Compliance

Last Modified on 12/15/2020 9:08 am EST

Overview

Our UCaaS product is tested annually for security and vulnerability by Pondurance, a global security and threat mitigation company.

In addition, Synkato is fully compliant in the following:

FISMA

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source.

Read more about FISMA Implementation and the Modernization Act of 2014.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection. Companies that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance. Covered entities (anyone providing treatment, payment, and operations in healthcare) and business associates (anyone who has access to patient information and provides support in treatment, payment, or operations) must meet HIPAA Compliance. Other entities, such as subcontractors and any other related business associates must also be in compliance.

HIPAA compliance is delivered through our Business Associate Agreements.

Read more about HIPAA .

SOC 2®

AICPA's System and Organization Controls (SOC) for Service Organizations are internal control reports on the services provided by a service organization that shares valuable information users need to assess and address the risks associated with an outsourced service.

SOC 2 Reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability and processing integrity of the systems the service organization uses to process users' data, and the confidentiality and privacy of the

information processed by these systems.

Read more about SOC.

PCI DATA SECURITY STANDARD

The PCI Data Security Standard (PCI DSS) provides an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents. The standards set the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

Read more about PCI DSS .

CALEA

The Communications Assistance for Law Enforcement Act (CALEA) was enacted by Congress in 1994 to require telecommunications carriers to provide law enforcement with certain technical capabilities when they conduct lawful electronic surveillance on telecommunications networks. The Federal Communications Commission issued an order in 2005 extending the coverage of CALEA to two-way interconnected VoIP and broadband Internet access.

The goal of CALEA is to preserve the ability of law enforcement to conduct lawful investigations despite evolutions in network technology. This goal is meant to be achieved while protecting telecommunications subscriber privacy and the ability of telecommunications carriers to launch new services and technologies.

Read more about CALEA.

SARBANES-OXLEY

The Sarbanes-Oxley (SOX) Act requires all financial reports to include an internal control report. This is designed to

show that not only are the company's financial data accurate, but the company has confidence in them because adequate controls are in place to safeguard financial data. Year-end financial reports must contain an assessment of the effectiveness of the internal controls.

Read more about the Sarbanes-Oxley Act and a history of the Act.