)(ii)(A)]

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Testimonial from the Metrics Workgroup of the MS-ISAC

"The NCSR is based on the standards of the NIST Cybersecurity Framework, a derivative of the NIST 800-53 standards. As in most cybersecurity standards or metrics, as well the HIPAA Security Rule, appropriate protections are delineated in concise rules, processes, and procedures. I have found that the NCSR results, if being taken by a 'HIPAA Covered' compliant agency, such as a county maintaining services for public and mental health programs supporting ePHI (electronic protected health information) data of its clients, can easily be utilized using the NCSR provided 'HIPAA Crosswalk' to 'answer' the majority of assessment questions in each of the three sections.

Instead of having to 'shake out' the results and then somehow 'match' the Cybersecurity Framework based results to the HIPAA Security Rule line items, MS-ISAC's Metrics Workgroup developed the 'crosswalk' report of your NCSR (NIST CSF Framework) results over to corresponding HIPAA Security Rule line items for just that purpose."

Gary Coverdale
Chief Information Security Officer (CISO), Mono County, California

This guide is provided by the MS-ISAC and the Metrics Workgroup.