How SonicWall Email Encryption service enables compliance

Ensure the secure exchange of email containing sensitive customer data or confidential information.

The SonicWall Email Encryption subscription service, an optional service available with SonicWall Email Security on-premises and hosted solutions, helps organizations achieve regulatory and industry compliance when moving PII (Personally Identifiable Information), PHI (Protected Health Information), proprietary data or any other types of sensitive information. HIPAA/HITECH, GLBA, PCI and other regulations require sensitive data be encrypted when transferred over a public network like the Internet. Since most organizations use email and simple file attachments as the preferred method for business communications, it’s imperative that these be secured when transmitting sensitive data.

The SonicWall Email Encryption service focuses on requirements surrounding the protection of data in motion, for example when sending messages and files to another person or system. Our services are just one part of your overall compliance strategy. Other services will be needed for local encryption such as disk, file or folder encryption.
All methods of accessing information in any direction are encrypted. Additionally any information stored on the Email Encryption service portal awaiting delivery is stored encrypted on the disk.

**SonicWall Email Encryption service and HIPAA/HITECH Compliance**

According to HIPAA regulations section § 164.312 Technical Safeguards, protected information must have the following safeguards. (Note: only safeguards relevant to data in motion are listed):

<table>
<thead>
<tr>
<th>HIPAA Safeguard</th>
<th>SonicWall Email Encryption service control</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control</strong></td>
<td>creates accounts which are used to uniquely identify and authenticate each user. Users are not allowed to gain access to another person’s information.</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>requires encryption such as SSL, TLS, SSH and AES for access and delivery methods.</td>
</tr>
<tr>
<td><strong>Audit Controls</strong></td>
<td>audits activity and tracks all messages regardless of how they are sent or received.</td>
</tr>
<tr>
<td><strong>Transmission Security</strong></td>
<td>encrypts all methods of accessing information.</td>
</tr>
</tbody>
</table>

**Additional HITECH requirements**

<table>
<thead>
<tr>
<th>Extension of HIPAA requirements to Business Associates</th>
<th>The Email Encryption service enables covered Business Associates to be compliant when communicating with your organization without any extra work for you or them.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption as a recognized method for protecting PHI</td>
<td>The Email Encryption service encrypts data in motion to ensure its confidentiality during transmission.</td>
</tr>
</tbody>
</table>

**SonicWall Email Encryption service and PCI-DSS Compliance**

For any organization that deals with billing or other financial information, regardless of industry, compliance with PCI-DSS is very important. While not a government-issued regulation, this industry standard has such broad backing that not following it can severely impact a business.

<table>
<thead>
<tr>
<th>PCI-DSS Compliance</th>
<th>SonicWall Email Encryption service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCI-DSS, Requirement 4.1</strong></td>
<td>uses SSL, TLS, SSH and AES encryption standards to provide secure transmission of data between the sender and recipient of any data.</td>
</tr>
<tr>
<td>Strong cryptography and security protocols must be used to safeguard sensitive cardholder data during transmission over public networks</td>
<td></td>
</tr>
<tr>
<td><strong>PCI-DSS, Requirement 4.2</strong></td>
<td>allows an organization to securely send information using email in compliance with requirement 4.2.</td>
</tr>
<tr>
<td>Account numbers must be encrypted when using “end-user messaging technologies” such as email</td>
<td></td>
</tr>
</tbody>
</table>
The Email Encryption service and Gramm-Leach-Bliley Act Compliance

The Gramm-Leach-Bliley Act (GLBA) has three primary requirements. Only two of these apply to service provided by the SonicWall Email Encryption service: the Financial Privacy Rule and the Safeguards Rule. Using the Email Encryption service, an organization can ensure the privacy of their consumer’s data while enabling it to be sent not only within their organization but also when exchanging data with the consumer directly. Additionally, for portions of communications running through the Email Encryption service, the safeguard rules are handled by the Encryption service as part of the service offering. Using the Email Encryption service provides a monitored, governed, high availability solution that automatically encrypts all data that is transferred and stored within the service.

“Using the SonicWall Email Encryption service, an organization can ensure the privacy of their consumer’s data while enabling it to be sent not only within their organization but also when exchanging data with the consumer directly.”
About Us

Over a 25 year history, SonicWall has been the industry’s trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.

www.sonicwall.com