Blauwdruk NTA7516 beleid voor veilige e-mail

23 maart 2023

Versie 1.0 | Auteur: Niels van den Berkmortel

Versiebeheer

Versie	Datum	Wat	Auteur
0.1	07-04-2022	Initiële opzet beleidsplan	Niels van den Berkmortel
0.1	09-05-2022	Review initiële opzet, aanpassingen gemaakt ten aanzien van toepasbaarheid	Gijs Schilten
0.2	17-05-2022	Aanpassingen op basis review Gijs Schilten	Niels van den Berkmortel
0.3	13-09-2022	Aanpassingen op basis review Mariska van Laarhoven	Sharda Kalloe

Inhoudsopgave

1 Inleiding

De NEN heeft in opdracht van het Ministerie van Volksgezondheid, Welzijn en Sport de Nederlands Technische Afspraak 7516 (bekend als NTA7516) ontwikkeld in samenwerking met zorgprofessionals en leveranciers van ad hoc communicatiediensten voor veilige e-mail en chat.

In samenwerking met de NEN, zorgprofessionals en leveranciers is de **NTA7516**:2019 [1]opgesteld. De norm stelt zowel functionele als technische eisen waaraan een leverancier van een veilige e-mailoplossing en ook een zorgaanbieder moet voldoen. De norm stelt eisen aan het veilig en interoperabel communiceren tussen verschillende zorgaanbieders met verschillende oplossingen.

Algemeen beleid – specificeren waar nodig
Om als zorgaanbieder aan de NTA7516 te voldoen wordt in paragraaf 6.3 een beleid vereist ten aanzien van veilige e-mail of chat. In het beleid moeten een aantal functionele zaken beschreven worden met betrekking tot rechten en plichten waaraan een zorgaanbieder moet voldoen.

Ten behoeve van de leesbaarheid wordt er verder in dit document alleen gerefereerd naar veilige e-mail(oplossingen) en niet naar chat functionaliteiten.

1.1 Doel

Het doel van dit document is om als blauwdruk te dienen voor het beleidsplan zoals deze vereist wordt in de NTA7516:2019 voor het uitwisselen van gegevens via veilige e-mail. In dit document worden de minimale vereisten vanuit de NTA behandeld met passende beleidsregels. Hiervoor is onder andere gebruik gemaakt van de stappenplannen van het Zorg Informatie Beraad.[2]

[1] https://www.nen.nl/nta-7516

[2] https://www.informatieberaadzorg.nl/programmas-en-projecten/publicaties/publicaties/2019/12/16/index, Deel 2 – Toolkit

2 Beleid NTA7516

2.1 Waarnemen

De zorg stelt hoge eisen aan informatiebeschikbaarheid en het is hierbij cruciaal dat informatie 24/7 beschikbaar gesteld kan worden voor het kunnen leveren van goede zorg. Daarom is het van belang binnen de organisatie een beleid te hebben opgesteld voor omgang met veilige e-mail ten aanzien van de waarneming bij de afwezigheid van een collega.

Bij een **functionele veilige e-mailbox** hebben meerdere zorgprofessionals binnen de organisatie toegang tot de informatie in de veilige e-mailbox en is het van belang dat de binnenkomende informatie goed wordt verwerkt en doorgegeven. Verder wordt er rekening gehouden met de aanwezigheid dan wel afwezigheid van collega's. Ook zijn in dit beleidsplan de rollen en verantwoordelijkheden gedefinieerd.

De zorgprofessional met een **persoonlijke veilige e-mailbox** is zelf verantwoordelijk voor het verwerken van de binnengekomen informatie. Ook het regelen van toegang dan wel doorsturen van informatie naar de betreffende waarnemende collega is een verantwoordelijkheid van de eigenaar van de persoonlijke mailbox.

Beleid functionele veilige e-mailbox
De functionele veilige e-mailbox wordt door meerdere personen beheerd en hiermee wordt voorzien dat de mailbox beheerd wordt tijdens (tijdelijke) afwezigheid van een directe collega.

Beleid persoonlijke veilige e-mailbox
Bij afwezigheid van de zorgprofessional met een persoonlijke veilige e-mailbox dient de afwezige collega, indien van toepassing en voor zover noodzakelijk voor de behandeling van een patiënt, na kennisneming van afwezigheid tijdig de taken en verantwoordelijkheden te hebben overgedragen. Hiervoor zijn er twee opties:

- Optie 1: De zorgprofessional heeft de toegang tot de persoonlijke e-mailbox overgedragen aan een waarnemende collega voor het doorsturen van urgente berichten binnen de organisatie (mandateren).
- Optie 2: De zorgprofessional heeft zowel de toegang als de verantwoordelijkheid overgedragen aan een waarnemende collega voor het controleren en beantwoorden van urgente berichten (delegeren).

Rol	Verantwoordelijkheid	E-mailadres	Intrekken of wijzigen van e-mailberichten
Eigenaar/ beheerder beveiligde e-mailbox	Dagelijkse afronding van de binnengekomen e-mail berichten, beantwoorden wanneer noodzakelijk of doorverwijzen. Binnen een werkdag de openstaande communicatie afhandelen en eventueel reageren op de e-mail. Daarnaast beleid opstellen, monitoringsplan opstellen, handhaving en acteren op bevindingen.	Bas.jansen@apotheekjansen.nl	Ja, mits toestemming is gegeven door de ontvanger Ja, bij berichten binnen hetzelfde domein is dit toegestaan Ja, berichten mogen ingetrokken worden, er moet wel rekening gehouden worden met de implicaties voor de ontvanger
Assistenten	Dagelijkse afhandeling van binnengekomen e-mailberichten volgens protocol. Archiveren van informatie in het XIS of archief Doorsturen binnengekomen e-mailbericht naar de juiste persoon binnen de organisatie.	assistenten@veiligemail.nl of recepten@veiligemail.nl	Ja, berichten wijzigen of intrekken is toegestaan mits expliciete toestemming van de beheerder van de beveiligde e-mailbox

Tabel 1. Overzicht met rollen en verantwoordelijkheden met betrekking tot de veilige e-mailoplossing

2.3 Toegang veilige e-mail zonder directe behandelrelatie

In de praktijk zijn het de assistenten en het secretariaat die toegang en beheer hebben van de beveiligde e-mailbox. Welke werkzaamheden en verantwoordelijkheden voor toegang van de beveiligde e-mailbox dat zijn is vastgelegd in Tabel 1.

Beleid

- Toegang tot e-mailberichten, die tot een patiëntendossier gerekend moeten worden, kan alleen worden verleend aan een medewerker die hiërarchisch valt onder de betreffende zorgverlener van de persoonlijk veilige e-mailbox.
- Een medewerker zonder directe behandelrelatie mag alleen veilige e-mailberichten openen wanneer het noodzakelijk is om de taken binnen de verantwoordelijkheden van de persoon/rol in kwestie uit te voeren.

2.3.1 Functionele e-mailboxen

Hiervoor dienen personen aangewezen te worden met toegang en de mogelijkheid om de informatie op de juiste plek in het systeem op te slaan (Tabel 1). Zij zijn verantwoordelijk voor het verwerken van de patiëntgegevens die binnenkomen op de functionele veilige e-mailbox (Box 1).

Box 1. Protocol verwerken patiëntgegevens vanuit de veilige e-mail

- Veilige e-mail komt binnen
- Belangrijke patiëntinformatie wordt geselecteerd
- De patiënt wordt opgezocht in het XIS op basis van
    - Naam + voorletters en achternaam
    - Geboortedatum
    - Indien bekend; BSN
- Informatie wordt opgeslagen als ongestructureerde tekst of gestructureerde informatie in het XIS
- De betreffende zorgprofessional met een directe behandelrelatie met de patiënt wordt op de hoogte gesteld van de nieuw binnengekomen informatie over de patiënt.

2.4 Gebruik adresboek

Bij het versturen van privacygevoelige informatie in een veilige e-mail is het belangrijk dat men het juiste e-mailadres gebruikt. Wanneer een eigen samengestelde adreslijst wordt gebruikt dienen er praktijkregels te worden opgesteld om zo goed mogelijk de gegevens up-to-date te houden.

Beleid

- *Voor het adresboek wordt gebruik gemaakt van een eigen adresboek in het XIS of e-mailclient (bijvoorbeeld Outlook);*
- *Voor het adresboek wordt gebruik gemaakt van het adresboek van de leverancier van de veilige e-mailoplossing;*
- *Voor het raadplegen van het adresboek wordt gebruik gemaakt van het landelijk ZORG-AB met integratie vanuit Microsoft Office (Add-in);*
- *Voor het ZORG-AB is alleen de eigenaar/beheerder bevoegd de in het ZORG-AB opgenomen gegevens aan te passen. Dit gebeurt via het webportaal van ZORG-AB (zie Bijlage A 2.22).*

Wanneer een e-mailadres uit het bovengenoemde adresboek wordt geselecteerd mag men ervan uitgaan dat het adres valide is en de informatie op de juiste plek terecht komt.

Mocht de mail niet naar de juiste persoon gestuurd zijn neem dan contact op met de onbedoelde ontvanger om de mail te verwijderen. De informatie is niet in te zien door

derden vanwege de benodigde authenticatie. Echter, het kan zijn dat het 06-nummer (voor de sms-verificatie) wordt gekozen dat hoort bij het verkeerde e-mailadres.

2.5 Intrekken of wijzigen van e-mail berichten

Binnen de veilige e-mailapplicatie is het mogelijk om berichten in te trekken of te wijzigen. Hierdoor is de originele informatie niet meer beschikbaar voor de ontvangende partij. De verantwoordelijkheid voor het intrekken van berichten is vastgelegd in Tabel 1.

Beleid

- ***Optie 1:*** *Men mag geen berichten intrekken of wijzigen zonder afstemming met de ontvanger.*
- ***Optie 2:*** *Men mag alleen berichten intrekken of wijzigen wanneer het veilige e-mailbericht binnen hetzelfde domein is verstuurd …@zorgverlener.nl*
- ***Optie 3:*** *Men mag berichten intrekken of wijzigen wanneer er gegronde redenen zijn dit te doen en er duidelijkheid bestaat over de implicaties van de verandering of verwijdering van het bericht voor de ontvanger. De gegronde redenen voor het intrekken van het bericht dienen wel vastgelegd te worden.*

2.6 Gebruik geautomatiseerde functies

Veilige e-mailapplicaties hebben vaak de mogelijkheid om geautomatiseerde functies in te stellen, waaronder de autoreply bij afwezigheid en de automatische leesbevestiging.

Autoreply: stel deze alleen in bij langere afwezigheid en wanneer er kans bestaat dat er een risico is voor de verzendende partij als het bericht niet gelezen wordt. Door het gebruik van een auto-reply is het voor de verzendende partij duidelijk wie zij moeten contacteren (Box 2.).

Box 2. Voorbeeld autoreply bericht

Beste lezer,

Bedankt voor het bericht. Op dit moment ben ik niet aanwezig en uw bericht zal niet worden gelezen of worden doorgestuurd. Ik ben per … terug en zal zo spoedig mogelijk bij u terugkomen met een antwoord. Mocht u eerder contact wensen neem dan contact op met:

Contactpersoon 1
Contactpersoon1@e-mail.nl
+31……

Met vriendelijke groet,

…..

Leesbevestiging: een automatische leesbevestiging wordt ingesteld wanneer de verzendende partij zeker wil zijn dat het bericht goed is aangekomen en wordt geopend.

Automatisch doorsturen: automatisch doorsturen kan worden ingesteld wanneer bij afwezigheid het bericht doorgestuurd moet worden naar een ander e-mailadres. Dit wordt afgeraden omdat het om patiëntengegevens gaat waarbij

Beleid

- ***De automatisch doorsturen functie*** *wordt niet gebruikt binnen de organisatie*
- ***De autoreply functie*** *wordt alleen in gebruik genomen bij afwezigheid langer dan 48 uur, waarbij een officiële overdracht is gedaan van rollen en verantwoordelijkheden binnen de organisatie. Box 2 geeft een voorbeeld van een autoreply bericht.*
- ***De functie automatische leesbevestiging*** *wordt niet gebruikt binnen de organisatie.*
- *Het* ***automatisch doorsturen*** *van berichten naar een ander domein (zoals een privé e-mailadres) is niet toegestaan.*

2.7 Bewaartermijnen

Een zorgprofessional is verplicht om een dossier bij te houden waarin alle relevantie (medische) gegevens staan. Wanneer een veilige e-mail binnenkomt met relevante informatie dient deze informatie bewaard te blijven, dit kan door deze informatie op te slaan in het XIS van de zorgprofessional. Daarna mag de correspondentie verwijderd worden.

E-mail is een transportmiddel om bijv. persoonsgegevens te transporteren, voor de **inhoud** van e-mailberichten gelden de wettelijke bewaartermijnen.
E-mailberichten maken geen deel uit van het patiëntdossier. Relevante informatie uit e-mailverkeer met patiënten dient daarom **onverwijld** in het patiëntdossier opgenomen te worden zodat het toegankelijk is voor allen die bij de behandeling zijn betrokken.

Beleid

De bewaartermijn voor een medisch dossier is 20 jaar na de laatste wijziging in het dossier [3].

Dit kan in samenspraak met de leverancier geautomatiseerd worden of dit wordt handmatig gedaan zoals in het protocol van afhandeling van patiëntinformatie besproken (paragraaf 3.3.1).

[3] https://www.rijksoverheid.nl/onderwerpen/rechten-van-patient-en-privacy/uw-medisch-dossier/bewaren-medisch-dossier#:~:text=Algemene%20bewaartermijn%20medisch%20dossier,laatste%20wijziging%20in%20uw%20dossier.

2.8 Sleutelbeheer

Het sleutelbeheer valt veelal onder de verantwoordelijkheid van de leverancier van de veilige e-mailoplossing. Met sleutelbeheer worden geen fysieke sleutels bedoeld maar cryptografische sleutels die het onmogelijk maken voor onbevoegden om toegang te krijgen tot de inhoud van het veilige e-mailbericht.

Bij het veranderen van de leverancier van veilige e-mailoplossing kan het door de versleuteling voorkomen dat het bericht niet te ontgrendelen is door een andere leverancier, dit is geen wenselijke situatie en hier dienen afspraken over gemaakt te worden met zowel de oude als de nieuwe leverancier van de veilige e-mailoplossing.

Voor een beheerder is het mogelijk om toegang te verlenen tot een mailbox ten behoeve van forensisch onderzoek, door middel van een wachtwoord reset en eventueel het verwijderen van 2FA.

Beleid

Bij het maken van afspraken met de leverancier van de veilige e-mailoplossing dienen alle veilige e-mailberichten mee gemigreerd te worden. Na migratie worden e-mailberichten vanuit de oude oplossing leesbaar getoond door de oplossing van de nieuwe leverancier. Dit wordt vooraf afgestemd met zowel de oude als de nieuwe leverancier van de veilige e-mailoplossing.

2.9 Verantwoordelijkheden

Uiteindelijk dienen verantwoordelijkheden nagekomen te worden. Onder andere het reageren of handelen op een veilige e-mailcommunicatie, maar ook het monitoren van bevindingen en het acteren op de bevindingen. Denk hierbij ook aan het onderhouden van het e-mailbeleid en het handelen bij uitzonderingen of wanneer er wijzigingen doorgevoerd dienen te worden (Tabel 1).

Chat applicaties zijn bij voorkeur beschreven in beleidsregels en gedragscodes en zijn van toepassing voor alle rollen binnen de organisatie. Denk daarbij aan o.a. het Informatiebeveiligingsbeleid, en Gedragscodes voor e-mail en internet gebruik.

Beleid

De rollen en verantwoordelijkheden zijn uitgewerkt in Tabel 1.

2.10 Verzendingsgronden

Verzendingsgronden zijn de grondslagen waarom (bijzondere) persoonsgegevens verstuurd mogen worden. De AVG telt zes grondslagen waarom de informatie toch gedeeld mag worden.

Beleid
Stel regels op over mogelijk van toepassing zijnde grondslagen voor verzending, in samenwerking met de functionaris gegevensbescherming binnen de zorgpraktijk, met de brancheorganisatie of anders met een specialist in privacy recht.

2.11 Continueren dienstverlening na faillissement

Het kan zijn dat de leverancier van de veilige e-mailoplossing ophoudt te bestaan, daarom moeten door middel van het contract regels opgesteld worden wat er gebeurt met de informatie die op de servers van de leverancier van de veilige e-mailoplossing staan.

Beleid

- *Stel een exit clausule op samen met de leverancier van de veilige e-mailoplossing, waardoor data altijd gemigreerd kan worden van de server van de leverancier naar een andere server of leverancier.*
- *Zoek aansluiting met maatregel 12.3.1 (back-up van informatie) uit de NEN7510*[4]
    - *Relevant voor oplossingen die worden gemanaged door de organisatie zelf, zie de eisen op de NEN-website*
    - *Stem de back-up protocollen af met de leverancier van de veilige e-mailoplossing.*
- *Zorg voor duidelijk afspraken ten aanzien van continuïteit, het doen van de selectie en het contracteren van de leverancier.*

2.12 Informeren over veilige e-mailvoorziening

Zorg dat via de verschillende communicatiekanalen aangegeven wordt dat veilige e-mail wordt gebruikt als communicatiemiddel bij het versturen of ontvangen van patiëntgegevens.

Beleid

- *Mails worden niet ingetrokken via een enkele druk op een knop, hier dient altijd een apart bericht voor gestuurd te worden. Hierop moet de ontvanger bevestigen dat deze hiermee akkoord gaat, de rollen die deze actie mogen uitvoeren zijn te vinden in Tabel 1.*
- *Mails die naar groepen gaan bevatten geen privacygevoelige informatie, en waarbij de ontvangers niet kunnen zien naar wie de mail nog meer is gestuurd (BCC), worden verstuurd via de gewone mail*
- *Onveilige e-mails vanuit patiënten worden altijd veilig beantwoord, ook wanneer de patiënt aangeeft de voorkeur te hebben voor een onveilige e-mail.*
- *E-mails vanuit de organisatie met medische inhoud en/of privacygevoelige informatie worden altijd door een zorgverlener of diens verantwoordelijke verstuurd via een beveiligde e-mail. Beveiligde e-mail maakt gebruik van minstens tweefactor authenticatie, waardoor toegang voor onbevoegden onmogelijk is.*

[4] https://www.webtoolmanagementsystemen.nl/nl/NormDetail?standardId=cc28b925-3d18-4036-bd60-196465c9a05b#downloads,

- *Communiceer via meerdere kanalen die beschikbaar zijn voor de organisatie over de beschikbaarheid van een veilige e-mailoplossing. Hierbij valt te denken aan:*
    - *Informatie aan het einde van de e-mail/ handtekening*
    - *Website/nieuwsbrief/patiëntinformatie (automatisch geprinte bijsluiter)*
    - *Formats van briefpapier/factuur*

Bijlage A. Definities

2.13 Ad-hoc communicatie

Onder ad hoc communicatie verstaan we onder andere communicatie via veilige mail of via een chat applicatie. Inzien van berichten binnen een beveiligd portaal valt niet onder ad-hoc communicatie.

2.14 Autoreply

Auto-reply berichten zijn automatisch verzonden berichten als antwoord op een binnengekomen e-mailbericht.

2.15 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn alle gegevens die gevoelig zijn van aard en het mogelijk maken door herleidbare kenmerken een persoon te identificeren. De bijzondere persoonsgegevens zijn door de wetgever extra beschermd[5]. Dit zijn onder andere medische gegevens van een persoon, maar ook etniciteit, politieke opvattingen en religie.

De autoriteit persoonsgegevens geeft verschillende redenen, ook wel grondslagen genoemd, aan wanneer bijzondere persoonsgegevens wel gedeeld mogen worden. In de zorg is de grondslag: uitdrukkelijke toestemming. Wanneer een patiënt toestemming geeft om gegevens te delen met een andere professional mogen deze ook daadwerkelijk gedeeld worden.[5]

2.16 Functionele e-mailbox

Functionele mailbox (bijvoorbeeld: recepten@apotheekjansen.nl) is een mailbox die toegankelijk is voor meerdere personen die samen verantwoordelijk zijn voor het juist afhandelen van de binnenkomende berichten.

2.17 Persoonlijke e-mailbox

Persoonlijke mailbox (bijvoorbeeld: bas.jansen@apotheekjansen.nl) is een mailbox die toegankelijk is voor één persoon met een directe behandelrelatie met de patiënt. De persoonlijke mailboxen mogen alleen ingericht worden voor professionals die een directe behandelrelatie hebben met patiënten.

---

[5] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wat-verstaat-de-avg-onder-bijzondere-persoonsgegevens-6339, geraadpleegd op 09-05-2022

2.18 Mandateren

Mandateren in het kader van de NTA7516 is de bevoegdheid geven om in de naam van een ander (e-mail)berichten te versturen of handelingen uitvoeren op (e-mail)berichten zonder de bijbehorende verantwoordelijkheden over te nemen.

2.19 Delegeren

Delegeren is het overdragen van bevoegdheden inclusief de bijbehorende verantwoordelijkheid aan een andere persoon of afdeling binnen de organisatie. In tegenstelling tot mandateren waar de verantwoordelijkheid niet wordt overgedragen wordt bij delegeren wel de verantwoordelijkheid over gedragen.

2.20 Sleutelbeheer

Bij het verzenden van veilige e-mails worden de mails versleuteld volgens een bepaalde standaard van encryptie. Encryptie is het (digitaal) versleutelen van een bestand of bericht. Doordat het bericht versleuteld is, is het niet mogelijk voor een onbevoegde derde om de inhoud van het bericht te lezen. Alleen de bedoelde ontvanger kan het bericht lezen doordat ontvanger in bezit is van de digitale sleutel. Deze digitale sleutel is niet zichtbaar voor de eindgebruiker maar wordt automatisch toegepast op het binnenkomende bericht.

Het digitale sleutelbeheer wordt in nagenoeg alle gevallen door de leverancier van veilige e-mail ingeregeld, daarom is hier geen expertise of beleid voor nodig anders dan de aangeleverde informatie vanuit uw leverancier zelf.

2.21 Verzendingsgronden

1. Veilige e-mails worden gestuurd wanneer er bijzondere persoonsgegevens gedeeld dienen te worden met een andere zorgprofessional en/of de patiënt. De algemene verordening gegevensbescherming (AVG) stelt de volgende grondslagen voor het rechtmatig verzenden van bijzondere persoonsgegevens[6]: Noodzakelijk in het kader van uitvoering van een overeenkomst (contract) met de betrokkene, dus niet de uitvoering van een contract met een ander;
2. Noodzakelijk om aan een wettelijke plicht te voldoen;
3. Noodzakelijk voor behartiging van gerechtvaardigde belangen van de verwerker;
4. Noodzakelijk voor taken van algemeen belang of opgedragen openbaar gezag;
5. Noodzakelijk voor bescherming van vitale belangen van betrokkene of derden;
6. Met toestemming van de betrokkene voor specifieke doelen.

2.22 ZORG-AB

ZORG-AB is het landelijke adresboek voor zorgverleners, het is een product van VZVZ. In dit adresboek zijn allerlei (adres)gegevens opgenomen over de zorgverleners.

---

[6] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken

Faexit heeft een additionele functie laten bouwen om via Outlook dit adresboek te bereiken en om gegevens aan te vullen in een webportaal. Deze functionaliteiten worden in Q1 2023 verwacht, houdtde website van Faexit in de gaten voor updates.