Praktijkhandleiding

Zorg Messenger

Veilige Mail - NTA 7516

Criteria, beleid en implementatie v.2.0

E Zorg

Inhoudsopgave

1. Een Praktijkhandleiding - wat is dat?

Deze handleiding is samengesteld voor alle professionals in de zorg die te maken hebben of krijgen met (ad-hoc-)communicatievraagstukken en privacy bij het gebruik van de Zorg Messenger Veilige Mail van E-Zorg. Insteek is hierbij heldere en zo praktisch mogelijke informatie aan te bieden. Voor managers, ict-medewerkers en alle andere professionals in de zorgsector. Ten aanzien van ad-hoc-communicatie heeft NEN in mei 2019 een nieuwe norm geintroduceerd met de aanduiding NTA 7516, waaraan elke organisatie die omgaat met gezondheidsinformatie moet voldoen.

Het document is dusdanig gesegmenteerd dat de informatie is ingedeeld op relevantie voor verschillende rollen binnen de zorgsector. Na een korte uiteenzetting over de achtergrond en impact van NTA 7516 behandelt deze handleiding de relevante criteria uit deze norm. Deze onderdelen geven een duidelijk en algemeen overzicht over NTA 7516 relevant voor alle rollen binnen de zorgsector. Vervolgens komen alle benodigde beleidselementen voor organisaties aan bod, vooral bedoeld voor beleidsmakers en managers. Het laatste onderdeel wordt gevormd door een uitermate praktisch overzicht over de te nemen (technische) implementatiestappen. Bedoeld voor de professionals belast met de ict-ondersteuning van de verschillende communicatieprocessen binnen een organisatie.

Door deze opzet biedt deze handleiding voor iedereen een overzichtelijke ordening en snelle toegang tot de gewenste of benodigde informatie, waarbij het niet nodig is het document als geheel door te nemen.


Brand Compliance

Certificaat

459/V4 - Certificaatnummer: NL 498.1.1

Uitgereikt aan:

E-Zorg B.V.

Locatie: Kanspeldreef 6b, 1101 CJ Amsterdam

Brand Compliance B.V. verklaart dat de e-mail-communicatiedienst van bovengenoemde organisatie beoordeeld is en in overeenstemming bevonden is met de eisen van de norm zoals hieronder vermeld.

Norm:

NTA 7516:2019

Scope:

KPN Zorg Messenger Veilig Mailen.

De in certificaatbijlage Versie 1.0 E-Zorg B.V. genoemde componenten van de door de organisatie geleverde applicatie.

NEN NTA 7516

Namens de certificatie instelling:
Brand Compliance B.V.
Hambakenwetering BD2
5231 DC 's-Hertogenbosch
Nederland

P. Janssen
Quality and Accreditation Manag

Afgiftedatum:
26 oktober 2020

Datum initieel certificatiebesluit:
22 oktober 2020

Behoudens het voorduurend v
aan de relevante eisen zoals
beschreven in de NTA 7516:2
certificaat geldig tot en met:
21 oktober 2023

Om de geldigheid van dit d
controleren kunt u bellen r
nummer: +31 (0)73 220 20

Verdere toelichting met b
de scope van dit certificaa
worden verleegen door
nemen met de gecertific
organisatie.

Brand Compliance

Certificaatbijlage 1.0 E-Zorg B.V.

Scope voor certificaat NL 498.1.1

De scope voor de NTA 7516:2019 certificering is beperkt tot de volgende componenten met bijbehorende versie nummers:

Component *	Versie **
KPN Zorg Messengerserver	1.5.0
KPN Zorg Messenger Web Client (veilig mailen / Portaal)	1.0.0.213
KPN Zorg Messenger API	0.0.128
Mailin	Versie 5, code 184

* Elk onderdeel dat niet in dit overzicht wordt vermeld maakt geen deel uit van de certificering.

** Wijzigingen in de scope of scope onderdelen die van invloed zijn op de certificering worden afgehandeld in overeenstemming met de NEN 7516:2020 clausule 7.10.

De scope is in overeenstemming met de volgende verklaring van in- en uitsluitingen:
NTA 7516 – Verklaring van in- en Uitsluitingen v1.3 10092020

Aanpassingen aan NTA 7516

Daar er zowel technische als beleidsmatige aspecten een rol spelen en er op beide vlakken steeds nieuwe ontwikkelingen plaatsvinden ligt het in de lijn der verwachting dat er na de eerste vastlegging nog aanpassingen aan de norm zullen plaatsvinden. Te denken valt aan mutaties bij bestaande criteria, maar dit kan ook het toevoegen van nieuwe additionele criteria zijn. Deze praktijkhandleiding is gebaseerd op de eerste versie van NTA 7516 (mei 2020). Zodra er aanpassingen komen, zullen we deze informatie op de relevante punten updaten naar de meest actuele stand van zaken.

2. NTA 7516 - een compact overzicht voor zorgprofessionals

De noodzaak tot veilig communiceren in de zorg behoeft geen uitleg. Door de veelheid aan zorginstellingen, leveranciers en communicatie-oplossingen echter, is het essentieel dat alle betrokkenen daarbij steeds kunnen terugvallen op een normen-set. Gezamenlijk onderschreven uitgangspunten voor veilige communicatie die borgen dat er te allen tijde een betrouwbare uitwisseling van persoonlijke gezondheidsinformatie plaatsvindt. Of het nu gaat om gestructureerde berichten of om zogenoemde ad-hoc-communicatie zoals e-mail, chat of messenger-achtige toepassingen.

2.1 Wat is NTA 7516 nu precies?

De NTA 7516 is een vanaf 20 mei 2020 geldende norm over veilige ad-hoc-communicatie in de zorg en is bedoeld om het gebruik van e-mail en chatapplicaties te voorzien van randvoorwaardes. Hiervoor is een set van 28 criteria opgesteld. Gebruikers met verschillende (technische) oplossingen kunnen volledig veilig communiceren onafhankelijk van de gekozen leverancier, de gekozen applicatie of het gekozen portaal. Daar ziet de NTA 7516 op toe. Deze is opgesteld met als uitgangspunt balans tussen veiligheid en gebruiksgemak en heeft twee belangrijke doelstellingen:

A] Integriteit & vertrouwelijkheid.
Ad hoc, of ook wel ongestructureerde, communicatie van gezondheidsinformatie gaat áltijd veilig. Standaard e-mail en chatverkeer voldoet zonder aanvullende technische en organisatorische maatregelen niet meer aan de eisen voor veilige gegevensuitwisseling. Vandaar een set criteria die de vertrouwelijkheid van de informatie borgen. Niemand anders dan alleen de bevoegde kan de informatie inzien.

B] Multikanaalcommunicatie tussen vendors.
De verschillende producten/systemen moeten altijd veilig onderling met elkaar kunnen communiceren. Binnen de NTA 7516 wordt dit ook wel aangeduid met de term interoperabiliteit. Het gaat hierbij dus om het feit dat je onafhankelijk van met welke oplossing je communiceert, weet dat de gegevens afgeschermd, versleuteld en daarmee veilig zijn. Die garantie heb je alleen als alle leveranciers hierover eenduidige afspraken hebben gemaakt. En die liggen dus vast in de NTA 7516.

2.2 Voor wie is NTA 7516 van toepassing?

De NTA 7516 geldt in principe voor iedere organisatie die bij het delen van (persoonlijke) gezondheidsinformatie gebruik maakt van ad-hoc-communicatie. Alle medewerkers die met gezondheidsinformatie omgaan en hierover communiceren dienen zich aan de eisen van de NTA 7516 te houden. Dit kunnen bijvoorbeeld zorgprofessionals zijn, werkzaam bij apotheken, ziekenhuizen, huisartsenpraktijken in de ouderenzorg of een andere zorgorganisatie. Denk hierbij echter ook werknemers bij de (lokale) overheid, het openbaar ministerie (OM) of een juridisch dienstverlener of een verzekeraar.

Het per mail versturen van afspraakbevestigingen of onderzoekuitslagen naar patiënten, hun familieleden dan wel mantelzorgers. Even chatten of mailen met een collega over een cliënt. Medische gegevens verzenden ten behoeve van een verzekering of beschikking. De voorbeelden van vormen van ad hoc delen van medische informatie via mail- en/of chatapplicaties zijn talrijk. Dit soort berichten is vaak eenmalig of voor een specifiek geval of situatie. Daarbij bestaat het risico, dat er net iets minder zorgvuldig mee wordt omgesprongen. De voorbeelden geven al wel aan dat de NTA 7516 voor een hele brede groep aan organisaties en hun medewerkers geldt.

Hoe is deze norm ontstaan?

De NTA 7516 is gebaseerd op de AVG | GDPR en eIDAS wetgeving. Daarnaast heeft de zorgsector zelf om verduidelijking gevraagd, specifiek voor veilige mail. In de AVG staat namelijk dat mailen mag, maar dat het veilig moet. Dus zowel vanuit de wet- en regelgeving alsook uit het werkveld zelf was er de behoefte normen over veilige communicatie in de zorg op te stellen en vast te leggen. Om zo ook tot een certificering te komen en duidelijkheid te scheppen voor alle betrokkenen in dit werkveld. E-Zorg is in het voortraject nauw betrokken geweest bij de totstandkoming van de nieuwe norm. Wij zijn gevraagd mee te denken bij het opstellen van de diverse criteria. E-Zorg niet alleen, maar ook andere leveranciers en zorgprofessionals. Daarmee is gewaarborgd dat de criteria niet alleen focussen op de privacywetgeving, maar ook op de technische haalbaarheid, de gebruiksvriendelijkheid en de wensen en eisen van de sector zelf.

2.3 Criteria van de NTA 7516

Hoe kunnen zorginstellingen, overheden en leveranciers veilig medische gegevens van burgers uitwisselen? In de NTA staat een compleet overzicht van technische en organisatorische maatregelen die genomen moeten worden in lijn en ter verduidelijking van de AVG|GDPR, die niet specifiek voor de zorgsector is opgesteld.

Een aantal criteria is gericht op beleidsregels, maar het grootse gedeelte focust op veilige technologie en gebruikersvriendelijkheid. Er zijn zes hoofdthema's te onderscheiden:

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Gebruiksvriendelijkheid
- Interoperabiliteit
- Logging

In het navolgende schema zie je de verschillende deelgebieden die hierbij van toepassing zijn. In het hoofdstuk **Zorg Messenger Veilige Mail en de criteria in de praktijk** gaan we dieper in op deze deelgebieden en de compliance van de Zorg Messenger Veilige Mail van E-Zorg.

NTA 7516 in Europa

Op het moment van samenstellen van deze informatie is NTA 7516 een Nederlandse norm. Het NEN-instituut heeft de ambitie en de intentie om een van deze norm ook een Europese CEN-norm voor veilige ad-hoc-communicatie te maken. Vooralsnog is Nederland het eerste en enige land met een uitgewerkte norm op dit gebied. Vaak worden dit soort normen overgenomen door andere (of alle) bij de CEN aangesloten landen, waaronder alle Europese lidstaten.

Groep	Criterium
Beschikbaarheid	Minimale beschikbaarheid (6.1.2)
	Maximale uitvalduur (6.1.3)
	Maximaal gegevensverlies (6.1.4)
Integriteit	Herkomstbevestiging (6.1.5)
	Data-integriteit (6.1.6)
	Onweerlegbaarheid verzender (6.1.7)
Vertrouwelijkheid	Gegevensvertrouwelijkheid (6.1.9)
	Toegangsvertrouwelijkheid (6.1.10)
	Communicatievertrouwelijkheid (6.1.11)
	Internationaal ad-hocberichtenverkeer (6.1.13)
Gebruiksvriendelijkheid	Continuïteit ad-hocberichtenverkeer - beantwoorden (6.1.14)
	Continuïteit ad-hocberichtenverkeer - doorsturen (6.1.15)
	Veiligheid als gemak (6.1.16)
	Leesbaarheid (6.1.17)
	Eigen kopie (6.1.18)
Interoperabiliteit	Dossierkoppeling (6.1.19)
	Multikanaalcommunicatie (7.2)
Logging	NEN 7513

3. Zorg Messenger Veilige Mail & de NTA 7516 criteria

Organisaties die niet ad hoc communiceren hoeven in principe niet te voldoen aan NTA 7516. Maar als er ook maar één persoon is die wel via ongestructureerde weg (mail, chat, messenger) medische informatie uitwisselt is het essentieel om aan de verschillende criteria te voldoen. Niet zo zeer omdat de norm zelf verplicht is, maar omdat deze voortvloeit uit andere wél verplichte wet- en regelgeving!

Voor dienstenleveranciers zoals E-Zorg geldt dat ze verplicht zijn te voldoen aan de multikanaalcommunicatie-eis. Dit betekent dat Zorg Messenger Veilige Mail altijd probleemloos over en weer kan communiceren met andere communicatiediensten die aan de NTA 7516 voldoen.

3.1 Verplichte en optionele NTA 7516 criteria

Interoperabiliteit is een verplicht onderdeel voor onze Zorg Messenger Veilige Mail-oplossing. De overige criteria zijn optioneel, maar dat wil niet zeggen dat E-Zorg er niet toch al aan voldoet. Zie de navolgende checklist van alle gestelde NTA 7516-criteria waar we aan voldoen. Bekijk wat ze in theorie betekenen, wat de grenswaardes zijn en, veel belangrijker, hoe dit praktisch gezien is ingericht bij Zorg Messenger Veilige Mail.

3.2 Zorg Messenger Veilige Mail NTA 7516 Checklist

3.2.1 Zorg Messenger Veilige Mail & Beschikbaarheid

Criterium: Minimale beschikbaarheid (NTA 7516 onderdeel 6.1.2)
Betekenis: De minimaal aanvaardbare tijd dat ad-hoc-berichtenverkeer mogelijk moet zijn. De grenswaarde is 99,8 % per jaar. Dat geldt voor de client-software die wordt gebruikt door professionals plus de technische infrastructuur (voor zover dit contractueel is vastgelegd).
Praktijk: De communicatieketen van Zorg Messenger Veilige Mail wordt door meerdere applicaties 'bewaakt'. Ontstaat er een onderbreking van die keten, waardoor Zorg Messenger Veilige Mail niet beschikbaar is of waarbij de beschikbaarheid in gevaar komt wordt er direct een signaal verzonden. Er gaat een signaal naar de supportafdeling en er wordt direct onderzoek ingesteld naar de verstoring om de storing zo snel mogelijk te verhelpen.

Criterium: Maximale uitvalsduur (NTA 7516 onderdeel 6.1.3)
Betekenis: De hoogst aanvaardbare aaneengesloten uitvalsduur van het ad-hoc-berichtenverkeer. De grenswaarde hiervoor bedraagt 24 uur. Dat geldt voor de door professionals gebruikte client-software plus de technische infrastructuur (voor zover dit onder contractueel bewind staat).
Praktijk: Net als bij de bewaking van de beschikbaarheid wordt ook bij het bewaken van dit criterium gebruik gemaakt van diverse applicaties. Deze controleren continu de beschikbaarheid van de Zorg Messenger Veilige Mail. Het proces van signalering, inventarisatie en probleemoplossing geldt hier dus precies zo, als bij de beschikbaarheids-norm.

Criterium: Maximaal gegevensverlies (NTA 7516 onderdeel 6.1.4)
Betekenis: De maximale hoeveelheid van ad-hoc-berichtenverkeer die verloren mag gaan. De grenswaarde hiervoor is 0! Tenzij de verzender binnen 24 uur na verzending wordt geïnformeerd over (mogelijk) gegevensverlies, is geen enkel gegevensverlies vanaf de verzendende client-software en de technische infrastructuur acceptabel.
Praktijk: Zorg Messenger Veilige Mail heeft als kerntaak berichten veilig en accuraat te verzenden. Simpel: informatie die wordt verzonden moet ook in zijn totaliteit arriveren bij de ontvanger. Zorg Messenger Veilige Mail is zo ingesteld, dat wanneer een bericht niet kan worden afgeleverd, het op de server bewaard wordt en de gebruiker hiervan een melding ontvangt. Worden de berichten afgeleverd in het Zorg Messenger Veilige Mail portaal dan worden deze in zijn geheel opgeslagen op de Zorg Messenger Veilige Mail servers. Ze gaan dus niet verloren als ze niet bezorgd kunnen worden.

>99,8% Zorg Messenger Veilige Mail beschikbaarheid

Wij meten doorlopend de beschikbaarheid van onze diensten én diensten die onder onze verantwoordelijkheid vallen. Ook vindt er preventief onderhoud plaats binnen een vastgesteld onderhoudsperiode (van 05:00 tot 07:00). Hierbij worden de laatste patches, updates en dergelijken geïnstalleerd. Gebruikers hebben hierdoor over het algemeen geen enkele last van onderhoud aan de infrastructuur en kunnen probleemloos werken. Door onze stabiele infrastructuur en de beschreven monitoring en onderhoud behalen we ruimschoots de gestelde eis van 99,8% en voldoen dus aan de norm. Dat was overigens altijd al het geval, ook vóór de invoering van NTA 7516.

NB De tijd dat de dienst niet beschikbaar is binnen het maintenance window telt niet mee bij de berekeningen van beschikbaarheid omdat dit ingeplande down time is.

E-Zorg Backup & Restore

Om de opgeslagen data zo optimaal mogelijk te beschermen, maken we gebruik van redundante servers die (geografisch van elkaar gescheiden) binnen verschillende Nederlandse datacentra zijn gehost. E-Zorg heeft daarnaast ook uitgebreide back-up en restore protocollen. Alle back-ups zijn geautomatiseerd en de rapportages worden per mail dagelijks geïnspecteerd door onze systeembeheerders. Om scherp te blijven vinden er regelmatig steekproeven plaats. Zo wordt er dus alles in het werk gesteld om ervoor te zorgen dat er geen data verloren gaan!

3.2.2 Zorg Messenger Veilige Mail & Integriteit

Criterium: Herkomstbevestiging (NTA 7516 onderdeel 6.1.5)

Betekenis: Er moet kunnen worden aangetoond dat de verzender daadwerkelijk degene is waarvoor hij/zij zich uitgeeft. Europese lidstaten hebben afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Deze verordening heet eIDAS: 'Electronic Identities And Trust Services'. Een onderdeel van die verordening is het grensoverschrijdend gebruik van in Europa erkende inlogmiddelen. Het betrouwbaarheidsniveau voor de authenticatiemethode moet volgens deze Europees afgesproken eIDAS regels minimaal het niveau 'substantieel' hebben. Dit kan alleen met een betrouwbare online identiteitscheck aan 'de voordeur'.
Praktijk: Checken en dubbelchecken! Dat is in de basis zoals de beveiliging bij Zorg Messenger Veilige Mail is ingericht. Concreet betekent dit dat voordat gebruikers gebruik kunnen maken van het Zorg Messenger Veilige Mail portaal, zij zich eerst dienen te identificeren met een verificatiemiddel zoals Microsoft Authenticator. Daarbovenop zit er in Zorg Messenger Veilige Mail een functionaliteit waarmee de domeinnaam van het afzendadres van een e-mail wordt gekoppeld aan een organisatie. Door het gebruik van organisatiemailadressen kan dus extra veiligheid worden ingebouwd. In de applicatie zit ook functionaliteit die het mogelijk maakt om misbruik van domeinnamen bij e-mail te voorkomen; een extra beveiliging. We raden gebruikers dan ook altijd aan om zich met hun werkmail te registreren voor Zorg Messenger Veilige Mail. Zo maak je gebruik van de beste beveiligingsopties die onze dienst te bieden heeft.

Criterium: Data-integriteit (NTA 7516 onderdeel 6.1.6)

Betekenis: Dat wat aankomt moet exact dat zijn, wat verzonden is. Wijziging van de inhoud van een ad-hoc-bericht tussen verzending en ontvangst is niet toegestaan. Tussenliggende componenten en eventueel betrokken personen/professionals mogen de inhoud van een ad-hoc-bericht nooit wijzigen.
Praktijk: Een gebruiker van Zorg Messenger Veilige Mail moet er te allen tijde van uit kunnen gaan dat een verstuurd bericht ook exact zo wordt ontvangen als het verstuurd is. De inhoud moet 100% overeenkomen. Om dit te garanderen gebruiken we een aantal technische maatregelen waaronder checksums en hashes.

- ***Checksum***. Het principe van een checksum (ook wel een "controlegetal" genoemd) is erg eenvoudig: op een reeks letters of cijfers (dat wil zeggen: het bericht dat wordt verstuurd) wordt met behulp van een algoritme een berekening uitgevoerd, met een nieuwe, kortere tekenreeks als resultaat. Door die berekening achteraf opnieuw uit te voeren en te vergelijken met de eerdere uitkomst, kan worden gecontroleerd of de tekenreeks nog volledig correct is.

- ***Hashing***. Het Engelse woord hashing betekent in het Nederlands 'mengelmoes'. Het is het proces waarbij de inhoud van een bericht wordt omgezet naar code met een vaste lengte. Een code is in deze context een reeks

Tips voor de zorgprofessional!

Medische informatie is te belangrijk om er lichtvaardig mee om te gaan. Sommige van de tips zullen als bijzonder vanzelfsprekend worden gezien. Maar beter een keer te veel dan een keer te weinig eraan herinnerd worden vinden wij:

- **Wil je toegang tot Zorg Messenger Veilige Mail via een (gedeelde) computer, zorg er dan voor dat je een uniek (niet al te voor de hand liggend) wachtwoord hebt en deel dit met niemand.**
- **Kies bij wachtwoorden nooit voor automatische inlogprocedures (bijvoorbeeld opgeslagen in de browser, onder een functietoets of in een macro).**
- **Schrijf wachtwoorden nooit op papier (bijv. op een notitieblok of post-it).**
- **Verstuur nooit wachtwoorden per e-mail. Beter is om wachtwoorden mondeling door te geven (bijv. wanneer een systeembeheerder een nieuw wachtwoord doorgeeft aan een nieuwe gebruiker).**

Tip voor de zorgprofessional

Zorg dat de zorgorganisatie de rechten en rollen van haar medewerkers met betrekking tot Zorg Messenger Veilige Mail regelmatig controleert. Indien de rechten en/of rollen niet meer kloppen, moeten deze zo spoedig mogelijk worden aangepast. De applicatiebeheerder binnen jouw organisatie kan deze rechten en rollen aanpassen.

getallen en/of letters. Een hash maakt het onmogelijk om de oorspronkelijke rij, of zelfs maar een deel daarvan, te reconstrueren. Het bericht kan hierdoor door niemand (tussen het verzenden en ontvangen) worden aangepast. Standaard worden alle bijlagen die worden verstuurd met Zorg Messenger Veilige Mail gehashed. Deze methode wordt door ons steeds doorontwikkeld zodat ook de tekst van berichten kan worden gehashed. Ook zullen deze hashes worden teruggestuurd naar het Zorg Messenger Veilige Mail platform, waardoor kan worden aangetoond dat de data-integriteit is gewaarborgd.

Een andere noemenswaardige integriteitsmaatregel is het feit dat berichten altijd via een TLS (Transport Layer Security) verbinding wordt verstuurd. Die is versleuteld en hierbij wordt gebruik gemaakt van certificate pinning: bij het proces van verzenden en ontvangen wordt automatisch gecontroleerd of er verbinding wordt gemaakt met de juiste server.

Criterium: Onweerlegbaarheid verzender (NTA 7516 onderdeel 6.1.7)
Betekenis: De garantie dat verzending van een ad-hoc-bericht niet kan worden ontkend door de verzender. Het daarbij behorende eIDAS betrouwbaarheidsniveau is minimaal 'substantieel'. Deze eis houdt in dat de ontvanger visueel moet kunnen vaststellen welke persoon of professional de afzender is van een ad-hoc-bericht. Bijvoorbeeld door de naam van de afzender te tonen bij het bericht in je mailbox.
Praktijk: Om aan deze eis te voldoen hebben we technische maatregelen ingebouwd tegen spoofing. Spoofing is het misbruiken van andermans e-mailadres. Nieuwe gebruikers ontvangen steeds een mail op hun persoonlijke, unieke e-mailadres, waarin zij het gebruik van de applicatie kunnen bevestigen en middels een link hun wachtwoord kunnen instellen.

Criterium: Autorisatie verzender (NTA 7516 onderdeel 6.1.8)
Betekenis: De organisatie van de verzender garandeert dat de verzender geautoriseerd is om een ad-hoc-bericht aan een ontvanger te sturen.
Praktijk: Zorg Messenger maakt gebruik van een beveiligde verbinding tussen de server van de organisatie en de E-Zorg Cloud. De organisatie regelt daarnaast zelf de specifieke autorisatie op werkplek- en medewerkersniveau.

3.2.3 Zorg Messenger Veilige Mail & Vertrouwelijkheid

Criterium: Gegevensvertrouwelijkheid (NTA 7516 onderdeel 6.1.9)
Betekenis: Door professionals opgeslagen ad-hoc-berichten mogen niet in handen van onbevoegden komen. Dat geldt zowel voor opgeslagen ad-hoc-berichten in de technische infrastructuur als in de client- software van de professional (voor zover deze onder contractueel bewind staan). Toegang tot de opgeslagen ad-hoc-berichten door partijen die daartoe geen geldige grond hebben, moet onmogelijk zijn. De opgeslagen berichtgegevens moeten in het geval ze onverhoopt toch in handen van onbevoegden komen, onleesbaar zijn.
Praktijk: Encryptie is het uitgangspunt bij alle berichtenverkeer binnen Zorg Messenger Veilige Mail. Alle informatie die via het portaal wordt uitgewisseld (incl. bijlagen), is zowel tijdens het sturen (in transit) als tijdens het opslaan (at rest) versleuteld. Er zijn verschillende manieren om data te versleutelen – de meest gangbare vorm is AES (Advanced Encryption Standard) met een sleutellengte van 128, 192 of 256 bits. In de basis geldt: hoe hoger het aantal bits des te sterker de versleuteling en dus hoe veiliger de data. De versleuteling die Zorg Messenger Veilige Mail gebruikt, hanteert de hoogste sleutellengte van 256 bits. Naast versleuteling maakt Zorg Messenger Veilige Mail ook gebruik van Firewalls. Firewalls dienen ertoe om ons E-Zorg netwerk te beschermen tegen ongeautoriseerde toegang van buitenaf. Inbraakpreventiesystemen bewaken activiteit in Zorg Messenger Veilige Mail en houden bij wat voor soort handelingen er plaatsvinden. Als er door dit detectiesysteem verdachte activiteit wordt waargenomen, zet het inbraakpreventiesysteem deze persoon in 'quarantaine'. De verdachte persoon heeft dan geen toegang meer tot Zorg Messenger Veilige Mail. We laten onze diensten ook regelmatig door externe partijen controleren op beveiligingsrisico's. Bijvoorbeeld door zogenaamde penetratietesten, waarbij ethische hackers de diensten proberen te hacken met als doel E-Zorg te

Tip voor de zorgprofessional

Het Zorg Messenger Veilige Mail portaal biedt zorgaanbieders additionele mogelijkheden om hun berichten te beschermen. Deze mogelijkheden bestaan uit: een pincode toevoegen aan de applicatie op een mobiel of tablet en het aanzetten van tweefactorauthenticatie. Indien in het Zorg Messenger Veilige Mail portaal groepsgesprekken worden gevoerd, bepaalt degene die het groepsgesprek gestart is of externen deel mogen uitmaken van de conversatie en of anderen ook deelnemers kunnen uitnodigen.

informeren over eventuele verbetermaatregelen om de applicatie nog veiliger te maken. Mocht iemand overigens per ongeluk een bericht naar een verkeerde persoon hebben gestuurd, dan biedt Zorg Messenger Veilige Mail de mogelijkheid om dit bericht via het portaal te verwijderen. NB: dit is uitsluitend mogelijk indien het bericht binnen het Zorg Messenger Veilige Mail portaal is afgeleverd.

Criterium: Toegangsvertrouwelijkheid (NTA 7516 onderdeel 6.1.10)
Betekenis: Je kunt geen ad-hoc-berichten versturen zonder minimaal een authenticatiemiddel eIDAS-betrouwbaarheidsniveau 'substantieel' (personen) of 'hoog' (professional)*. Datzelfde geldt voor de beoogde ontvanger. Die kan de inhoud van ad-hoc-berichten alleen maar lezen of verwerken na het toepassen van een authenticatiemiddel van het niveau'substantieel' voor personen of 'hoog' voor professionals.
*voor gegevens waarop het wettelijk beroepsgeheim rust
Praktijk: Het inrichten van de diverse authenticatiemiddelen (conform de eIDAS standaard) is afhankelijk van de technische inrichting van de organisatie. Organisaties kiezen uiteraard hun eigen technische inrichting en zijn hier dan ook zelf verantwoordelijk voor. Authenticatie zal plaatsvinden op de werkplek of op het device van de gebruiker en kan daarom dus ook geen deel uitmaken van de door E-Zorg aangeboden dienst.

Criterium: Communicatievertrouwelijkheid (NTA 7516 onderdeel 6.1.11)
Betekenis: Toegang tot ad-hoc-berichten door partijen die daartoe geen geldige grond hebben, moet onmogelijk zijn. De inhoud van ad-hoc-berichten mag dus gedurende het transport (in transit) niet in handen van onbevoegden komen. Als een ad- hoc bericht onverhoopt toch in handen van onbevoegden komt, dan moet het ad-hoc-bericht onleesbaar zijn.
Praktijk: We maken voor Zorg Messenger Veilige Mail gebruik van het E-Zorg netwerk aangevuld met diverse andere technische maatregelen (zie ook technische handreiking NTA 7516) om de gegevensvertrouwelijkheid te waarborgen. Mocht onverhoopt een technische fout optreden waardoor berichten niet kunnen worden afgeleverd, dan gaan deze nooit verloren.
Zorg Messenger Veilige Mail plaatst deze dan in een wachtrij en daar blijven ze staan totdat een eventueel probleem is opgelost. Daarna worden ze direct alsnog verstuurd naar de ontvanger.
NB Aan een bericht wordt uitsluitend metadata gekoppeld die essentieel is voor de dienstverlening en voor het audit trail log, zodat er geen misbruik kan worden gemaakt van deze karakteristieken.

Criterium: Verzendingsgrond (NTA 7516 onderdeel 6.1.12)
Betekenis: De (organisatie van de) verzender bepaalt of a) de verzender het ad-hoc-bericht mag versturen en b) of de ontvanger voldoende gerechtigd is dat bericht te ontvangen. Om het voorgaande te kunnen bepalen moet er in beleid zijn vastgelegd welke professionals welke verzendingsgronden mogen hanteren bij ad-hoc -communicatie.
Praktijk: Het is niet de communicatieleverancier, wij dus, maar de zorgorganisatie zelf die dit criterium dient in te richten. De organisatie van waaruit de communicatie plaatsvindt moet zelf het beleid opstellen en borgen en dus toezien op de uitvoering ervan. De leverancier kan hierin alleen adviseren (zie ook 4. Beleid opstellen rondom NTA 7516).

Criterium: Internationaal ad-hoc-berichtenverkeer (NTA 7516 onderdeel 6.1.13)
Betekenis: Ad-hoc-berichtenverkeer mag slechts in overeenstemming met de AVG de buitengrenzen van de Europese Economische Ruimte (EER) overschrijden. Dit om te voorkomen dat de communicatie buiten (een) non-compatibele jurisdictie(s) geraakt.
Praktijk: Het criterium is heel formeel, maar wel noodzakelijk omdat er binnen de Europese Economische Ruimte (EER) afspraken gelden die daarbuiten niet gelden. Daarom zorgen wij ervoor dat de gegevens altijd binnen de Europese Economische Ruimte (EER) blijven. Ons Zorg Messenger Veilige Mail platform wordt gehost in twee geografisch gescheiden datacentra in Nederland en alle data staan opgeslagen in de ZorgCloud. Deze Cloud is afgeschermd van openbare netwerken zoals het Internet en is uitsluitend beschikbaar in Nederland.

NB Indien een bericht naar een ander NTA 7516 compliant platform wordt verstuurd, dan draagt de leveranciers daarvan de verantwoordelijkheid dat de berichten de EER niet verlaten, conform NTA 7516-norm.

3.2.4 Zorg Messenger Veilige Mail & Gebruiksvriendelijkheid

Criterium: Continuïteit van ad-hoc-berichtenverkeer – Beantwoorden (NTA 7516 onderdeel 6.1.14)
Betekenis: Het beantwoorden van een ad-hoc-bericht dat eerder door een professional is toegestuurd, moet altijd veilig kunnen plaatsvinden. Ad-hoc-berichtenverkeer dat is gestart door een professional, moet door een ontvangende persoon kunnen worden beantwoord en de ontvanger moet hierbij visueel kunnen vaststellen of een ad-hoc-bericht veilig is verzonden of niet.
Praktijk: Wordt een bericht in ons Zorg Messenger Veilige Mail portaal afgeleverd, dan weet de ontvanger dat het bericht van een veilige verzender afkomstig is. We leveren ook af buiten het portaal, maar dan uitsluitend als de organisatie waar de ontvanger deel van uit maakt ook voldoet aan de NTA 7516-norm. Komt een bericht op ons portaal en ben je als ontvanger aangesloten op het Zorg Messenger Veilige Mail platform of een ander NTA 7516 compliant platform dan kun je direct reageren op de ontvangen mail.

NB Veilige berichten worden binnen Zorg Messenger Veilige Mail voorzien van een footer (mailonderschrift) waarin is opgenomen dat het bericht NTA 7516 compliant is verstuurd.

Criterium: Continuïteit van ad-hoc-berichtenverkeer – Doorsturen (NTA 7516 onderdeel 6.1.15)
Betekenis: Ad-hoc-berichtenverkeer gestart of voortgezet door een professional moet door een ontvangende persoon kunnen worden doorgestuurd. Het doorsturen van een ad-hoc-bericht dat eerder door een professional is toegestuurd, is daarbij voor verantwoordelijkheid van degene die het doorstuurt.
Praktijk: In het Zorg Messenger Veilige Mail portaal kunnen berichten zonder meer worden doorgestuurd naar contactpersonen die in het portaal geregistreerd staan. Berichten kunnen bovendien ook aan personen die (nog) niet bij Zorg Messenger Veilige Mail portaal en/of chat zijn geregistreerd worden doorgestuurd. Zij krijgen dan een uitnodiging om zich te registreren (en te verifiëren), waarna zij het betreffende bericht kunnen bekijken. Bij aflevering in een veilige e-mailbox, is dit overigens afhankelijk van het beleid en de mail client van de organisatie.

Criterium: Veiligheid als gemak (NTA 7516 onderdeel 6.1.16)
Betekenis: Als verschillende opties tot uiteenlopende niveaus van bescherming leiden, moet de veiligste keuze als standaard worden aangeboden. Dus alle keuzemogelijkheden moeten standaard op de veiligste optie staan.
Praktijk: Veilige communicatie is de kerntaak van de Zorg Messenger diensten. Naast de technische veilige inrichting van de applicatie biedt E-Zorg daarnaast ook de mogelijkheid om additionele veiligheidsmaatregelen te treffen. Voorbeelden hiervan zijn het instellen van een pincode bij het gebruik van de applicatie op een mobiel/laptop of het aanzetten van tweefactor- authenticatie voor alle gebruikers van een organisatie.

Criterium: Leesbaarheid (NTA 7516 onderdeel 6.1.17)
Betekenis: Dit criterium heeft meerdere doelen:
De ontvanger van een ad-hoc-bericht moet dit (exclusief eventuele bijlagen) kunnen lezen met behulp van reguliere client-software en zonder aanvullende programmatuur. Ook moet lezen mogelijk zijn zonder dat er een account bij de betreffende communicatiedienstenaanbieder moet worden aangemaakt. En als laatste moet de op een persoon gerichte online-omgeving voldoen aan de eisen van EN 301 549 (een norm met betrekking tot de toegankelijkheid van applicaties en websites).
Praktijk: Berichten kunnen in het Zorg Messenger Veilige Mail portaal worden gelezen zonder dat een account hoeft te worden aangemaakt. Maar alleen dan als de gebruiker zich kan identificeren middels een erkende verificatiedienst en voldoet aan de NTA 7516-normen.
Zorg Messenger Veilige Mail is daarnaast ingericht op een manier die het voor elke burger mogelijk moet maken om de applicatie te snappen (denk hierbij aan simpele begrijpbare woorden en zinnen, etc.) en voldoet daarmee aan de door EN 301 549 gestelde eisen.

Criterium: Eigen kopie (NTA 7516 onderdeel 6.1.18)
Betekenis: Met minimale inspanning van de ontvanger kan deze een ad-hoc-bericht opslaan op een zelfgekozen locatie en in een formaat dat met reguliere client-software leesbaar is.
Praktijk: Als er gebruik wordt gemaakt van het Zorg Messenger Veilige Mail portaal dan kunnen de berichten simpel door middel van een PDF gedownload worden naar een lokale schijf. Ook is het mogelijk om het platform op basis van de API te koppelen aan een vaste applicatie zoals een HIS. Deze functionaliteit is uitsluitend beschikbaar voor professionals. Maakt de ontvanger gebruik van een cliënt-server-mail-oplossing en staat het beleid van de organisatie dit toe, dan kan een kopie bewaard worden op de mail-server van de organisatie, de mail-cliënt of via de mail-cliënt op een andere locatie.

3.2.5 Zorg Messenger Veilige Mail & Interoperabiliteit

Criterium: Dossierkoppeling (NTA onderdeel 6.1.19)
Betekenis: Met minimale inspanning van de professional kan een ad-hoc-bericht veilig en eenvoudig aan een dossier van een professional te kunnen worden toegevoegd.
Praktijk: Als er gebruik wordt gemaakt van het Zorg Messenger Veilige Mail portaal dan kunnen de berichten door middel van een PDF gedownload worden naar een lokale schijf. Ook is het mogelijk om het platform op basis van de API te koppelen aan een vaste applicatie zoals een

Tip voor de beleidsmakers

Stel een duidelijk beleid op waarin duidelijke richtlijnen staan ten aanzien van (ad-hoc-)berichtenverkeer op het gebied van medische informatie. Het is daarbij belangrijk dat de zorgprofessionals zich ervan bewust worden dat ze zelf verantwoordelijk zijn voor het doorsturen van een bericht. Indien de gebruiker ervoor kiest om een bericht op een onveilige manier te forwarden (bijv. door middel van kopiëren en plakken), dan is de gebruiker verantwoordelijk voor de risico's die hiermee gepaard gaan. Onderstreep dus het belang van het gebruik van het Zorg Messenger Veilige Mail portaal voor alle ad-hoc-communicatie; op deze manier kan gegarandeerd worden, dat berichten veilig worden verstuurd.

HIS. Deze functionaliteit is uitsluitend beschikbaar voor professionals.

NB Mocht de ontvanger zijn berichten ontvangen op zijn werkplek, dan is het kunnen maken van een eigen kopie afhankelijk van het beleid van de organisatie waarvoor de professional werkt.

Criterium: Multikanaalcommunicatie (NTA onderdeel 7.2)

Betekenis: Interoperabiliteit: de mogelijkheid om zonder beperkingen ad-hoc-berichten die van een andere NTA 7516 compliant communicatiedienstenaanbieder afkomstig zijn, verder te verwerken en omgekeerd.
Praktijk: Zorg Messenger Veilige Mail kan probleemloos over en weer communiceren met andere communicatiediensten die aan de NTA 7516 voldoen. Berichten verstuurd via Zorg Messenger Veilige Mail kunnen dus ook gelezen worden in een andere mail- of berichten--applicatie zolang deze ook voldoet aan NTA 7516. Over het algemeen geldt dat de ontvangende communicatiedienst verantwoordelijk is voor een adequate aflevering in de mailbox van de ontvanger. Indien de mailbox van de ontvanger voldoet aan de norm, dan kan de ontvangende communicatiedienst een bericht in de mailbox afleveren zonder dat de ontvanger extra handelingen hoeft te verrichten voor het lezen van de inhoud.

Criterium: Logging (NEN 7513)

Een zorgaanbieder die volledig aan de norm wil voldoen, moet (wanneer hij veilig ad-hoc-berichtenverkeer met persoonlijke gezondheidsinformatie wil uitwisselen met andere professionals en/of personen) voor de uitwisseling voldoen aan NEN 7513:2018 (met uitzondering van 6.2: de te loggen operationele gebeurtenissen) In deze norm gaat het over het loggen van gegevens; met andere woorden: het achter de schermen behouden en opslaan van handelingen die door een zorgprofessional zijn gedaan in de applicatie.

E-Zorg ondersteunt de zorgaanbieder hierin! Op dit moment wordt gewerkt om onderstaande benodigde categorieën te loggen:

- **alle gebeurtenissen met betrekking tot het versturen van ad-hoc-berichten (ongeacht of deze succesvol waren)**
- **het intrekken van verzonden ad-hoc-berichten**
- **het wijzigen van verzonden ad-hoc-berichten**
- **het verwijderen (bij de verzender) van verzonden ad-hoc-berichten**
- **alle gebeurtenissen met betrekking tot het ontvangen van ad-hoc-berichten**
- **het raadplegen van ontvangen ad-hoc-berichten**
- **het verwijderen van ontvangen ad-hoc-berichten**
- **het doorsturen van ontvangen ad-hoc-berichten**
- **het aanmaken en opheffen van een e-mail-en/of portaalaccount**
- **het toekennen, wijzigen en intrekken van rechten aan een e-mail- en/of portaalaccount**
- **alle gebeurtenissen met betrekking tot de authenticatie van gebruikers voor het uitvoeren van handelingen op ad-hoc-berichten**
- **de toegang tot loggegevens**
- **het wijzigen of verwijderen van loggegevens**

4. Beleid maken ten aanzien van NTA 7516

Stel beleid op! Veilige (ad-hoc) communicatie raakt direct aan de bedrijfsvoering van iedere organisatie die zich bezighoudt met het uitwisselen en verwerken van persoonlijke medische informatie. Op dit gebied is er geen ruimte voor fouten. In de communicatieketen moet iedereen op gelijke wijze handelen, vandaar ook een normen-set.

De reputatie van een organisatie is voor een groot deel afhankelijk van de veiligheid inzake gegevensuitwisseling. Mocht er ergens toch een datalek optreden, dan maakt het voor de buitenwacht niet uit bij wie in de keten dat heeft plaatsgevonden. Dus moet de keten overal even sterk zijn. Iedereen moet erop kunnen vertrouwen dat gegevens veilig zijn en met de uiterste zorgvuldigheid worden behandeld.

4.1 Stel duidelijke richtlijnen op

Alle technische implementaties zijn steeds afhankelijk van het juiste gebruik en de juiste toepassing ervan. Voldoen aan NTA 7516 is daarom niet alleen een puur praktisch onderdeel, maar voor een net zo groot deel een beleidskwestie. Iedereen binnen een organisatie moet aan de hand van kristalheldere richtlijnen kunnen werken. Richtlijnen die voor iedereen gelijk zijn en maar op één manier uit te leggen zijn. De NTA 7516 zegt hier over: "De professional moet regels vaststellen (beleid) over hoe hij en degenen die voor hem werken, gebruik mogen maken van geïmplementeerde communicatiemogelijkheden."

Het is aan iedere organisatie om toe te zien op het vormen en vastleggen van dit beleid. Er moet echter minimaal regels worden opgesteld over de volgende zaken:

- **Het waarnemen van collega's tijdens afwezigheid**
- **Mandatering en delegeren van toegang tot berichten (wie mag er wat inzien en hoe kan deze verantwoordelijkheid worden gedelegeerd)**
- **Toegang tot de (medische) informatie zonder dat er een directe behandelrelatie bestaat**
- **Toegang tot functionele mailboxen**
- **Het gebruik van het adresboek**
- **Het intrekken of wijzigen van berichten**
- **Het gebruik van geautomatiseerde functies (zoals bijvoorbeeld e-mailregels voor autoreply of leesbevestiging)**
- **Het bewaren en vernietigen van berichten (o.a. de bewaartermijnen)**
- **Het omgaan met cryptografische sleutels**
- **Verantwoordelijkheden**
- **Verzendingsgronden (hoe weet de ontvanger zeker, dat de afzender gerechtigd was om het bericht te versturen?)**
- **De continuïteit van de dienstverlening (bij bijvoorbeeld uitval bij of faillissement van de e-mailprovider)**
- **Het informeren van personen over veilige e-mail**

4.2 Monitor, toets en actualiseer het beleid

Een vereiste van NTA 7516 is verder ook dat na het opstellen van het beleid dit ook bewaakt wordt om zo te kunnen toetsen of alle richtlijnen door alle medewerkers worden nageleefd en ook over er eventueel wijzigingen aan het beleid nodig zijn. Bijvoorbeeld omdat er toch nog onduidelijkheden bestaan bij sommige richtlijnen. Het opgestelde beleid moet dus ook regelmatig geëvalueerd worden. NTA 7516-norm geeft hiervoor duidelijke uitgangspunten in NTA 7516 onderdeel 6.4.1 – Toezicht/naleving – Algemeen.

De professional moet een programma vaststellen waarmee:

- **Continu de naleving van de gebruiksregels wordt gemonitord**
- **Jaarlijks de geschiktheid van de geselecteerde en geïmplementeerde communicatie-mogelijkheden worden vergeleken met de criteria die daarvoor zijn vastgelegd**
- **Tweejaarlijks de vastgelegde criteria worden beoordeeld op geschiktheid en passendheid**

4.3 Als organisatie voldoen aan NTA 7516

Om te voldoen aan NTA 7516 is het dus niet voldoende om aan alle technische specificaties en criteria te voldoen. Je hebt ook beleid nodig voor de gehele organisatie. Gebruik hiervoor de in 4.1 beschreven checklist en bedenk dat dat de minimale eisen zijn die worden gesteld aan de richtlijnen.

Het kan voor specifieke organisaties of specifieke personen nodig zijn een uitgebreidere set regels op te stellen. Die verantwoordelijkheid ligt bij de beleidsmakers. Ga er dus niet zonder meer van uit dat de beleids-checklist altijd alle aspecten van jouw organisatie afdekt.

En als laatste is het hebben van de juiste infrastructuur en technische inrichting inclusief richtlijnen ook nog niet voldoende om gecertificeerd te raken/blijven. Hou het naleven van de regels in de gaten, hou de werking ervan in de gaten en pas aan waar nodig. Daartoe moet je dus minimaal eenmaal per twee jaar een evaluatie houden.

5. Zorg Messenger Veilige Mail implementatie conform NTA 7516

Voor het implementeren van Zorg Messenger Veilige Mail conform NTA 7516 moet een aantal stappen doorlopen worden. Volg je de navolgende instructies, dan voldoet jouw Zorg Messenger Veilige Mail omgeving aan de vereiste criteria.

5.1 Overzicht van het implementatieproces

Stap 1: E-Zorg verbinding en routerinstallatie

- Een fysieke verbinding met het E-Zorg netwerk is een voorwaarde voor implementatie van de Zorg Messenger Veilige Mail. Daarnaast is een door ons geconfigureerde router noodzakelijk zodat het interne netwerk verbonden kan worden met het E-Zorg netwerk.

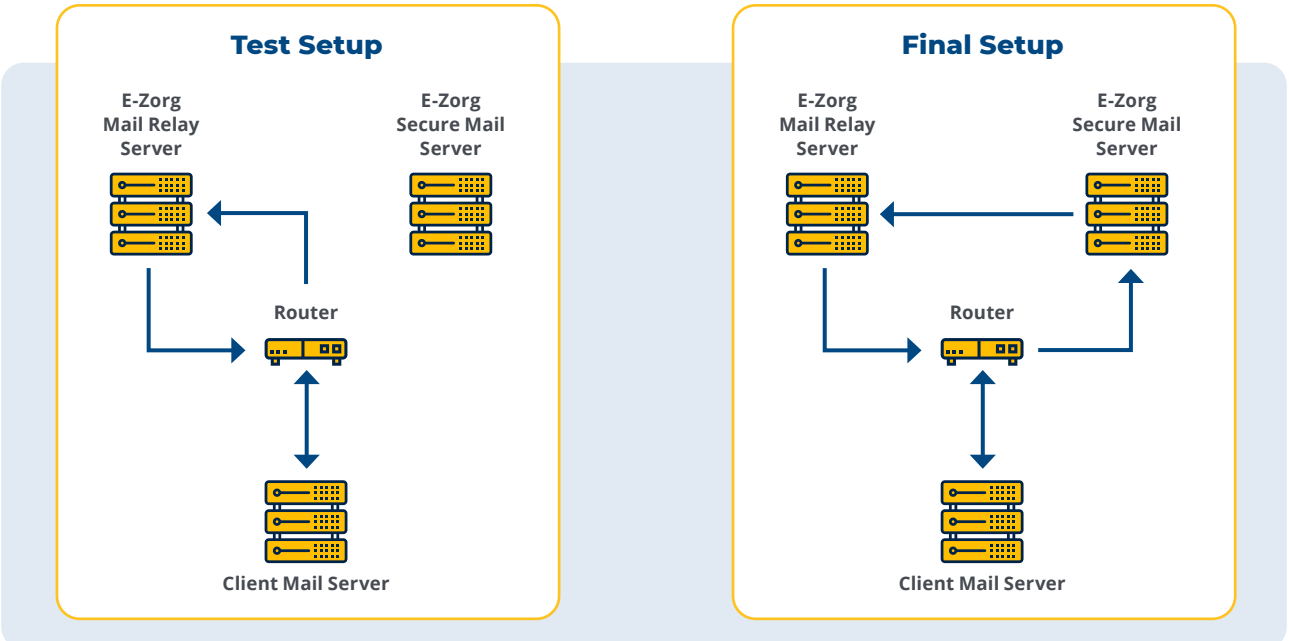
Stap 2: Netwerkconfiguratie

- Het configureren van firewalls en routers zodat het interne netwerk gekoppeld wordt aan het E-Zorg netwerk.

Stap 3: Configuratie mailomgeving

- Het instellen van de aanwezige mailserver zodat uitgaande en inkomende mail via de juiste routes wordt afgeleverd. De instellingen zullen eerst worden getest voordat de routing definitief wordt omgezet. Tijdens de configuratie zullen alle in gebruik zijnde maildomeinen worden opgenomen in de E-Zorg Mail Relay server.
- Instellen veilig mailen met X-Headers
- Zijn de testen geslaagd dan wordt veilig mailen geïmplementeerd door het instellen en testen van de juiste X-Headers.
- Uitgaande mail omzetten naar E-Zorg Secure Mail server
- Als laatste stap wordt de uitgaande mail naar de E-Zorg Secure Mail server geleid om veilig te kunnen mailen. Het inkomende mailverkeer vanuit de het E-Zorg netwerk zal altijd via de E-Zorg Mail Relay server binnenkomen. Het verschil tussen de tijdelijke testsituatie en de uiteindelijke productiesituatie is te vinden in Figuur 1.

Deze handleiding bevat voldoende informatie voor een succesvolle implementatie van de Zorg Messenger Veilige Mail mits je ervaren bent in het doorvoeren van technische wijzigingen in IT infrastructuren. Het is altijd mogelijk om E-Zorg in te schakelen om de implementatie uit te voeren. Neem daarvoor contact op met je contactpersoon bij E-Zorg.



Figuur 1: Versimpelde weergave van zowel de test configuratie als de uiteindelijke configuratie

5.2 Overzicht aansluitgegevens

Onderstaande tabel toont een overzicht van enkele veelgebruikte instellingen en bijbehorende opmerkingen.

Naam	Waarde	Opmerkingen
Hostname E-Zorg Mail Relay Server	inside-relay.ezorg.nl	De E-Zorg Mail Relay server zal in de testfase zowel uitgaand als inkomend mailverkeer afhandelen. Na beëindigen van de test alleen het inkomende mailverkeer.
IP-adres E-Zorg Mail Relay Server	10.254.253.199	
Poortnummer E-Zorg Mail Relay Server	587	
Hostname E-Zorg Secure Mail Server	secure-smtpnodes.ezorg.nl	De E-Zorg Secure Mail server zal uiteindelijk alleen het uitgaande mailverkeer afhandelen. Inkomend verkeer komt altijd van de E-Zorg Mail Relay server.
IP-adres E-Zorg Secure Mail Server	10.254.253.86/10.254.253.87	
Poortnummer E-Zorg Secure Mail Server	587	
MX Records	MX 10 mailfilters.ezorg.nl	
	MX 20 mailfilter01.ezorg.nl	
	MX 30 mailfilter02.ezorg.nl	
	MX 40 mailfilter03.ezorg.nl	
X-Header veilig mailen	x-ezorg-secbypass	default: false
Gebruikersnaam E-Zorg Secure Mail Server	[.....]	Wordt gebruikt ter authenticatie en ontvang je tijdens het implementatieproces
Wachtwoord E-Zorg Secure Mail Server	[.....]	Wordt gebruikt ter authenticatie en ontvang je tijdens het implementatieproces

Tabel 1: Verzameling van configuratieparameters

5.3 Check van de aansluitvoorwaarden

Voor een succesvolle implementatie is het noodzakelijk aan alle onderstaande voorwaarden te voldoen:

- **Een werkende E-Zorg verbinding**
- **Een geïnstalleerde router die de E-Zorg verbinding koppelt aan het eigen netwerk.**
- **Het bekend zijn van de volgende aansluitwaarden bij E-Zorg:**
  - **Intern IP-adres en poortnummer(s) van je mailomgeving.**
  - **Maildomeinen waarmee je organisatie mail verstuurd én maildomeinen waar je organisatie mail op ontvangt. Ieder domein waarop ontvangen wordt moet ook kunnen versturen en vice versa. Domeinen die niet bij E-Zorg zijn aangemeld kunnen geen mail versturen of ontvangen.**
  - **Gebruikte mailsoftware en de versie daarvan binnen je organisatie. Bijvoorbeeld Microsoft Exchange 2013 etc.**
  - **Contactgegevens van uitvoerder implementatie Zorg Messenger Veilige Mail.**
  - **Contactgegevens van de beheerder van Zorg Messenger Veilige Mail binnen de organisatie. Deze persoon zal binnen de Zorg Messenger Veilige Mail organisatie-specifieke instellingen kunnen aanpassen en beheren. De beheerder heeft de mogelijkheid om later iemand anders beheer-rechten toe te wijzen.**
- **Beleid inzake veilig mailen. Binnen de organisatie moet duidelijk zijn op welke manier je gebruik gaat maken van veilig/onveilig mailen. Wie mag en moet veilig mailen en op welke manier wordt dit aangeboden?**

5.4 Netwerkconfiguratie

Het interne netwerk zal op de juiste manier geconfigureerd moeten worden om de verbinding met het E-Zorg netwerk daadwerkelijk te benutten. Zie tabel 1 voor de juiste adressen en poorten. De genoemde IP-adressen en poortnummers zullen in de infrastructuur correct naar het E-Zorg netwerk gerouteerd moeten worden en firewalls (indien aanwezig) moeten aangepast worden om het verkeer door te laten. Zorg ervoor dat de interne mailserver configuratie een ingaande en een uitgaande verbinding heeft met de E-Zorg Mail Relay server. De mailserver hoeft naar de E-Zorg Secure Mail server alleen een uitgaande verbinding te hebben.

5.5 Mailomgeving configuratie

Ongeacht welke mailomgeving je gebruikt in je organisatie moeten er enkele globale instellingen gemaakt of aangepast worden. Hieronder een opsomming van deze instellingen en een korte uitleg.

- **Mail moet op basis van TLS1.3/STARTTLS verstuurd worden naar de E-Zorg Mail Relay server en de E-Zorg Secure Mail server. (Send connector)**
- **Mail moet op basis van TLS1.3/STARTTLS ontvangen worden op de mailserver van je organisatie. (Receive connector)**
- **Eventuele SPF controle op binnenkomende mail vanuit het E-Zorg netwerk moet uitgeschakeld zijn.**
- **De externe IP-adressen van de mailservers van E-Zorg zullen toegevoegd moeten worden aan de SPF-records van de organisatie. Dit in verband met het feit dat E-Zorg ook namens jouw domein mailverkeer leidt. Voeg daarvoor volgende regel toe aan het SPF-record (zonder ""): "include:_spf.ezorg.nl"**
- **Een geldig certificaat moet toegewezen worden aan de SMTP service, zodat de mailserver het certificaat voor encryptie kan gebruiken.**

TLS & STARTTLS

De Zorg Messenger dienst Veilige Mail maakt gebruik van versleutelde TLS-verbindingen in de vorm van SMTP in combinatie met STARTTLS en vereist dit ook van de gekoppelde mailserver (Mail Transfer Agent).

Deze uitleg over de instellingen van de mailomgeving is afgestemd op het gebruik van een Microsoft Exchange omgeving. Overeenkomstige instellingen in een andere mailomgeving zijn van toepassing maar kunnen daar een andere benaming of waarde hebben.

5.5.1 Verbinding E-Zorg Mail Relay naar lokale mailomgeving (Receive connector)

De mailserver van de organisatie moet inkomend mailverkeer van de E-Zorg Mail Relay server kunnen ontvangen. De Receive connector moet aangepast of gecreëerd worden om mail te ontvangen van de E-Zorg Mail Relay server met hostname: inside-relay.ezorg.nl en IP-adres: 10.254.253.199 . Deze informatie is tevens terug te vinden in Tabel 1.

5.5.2 Verbinding lokale mailomgeving naar E-Zorg Mail Relay (Send connector)

De mailserver moet uitgaand mailverkeer naar de E-Zorg Mail Relay server doorsturen (voor het geval van de test configuratie). Zorg ervoor dat uitgaande mail naar de E-Zorg Mail Relay server wordt doorgestuurd voor mailberichten naar het voorlopige testdomein: ezorg.nl (of een eigen testdomein). Maak een Send connector om mail te verzenden naar de E-Zorg Mail Relay server met hostname: inside-relay.ezorg.nl met IP-adres: 10.254.253.199 en poort 587. Let op! Dit is een tijdelijke testsituatie. Wij testen op deze manier of de routes correct zijn ingesteld. Uiteindelijk zal de uitgaande mailstroom omgezet worden naar de E-Zorg Secure Mail server. Inkomend mailverkeer vanuit het E-Zorg netwerk zal altijd vanuit de E-Zorg Mail Relay blijven komen.

5.5.3 Testen van routes van/naar E-Zorg Mail Relay server

Om te testen of de routes voor mailverkeer van en naar de E-Zorg Mail Relay server goed zijn ingesteld vragen we je een testmail te sturen naar een testdomein met ontvanger helpdesk@e-zorg.nl en een CC naar helpdesk@ezorg.nl (Let op! Verschil in mailadressen vanwege het minteken (-)). Het is ook mogelijk een eigen testdomein te gebruiken. Neem na het versturen van de mail contact op met de helpdesk op 020-4309033, kies voor de optie techniek, om te controleren of het bericht in goede orde is ontvangen en of de routes op de juiste manier via de E-Zorg Mail Relay server lopen. Tevens zal je een bericht teruggestuurd krijgen om ook de inkomende mail te testen.

5.5.4 Toevoegen van maildomeinen

Na het succesvol testen van de routes van en naar de E-Zorg Mail Relay server zullen wij de maildomein(en) die je eerder beschikbaar hebt gesteld toevoegen aan de E-Zorg Mail Relay zodat deze domeinen vertrouwd worden binnen het E-Zorg netwerk. Tevens worden de uitgaande domeinen opgevoerd in de centrale E-Zorg spamfilter.

5.5.5 Zorg Messenger Veilige Mail instellen met X-Headers

Uitgaande mail die via de E-Zorg Secure Mail server verloopt wordt, mede op basis van een vooraf ingestelde X-Header, via een veilige of onveilige weg verstuurd. Deze X-Header wordt meegegeven in de metadata van het verstuurde mailadres en is terug te vinden in tabel 1. Om te voldoen aan de NTA7516 moet de default X-Header gezet te worden. Sowieso zal altijd gecontroleerd worden of de ontvangende mailserver voldoet aan gestelde NTA7516 voorwaarden. Zo ja, dan zal de mail direct via deze route worden afgeleverd. Dat gebeurt ook als de ontvanger is aangesloten op het E-Zorg netwerk. In het geval dat de ontvanger niet op het E-Zorg netwerk is aangesloten zal de e-mail op basis van de voorkeuren van je organisatie veilig verstuurd worden met behulp van de Zorg Messenger Veilige Mail, of onveilig verstuurd worden via het internet. Denk in het laatste geval bijvoorbeeld aan mailverkeer tussen de organisatie en leveranciers die geen gevoelige informatie bevat. Dit mailverkeer wil je wellicht niet perse via de veilige manier verzenden. Het is daarom belangrijk voor de implementatie van de Zorg Messenger Veilige Mail dat het voor je organisatie helder is welke personen/domeinen/subdomeinen standaard veilig of onveilig mailen.

5.5.5.1 Active Directory groups

Afhankelijk van hoe de organisatie het veilig mailen beleid hanteert, zijn er verschillende manieren om dit beleid binnen je mailomgeving te implementeren. Eén van de meest gebruikte manieren is het implementeren van twee Active Directory Universal Security groups. Deze zullen het onderscheid maken tussen de groep die veilig mailt (bv. default-Securemail) en de groep die standaard onveilig mailt (bv. defaultSecuremail-Bypass). Deze kunnen vanuit Exchange (mits u die omgeving draait) gedefinieerd worden en worden dan automatisch in de Active Directory aangemaakt. Let op! Het kan een tijd duren voordat de Active Directory-based Group Policy instellingen daadwerkelijk toegepast zijn. Het is mogelijk om deze policy instellingen te forceren (gpupdate).
Het is nu mogelijk om met behulp van transportregels (Transport Rules) de condities aan te geven wanneer de betreffende X-Header moet worden meegegeven. In het voorbeeld de X-Header: x-ezorg-secbypass = false aan mails van de leden van groep default-Securemail en de X-Header: x-ezorg-secbypass = true aan leden van de groep default-Securemail-Bypass. Stel tevens in dat in het geval dat de betreffende X-Header (x-ezorg-secbypass) al gezet is, de waarde niet overschreven moet worden. Dit is belangrijk in combinatie met de Outlook-addin zoals beschreven in 1.5.5.2.

5.5.5.2 Outlook-addin

Het is mogelijk eindgebruikers meer vrijheid te geven door ze zelf de optie te geven om veilig of onveilig mail te versturen. Met behulp van een Outlook-addin kan aan de Outlook-client van de eindgebruiker een knop voor 'Veilig verzenden', 'Onveilig verzenden', of beide toegevoegd worden. Ga je de Outlook-addin gebruiken, zorg dan dat de addin al is geïnstalleerd op een (test)client. Dan is bij het testen direct vast te stellen of de Outlook-addin de headers op de juiste manier meegeeft. Details voor het installeren van de Outlook-addin zijn beschreven in 5.6.

5.5.6 Testen X-Headers

Na het instellen van de X-Headers is het nuttig om te testen of deze doorkomen én of ze in de juiste gevallen, zoals vastgelegd in het beleid van de organisatie, verstuurd worden. Testen kan door opnieuw een mail te versturen naar helpdesk@e-zorg.nl en een CC naar helpdesk@ezorg.nl. Neem vervolgens opnieuw contact op met de helpdesk (020-4309033), en kies voor de optie techniek, om te controleren of de X-Headers op de juiste manier verstuurd en ontvangen worden.

5.5.7 Omzetten uitgaande mail (voor testdomein) naar E-Zorg Secure Mail server (Send connector)

Als de X-Headers in alle gevallen goed doorkomen, kan de uitgaande testverbinding omgezet worden naar de EZorg Secure Mail server. Dit betekent dat uitgaande mail verstuurd moet worden naar de EZorg Secure Mail server in plaats van de E-Zorg Mail Relay server. In het geval van het gebruik van een Exchange server zal de Send connector aangepast moeten worden om mail te verzenden naar de E-Zorg Secure Mail server met hostname: secure-smtpnodes.ezorg.nl met IP-adres: 10.254.253.86/10.254.253.87 en poort 587. Deze informatie is tevens terug te vinden in tabel 1. Zorg ervoor dat ook hier alleen uitgaande mail naar het testdomein e-zorg.nl (of een eigen testdomein) wordt verzonden. In tegenstelling tot de E-Zorg Mail Relay server is er voor

de E-Zorg Secure Mail server extra authenticatie nodig. Voor deze authenticatie wordt er basic authentication gebruikt in de vorm van een gebruikersnaam en wachtwoord. Deze zullen tijdens het implementatieproces aan u worden verschaft. In het geval van een Exchange server zal ook deze instelling bij de Send connector onder het kopje Authentication ingesteld kunnen worden.

5.5.8 Testen uiteindelijke route

Na omzetten van de verbinding wordt er een laatste check uitgevoerd of ook de routes via de E-Zorg Secure Mail server correct lopen. Testen kan door opnieuw een mail te versturen naar helpdesk@e-zorg.nl en een CC naar helpdesk@ezorg.nl. Neem vervolgens opnieuw contact op met de helpdesk (020-4309033), en kies voor de optie techniek, om te controleren of de omzetting naar behoren voltooid is. Tevens zult u een bericht teruggestuurd krijgen om ook de inkomende mail te testen.

5.5.9 Omzetten alle uitgaande mail

Als ook de laatste check positief is, kan niet alleen het mailverkeer naar het testdomein ezorg.nl (of een eigen testdomein) worden verstuurd via de E-Zorg Secure Mail server, maar al het uitgaande verkeer. In het geval van een Exchange server gebeurt dit door in de betreffende Send connector de Address space te veranderen van e-zorg.nl naar de wildcard * (sterretje). Deze wildcard staat voor alle uitgaande domeinen.

5.6 Outlook-addin Veilig/Onveilig-mailen knop

Het is mogelijk eindgebruikers meer vrijheid te geven door ze zelf de optie te geven om veilig of onveilig mail te versturen. Met behulp van een Outlook-addin kan aan de Outlook-client van de eindgebruiker een knop voor 'Veilig verzenden', 'Onveilig verzenden, of beide toegevoegd worden. Met het indrukken van de 'Veilig verzenden'-knop wordt de X-Header (x-ezorg-secbypass: false) meegegeven. Bij de 'Onveilig verzenden'-knop wordt de X-Header (x-ezorg-secbypass: true) meegegeven. Omdat de X-Headers zowel vanuit de transportregels op de mailserver als vanuit de Outlook-client kunnen worden meegegeven, kunnen deze met elkaar conflicteren. Wat de uitkomst is met betrekking tot veilig/onveilig mailen voor de verschillende combinaties van meegeven van X-Headers is te vinden in tabel 2.
De Outlook-addin is een .exe-bestand dat voor kleine organisaties lokaal per client kan worden geïnstalleerd of voor grote installaties centraal wordt uitgerold binnen de eigen omgeving.

5.7 Specifieke instellingen NTA 7516

Om te voldoen aan de NTA 7516 dien je nog aan een aantal zaken te voldoen. Deze instellingen zijn ook opgenomen in de bijlage "Checklist behorende bij Conformiteitsverklaring"

Outlook knop niet veilig	Exchange groep niet veilig	Exchange groep veilig	Mail veilig
X	X	X	Ja
X	X	V	Ja
X	V	X	Nee
V	X	X	Nee
V	V	X	Nee
V	X	V	Nee

Tabel 2: Resultaat veilig mailen voor verschillende combinaties Exchange-groepen en gebruik Outlookaddin

5.7.1 DMARC

Je dient maatregelen te nemen om aan te kunnen tonen dat de verzender van de organisatie, ook daadwerkelijk de verzender is. De implementatie van DMARC begint met het publiceren van een geldig DMARC Record. Je dient zorg dragen dat DMARC policy actief is en juist is ingeregeld.

5.7.2 DKIM

De ontvangen inhoud moet gelijk zijn aan de verzonden inhoud door toepassing van DKIM. DKIM voegt een versleutelde handtekening toe aan de koptekst van alle uitgaande berichten. Zie voor meer informatie over het activeren van DKIM: https://faq.ezorg.nl/KB/dkim-signing-voor-relay-domeinen/

5.7.3 MX Records

Voor de inkomende mail dienen de MX records aangepast naar onderstaande instellingen.

MX 10 mailfilters.ezorg.nl
MX 20 mailfilter01.ezorg.nl
MX 30 mailfilter02.ezorg.nl
MX 40 mailfilter03.ezorg.nl

Deze informatie is tevens terug te vinden in tabel 1.

5.7.4 Multikanaalcommunicatie

Voor een goede werking van de mail-uitwisseling via de NTA 7516 multikanaalcommunicatie tussen de verschillende mail-diensten van verschillende leveranciers en hun klanten die voldoen aan het gestelde in de NTA7516, dient DNSSEC voor alle maildomeinen aan te staan.
Je kunt dit controleren via sidn.nl/whois
Staat DNSSEC aan voor alle maildomeinen geen verder actie nodig. Mocht op DNSSEC niet of niet op alle domeinen aan staan, laat dan door de beheerder dit aanzetten voor je maildomeinen(en)

6. Contactinformatie

Indien je meer informatie over de toepassing in jouw organisatie wilt ontvangen kun je deze opvragen bij E-Zorg.

Dit kan per mail op **verkoop@e-zorg.nl** en telefonisch op **020 - 430 90 33.**

Je kan je ook wenden tot je E-Zorg accountmanager.

Op de Zorg Messenger zijn de E-Zorg Algemene Leveringsvoorwaarden en de Aanvullende Voorwaarden Online diensten van toepassing. Vraag je E-Zorg contactpersoon naar een kopie van deze voorwaarden of kijk op **e-zorg.nl**, zoekterm 'algemene voorwaarden'.

Webadres: www.ezorg.nl
Telefoonnummer: 020-4309033
E-mailadressen: info@ezorg.nl
Bezoekadres: Karspeldreef 6-b, 1101 CJ Amsterdam

Onze Prijslijst!
Scan deze QR-code met de camera van een telefoon voor de actuele prijzen.

NB geen aparte app benodigd.