Why should your EHR Vendor and their Hosting Facility have SOC 2?

It seems everyone understands that a SaaS Hosting Facility must be certified at the highest current federal standards. But no-one seems to question why their EHR vendor, who has access to the same patient ePHI, hasn't completed the same examinations.

The following information is provided to help explain why your EHR vendor should be examined by an independent third party, what SOC is, why Medicat chose the more rigorous Type 2 SOC 2 Examination on your behalf, and what that means to you.

The short version is that the Sarbanes Oxley Act (SOX) requires all publicly traded companies to establish internal controls and procedures for financial reporting to reduce the possibility of fraud. To properly conduct this financial statement examination, an audit must be performed for any organizations that affect the security or financials of the publicly traded organization. All such organizations should also be audited using SOC 1 (financial reporting) or SOC 2 (security reporting). The same holds true for privately held Hosting Facilities and their relationship with their clients (e.g., EHR vendors); both should pass audits at the highest Federal and Industry standards to ensure the security of your students' ePHI.

What is SOC?

Service Organization Control (SOC) reports—created by the American Institute of Certified Public Accountants (AICPA)—are internal control reports on the offerings furnished by a service organization, which provide important information for users to appraise the risks involved with an outsourced service. These reports are essential for service providers to build trust with clients, as they are performed by an independent third party.

SOC 2 reports focus on service providers that host or store data, ensuring that they are following industry best practices and their operations are up to code. The SOC 2 report contains a description of the infrastructure, software, people, and procedures (the "system") that the company has in place to protect and safeguard data. A SOC 2 report contains descriptions of what components the company has and what it does to make sure it successfully delivers on the five **Trust Service Principles**.

- **Security -** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- **Availability -** Information and systems are available for operation and use to meet the entity's objectives.
- **Processing integrity -** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

- **Confidentiality -** Information designated as confidential is protected to meet the entity's objectives.
- **Privacy -** Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

Service organizations can choose which type of SOC 2 audit to undertake: Type 1 or Type 2.

- **Type 1** SOC 2 report - a layout of procedures and controls that the service provider has established as of a certain point in time.
- **Type 2** SOC 2 report - includes all the information in Type 1, but also supplies evidence as to how effective those procedures and controls were over a specified period. The audit period in a Type 2 report is typically no less than six months—enough time for a comprehensive evaluation.

Why is it important for your EHR vendor to have SOC 2?

Type 2 SOC 2 compliance is an outstanding standard for business owners and decision makers because it provides them with the peace of mind that the service provider they choose can deliver what it promises.

A company that has performed Type 2 SOC 2 Examination has therefore proven that its system is designed to keep its clients' sensitive data secure over time. When it comes to the cloud and related IT services, such performance and reliability is essential, and is being required more often by regulators, examiners, and auditors.

When asked if they are HIPAA compliant, EHR vendors usually answer "yes." But how do they demonstrate their compliance? The only way to prove compliance is for the vendor to successfully complete an external audit, preferably one conducted by a reputable audit firm with HIPAA experience.

Performing a Type 2 SOC 2 Examination requires significantly more time, effort, and resources than does a HIPAA audit, and is a more significant assessment for security and compliance. An EHR vendor should be willing to invest in the highest available compliance for data security on your behalf, which is the Type 2 SOC 2 Examination.

Medicat's Hosted Solution

Medicat's Private Cloud Infrastructure ensures the storage and handling of your students' electronic Patient Health Information (ePHI) meets and exceeds all government and industry standards. There are two components of that infrastructure:

- **The TierPoint Hosting Facility** where your students' ePHI is stored. TierPoint's Facilities in North Carolina's Research Triangle Park (RTP), and in Chicago, are both rated to the highest Federal and Industry Standards, including Type 2 SOC 2 Examination. Your student's ePHI could not be safer.

- **Medicat's significant investments** in its own infrastructure and security framework to better protect our Clients' ePHI. To substantiate that investment, Medicat has gone through the same third-party audit process as the leading data centers in the country and has completed Type 2 SOC 2 Examination.

Summary

These rigorous requirements provide an important level of confidence and comfort when considering a move to the cloud. It is critical to insist on an EHR partner that has achieved a level of security that meets these standards.

That is why SOC 2 audits matter, and why Medicat has invested in the highest compliance possible; the Type 2 SOC 2 Examination. After all, the security of your patients' data depends on it!

For more information, contact Sales@medicat.com

rev. 12182018