Protecting Sensitive Patient Data with Retarus E-Mail Encryption

The challenge

Long-term care planning, complaint management or up-to-date information about the progression of a disease — for old-age care facilities and nursing homes working in the healthcare industry, daily communication with family members is essential.
The preferred channel of communication these days is email, the easiest and fastest way to exchange information around the clock and inexpensively. The problem is that sending an email via the internet is like sending a postcard. Anyone involved in delivering the message can read it without being noticed. As a rule, data transmitted in the health industry is personal and highly sensitive, and must be protected from unauthorized access using appropriate encryption technology.

The background

In accordance with stringent statutory requirements, medical facilities have to ensure that confidential information sent by email cannot be accessed by unauthorized third parties under any circumstances. However, in the email accounts of family members the required encryption infrastructure is seldom activated. Installing complex end-to-end encryption often involves too much effort for private users. Senior care facilities and nursing homes are not in the position to provide IT support for end users, nor are they able to manage encryption themselves. They need an encryption solution that not only guarantees the secure exchange of information with end users, but also works smoothly without requiring setup and support.

The solution

Retarus E-Mail Encryption enables emails and their attachments to be encrypted, using established standards such as S/MIME, PGP, and OpenPGP. This innovative encryption service can be used with all common email systems. Connection via VPN or TLS ensures that sensitive information is protected from unauthorized access at all times, during each phase of the transmission process. Retarus E-Mail Encryption is operated in Retarus' own data centers in accordance with compliance guidelines and local data protection regulations.

Customer benefits

- Legally compliant data encryption
- Reliable protection of sensitive information
- Discreet communication with end users
- Maximum usability
- Increased IT capacity for other tasks

Benefits at a glance

- Complete encryption of email content including all attachments
- Encryption with S/MIME, PGP and OpenPGP
- Filters for viruses and spam despite encryption
- Compatible with all SMTP-based email systems (including Microsoft Exchange, Office 365, IBM Notes/Domino)
- Web portal for sending encrypted emails to recipients with no internal encryption solutions
- Simple implementation
- Central key management by Retarus
- No training necessary

Use Case

With Retarus E-Mail Encryption, healthcare companies can safeguard the confidentiality of their communications and effortlessly comply with applicable data protection regulations, such as the security measures set out in the German Federal Data Protection Act to prevent unauthorized access of personal data during transmission. Using a customer-specific set of rules, confidential messages and all file attachments are automatically encrypted and then forwarded securely to the recipient. The intelligent email filtering function provided by Retarus E-Mail Security Services ensures that outbound emails (before encryption) and inbound emails (after decryption) are always checked for viruses and blocked as needed.

For communication partners who use neither S/MIME nor PGP, Retarus offers Secure Webmailer. Confidential emails are automatically encrypted for the recipient and stored on this web-based portal. The recipient receives an email containing a link, and via an HTTPS connection, is not only able to access the email securely, but also to send an encrypted response directly from the platform. The company does not need to assign individual access passwords, because the recipient receives an initial password, which can be changed at any time, with the first email. As an alternative to encrypted email transmission via Secure Webmailer, the email which is to be encrypted can also be delivered to the recipient within a password-protected PDF document. All the recipient has to do is enter the correct decryption password. The PDF document contains both the email text and all attachments that were contained in the original email.

To use Retarus E-Mail Encryption, companies neither need to modify existing servers, desktops or email clients, nor do users require any special training. On request, Retarus can administrate the keys for all users and the certificates for their communication partners. In this way, administrators are completely relieved of time-consuming key management tasks.

Did you know?

According to a recent online study by ARD and ZDF television broadcasters, 76% of people in their 50s and 60s communicate by email, as do 67% of people over 70.

Other scenarios

Archiving and encrypting
With Retarus E-Mail Security you can archive encrypted emails - legally compliant and retrievable in just a few clicks — without time-consuming key management.

Virus protection and encryption
Using an intelligent combination of gateway services, outgoing messages are checked for viruses dependably prior to encryption, and incoming messages following decryption, and blocked if necessary.

Email management
Managing the flood of emails not only takes a lot of time, but is also often nerve-racking. Retarus E-Mail Security offers innovative functions that facilitate efficient email management.