Sensitive Data Distribution via Secure Email

Secure email solution to distribute healthcare personal data

Customer Background

A large healthcare corporation managing both occupational and private healthcare clients with over 30.000 employees and private practitioners offering comprehensive high-quality services in Nordics. The corporation is a rapidly developing and growing leader in the industry. They invest in the possibilities of digitalisation and the effectiveness and quality of care in all its business areas.

Challenge

Managing sensitive health data in such an extensive network of employees, private practitioners, and patients is extremely challenging as health data is highly sensitive, confidential, and restricted in nature and therefore under lot of regulation when it comes to how it is managed and shared.

One of the key stumbling blocks was distributing relevant patient data to patients outside the healthcare facility. Traditional mail is slow and expensive - but sensitive data cannot be sent in regular mail, rather it requires using registered mail.

Digital distribution via email was deemed the preferred option as majority of people have at least one email address. However, challenges with most popular email services like Gmail, Yahoo Mail, Hotmail, or Roadrunner were also acknowledged – they are not secure enough to send sensitive health and patient data over. Regular email services do not fulfill the stringent legal requirements and standards set upon healthcare data.

Another hurdle to tackle was the verification of the data recipient. With registered mail, this is done by asking for a proof of identification before the mail is handed over. In the case of email, regular email services fall short on this aspect. There is no way to verify that the person on the other end of the communication is the intended recipient.

Thirdly, as with registered mail, there is the requirement to have a comprehensive audit trail of who, how, when, and to whom the data has been delivered.

The email service that the healthcare corporation started to look for had four prerequisites:

- identity verification,
- tamper-evident technology,
- comprehensive audit trail,
- and it needs to function with any existing email service with no additional email accounts needed.

Solution

The healthcare institution chose SalaX Secure Mail as the solution. Secure Mail is an encrypted email communication platform to fully secure sensitive communications.

The main features of Secure Mail include:

- Guaranteed security
- Microsoft integration
- Easy-to-use
- Secure Mail is an add-on to the existing email service, therefore sending an email is easy and simple with normal e-mail client – same functions in use
- Messages are stored in encrypted form and the recipient receives a notification message with protected link leading to the encrypted message making the message tamper-proof
- Choice for level of security of the content (sensitive, confidential, restricted) - depending on the security level, the recipient needs to authenticate themselves with PIN code or strong electronic authentication (bank ID or similar)

- The recipient reads the message over a secure browser connection
- Secure Mail automatically encrypts email messages considered confidential or blocks sending of these messages depending on pre-created rules and data security policy configured in the service
- Audit trail and statistics of how the confidential material is being handled
- The recipient can among other things:
    - Reply to messages by using the same secure channel - the reply will be delivered to sender's inbox
    - Open and save attachments
    - Save the original message (txt/html/zip/encrypted zip or S/MIME encrypted eml)
- An external party can proactively start confidential messaging with browser-based sending function - the external party can start secure communication without any licenses
- Secure Mail allows sending large attachments (up to 1GB)
- Hybrid implementation option – on-premises or in the cloud

The software includes a web-based management tool for system administrators including functions: logs, statistics, server configuration, tools, user management, system update and settings, access rights, and user permissions.

Results

- Healthcare data protection and sharing in a compliant manner
- Protecting confidential emails is straightforward
- Large confidential files easily accessible for the patient as well as their practitioner
- Sharing information with different groups safely and effortlessly

The most significant benefit of secure email service is that it allowed the corporation to ensure that it met the stringent healthcare data protection requirements (HIPAA). All confidential healthcare information is safeguarded, thus it is meeting all security regulations.

The Zero Access principle is followed – SSH as the solution provider does not have access to the contents of emails on their servers, thanks to zero-access encryption. This limited healthcare company vulnerability (and liability) in case of a data breach.

Let’s get to know each other

Want to find out more about how we safeguard mission-critical data in transit, in use, and at rest for leading organizations around the world? We’d love to hear from you.

REQUEST A DEMO

SSH