

Complying with Regulation

HIPAA

Most countries have regulations on how patient information is to be used, stored, and transferred. In the United States for example, privacy portion of the Health Insurance Portability and Accountability Act (HIPAA) is steering health care organizations. HIPAA is an initiative to develop standards and requirements for the secure transfer of any health information that could identify individual patients. Health care organizations have to be compliant with three aspects of the Act: electronic transaction sets, privacy, and security.

In Europe, an example of regulation affecting the health care industry would be the Data Protection Act 1998 in the UK.

HIPAA Security Requirements and StoneGate

A properly configured StoneGate security solution enables an organization or institution to achieve compliance with relevant sections of the act. The HIPAA Security Rule has six sections out of which the Administrative Safeguards and Technical Safeguards deal with requirements addressable by a network security solution. Below we list requirements from the Security Rule and examples on how StoneGate can help meet those requirements.

§	Description	The Requirement	How StoneGate meets the requirement
Administrative Safeguards § 164.308			
<i>Security Incident Procedures 164.308 (a)(6)</i>	<i>Response and Reporting</i>	Implement policies and procedures to address security incidents.	StoneGate Security Platform can help in establishing ways to report and respond to security incidents. With extensive reporting capabilities StoneGate provides a way to coordinate the security incident procedures.
<i>Contingency Plan 164.308 (a)(7)</i>	<i>Data Backup Plan, Disaster Recovery Plan</i>	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information	StoneGate Security Platform has built-in backup capabilities for network traffic information and security solution backup utilities. In case of an emergency StoneGate can also help provide alternative network links to provide high availability not only for the security solution but also to connectivity.

§	Description	The Requirement	How StoneGate meets the requirement
Technical Safeguards § 164.312			
§ 164.312 (a) (1)	<i>Access Control - e.g., Unique User Identification, Encryption/Decryption (with e.g., automatic logoff after timeout, access termination if no longer required)</i>	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted rights as specified in (Facility Access Controls)	StoneGate Firewall & VPN secure the access to the networks but also handle the authentication, which addresses the unique user ID requirement of the Act. In addition the authentication in StoneGate is very granular and can be done on a rule-by-rule basis. StoneGate VPN Client (unlimited license at no extra charge) secures the remote users and requires re-authentication from users after specified time. To further ensure the data is kept confidential all traffic if necessary can be encrypted using StoneGate Firewall & VPN.
§ 164.312 (b)	<i>Audit Controls</i>	Implement hardware, software, and/or procedural mechanisms that records and examine activity in information systems that contain protected health information. All network traffic also is required to be stored for a certain period of time.	StoneGate Firewall & VPN solution has extensive logging and searching capabilities for network and administrator activity. StoneGate also helps with the storage of the log data, as that data tends to get extensive due to the technical requirement. Additionally StoneGate can provide detailed log analysis, live statistics, and reporting to facilitate adhering to the auditing requirements.
§ 164.312 (c) (1)	<i>Integrity</i>	Mechanisms to Authenticate Information Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	StoneGate VPN encrypts the data, which ensures that the data is kept not only confidential but also protects from improper alteration or destruction. StoneGate helps in identifying all users who have been authorized to access either the network or a specific address.
§ 164.312 (d)	<i>Person or Entity Authentication</i>	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	StoneGate Firewall & VPN support various authentication methods including: passwords, smart cards, tokens, digital certificates, and other methods.
§ 164.312 (e) (1)	<i>Transmission Security - e.g., Encryption</i>	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	StoneGate Firewall & VPN can protect the data being transmitted by performing encryption. The following algorithms are available with StoneGate: AES-128, AES-256, DES, 3DES, CAST-128, Blowfish, and Twofish.