

Avaya Scopia HIPAA Statement

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) is an act that sets standards for electronic healthcare transactions. As such HIPAA sets standards for security and privacy of patient data.

To Comply with HIPAA, Healthcare providers turn to use verified network security architectures. The U.S. Department of Health and Human Services (HHS) recommends the usage of the 'Federal Information Process Standard' (FIPS) 140-2 encryption to protect healthcare data. FIPS 140-2 is a powerful security solution, which is already mandated by the U.S. Department of Defense (DoD) for encryption. Its use reduces risk without increasing costs.

FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard by the National Institute of Standards and Technology (NIST) used to accredit cryptographic modules.

FIPS 140-2 lists approved methods for encrypting sensitive information, one of which is AES-128 (Advanced Encryption Standard). AES-128 is a 128-bit symmetric key encryption method, which means the same key is used for both encryption and decryption.

Scopia Desktop and Mobile

Scopia Desktop and Mobile, starting with release 8.2 FP1, support AES-128 encryption for GUI and signaling over HTTPS and for Media over SRTP. Using a FIPS approved encryption algorithm (AES-128) ensures patient health information protection and privacy, in line with the HIPAA requirements.

Sincerely,

Amir Alrod

Scopia Desktop & Mobile Product Manager
Radvision, An Avaya Company