SSAE 18 REPLACES SSAE 16 DATA SECURITY AUDIT STANDARD – PRACTICAL TAKEAWAYS

As hospitals and health-related entities, like other businesses, continue to shift application hosting and data storage to the cloud and to third party data centers, they should consider what obligations to place on vendors that provide such hosting and data storage services to promote data security. One such obligation may be to require hosting service providers to undergo an annual review of security standards and internal controls, not only for their own data centers, but also for any third party service providers used by the hosting service provider. Such a review could identify security vulnerabilities before a data breach or other exposure occurs. However, the type of security audit performed factors into the usefulness of the review and its results. Therefore, health-related entities should stay informed about the most current security audit standards and options available to them as they discuss data security obligations with hosting service providers. Changes in auditing standards resulting from the transition from SSAE 16 to SSAE 18 should prompt health-related entities to update vendor contracts and system policies as they relate to third party data storage centers and other service providers that host data.

BACKGROUND

Various auditing standards are used to assess and report on organizational security and compliance controls. These reports can provide valuable insight to help ensure proper security safeguards are in place. Reviewing these reports regarding service organizations' controls also assists with a health organization's compliance with HIPAA requirements by including security vulnerabilities in the health organization's risk assessment.[1] There may be different levels of assessment and reporting available to auditors depending on the auditing standard chosen, the reason for the audit and the timeframe over which security and controls are reviewed. These standards change over time as technology advances. The Statement on Auditing Standards No. 70 (or SAS 70) was a common auditing standard for the technology industry from 1992 until 2011 when it was replaced by the Statement on Standards for Attestation Engagements ("SSAE") published by the American Institute of Certified Public Accounts ("AICPA"). SSAE reviews evaluate how "service organizations" (for example, entities that provide hosting, colocation, payroll processing, medical claims processing, software as a service vendors, etc.) and their subcontractors (referred to as "subservice organizations") implement controls over activities that may impact its user organizations (that is, its customers).

The assessment and reporting options available as part of an SSAE audit include SOC 1, SOC 2, SOC 3 assessments, and Type 1 or Type 2 reports.

A SOC 1 report evaluates a service organization’s internal controls that may impact the financial reporting of its customers.

A SOC 2 report evaluates a service organization's internal controls with respect to security, availability and processing integrity of information technology assets and confidentiality and/or privacy of data. The SOC 2 report was created primarily in response to the growth of cloud computing and software as a service offerings and the outsourcing of certain business functions to hosting service providers. Because a SOC 2 report contains confidential information, its distribution is typically limited.

A SOC 3 report also evaluates whether the hosting service provider has successfully completed a SOC 2 assessment but only provides information that is distributed to public parties.

SOC 1 reports are especially relevant for publicly traded companies, whereas SOC 2 and SOC 3 reports are intended for companies that offer services that include technology or data components because they include assessment of information security and information system availability metrics.

Type 1 reports provide a snapshot of the suitability of the service organization's design of controls to achieve related control objectives at the time the assessment is conducted. Type 2 reports are used to report on the suitability of design and effectiveness of controls over a period of time - at least 6 months and often up to 12 months. Because the Type 2 report evaluates controls over an operational period, it provides insight into the operational effectiveness of controls as implemented by the service organization.

As of May 1, 2017, AIPCA transitioned from SSAE 16 to SSAE 18. This new standard is designed to address concerns over clarity, length and complexity of the audit standards. Many vendors began conducting audits under the new SSAE 18 standard in the second half of 2017, and

all others are expected to do so in 2018.

ANALYSIS

The transition to SSAE 18 changes the scope of the audit for the independent auditor, the service organization and subservice organizations. The most significant change for service organizations is a requirement to conduct and document risk assessments. In addition, the service organization must monitor the effectiveness of controls for its subservice organizations through an effective third party vendor management process.

Under the SSAE 18 standards, monitoring by the service organization can be accomplished by the following activities:

- Reviewing and reconciling output reports.
- Holding periodic discussions with the subservice organization.
- Making regular site visits to the subservice organization.
- Testing controls at the subservice organization by members of the service organization's internal audit team.
- Reviewing Type 1 or Type 2 reports on the subservice organization's system.
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization. Additionally, all system-generated reports must be fully disclosed and thoroughly described. Previously, this requirement could be met by describing the service organization's internal system for the auditor. The new disclosure and description requirements will allow service auditors to evaluate whether information used for an assessment is sufficiently reliable and will provide evidence of the system's accuracy and completeness.

PRACTICAL TAKEAWAYS

Implement a robust vendor management program. Health-related entities should be monitoring all vendors that provide data-related services, including service organizations and subservice organizations, to ensure strong information technology practices. As discussed above and pursuant to HIPAA guidance from the Office of Civil Rights, the risks to the confidentiality, integrity and availability of data that arise due to the activities of these vendors must be included in the risk assessment of the health-related entity. Consider how those risks have been mitigated by reviewing audit reports, penetration tests and similar security documentation to ensure that such service organizations have implemented appropriate safeguards and are monitoring internal compliance, security and financial reporting controls on an ongoing basis. Require vendors to provide information demonstrating that they are also monitoring the risks and safeguards of their subservice organizations. Implementing a robust third party vendor due diligence and management program will help ensure that security and compliance vulnerabilities are appropriately identified and remediated to mitigate potential financial and reputational liability.

Contractually obligate vendors to mitigate security and compliance risks. During the procurement and annual service renewal processes, health-related entities should contractually obligate vendors to comply with industry-standard data security standards. Health-related entities should consider including specific language to address the potential risks indicated during the vendor due diligence process as well as security and compliance obligations, including vendor obligations to provide audit reports, penetration tests and similar security documentation. This may also include drafting vendor security questionnaires and template language for security organizations that create, maintain, transmit or store data or provide hosting services, as well as reviewing existing terms and conditions to ensure adequate compliance obligations and remedies are included in the event of a breach. Health-related entities should engage counsel to ensure their rights and obligations are protected to shield them from unnecessary risk and liability.

For more information, please contact:

- Melissa Markey at (248) 310-4876 or mmarkey@hallrender.com;
- Tony Caldwell at (317) 977-1469 or acaldwell@hallrender.com; or
- Your regular Hall Render attorney.

Special thanks to Aaron Mulgrue, law clerk, for his assistance with the preparation of this article.

[1] See Guidance on HIPAA & Cloud Computing, available here.