zivver

NTA 7516 Checklist

Everything you need to know about the standard for secure ad hoc communication

□ Checklist

Contents

Introduction

In September 2018, the NEN was commissioned by the Dutch Ministry of Health, Welfare and Sport and the Healthcare Information Council to develop the NTA 7516. The Dutch Data Protection Authority (AP) found that the majority of data leaks occur in relation to the exchange of personal, often healthcare related, information.

Although a great deal of these data leaks were related to human error, such as misdirected email, it also became clear that many organisations still used ‘regular’ email to share sensitive healthcare related information. However, regular email lacks the encryption and authentication controls required under GDPR (General Data Protection Regulation) and other relevant laws and standards to ensure communications are properly secured.

There was also a need for clarity concerning how digital communication channels, such as email, could be used to securely exchange sensitive information between separate solutions; this is known as interoperability.

The NTA 7516 was designed to address the above issues. The NTA 7516 standard currently applies in the Netherlands only. However, it is expected that this or similar more stringent standards will be rolled out further within the European Union (EU).

What is NTA 7516?

The NTA 7516 is the standard for secure ad hoc communication of healthcare related information. The standard was created by the NEN on behalf of the Ministry of Health, Welfare and Sport, the Healthcare Information Council and municipalities.

Ad hoc communication includes email, chat, portals, messengers, and so on. In other words, all forms of communication that take place between people.

The standard describes over 25 requirements concerning availability, integrity, confidentiality, user-friendliness, interoperability, policy and logging, which organisations and the solutions they use must meet in order to be compliant.

NTA 7516 has two key objectives:

- To provide clear conditions around the use of email, chat, and messaging solutions. This ensures the secure and reliable exchange of personal health information
- Ensures that messages can be exchanged between solutions, regardless of supplier. This is known as interoperability or multichannel communication.

Compliance with NTA 7516 is not compulsory. Ad hoc communication happens on a voluntary basis, after all. Many systems used by various organizations are already connected; this is covered by NEN 7512. If your organization does engage in ad hoc communication, every professional handling health information must comply with the requirements of NTA 7516.

There are other standards for structured (so not ad hoc) communication, such as NEN 7512.

Who must comply with NTA 7516?

NTA 7516 applies to all organizations that use ad hoc communication to share health information. For example, this includes emailing examination results, confirming an appointment, using a chat functionality with colleagues, or sharing medical data through email with an insurance company.

NTA 7516 is also the foundation for information exchange in the chain described in the Mandatory Mental Health Care Act (Wet verplichte ggz, or Wvggz). As a result, NTA 7516 not only applies to hospitals, mental health institutions, elderly care organisations, general practitioners and other healthcare organisations and professionals, but also to municipalities, the public prosecutor's office (OM), and legal service providers and insurers. Organizations must use of NTA 7516-compliant solutions which meet the standards outlined for secure email or chat.

This means that (a large part of) the standard also applies to solution providers who want to qualify as a solution for secure e-mail or secure chat. We recommend that you use our supplier checklist. This ensures that your organization and the suppliers you work with are prepared for the new standard that will soon be enforced by the Dutch Data Protection Authority.

While, for now, NTA 7516 is a Dutch standard, the NEN has announced plans to initiate a procedure to make it a European CEN standard.

The Netherlands is the first country to establish a standard for secure ad hoc communication, but such standards are usually accepted by other CEN members (either individually or as a group), which include all 28 member states of the European Union.

Prepare for NTA 7516

The next section includes a checklist to help your organisation meet the requirements for NTA 7516.

Checklist: How to comply with NTA 7516

Our useful NTA 7516 checklist will help you to identify what your organization needs to do to comply with the standard. Please note, where the 'supplier' is mentioned we are referring specifically to the suppliers of solutions used for ad hoc communication.

Each item is followed by a number in brackets which refers to the relevant article of the NTA 7516. There, you will find more background information for that subject.

Record minimum requirements (6.1.1)

□ We have recorded minimum requirements and their rationale for all normative criteria.

Minimum Availability (6.1.2)

□ Our supplier SLAs include measurable agreements on >99.8% availability, with clear consequences should the supplier fail to meet these commitments.

□ All relevant suppliers will provide current, verifiable and objective insight into availability for the past 12 months, preferably in real time through a status page.

Maximum Data Loss (6.1.4)

□ Our supplier SLAs include clear and measurable agreements regarding the prevention of data loss, along with a guarantee to inform the sender within 24 hours if information cannot be delivered, with clear consequences should the supplier fail to meet these commitments.

Verification of Origin (6.1.5)

□ We have ensured that access to any mailbox, from any client (for example, logging into Outlook from work, from a mobile app, or remotely), is only possible with verified multi factor authentication. It is therefore impossible to access sensitive information with only a password.

□ We have ensured that all emails which include personal health information are sent with a DKIM signature, as described in the relevant sections of the Technical guideline NTA 7516 for suppliers of email services from Informatieberaad Zorg.

□ We have ensured that all emails which include personal health information are sent with a digital CAdES signature, as described in the relevant sections of the technical guideline mentioned above.

Data Integrity (6.1.6)

□ We have ensured that communication between all email clients and our mail server is secured with the appropriate safeguards (TLS 1.2 or higher and validation of certificates).

Non-Repudiation of Sender (6.1.7)

□ For our email service, we have implemented DKIM, DMARC and SPF in line with the instructions in the relevant sections of the technical guidelines.

□ We ensure that the recipient has visibility of which individual has sent an email from a functional mailbox. We have also ensured that the recipient can visually assess whether a message was sent securely.

Authorization of Sender (6.1.8)

□ We have established a policy detailing the types of care providers which are authorized to access and/or communicate about information of patients/clients. This policy has been developed into technical access to functional (team) or delegated mailboxes.

□ We have safeguarded logging of access by individual employees to mailboxes and specific email.

Data Confidentiality (6.1.9)

□ We have ensured that messages are stored encrypted on both our suppliers' mail servers as well as on the client software servers located in GDPR-compatible jurisdictions.

□ We have ensured that individuals without authorization cannot access the data or keys required to access data.

□ We are aware of our suppliers' options for safeguarding data confidentiality in the event that a message is accidentally sent to a receiver without authorization to access that message.

□ We have concluded a data processing agreement with all suppliers involved in sending and receiving emails containing personal health information.

Access Confidentiality (6.1.10)

□ We have ensured that access to any mailbox from any client (for example, logging into Outlook from work, from a mobile app, or remotely) is only possible after logging in.

□ We have ensured that access by our own employees to messages received is logged at an individual level.

□ We have ensured that emails containing personal health information which are sent to recipients who do not comply with NTA 7516 are only accessible after the receiver has been verified with multi factor authentication (for example, by sending an SMS message to a verified telephone number).

Communication Confidentiality (6.1.11)

□ We have ensured that during data transfer via the internet or between client and servers, messages are protected against unauthorized access.

□ We have ensured that, in the event that a receiver does not comply with NTA, emails are sent as notification emails only. As such, the message can only be accessed once verified by multi factor authentication. In the event that the receiver complies or claims to comply, this can only occur in accordance with the requirements described in the technical guideline. Emails containing personal health information are not sent as 'regular' emails.

Transfer reasons (6.1.12)

- □ We have established a policy that clearly defines the rules any professional should follow when sending messages, as well as the various confidentiality considerations. It describes the valid reasons for transferring the information (sending the message), and the party tasked with monitoring enforcement of the policy.

International Ad Hoc Messaging (6.1.13)

- □ We have ensured that messages which we are responsible for are stored in the EEA (European Economic Area).
- □ We have ensured that messages sent from outside the EEA (European Economic Area) are protected appropriately.

Communication Continuity – Replies (6.1.14)

- □ We have ensured that any recipient who does not comply with the NTA can reply securely through our secure email service without having to create an account.

Communication Continuity – Forwarding (6.1.15)

- □ We have ensured that any recipient that does not comply with the NTA can forward a message to a third party securely. In the event that, when forwarding, security cannot be ensured, the recipient is notified of this.

Security by Convenience (6.1.16)

- □ We have ensured that in the event that personal health information is sent, the 'regular' send button initiates secure transfer that complies with the NTA. Users do not have to click another 'Send' button.

Legibility (6.1.17)

- □ We have ensured that recipients of secure messages are not required to create an account with our secure email service in order to read, reply to, forward or download a message.
- □ Our secure email solution complies with the relevant requirements of the WCAG 2.0, ensuring recipients can access, read, reply to etc. secure messages. The supplier of our secure email solution has published on their website a statement of accessibility concerning the guideline WCAG 2.0.

Individual Copy (6.1.18)

- □ Recipients of secure messages can easily and securely save a message at a location of their choice, in a format that is accessible for regular client software (for example as a .emi file).

Connecting Records (6.1.19)

- □ Employees can easily and securely store messages in the Electronic Patient Record.

Implementation Requirements (6.2)

Based on the requirements listed under 6.1, we have selected one or more solutions for secure email and chat applications. We have recorded how the suppliers of these solutions safeguard these requirements. The implementation requirements have been recorded for:

- □ Email (6.2.2): concerning the establishment of a secure connection (6.2.2.1) and the exclusive limitation of metadata to what is strictly necessary, or the securing of these metadata (6.2.2.2).
- □ Secure chat applications (6.2.3).

Usage Policy (6.3)

We have adopted a policy on the deployment of the implemented communication tools. This policy includes rules on:

□ Replacing colleagues during their absence.

□ Mandating and delegating access to ad hoc messages.

□ Access to information in the absence of a formal therapeutic relationship (in care institutions).

□ Access to functional mailboxes (for example: orthopedics@example.com).

□ Usage of a directory.

□ Usage of functionalities that can result in the withdrawal or modification of ad hoc messages.

□ Usage of automated functionalities for the receipt of ad hoc messages (including but not limited to auto reply and read reports).

□ Retention periods.

□ Key management, if appropriate – options for forensic investigation (see NEN 7510 2:2017, 16.1.1) and key escrow.

□ Responsibilities.

□ Transfer reasons.

□ Continuation of service provision in the event of bankruptcy of the communication solution provider.

□ Informing individuals of the secure email service.

Program for Monitoring and Compliance (6.4.1)

We have adopted a program to:

□ i) Continuously monitor compliance with the rules of usage.

□ ii) Annually compare the selected and implemented communication tools against the set criteria.

□ iii) Biannually assess the set criteria for appropriateness and suitability.

Compulsory Logging of Actions and Events (6.4.2)

Categories of events that must be logged:

□ All events concerning the sending of messages.

□ Withdrawal of sent messages.

□ Modification of sent messages.

□ Deletion of sent messages at the sender‘s end.

□ All events concerning the receipt of messages.

□ Access to received messages.

□ Deletion of received messages.

□ Forwarding of received messages.

□ Creation or deletion of an email or chat account.

□ Assignment, modification and withdrawal of authority for an email and/or a chat account.

All events related to user verification for:

□ Reacting to messages.

□ Accessing log data.

□ Modifying or deleting log data.

Communication Initiated by Individuals (6.5)

□ We have widely announced the easy ways in which individuals can initiate secure communication with our organisation (for example, on our website).

Assurances (7.1)

□ We only partner with suppliers of secure email solutions who publish in a publicly accessible register which criteria their solution does and does not meet.

Multichannel Communication (7.2)

□ We have ensured that our secure email service can be connected to other NTA 7516 services, based on the standards and requirements described in the technical guideline.

Implementation (7.3)

□ We have ensured that our suppliers of secure email solutions publish in a transparent manner which requirements from the NTA 7516 are met by the secure email service, and in what way.

Usage Rules for the Communication Service Supplier (7.4)

□ We have safeguarded that our suppliers of secure email solutions have adopted rules for how they and those who work for them may use their authority for processing ad hoc messages, in line with the requirements of ISO 27001, NEN 7510 and NEN 7513.

Monitoring and Compliance (7.5)

□ We only work with communication service providers of suppliers of secure email solutions with a valid NEN-ENISO/IEC 27001 certificate, or a valid NEN 7510 certificate that includes the items of NTA 7516.

□ We have determined that our suppliers have a program in place for the continuous monitoring of the performance of the published criteria. The appropriateness of the published implementation regulations and compliance with the usage rules are annually assessed, and the subsequent results are recorded.

Certification (7.6)

□ We only work with communication service providers that extend guarantees that they will meet the requirements of NTA 7516 that apply to them as soon as possible.

Practical steps, policy and timelines

Implementation of NTA 7516 can have implications on various parts of your organisation. To help you prepare and identify any necessary changes, we made an overview of the recommended actions. Follow these guidelines to prepare your organisation for full compliance with the new standard. You can save time by using the handy checklists and overviews we share in this guide.

Overview of practical steps

1. Establish a policy
2. Ensure proper security for the mail server with the stored emails
3. Implement a service for secure email communication
4. Implement a solution for secure outgoing communication to receivers who do not comply with NTA
5. Implement a solution that safeguards interoperability with NTA-7516 compliant receivers
6. Implement a solution for third parties to initiate communication securely
7. Consider a solution for smooth inclusion of emails in medical records

Step 1

Establish a policy on:

- Replacing absent colleagues.
- Mandating and delegating access to ad hoc messages.
- Access to information in the absence of a formal therapeutic relationship (in care institutions).
- Access to functional mailboxes (for example: orthopedics@example.com).
- Usage of a directory.
- Usage of functionalities that can result in the withdrawal or modification of messages.
- Usage of automated functionalities for the receipt of messages (for example: autoreply and read reports).
- Retention periods.
- Key management, if appropriate; options for forensic investigation and key escrow.
- Responsibilities.
- Transfer reason: how can the receiver ensure that the sender was authorized to send the ad hoc message?
- Continuation of service provision in the event of bankruptcy of the communication solution provider.

Step 2

Ensure proper security for the mail server with the stored emails. This implies:

- Employees can only access sensitive data using 2FA.
- Access to sensitive information must be logged.
- Implement appropriate safeguards for availability and accessibility.

Step 3

Implement a service for receiving email securely. This implies:

- The service must support DANE, or it must be possible to validate the certificate using PHIX.
- Implement appropriate safeguards for availability and accessibility.

Step 4

Implement a solution for secure outgoing communication to receivers who do not comply with NTA. This solution must:

- Safeguard superb receiver authentication.
- Ensure superb encryption without access to unauthorized people.
- Provide security by default.
- Not force receivers to create an account.
- Offer receivers the opportunity to reply securely.
- Offer receivers the opportunity to forward securely.
- Be ISO 27001/NEN 7510 certified.
- Log employee actions and access to information by guests.
- Offer appropriate safeguards for availability and accessibility.

Step 5

Implement a solution that safeguards interoperability with NTA-compliant receivers.

- Focus on how integration is established with users who are not NTA-compliant.
- Ensure logging of all transactions and actions.
- Implement appropriate safeguards for availability and accessibility.

Step 6

Implement a solution for third parties to initiate communication securely. This implies:

- Third parties must be able to securely initiate contact with the organisation.
- Recipients do not need an account.
- Announce the solution clearly on your own website.

Step 7

Consider a solution for smooth inclusion of emails in medical records.

- Professionals can easily prepare an ad hoc message for connection, after which it can be securely connected to the right record.

Timelines

Organisations (professionals) are responsible for compliance with NTA 7516. They must select one or more compliant suppliers of solutions which allow for secure information exchange. Below, you can find an indication of the time needed to complete the required activities to comply with the standard NTA 7516.

Indication of the time required	Activities
Approximately 1 month	• Inventory of current flows for ad hoc communication. • Determination of the requirement gaps for NTA 7516. • Deciding on how to close the gaps (policy, current or new supplier).
Approximately 1 month	• Finish market research of possible suppliers. • Conclude contracts with new suppliers. • Develop new/additional policies.
Approximately 1.5 month	• Start preparations for the onboarding of new suppliers. • Start preparing new policy.
Approximately 1 month	• Technical onboarding new suppliers. • Introduction of new suppliers and policies to employees. • Fine-tuning compliance monitoring.

zivver

Zivver

59-60 Gainsborough House,
Thames Street Windsor,
Berkshire, SL4 1TX
United Kingdom

+44 (0) 203 285 6300
contact@zivver.com

zivver.com

Kon. Wilhelminaplein 30
1062 KR Amsterdam

085 016 0555
contact@zivver.com

zivver.nl

linkedin.com/company/zivver facebook.com/zivver @zivver_en / @zivver_nl

← →