SAND2019-8168D

The Center for Cyber Defenders

Expanding computer security knowledge

Mapping Security Controls

HIPAA and NIST SP 800-53 Security Controls

Sherry Chen, Georgia Institute of Technology

Project Mentor: Kim Ta, Org. 09311

Problem Statement:

As a covered entity, Sandia must comply with the security and privacy standards of the Health Insurance Portability and Accountability Act (HIPAA). Sandia follows the NIST Special Publication 800-53, a catalog of security controls for all U.S. federal information systems. To assess Sandia's HIPAA compliance, this security control maps the HIPAA standards against the NIST SP 800-53 (rev 5) security control.

Objectives and Approach:

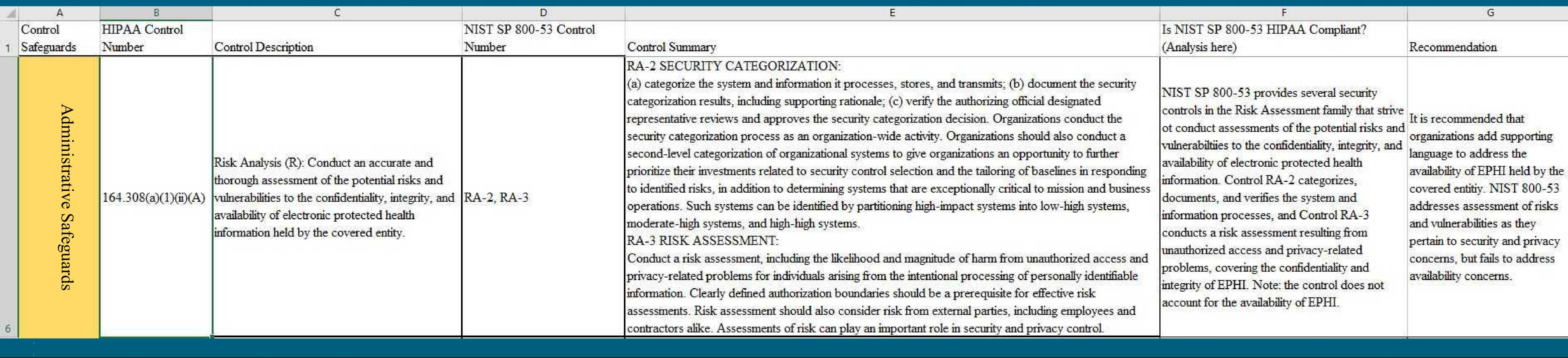
The objective of this project is to assess the compliance of the NIST security controls against the Security and Privacy standards of HIPAA. The mapping is presented in an excel document, matching the corresponding security controls from NIST 800-53 and HIPAA.

Results:

- The mapping found that NIST SP 800-53 addressed most of HIPAA's privacy and security standards. Supplementary controls may be added to the following areas:
  - Increase focus on maintaining availability/access to information; NIST 800-53 focuses on the confidentiality and integrity of information
  - Require written contracts with external service providers to ensure that they are meeting security and privacy requirements.

Impact and Benefits:

- The security control mapping assesses the degree to which NIST SP 800-53 is compliant with the security and privacy standards set out by HIPAA. Compliance is mandatory, and this mapping identifies key areas security control gaps.



	A	B	C	D	E	F	G
1	Control Safeguards	HIPAA Control Number	Control Description	NIST SP 800-53 Control Number	Control Summary	Is NIST SP 800-53 HIPAA Compliant? (Analysis here)	Recommendation
6	Administrative Safeguards	164.308(a)(1)(ii)(A)	Risk Analysis (R): 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.	RA-2, RA-3	RA-2 SECURITY CATEGORIZATION: (a) categorize the system and information it processes, stores, and transmits; (b) document the security categorization results, including supporting rationale; (c) verify the authorizing official designated representative reviews and approves the security categorization decision. Organizations conduct the security categorization process as an organization-wide activity. Organizations should also conduct a second-level categorization of organizational systems to give organizations an opportunity to further prioritize their investments related to security control selection and the tailoring of baselines in responding to identified risks, in addition to determining systems that are exceptionally critical to mission and business operations. Such systems can be identified by partitioning high-impact systems into low-high systems, moderate-high systems, and high-high systems. RA-3 RISK ASSESSMENT: Conduct a risk assessment, including the likelihood and magnitude of harm from unauthorized access and privacy-related problems for individuals arising from the intentional processing of personally identifiable information. Clearly defined authorization boundaries should be a prerequisite for effective risk assessments. Risk assessment should also consider risk from external parties, including employees and contractors alike. Assessments of risk can play an important role in security and privacy control.	NIST SP 800-53 provides several security controls in the Risk Assessment family that strive ot conduct assessments of the potential risks and vulnerabiltiies to the confidentiality, integrity, and availability of electronic protected health information. Control RA-2 categorizes, documents, and verifies the system and information processes, and Control RA-3 conducts a risk assessment resulting from unauthorized access and privacy-related problems, covering the confidentiality and integrity of EPHI. Note: the control does not account for the availability of EPHI.	It is recommended that organizations add supporting language to address the availability of EPHI held by the covered entitiy. NIST 800-53 addresses assessment of risks and vulnerabilities as they pertain to security and privacy concerns, but fails to address availability concerns.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration