SecuMailer

Secure emailing in accordance with NTA 7516 in healthcare

SecuMailer is the solution for sending and receiving medical data in accordance with the NTA 7516.

Website
www.secumailer.com

Whitepaper
NTA 7516 Healthcare

Contents

Introduction		3
1.	**How SecuMailer works**	5
1.1	Encrypted connetion	5
1.2	Two factor Authentication (2FA)	5
1.3	Digital signature	6
1.4	Proof of delivery	6
2.	**Additional features**	7
2.1	Share large files	7
2.2	Manual shutdown 2FA	7
3.	**Implementation and management**	8
3.1	Preparation	8
3.2	Implementation	8
3.3	Management	9
4.	**Quality and security**	10
4.1	Privacy by Design	10
4.2	Security by Default	10
4.3	Guaranteed security!	11
Experience SecuMailer?		12

Introduction

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

Hospitals, pharmacies, general practitioners and other healthcare providers are exchanging more and more information online with each other and also with patients. This works quickly and efficiently, but there are also risks involved. Nobody wants medical data to be exposed. Patients must have faith that their privacy is guaranteed. That is why there are strict rules for sharing medical information. These are enshrined in the GDPR and NTA 7516.

The callenge

Although the GDPR and NTA 7516 have been in effect for several years, many organizations are still struggling to implement them effectively. Complicated security protocols can come at the expense of productivity and flexibility. For example, online portals often miss their target because most people are not waiting to log into another account and enter another password . We fully understand this drawback, and because in healthcare it is important to communicate in a targeted and effective way with patients and healthcare partners, is why we have developed a solution without notification messages and portals, entirely in accordance with the NTA 7516.

Our solution

There are several providers of secure e-mailing. SecuMailer is unique because it keeps the regular mail experience intact. As a user you don't have to do anything extra. With SecuMailer you can e-mail everything you want in a secure way. The messages arrive undamaged to the correct recipient. SecuMailer automatically performs a number of checks in the background to ensure that the e-mail traffic goes according to the GDPR and NTA7516 guidelines.

- If you send an e-mail via SecuMailer, it will always be sent via a secure connection (encrypted).
- Before we deliver e-mails to other parties that process confidential medical data, we ensure that both the sender and recipient are authenticated with 2FA by default.
- SecuMailer captures and records exactly who sends a certain message, when and to whom. Everything is accurately logged so that you always have legal proof of delivery.
- It is unique that we deliver more than 98% of the e-mails directly to the mailbox of the addressee. Only 2% of the recipients receive a notification with which they can retrieve their e-mail with an SMS message.

Innovative and unique

With our solution we are ahead of all other secure e-mail suppliers such as Zorgmail, Zivver or SmartLock. By default, we do not send a notification message with which recipients can retrieve the actual message via a separate portal. At SecuMailer we simply deliver the e-mail securely to the inbox. Only in exceptional cases, we use an alternative delivery secured with SMS message.

Our solution is groundbreaking and unique in the market, and should not be considered a superfluous luxury,. This is because in terms of security and user-friendliness there are major disadvantages to working with other portals and notification message services, that can routinely miss their goal. That is why we have opted for a radically different approach.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

The unique solution from SecuMailer

The secret of SecuMailer is under the hood. Behind the scenes we do all kinds of advanced checks to proactively check whether a secure connection can be set up with the recipient. Based on this, we can guarantee security in more than 98% of the e-mail traffic and we only have to offer an alternative route for the remaining 2%. Our solution is technically very complex, but makes it very simple for the users (both senders and recipients). They simply continue to e-mail as they always do and can be sure that the e-mail traffic is 100% secure and according to the NTA7516 guidelines.

In practice

SecuMailer can be used together with all common e-mail servers. The workplace environment will not change, so you can continue to use all your applications and platforms such as: Outlook, Office 365, Exchange, Iphone, Ipad, Macbook, Gmail for Business and the common patient records applications, HIS and ZIS (general practitioner and hospital information systems). Our solution fully meets the requirements of the NTA 7516. This makes all kinds of practical applications possible, such as:

- Making appointments and/or sharing medical results with patients.
- The granting of requests for access to (medical) files to patients and care providers.
- Transferring medical information to other healthcare providers.
- Using functional or shared mailboxes together with your colleagues.
- The provision of e-consults, reimbursed by the insurer.
- Working from home, meeting online and then sharing important matters by e-mail with colleagues, other care professionals and even patients and informal carers.

SecuMailer: The perfect balance between safety and user-friendliness in healthcare!

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

1. How SecuMailer works

With SecuMailer we make secure mailing accessible to everyone. The platform carries out the following background processes which ensures that the mail traffic fully complies with the rules and regulations of the NTA7516.

1.1 Encrypted connection

The GDPR states that the person who sends an e-mail is also responsible for the encrypted delivery of the message. That seems logical, but end-to-end encryption is not self-evident because the traditional mail puts delivery over security. No matter how well you have your own affairs in order, without extra measures you still run the risk that your message will go over an insecure connection because the recipient's mail server is not set up properly.

How do you prevent data leaks that arise because the recipient does not have a secured connection? The classic solution is to send the recipient a notification message with the request to retrieve the actual message via a secured portal. This means that organizations need an extra secured environment to make the messages available and that the recipients have to make an effort to get to their message. All in all, a cumbersome and inconvenient process. Moreover, it is unsecure because it creates a data concentration.

That is why SecuMailer has developed a completely new concept. Before we deliver a message, we check if the recipient has an encrypted connection. To do this, the software performs all kinds of complex, advanced checks in the background. The users will not notice this at all. In more than 98% of the cases, we manage to set up a secured connection and we deliver the secured e-mail immediately to the recipient's mailbox. In less than 2% of the cases we have to deliver the message via an alternative route protected by an SMS.

1.2 Two factor Authentication (2FA)

According to the NTA7516, you should not only ensure that your messages are securely encrypted, but also that both the sender and recipient are authenticated with 2FA. We also facilitate that in a simple way:

- The healthcare worker who sends the e-mail has to be authenticated so that the recipient can be sure that the message comes from a reliable source. As an organization you can arrange this in various ways, for example logging into the work environment with 2FA. For SecuMailer it doesn't really matter how an organization organizes this, we are able to connect to everything.
- The person to whom the e-mail is addressed must be authenticated so the sender can be sure that the message is sent to the correct person. SecuMailer has set up a special workflow for this that allows the recipient to go through all the necessary steps easily. This is done on the basis of an e-mail with a link to a secured environment and an SMS code. Once the authentication is successful, we deliver the original e-mail to the recipient's inbox. The e-mail therefore always is where you expect it: in the sent items and in the inbox.

Important note for the users: the person who sends an e-mail for the first time to a new address, indicates the mobile number to which the SMS code should be sent. This is a one-off action and we have also set up a "low labour" process for this.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

Only 2FA if you have to!

The authentication process involves extra e-mail and SMS traffic. We ***never*** unnecessarily bother users with this: SecuMailer only enforces the 2FA check if it is necessary. The 2FA is not necessary in the following cases:

- **The recipient has recently authenticated itself**
  If someone has successfully completed the 2FA process via SecuMailer, that authentication will in principle remain valid for 90 days. During that time, we deliver all e-mails securely to the recipient's inbox. In this we are unique! With other providers of secure mailing, the recipient must re-authenticate with each e-mail.

- **E- mailing with an external party that uses an NTA 7516 certified product**
  An important advantage in the NTA 7516 is the realization of interoperability between the certified suppliers. If you e-mail with an external party that uses SecuMailer or another certified NTA 7516 e-mail product (e.g. Zorgmail or Zivver), the recipient does not need to authenticate. We simply deliver the e-mail. Even if someone e-mails you, you never have to authenticate yourself again to receive the e-mail.

- **Internal e-mail**
  If colleagues within the same e-mail domain send each other messages, the e-mail server handles that internally and SecuMailer will not intervene.

- **Exceptions**
  SecuMailer makes it possible to register certain e-mail addresses and/or domains at a central level for which 2FA never needs to take place. For example, think of general newsletters or e-mails from the local services where you order your lunch.

1.3 Digital signature

SecuMailer automatically sends a digital signature with all outgoing e-mails. As a result, no one can change the message unnoticed. The signature guarantees the integrity of the e-mail. That also is one of the requirements of the NTA 7516.

1.4 Proof of delivery

SecuMailer records all information about sending and receipt in a log file which is accessible via the management portal. This log is the indisputable proof of delivery (like a fax). We can also send these proofs of delivery as a report.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

2. Additional Features

In addition to the standard functionality, we offer a few additional features that make it even easier for our customers to exchange information securely via email.

2.1 Share large files

In the medical world, many patient records and other confidential documents go back and forth. They also take up a lot of space in digital form. SecuMailer users can send up to 25 MB of attachments by e-mail by default, but that is not always sufficient. With our Outlook plug-in it is possible to securely share large files up to **5 Terrabytes**!

How does the SecuMailer plug-in works?
After installing the Outlook plug-in, as a user you will see an extra menu option in the mail environment with which you can upload large files to a secure environment. After uploading, SecuMailer automatically adds a link to the e-mail. The recipient of the e-mail can download the files via this link.

The uploaded files are stored securely within the EEA. As a healthcare organization you decide how long they should remain available to the recipient (maximum 90 days). After that, they are automatically deleted.

2.2 Choose manual or AI supported for 2FA

As an organization you can choose to have all employees work NTA7516 compliant, but in practice there is usually only a limited group of healthcare professionals who will have to e-mail confidential medical data as standard. Other employees come into contact with this type of sensitive information less, and therefore do not always need 2FA.

We offer them the option of installing a plug-in that allows them to determine by every e-mail whether the recipient needs additional authentication or not. The e-mails are then still sent by default with GDPR security (over an encrypted connection), only the 2FA is optional.

Nice to know
To help senders determine whether 2FA is needed, the SecuMailer plug-in contains some useful business rules so that they are advised to use 2FA at the right time. This Artificial intelligence (AI) functionality is also easy to deactivate.

2.3 Delivery of automatic mail

We have developed an API link to integrate SecuMailer with the back office to securely send automatically generated e-mails. Such a link is particularly interesting for healthcare organizations that generate large flows of personalized e-mails and who want to be sure that all those messages via an encrypted connection arrive securely in the recipient's mailbox.

Practical example: A number of medical laboratories and Corona test sites use SecuMailer to automate all mail traffic related to corona tests. In the first half of 2021 alone, we securely sent more than six million automatically personalized e-mails. An extensive workflow has been set up for this. Anyone who schedules, changes or cancels a test appointment will receive an

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

3. Implementation and Management

3.1 Preperation

The use of secure e-mailing is an important precondition for complying with the NTA7516 standard, but this is not enough. Every organization that uses SecuMailer must also take a number of other organizational measures to start working in accordance with NTA7516. The main ones are:

- Include information security policies for secure e-mail in the quality system.
- Set up 2FA at eIDAS level 'Substantial' or 'High' in the workplace.
- Organization specific measures such as:
  - Check validity of BIG registrations.
  - Set up rules for managing mailboxes when absent.
  - Inform employees, clients and partners about the impact of secure e-mailing.
  - Inventorize user groups (GDPR, NTA7516 standard or optional).
  - Inventorize e-mail addresses and mobile numbers of recipients for 2FA.
  - Inventory of exceptions to e-mail addresses/domains.

There are also some things that need to be arranged on a technical level. SecuMailer is a member of the secure e-mail coalition and supports the security institutions that internet.nl advises. Our solution uses SPF, DKIM, DNSSEC, DANE and DMARC to protect incoming and outgoing e- mail. We agree with our customers how they can make optimal use of this by means of a mandatory change in the DNS.

NTA 7516 Self-declaration
The NTA 7516 Specialist from SecuMailer will come by to give a workshop for everyone involved in the rollout. This is to ensure that the organization enters the implementation phase well prepared. The organization completes an NTA 7516 self-declaration at the end of the workshop.

3.2 Implementation

The implementation itself is very simple and takes about an hour. The customer itself (or its external management party) makes the changes in the DNS and sets up the mail relay with user groups. We provide the technical instructions for this and, if necessary, also offer further support. The implementation of the basic functionality does not affect the client environment of the users.

The implementation of the optional additional user functions is as follows:

- Users who want to use the 'Share large files' and/or 'Choose manual shutdown for 2FA' function will need a plugin which is available for Outlook 2013 and higher. The administrator manages the installation centrally or can leave it up to the individual users themselves.

We offer a REST API and SMTP API for organizations that want to automate their mail flows with a guarantee of encrypted transmission and reception. The APIs work with open standards and interfaces, making them easy to integrate. An extensive description of these interfaces is available with which customers can realize the link with SecuMailer themselves.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

3.3 Management

SecuMailer runs as SaaS in Amazon's European cloud in Dublin. That makes us very flexible. If necessary, we scale from a single message to millions of e-mails in milliseconds without any infrastructure or software changes. In terms of performance or stability, it makes no difference how many users use the application or how intensively they do it. We do not have to make any agreements about this in advance. Our customers mail as much as necessary, and only pay for the capacity they actually use. Because SecuMailer runs centrally in the cloud, you don't have to worry about technology and you can focus entirely on functional management.

All customers get access to their own management portal where the following functionality can be found:

Events: This concerns the comprehensive audit log in which all information about the shipment and delivery is recorded. This gives customers insight into all their e-mail traffic. If an e-mail is refused (eg in the event of a typo in the e-mail address), this can also be found in the log. The organization always has conclusive proof of all e-mails that have been securely delivered.

Accounts: A list of e-mail addresses and telephone numbers that SecuMailer uses to send the recipients an SMS with a code to authenticate themselves. This list can be entered into the SecuMailer platform via batch entry of all known contacts. In addition, senders can easily add the details of new contacts to the list individually themselves.

Mailbox Settings: For each e-mail domain, the customer configures a number of settings here (eg: a list of e-mail domains and/or addresses that are exempt from NTA7516, the location and storage period of large files and error messages).

Customers also get access to their own online environment to submit reports, questions or change requests to the SecuMailer support team. All user manuals and technical documentation are also available in the management portal.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

4. Quality and security

4.1 Legal framework

The care solution from SecuMailer is based on the GDPR and the NTA7516 standard. Both standards require different operational organization and measures.

In brief:

- The NTA7516 is about sending e-mails that contain personal health information. The sender is not only responsible for encrypted transmission (preventing data leaks), but must also verify whether the e-mail reaches the correct recipient (to ensure the professional confidentiality of the doctor).

The SecuMailer software is fully NTA 7516 certified. This goes further than the extra authentication, the NTA 7516 describes exactly the requirements suppliers of e-mail solutions must meet in the field of availability, integrity, confidentiality, user-friendliness and interoperability. These pillars are further specified in the so-called statement of inclusions and exclusions, which provides a complete overview of all NTA 7516 criteria.

SecuMailer is one of the initiators of the NTA 7516 standard and therefore knows exactly how the standard works. In fact we are proud that the standard is partly based on the architecture of SecuMailer.

4.2 Privacy by Design, Security by Default

SecuMailer is a Dutch company. We develop all our software with user security and privacy in mind. We use cloud computing services from AWS Dublin and Frankfurt. AWS has direct agreements with the European Union about privacy legislation and measures to prevent data from European companies from falling into American hands. The messages you send via SecuMailer are 100% secure with us.

Less is more
An important principle in the GDPR is ***data minimization***. That has always been the starting point for our solution. We do not store data that we do not need, so that we do not run unnecessary risks of data leaks. The e-mails we transport are gone from our system within seconds. We do not do anything with them and do not store them. We only keep delivery notes with metadata about the e-mails to prove that the message was delivered securely.

"An e-mail message takes less than 3 seconds on the SecuMailer platform. We do not store it, but deliver it directly to the recipient. Very secure, because nothing can leak that way."

We only keep the encrypted (unreadable) message if we do not deliver the message immediately because the recipient does not have a secure connection. We do this for a maximum of 90 days in a secure place in the European (EEA) cloud. When the retention period has expired, it will be permanently deleted.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

User-friendly and secure
The GDPR states that employers must take measures to prevent human errors. This does not mean that you can just monitor employees to check whether they are ignoring certain warnings, for example. That is not necessary with SecuMailer as we place as little responsibility as possible on the users. Our software enforces that confidential e-mails also remain confidential. The GDPR and NTA7516 checks take place automatically if and when necessary, no more and no less.

Transparency and **equality** are important starting points for the GDPR. That is why we do not monitor how, where or when recipients read their e-mail. We only log when the encrypted message has been delivered to the recipient's mail server. With this confirmation of delivery you fully comply with your information obligation from a legal point of view.

Our choice for Privacy by Design and Security by Default has a number of functional consequences. For instance, SecuMailer deliberately does not support the following functions:
- Withdraw sent messages
- Monitoring employee e-mail behavior
- Read receipt from the recipient

4.3 Guaranteed security!

SecuMailer is all about security. That is the core of our proposition. In terms of data security, we are the absolute frontrunner in the market. We meet the most stringent requirements in the field of e-mail security and are ISO 27001/:2017, NEN 7510: 2017 and NTA 7516:2019 certified. We have had an IT security assessment performed by Securify.

External audit confirms it: SecuMailer is waterproof and 100% NTA 7516-proof!

Some quotes from the report:

"SecuMailer provides a secure e-mail platform to customers. All e-mail communication is performed over GDPR-compliant secure channels. If a remote server does not support a secure (TLS) connection, the e-mail is blocked to ensure that no information is transmitted in clear text."

"Securify has performed several tests, but has been unable to compromise the SecuMailer platform during the assessment. SecuMailer is being built with security in mind, giving the platform a secure foundation for future development."

"The overall security level of SecuMailer is good. The developers clearly use a defensive style with security in mind as they are developing the program. This ensures that the end product will be more secure from outside attacks."

"Securify was not able to find any way for an outside organization to obtain data and / or e-mails from other organizations."

Secumailer
+31320337381
info@secumailer.com
www.secumailer.nl

Experience SecuMailer?

Discover the convenience of SecuMailer and request a free trial account. This allows you to send no less than 20 secure emails in two weeks. Of course we are also happy to come by for a demo without any obligation.

Do you have any other questions? Please feel free to contact info@secumailer.com or 0320-337381.

Yvonne Hoogendoorn, CEO SecuMailer