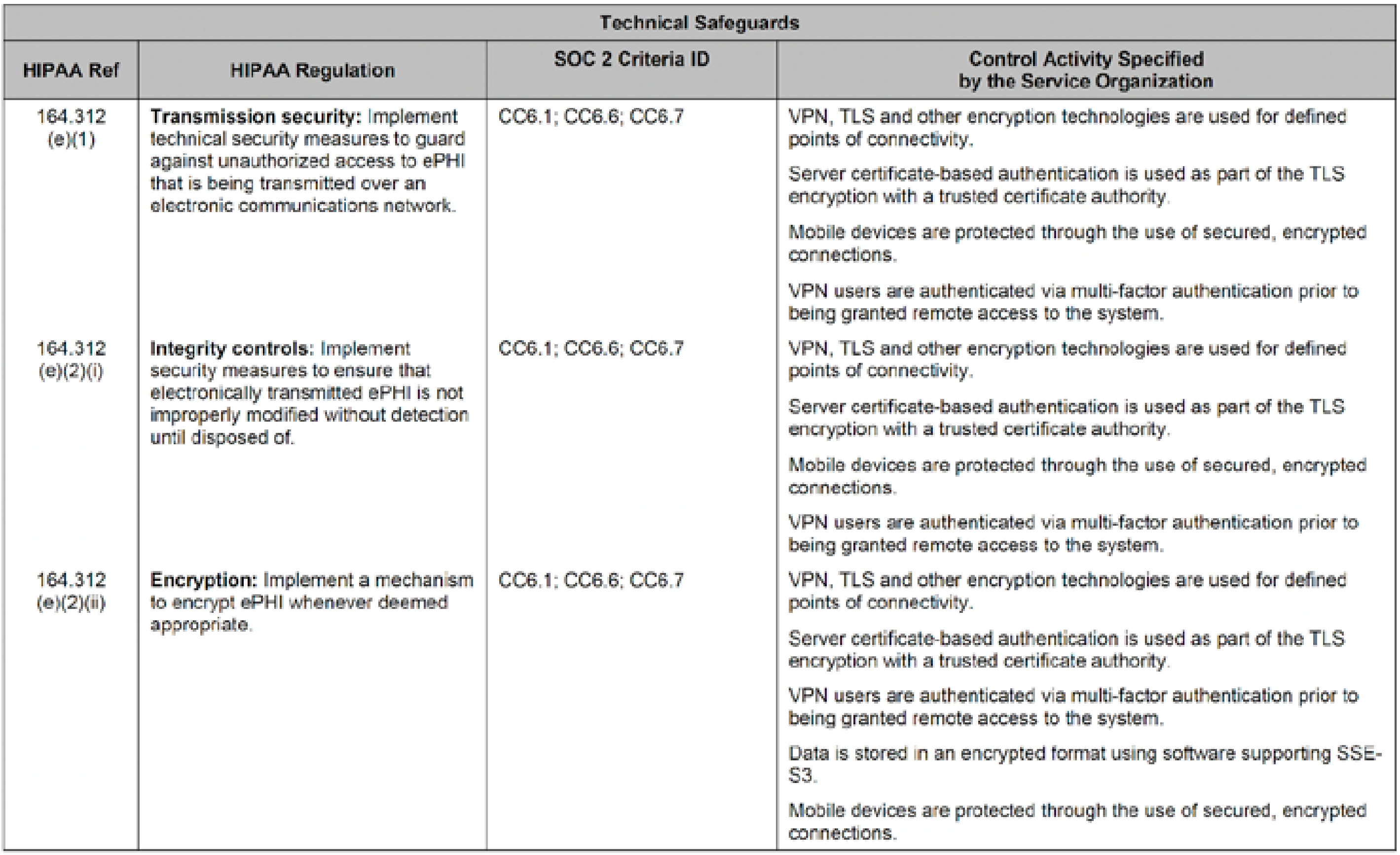
HIPAA Security Rule Compliance

The Health Insurance Portability and Accountability Act (HIPAA) stipulates how Personally Identifiable Information (PII) maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft.

8x8's third-party auditing organization, A-Lign, assessed our controls for SOC 2 Type 2 compliance and they completed an in-depth mapping to HIPAA requirements for our entire product offering. The mapping demonstrates proper controls between our SOC and HIPAA requirements. A-Ligns' auditors have validated that our environment does protect HIPAA data. Below is a sample from the auditors report:



Technical Safeguards			
HIPAA Ref	**HIPAA Regulation**	**SOC 2 Criteria ID**	**Control Activity Specified by the Service Organization**
164.312 (e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	CC6.1; CC6.6; CC6.7	VPN, TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Mobile devices are protected through the use of secured, encrypted connections. VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	CC6.1; CC6.6; CC6.7	VPN, TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Mobile devices are protected through the use of secured, encrypted connections. VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	CC6.1; CC6.6; CC6.7	VPN, TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system. Data is stored in an encrypted format using software supporting SSE-S3. Mobile devices are protected through the use of secured, encrypted connections.

When properly configured, 8x8 products and services are HIPAA compliant.