NCSA announces SOC 2 Blog Series

NCSA's Advanced Computational Health Enclave (ACHE) is a multi-tenant environment providing high-performance computing (HPC) for research involving electronic Protected Health Information (ePHI). NCSA follows HIPAA standards and has implemented a set of security controls to ensure the protection of ePHI.

As a validation of our controls, NCSA is pursuing a SOC 2 Type 2 certification for its ACHE environment. A SOC 2 is an assessment of a service organization's system and organizational controls. These internal controls, including policies, business processes, and technical controls, are assessed according to one or more of the AICPA's Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

To become SOC 2 Type 2 certified, a service organization undergoes a third-party auditing procedure which examines both the design and operating effectiveness of the controls. During the evaluation, the service organization presents evidence that controls are well-designed, sufficiently meet the relevant Trust Service Criteria, and are operating as expected over time.

In this first certification process NCSA will be evaluated over a six-month period. Beginning July 1, 2020, we are documenting our controls, periodically testing them, collecting operational evidence, and mitigating non-compliance, following a methodology similar to internal compliance management. In this blog series we will describe the systems and methods we have set up including how we keep track of our controls, how we test our controls, and workflows we have configured to manage evidence collection. As we go through the attestation process we will also note lessons learned and how we will adjust our processes in the future.