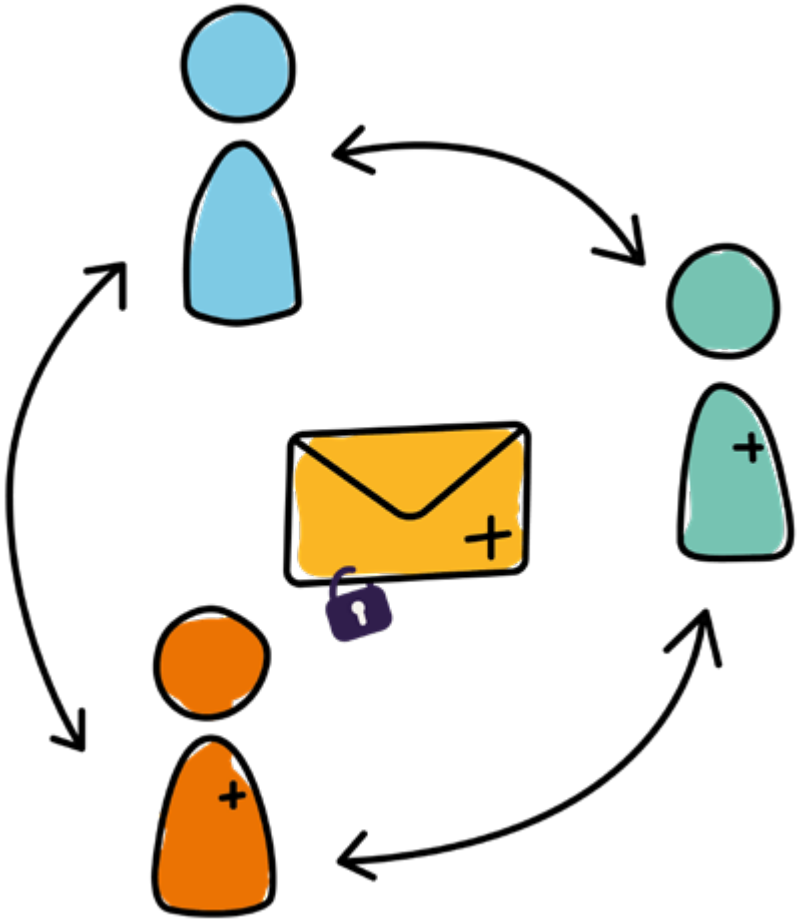
VEILIG MAILEN, HOE REGELEN WE DAT?!

Implementatiehandboek voor de kleine zorgpraktijk



Deel 2. Toolkit

INFORMATIE BERAAD

Er zijn diverse manieren om in de zorg informatie digitaal uit te wisselen. Bijvoorbeeld tussen informatiesystemen, zodat informatie direct op de juiste plek terecht komt. Of waar dat niet kan, met andere oplossingen. Mailen is er daar een van. Zorgverleners moeten afdoende maatregelen nemen om de veiligheid van de informatie te kunnen garanderen. De norm NTA 7516 beschrijft de eisen die worden gesteld aan veilige e-mail. Als je niet voldoet aan deze norm dan ben je als zorgverlener aansprakelijk. Dus, aan de slag! Dit handboek helpt je daarbij.

Deel 2. Toolkit
De Toolkit gaat in op een aantal praktische zaken rondom de selectie en implementatie van een veilige e-maildienst.

Dit handboek is geschreven voor tandartsen, fysiotherapeuten, huisartsen, apothekers en iedereen die werkt binnen een kleine zorgpraktijk.

Het handboek bestaat uit drie delen:

Deel 1.
Stappenplan

Deel 2.
Toolkit

Deel 3.
Praktijkscenario's

Tip
Start met de 'Praktijkscenario's' en lees daarna het 'Stappenplan'. Vanuit het 'Stappenplan' wordt verwezen naar de 'Toolkit'.

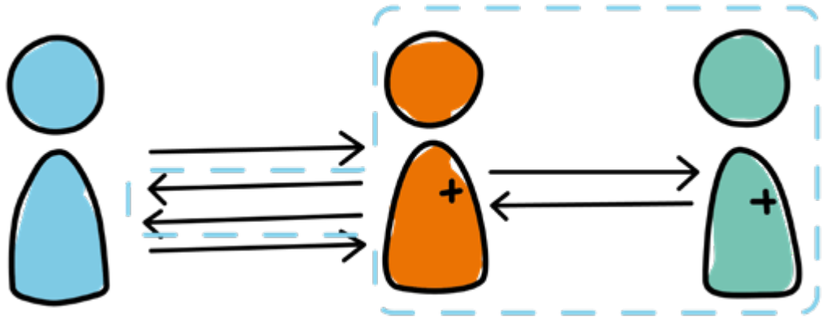
Deel 2. Toolkit

Achtergrondinformatie

- De kaders van NTA 7516.
- Wat is persoonlijke gezondheidsinformatie?
- Voldoen aan NTA 7516.

De kaders van NTA 7516

In mei 2019 is NTA 7516 gepubliceerd (https://www.nen.nl/Alles-over-NEN-7510/NTA-7516.htm). Deze norm stelt regels aan het veilig gebruik van e-mail. Als zorgverlener ben je verantwoordelijk voor veilige communicatie over persoonlijke gezondheidsgegevens. Dit geldt voor communicatie met collega zorgverleners en met patiënten en andere personen.



Aan patiënten worden in de norm geen eisen gesteld. Je bent als zorgverlener verantwoordelijk voor het veilig communiceren, ook als de patiënt onveilig mailt. Als zorgverlener kun je niet afdwingen dat een patiënt op een veilige manier contact zoekt. Wel kun je veilige communicatie aanmoedigen door alternatieven voor te stellen en te promoten.

Uitgangspunten

- De norm geldt niet voor patiënten en hun netwerk.
- Als zorgverlener ben je er verantwoordelijk voor dat het communiceren over persoonlijke gezondheidsinformatie op een veilige manier gebeurt. Ook in reactie op een onveilige e-mail van een patiënt.
- Verzender en ontvanger moeten allebei een persoon zijn. Automatisch verzonden berichten uit een informatiesysteem zoals een HIS/ECD/EPD/XIS vallen buiten het toepassingsgebied.

De patiënt valt dus buiten de grenzen van de norm. De norm beschrijft afspraken die enkel gelden voor het zorgdomein. Als zorgverlener moet je aan verschillende eisen voldoen zoals die in NTA 7516 zijn beschreven:

Groep	Criterium	Onderdeel NTA 7516
Beschikbaarheid	Minimale beschikbaarheid Maximale uitvalsduur Maximaal gegevensverlies	6.1.2 6.1.3 6.1.4
Integriteit	Herkomstbevestiging Data-integriteit Onweerlegbaarheid verzender Autorisatie verzender	6.1.5 6.1.6 6.1.7 6.1.8
Vertrouwelijkheid	Gegevensvertrouwelijkheid Toegangsvertrouwelijkheid Communicatievertrouwelijkheid Verzendingsgrond Internationaal ad-hoc berichtenverkeer	6.1.9 6.1.10 6.1.11 6.1.12 6.1.13
Gebruiksvriendelijkheid	Continuïteit van ad-hoc berichtenverkeer – beantwoorden Continuïteit van ad-hoc berichtenverkeer – doorsturen Veiligheid als gemak Leesbaarheid Eigen kopie	6.1.14 6.1.15 6.1.16 6.1.17 6.1.18
Interoperabiliteit	Dossierkoppeling	6.1.19

Ook moet er voor verschillende onderdelen beleid worden opgesteld:

- waarneming tijdens afwezigheid;
- mandatering en delegatie van toegang tot gegevens;
- toegang zonder een directe behandelrelatie;
- toegang tot functionele mailboxen;
- gebruik van een adresboek;
- intrekken of wijzigingen van e-mailberichten;
- gebruik maken van geautomatiseerde functies (zoals e-mailregels);
- bewaren en vernietigen van e-mailberichten;
- omgang met cryptografische sleutels;
- verantwoordelijkheden;
- verzendingsgronden;
- continuïteit bij uitval van e-mailprovider;
- informeren van personen over veilige e-mail.

Als zorgverlener moet je uiteindelijk alle onderdelen die hierboven zijn beschreven, hebben geregeld. Deels met de leverancier van je veilige e-maildienst en deels door te beschrijven hoe zaken zijn ingericht. In de hoofdstukken 'Praktijkregels' en 'Programma van Eisen' gaan we hier dieper op in.

- Ook diensten als de gemeente, functionarissen van justitie en politie vallen binnen de grenzen van NTA 7516.
- In de praktijk zullen de meeste eisen uit NTA 7516 (hoofdstuk 6.1.1 t/m 6.1.19 maar ook loggingsvereisten en beleid) voor een groot deel worden ingevuld door leveranciers van veilige e-maldiensten. Leveranciers kunnen ervoor kiezen niet aan alle onderdelen van de norm te voldoen. Zorg er met andere diensten – mogelijk bij een andere leverancier – voor dat je praktijk wel aan alle onderdelen voldoet. Soms is een combinatie van verschillende diensten noodzakelijk.
- NTA 7516 kan worden gezien als een specifieke invulling van NEN 7510. Wanneer je je voor veilige e-mail houdt aan de kaders van NTA 7516, dan is voor deze toepassing de NEN 7510 ook geregeld.

Wat is persoonlijke gezondheidsinformatie?

Veilige e-mail moet gebruikt worden als je over persoonlijke gezondheidsinformatie communiceert. Maar wat is persoonlijke gezondheidsinformatie precies? In de praktijk is het vaak contextafhankelijk wat als persoonlijke gezondheidsinformatie beschouwd wordt en wat niet. Een afspraakbevestiging van een huisarts wordt anders beoordeeld dan een afspraakbevestiging van een GGZ-instelling of een SOA-kliniek.

De NEN 7510 definieert persoonlijke gezondheidsinformatie als:

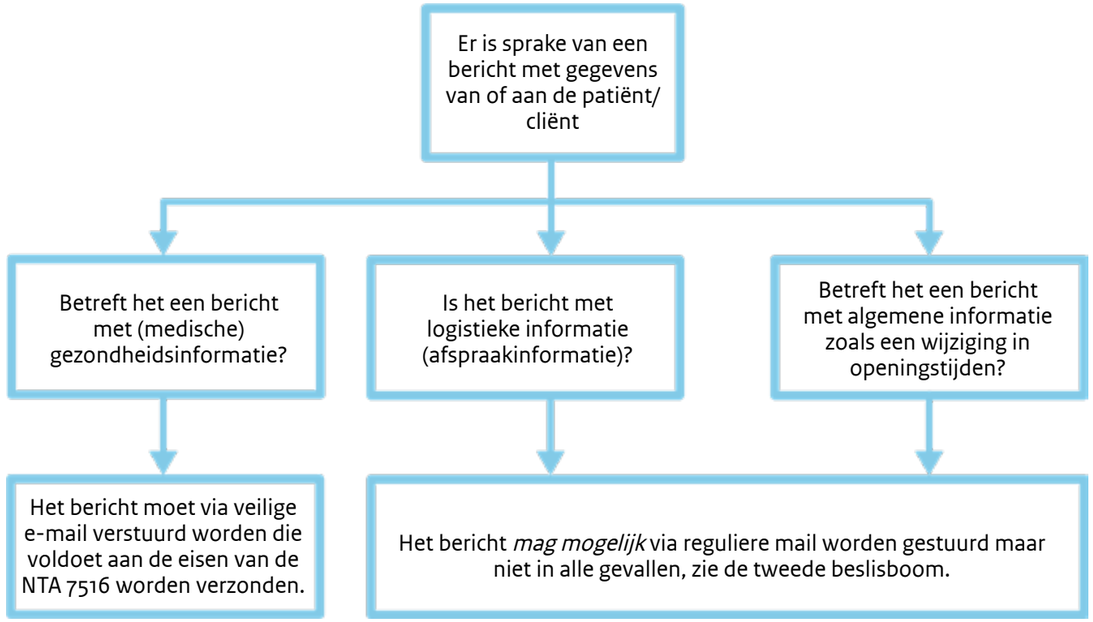
'Informatie over een identificeerbare persoon die verband houdt met de lichamelijke of geestelijke gesteldheid van, of de verlening van zorgdiensten aan de persoon in kwestie'.

Een afspraakbevestiging of andere logistieke informatie valt ook onder deze definitie. Toch verzenden veel zorgverleners met name een afspraakbevestiging (na toestemming) via de gewone e-mail. Er is in de praktijk een grijs gebied. In 'Praktijkscenario's' beschrijven we verschillende situaties en lichten we de afwegingen toe.

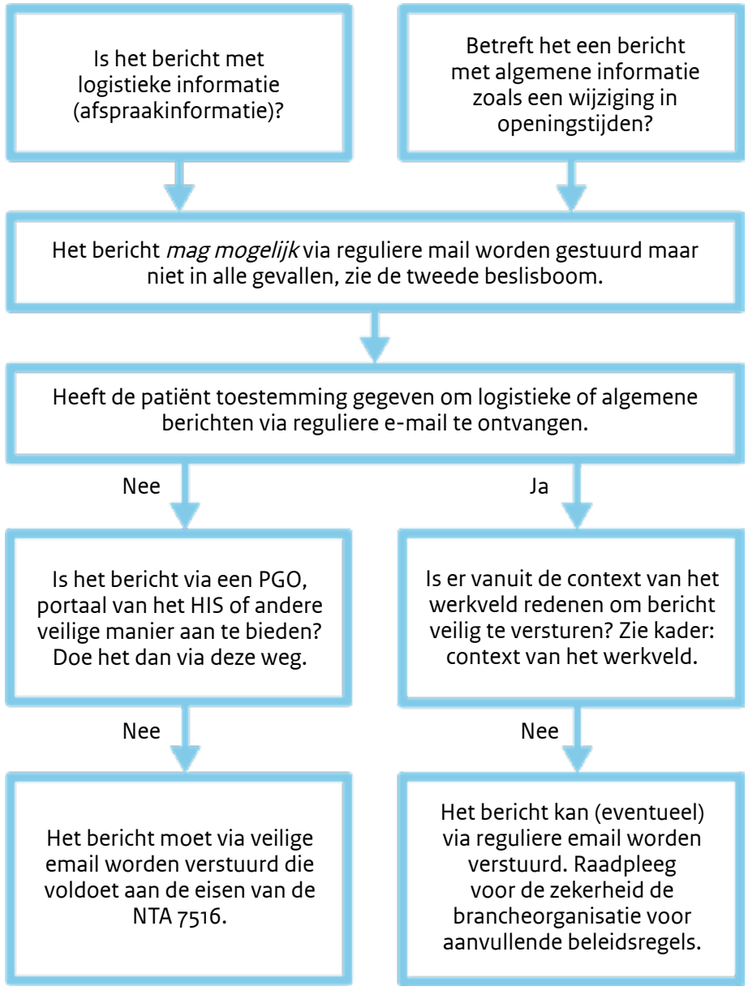
Let op: ook al geeft de patiënt expliciet toestemming om via gewone (onveilige) e-mailgegevens te versturen die duidelijk tot de categorie 'persoonlijke gezondheidsgegevens' behoren, als professional mag je niet op een dergelijk verzoek ingaan. Je moet je altijd houden aan de kaders van NTA 7516 houden.

De onderstaande beslisboom ‘Moet ik veilige e-mail gebruiken?’ helpt je om te bepalen in welke situaties je een veilige e-maildienst moet gebruiken.

Basis beslissing



Sub beslissing



De context van het werkveld
De definitie van persoonlijke gezondheidsinformatie is niet gekoppeld aan het werkveld van de professional. Toch zijn er in de praktijk zorgverleners/sectoren die anders omgaan met bepaalde type informatie/e-mails naar patiënten/cliënten.

Voorbeelden uit de praktijk:
- een afspraakbevestiging van een huisarts wordt anders beoordeeld dan een afspraak bevestiging van een GGZ-instelling;
- de openingstijden van een SOA-kliniek worden anders beoordeeld dan de openingstijden van een algemeen gezondheidscentrum;
- in het kader van terugbrengen van de no-show wordt een bericht vanuit een ziekenhuis naar een patiënt gestuurd met enkel de tijd van de afspraak, zonder verdere informatie over polikliniek of andere verwijzing naar de aard van het bezoek.

Informeer bij je brancheorganisatie naar richtlijnen voor het gebruik van e-mail voor de ondersteuning in het maken van de juiste afweging. Gebruik bij twijfel altijd een toepassing die voldoet aan NTA 7516

Voldoen aan NTA 7516
Je voldoet aan NTA 7516 als:
- je aan kunt tonen dat alle normelementen uit hoofdstuk 6 van NTA 7516 normatief ingevuld zijn. Dit betekent dat je alle normelementen waarin het woord ‘moet(en)’ vermeld staat, moet kunnen afvinken.
- je praktijkregels hebt opgesteld. In het hoofdstuk ‘Praktijkregels’ gaan we hier verder op in.

Gelukkig hoef je het niet allemaal zelf te regelen. Heel veel normelementen worden in veilige e-maildiensten geregeld. Check wel of deze voldoen aan NTA 7516 en welke normelementen uit de norm ze invullen. Gebruik hiervoor het programma van eisen verderop in dit boekje.

Het is ook mogelijk om gebruik te maken van meerdere veilige e-maildiensten of leveranciers om aan alle onderdelen van de norm te voldoen. Leveranciers kunnen ervoor kiezen niet aan alle onderdelen te voldoen waardoor je een andere leverancier nodig hebt om de overige onderdelen aan te vullen. Er zijn veel combinaties mogelijk. Het belangrijkste is dat je het overzicht hebt en houdt en bijhoudt of je aan alle elementen van de norm voldoet.

Onderdelen van het projectplan

Een projectplan geeft je houvast en zorgt dat je niets vergeet. Hierin vermeld je welke stappen je moet doorlopen, wat je nodig hebt en hoeveel tijd je verwacht bezig te zijn. Het projectplan hoeft niet een heel boekwerk te zijn. Een aantal A4'tjes met de essentiële informatie is genoeg.

Onderdelen die het projectplan moeten bevatten, zijn:

- opdrachtomschrijving: wat houdt het project in en met welke kaders werk je?
- doelstelling: wat willen jullie met het traject precies bereiken?
- projectinrichting: wie zijn erbij betrokken en welke verantwoordelijkheden hebben ze?
- voorwaarden: welke voorwaarden stellen jullie? Is het bijvoorbeeld belangrijk dat je dit traject gezamenlijk met andere praktijken oppakt?;
- risico's & tegenmaatregelen: beschrijf welke risico's je ziet en hoe je deze wilt ondervangen.
- afhankelijkheden: op welke punten in het traject zitten afhankelijkheden? Bijvoorbeeld met de leverancier of doordat een actie nog niet afgerond is waardoor een volgende actie niet gestart kan worden.;
- planning met activiteiten & mijlpalen: wanneer moet wat zijn afgerond? En hoe verhouden activiteiten zich tot elkaar? Het is aan te raden te werken met verschillende fases. Twee activiteiten die er sowieso in moeten zijn het programma van eisen en het opstellen van praktijkregels. In de hoofdstukken 'Praktijkregels' en 'Programma van Eisen' gaan we hier dieper op in.;
- financieel plaatje: hoeveel geld is er beschikbaar en hoe is het over de verschillende posten verdeeld? Hou ook rekening met eventuele tegenvallers en budgetoverschrijding. Zijn er middelen om dit aan te vullen?

Praktijkregels

Praktijkregels zijn nodig wanneer veilige mail in je eigen (zorg)proces gebruikt wordt. NTA 7516 vereist praktijkregels op de volgende onderdelen:

- waarneming tijdens afwezigheid;
- mandatering en delegatie van toegang tot gegevens;
- toegang zonder een directe behandelrelatie;
- toegang tot functionele mailboxen;
- gebruik van een adresboek;
- intrekken of wijzigingen van e-mailberichten;
- gebruik maken van geautomatiseerde functies (zoals e-mailregels);
- bewaren en vernietigen van e-mailberichten;
- omgang met cryptogafische sleutels;
- verantwoordelijkheden;
- verzendingsgronden;
- continuïteit bij uitval van e-mailprovider;
- informeren van patiënten over veilige e-mail.

Per onderdeel geven we in onderstaande paragrafen suggesties hoe je er mee om kunt gaan.

We werken met suggesties van praktijkregels, omdat de regels context en domeinafhankelijk zijn. Informeer bij je brancheorganisatie of ze een set aan specifieke voorbeeldpraktijkregels hebben opgesteld die je kunt gebruiken.

Waarneming tijdens afwezigheid

Medewerker Tom is afwezig. Vanuit het oogpunt van toegangsvertrouwelijkheid mag een willekeurige collega niet zomaar de aan Tom gerichte mails lezen.

Suggestie voor praktijkregels:

- bij afwezigheid heeft de leidinggevende toegang tot de mailbox;
- bij afwezigheid controleert een naaste collega op urgente mailberichten en legt deze voor aan de leidinggevende;
- bij afwezigheid controleert degene die de afwezige vervangt, ook zijn of haar mailbox.

Daarnaast zijn ook regels nodig om een en ander soepel te laten verlopen, bijvoorbeeld:

- de leidinggevende is verantwoordelijk voor het verlenen van toegang;
- de medewerker is verantwoordelijk voor het verlenen van toegang in geval van afwezigheid.

Ook de volgende regels kunnen nuttig zijn:

- de ICT-beheerder verleent uitsluitend toegang op schriftelijk verzoek van een lijnverantwoordelijke van degene wiens mailaccount het betreft;
- de ICT-beheerder verleent uitsluitend toegang conform de beleidsregels;
- degene die toegang heeft tot de mailbox van een ander, zal nimmer berichten raadplegen die zijn opgeslagen in de map met als naam ‘privé’ of ‘private’;
- degene die toegang heeft tot de mailbox van een ander, zal nimmer berichten raadplegen waarvan uit de onderwerpregel (‘subject’) zonneklaar het privékarakter van dergelijke berichten blijkt.

Omdat veel zorgpraktijken aan medewerkers een beperkt privégebruik van mailvoorziening toestaan -vaak aangeduid als *acceptable use*- is toegang tot de mailbox van een ander niet onomstreden. Het is daarom verstandig binnen de praktijk de regels rondom het privégebruik van de mailbox af te stemmen.

Mandatering en delegatie van toegang

Onder mandatering verstaan we: in naam van een ander berichten versturen of andere handelingen (zoals verplaatsen, kopieren, intrekken, etc) uitvoeren op berichten. Bijvoorbeeld: Mia die in naam van Tom een mailbericht verstuurt: Mia stelt de tekst op, maar de ontvanger van het bericht ziet dat Tom het heeft verzonden.

Onder delegatie verstaan we: het overdragen van bevoegdheden. Bijvoorbeeld: iemand vraagt iets aan Tom, maar Mia beantwoordt de vraag. De ontvanger van het bericht ziet dat Mia heeft geantwoord.

Om op veilige wijze e-mailberichten te verwerken, moeten beperkingen gelden voor mandatering en delegatie. Veel e-maildiensten bieden de gebruiker de mogelijkheid om anderen — weliswaar binnen hetzelfde maildomein (alles achter het teken @ in het mailadres) — schrijf- en/of leesrechten te bieden.

Suggestie voor praktijkregels:

- mandatering is uitsluitend toegestaan met instemming van een leidinggevende.
- delegatie is slechts toegestaan aan één persoon, die bovendien in loondienst is van de zorgpraktijk en hiërarchisch onder degene die delegeert valt.
- mandatering of delegatie verandert niets aan de verantwoordelijkheid van degene die mandateert of delegeert (met andere woorden: verantwoordelijkheid kan niet worden gemandateerd of gedelegeerd);
- mandatering en delegatie zijn niet toegestaan.

Toegang zonder directe behandelrelatie

Deze regels gelden uitsluitend voor zorgverleners die in het kader van de Wet op de geneeskundige behandelovereenkomst (WGBO) een patiëntendossier voeren en hiermee te maken krijgen met de definities van (directe) behandelrelatie en de beperkingen in de toegang tot patiëntendossiers.

Mailcorrespondentie met een patiënt - of over een patiënt met een collega - wordt gerekend tot het patiëntendossier. De patiënt - of zijn/haar vertegenwoordiger – heeft zelf toegang tot het dossier. Net als de personen die rechtstreeks betrokken zijn bij de uitvoering van de zorg, voor zover het delen van informatie noodzakelijk is voor het leveren van zorg.

Met de 'rechtstreeks bij de behandelingsovereenkomst betrokkenen' worden degenen bedoeld die we in deze paragraaf op het oog hebben. Het gaat vaak om de ondersteuning van de zorgverlener, zoals medisch secretaresse, assistenten, laboranten, apotheker etc. Wat betreft NTA 7516 zal het in de praktijk vooral gaan om de medisch secretaresse die toegang heeft tot de mailbox van een zorgverlener.

Suggestie voor een praktijkregel voor toegang zonder directe behandelrelatie:

- toegang tot mailberichten die tot een patiëntendossier gerekend moeten worden, kan
  - alleen worden verleend aan medewerkers die hiërarchisch valt onder de betreffende zorgverlener
  - alleen worden verschaft voor berichten die minder dan een week oud zijn en voor berichten over een patiënt met een actuele zorgepisode.

Toegang tot functionele mailboxen

Met functionele mailboxen worden mailboxen bedoeld die niet rechtstreeks aan één medewerker zijn gekoppeld. Denk bijvoorbeeld aan ziekmelding@arboorganisatie.nl of orthopedie@ziekenhuis.nl. Er zijn twee zaken waar je rekening mee moet houden:

- Er moet nagedacht worden wat de zender verwacht van zo'n mailadres. Als een patiënt een mail stuurt naar orthopedie@ziekenhuis.nl, dan verwacht hij dat een bevoegde medewerker van de afdeling orthopedie zijn bericht opent. Bij het toewijzen aan gebruiksrechten van zo'n functionele mailbox moet dus rekening worden gehouden met de gerechtvaardigde verwachtingen van een willekeurige zender.
- Er moet nagedacht worden over het operationele beheer van een functionele mailbox. Als een ziekmelding wordt verstuurd naar ziekmelding@arboorganisatie.nl, dan mag worden verwacht dat die wordt gecommuniceerd naar degene die het aangaat.

Suggesties voor praktijkregels:

- formuleer onder welke voorwaarden intern een functionele mailboxen mag worden gebruikt;
- formuleer op welke wijze toegangsbeheer wordt beheerd;
- formuleer hoe toegang gecontroleerd wordt m.b.v. logging die tot een patiënt herleidbaar is.

Gebruik van een adresboek

Een e-mail adresboek kan in verschillende systemen staan zoals in de reguliere mailapplicatie, veilige mailapplicatie, een CRM, etc. Voor elke toepassing geldt dat correct gebruik de kans vermindert dat er een verkeerd geadresseerd bericht wordt verzonden.

Vragen die bij het opstellen van de praktijkregels beantwoord moeten worden.

- Hoe houden we adresboeken up-to-date? Als contactgegevens in een CRM- of HRM-systeem wijzigen, worden de adresboeken dan automatisch aangepast?
- Hoe beheersen we de samenstelling van distributielijsten?
- Hoe bewaken we de veiligheid van de adresboeken? Stel er wordt een lijst aangelegd met alle cliënten/patiënten. Vaak zijn de beveiligingsmaatregelen in e-mailprogramma's van een andere orde dan die van een EPD/ECD of een specifiek hiervoor ontwikkelde veilige mailapplicatie die deze functionaliteit aanbiedt.

Belangrijk is dat je als praktijk een weloverwogen keuze maakt: verbied je het gebruik van het adresboek of maak je een koppeling vanuit de andere systemen met het adresboek?

Het kan gebeuren dat een e-mail verkeerd geadresseerd is. De e-mail is niet zomaar in te zien door de ontvanger vanwege authenticatie. Voor de zekerheid is contact opnemen met de verkeerde ontvanger met het verzoek de e-mail te verwijderen relevant.

Intrekken of wijzigen van mailberichten

Vaak bieden e-maildiensten de mogelijkheid om een verzonden bericht terug te trekken. Soms kan dat direct, maar soms vereist het instemming van de ontvanger. Er zijn meerdere situaties denkbaar.

- Het intrekken beperken tot geadresseerden binnen hetzelfde maildomein (alles achter het teken @ in het mailadres) als de zender.
- Het wijzigen van mailberichten nadat ze zijn verstuurd. Wel moet rekening gehouden worden dat het intrekken of wijzigen van een bericht mogelijk geen gevolgen heeft voor de gedownloade bijlages.

In de praktijkregels kan hiermee rekening gehouden worden door bijvoorbeeld intrekken en wijzigen niet toe te staan. En voor iedere correctie een verzoek tot intrekken te doen via een los bericht aan de ontvanger.

Gebruik van geautomatiseerde functies

De meeste e-maildiensten hebben verschillende geautomatiseerde functies. Soms aangeduid als filters of regels.

Automatisch doorsturen

Het is vaak mogelijk om e-mails direct door te sturen naar een ander mailaccount (automatic forwarding). De risico's van het automatisch doorsturen zijn:

- mailberichten die veilig zijn ontvangen kunnen geheel onbeveiligd doorgestuurd worden;
- automatisch doorgestuurde berichten kunnen worden doorgestuurd aan personen/mailboxen buiten de praktijk en daarmee zich ontrekken aan de naleving van de praktijkregels.

De bovengenoemde risico's kunnen redenen zijn om het automatisch doorsturen niet te gebruiken in je praktijk.

Leesbevestiging

Een andere geautomatiseerde functie is leesbevestiging. In veel gevallen hebben ontvangers van een bericht deze functie uitstaan. Je kunt je dan afvragen of het gebruik van leesbevestiging niet juist tot verwarrende informatie leidt ('heeft Jan het niet ontvangen of heeft hij leesbevestiging uitstaan?').

Automatisch antwoorden

Het automatisch antwoorden wordt vaak gebruikt in periodes van afwezigheid, zoals vakantie. Het kan vaak worden ingeregeld voor:

- het ontvangen van berichten vanuit het eigen maildomein (alles achter het teken @ in het mailadres, vaak collega's);
- berichten van daarbuiten (externen).

Suggestie voor praktijkregels:

- als waarneming tijdens afwezigheid is geregeld (zie de paragraaf over 'waarneming tijdens afwezigheid'), dan moet het automatisch antwoordenbericht richting externen geen tegenstrijdige informatie geven. Er kan worden besloten om een automatisch antwoord naar externen als niet wenselijk op te nemen in de praktijkregels.

Bewaren en vernietigen van mailberichten

Voor het bewaren en vernietigen van e-mails geldt vaak specifieke wetgeving. Raadpleeg een jurist om te achterhalen welke regelgeving van toepassing is. En in welke gevallen een e-mail onderdeel is van bijvoorbeeld het patiëntendossier. Als er sprake is van een vernietigingsplicht, ga dan na hoe dat te realiseren is in het geval oudere berichten automatisch in een archief worden geplaatst. Het tegenovergestelde is ook een uitdaging: hoe voorkom je dat de mailomgeving niet voortijdig oude, maar nog niet te oude berichten wist?

Omgang met cryptografische sleutels

Versleuteling zal altijd een rol spelen bij veilig mailen. Bij het transport van e-mail over netwerken - zoals internet - is het beheer van encryptiesleutels van een veilige e-maildienst automatisch geregeld. Maar versleuteling van de berichten zelf is dan niet het geval. In het geval dat een bericht toch in de handen van derden valt, blijft de inhoud van het bericht leesbaar. Indien er voor veilige mail een apart product voor encryptie wordt gebruik, informeer dan bij de aanbieder hoe dit is geregeld en let hierbij op dat multikanaalcommunicatie (interoperabiliteit tussen verschillende veilige emailpakketten) is gewaarborgd.

Suggestie voor praktijkregels:

- zorg ervoor dat er duidelijke afspraken zijn met de leverancier over toegang tot beveilingssleutels. Als je naar een andere leverancier gaat wil je niet dat je met oude mail blijft zitten die niet onsleuteld kan worden.

Wordt er gekozen om een eigen methode van versleuteling op de eigen mailberichten toe te passen, hou dan ook de multikanaalcommunicatie eisen van NTA 7516 in de gaten. Zoek in ieder geval aansluiting bij maatregelen 10.1.1 (Beleid inzake het gebruik van cryptografische beheersmaatregelen) en 10.1.2 (Sleutelbeheer) van ISO 27002 resp. NEN 7510.

Verantwoordelijkheden

Alle regels die in dit hoofdstuk (zie ook NTA 7516 paragraaf 6.3) naar voren komen, hebben weinig zin als de verantwoordelijkheid voor de gebruikers van de veilige e-maildienst niet duidelijk is. Zorg dat er actief wordt gecommuniceerd over de praktijkregels.

Daarnaast kunnen ook meer algemeen geldende regels van toepassing zijn, bijvoorbeeld:

- elk ontvangen mailbericht wordt binnen 24 uur gelezen en zo nodig actie op zijn ondernomen.

Suggestie voor praktijkregels:

- communiceer duidelijk op de website van de praktijk op welke wijze veilig wordt gecommuniceerd. Ook kan dit op een inschrijvingsformulier worden opgenomen.

Verzendingsgronden

Deze regels gelden uitsluitend voor situaties waarbij persoonsgegevens worden verzonden. Volgens de Algemene Verordening Gegevensbescherming (AVG) zijn persoonsgegevens alle informatie over een geïdentificeerde of identificeerbare persoon (de 'betrokkene'). Een van de beginselen van de AVG is dat persoonsgegevens uitsluitend rechtmatig mogen worden verwerkt. Rechtmatige verwerking — of in geval van NTA 7516 rechtmatige verzending — vereist een grondslag. De AVG kent de volgende zes grondslagen:

1. 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.

Voor zogenaamde bijzondere persoonsgegevens - zoals persoonlijke gezondheidsinformatie - gelden de nodige uitbereidingen van de grondslagen.

De grondslagen vanuit de AVG luisteren nauw, maar worden door specifieke wet- en regelgeving in specifieke sectoren (denk aan de WGBO, WPG, WMO, etc) deels aangevuld. Stel regels op over mogelijk van toepassing zijnde grondslagen voor verzending, in samenwerking met de functionaris gegevensbescherming binnen de (zorg)praktijk, met de brancheorganisatie of anders met een specialist in privacy recht. Geef aan onder welke omstandigheden bepaalde grondslagen kunnen worden gehanteerd en door wie.

Continuïteit bij uitval mailprovider

Het is niet uit te sluiten dat een leverancier de veilige e-maildienst beëindigt. Voorkomen moet worden dat oude mailberichten die nog op de servers van de leverancier staan, verloren raken of in handen komen van onbevoegden.

Uitval kan langer duren dan de maximale met de mailprovider afgesproken duur, bijvoorbeeld in geval van faillissement of een andere vorm van grote overmacht. Zoek hiervoor aansluiting met clausule 17 (Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer) van ISO 27002 resp. NEN 7510-2.

Zoek waar mogelijk hier al tijdens contracteren van de e-maildienst aansluiting bij de - al dan niet vrijwillige - exit clausule die wordt overeengekomen.

Suggestie voor praktijkregels:
- zoek aansluiting met maatregel 12.3.1 (Back-up van informatie) uit de NEN 7510;
- zorg ervoor dat er duidelijke afspraken over de continuïteit zijn gemaakt bij de selectie en contractering van de veilig mailoplossing.

Informeren van patiënt over veilig mail

Personen moeten op grond van NTA 7516 ook veilig kunnen communiceren met een professional. Het ligt niet voor de hand dat patiënten/cliënten over een NTA 7516-proof veilige mailvoorziening beschikken. Het is onder meer van belang dat patiënten/cliënten over de mogelijkheid van veilig communiceren worden geïnformeerd. Maar ook van belang is dat medewerkers van de professional hier ook een rol in spelen door de juiste informatie hierover te geven.

Suggesties voor praktijkregels
- Mails worden niet via een knop ingetrokken of vervangen, indien een bericht moet worden ingetrokken doen we dit altijd via een apart bericht en laten dit door de ontvanger bevestigen.
- Er worden enkel functionele mailboxen gebruikt voor het ontvangen van berichten uit systemen zoals doorverwijzigingsapplicaties. De toegang is op individuele basis geregeld.
- Iedere e-mail die naar een individuele patiënt vanuit de praktijk gestuurd wordt, doen we via een veilig kanaal. Ook als een patiënt ons via een onveilige weg mailt, het prima vindt als we via diezelfde weg terugmailen en als het om niet medische informatie gaat.
- Mails die we naar groepen van onze patiënten sturen (waarbij ontvangers niet kunnen zien naar wie het bericht nog meer is gestuurd) zoals een nieuwsbrief of een wijziging van openingstijden worden bij ons via gewone e-mail gestuurd (voorbeeld fysiotherapiepraktijk, zie verder de praktijkvoorbeelden in het deel ‘Praktijkscenario’s’).
- Er worden geen mails onveilig gestuurd, ook niet over openingstijden. Alle digitale communicatie gaat veilig en op individueel niveau (voorbeeld fertiliteitskliniek, zie verder de praktijkvoorbeelden in het deel ‘Praktijkscenario’s’).
- Een e-mail die wij van een patiënt ontvangen waarin wordt ingegaan op een individuele afspraak, medische gegevens of enigszins anders aan de gezondheid van de patiënt gerelateerd, worden altijd veilig beantwoord.
- Een patiënt ontvangt binnen een werkdag antwoord.
- E-mails vanuit de praktijk met medische inhoud gaan altijd via een zorgverlener die direct betrokken is bij de behandelrelatie.
- Het streven is altijd via het portaal te mailen, uitzonderingen daar gelaten.
- Er wordt niet gewerkt met persoonlijke gezondheidsinformatie in gedeelde mailboxen.

Tip
Hou uiteindelijk de praktijkregels compact en leesbaar.

Programma van eisen

Leveranciers van veilige e-maildiensten hebben een belangrijke positie in het ondersteunen van veilige e-mail. Het selecteren van een leverancier en een dienst vereist een zorgvuldige afweging tussen:

- (zorg)praktijk specifieke wensen gebaseerd op de eigen processen;
- gebruikersgemak;
- kosten;
- ondersteuning.

Onderstaand programma van eisen (PvE) helpt je om een leverancier van veilige e-maildienst te selecteren die bij jouw zorgpraktijk past.

Onderdeel NTA 7516	Element	Eis/wens
6.1.2	Leverancier garandeert de beschikbaarheidseis van 99,8% en beschrijft wat wordt er hierbij van de ICT van de zorgverlener verwacht.	Eis
6.1.2	Leverancier beschrijft de definitie van beschikbaarheid en wat de beschikbaarheid over de afgelopen 12 maanden is geweest.	Wens
6.1.3	Leverancier committeert zich dat de dienst een maximale uitvalsduur van 24 uur heeft.	Eis
6.1.3	Leverancier informeert over de maximale uitvalsduur van de dienst in de afgelopen 12 maanden.	Wens
6.1.3	Leverancier geeft aan op welke wijze (zorg)praktijk geïnformeerd worden over onbeschikbaarheid van de dienst en het niet tijdig (binnen 24 uur) afleveren van een bericht.	Eis
6.1.4	Leverancier garandeert dat er geen sprake kan zijn van gegevensverlies. En beschrijft op welke wijze dit is ingevuld.	Eis
6.1.5	Leverancier ondersteunt dat de verzender geauthentiseerd is met een UeIDAS middel substantieel en wat hierbij verwacht van de zorgverlener.	Eis
6.1.5	Leverancier informeert op welke manier de (zorg)praktijk authenticatiemiddelen voor ontvangers instellen en beheren.	Eis
6.1.5	Leverancier informeert de zorgverlener over de best-practice hoe vaak de medewerkers in de zorgpraktijk zich opnieuw moeten authentiseren binnen de veilige e-maildienst (als verzender en/of ontvanger)? Bijvoorbeeld, een medewerker moet zich dagelijks opnieuw authentiseren.	Wens, de norm stelt geen eis.
6.1.5	Leverancier biedt gebruiksvriendelijke en veilige toegang volgens de eIDAS norm aan (2-staps authenticatie). En beschrijft op welke wijze dit is ingevuld.	Wens, als er in de praktijk nog geen gebruik gemaakt wordt van 2 factor-authenticatie bij inloggen op de PC is het handig dit hier mee te nemen
6.1.6	Leverancier geeft aan indien de inhoud gewijzigd wordt (bv. door een virusscanner) hoe verzender en ontvanger hierover worden geïnformeerd.	Eis
6.1.7	Leverancier geeft aan, op welke manier de veilige e-maildienst de ondertekening valideert bij inkomende e-mails.	Eis
6.1.7	Leverancier geeft aan hoe zichtbaar gemaakt wordt welke persoon vanuit een functionele mailbox een e-mail heeft verstuurd. Deze moet bij de ontvanger zichtbaar zijn.	Eis
6.1.7	Leverancier geeft aan op welke wijze een ontvanger kan vaststellen dat een bericht veilig is verstuurd.	Eis
6.1.8	Leverancier geeft aan op welke wijze wordt gegarandeerd dat een (nog) niet geautoriseerde persoon een bericht via de veilige e-maildienst kan versturen namens de (zorg)praktijk.	Eis
6.1.8	Leverancier geeft aan op welke wijze professionals kunnen worden toegevoegd aan de veilige e-maildienst. Ook voor tijdelijke medewerkers.	Wens
6.1.9	Leverancier geeft aan hoe wordt gewaarborgd dat onbevoegden geen toegang hebben tot (versleutelde) berichten en hoe omgegaan wordt met de vertrouwelijkheid van encryptiesleutels.	Eis
6.1.9	Leverancier geeft aan welke mogelijkheden de veilige e-maildienst biedt om gegevensvertrouwelijkheid te garanderen als een bericht onverhoopt wordt verstuurd aan iemand die daartoe geen geldige grond heeft.	Eis

Onderdeel NTA 7516	Element	Eis/wens
6.1.9	Leverancier geeft aan waar de opslag van de gegevens van klanten precies plaats vindt.	Wens, vanuit de norm wordt enkel gesteld dat data niet in non-compatibele jurisdicties mag komen
6.1.9	Leverancier geeft aan hoe de veilige e-maildienst waarborgt dat wijziging van de inhoud van een bericht tussen verzending en ontvangst niet mogelijk is.	Eis
6.1.10	Leverancier zorgt dat toegang tot ontvangen berichten alleen mogelijk is na het toepassen van een UeIDAS middel met niveau 'Substantieel'.	Eis
6.1.11	Leverancier zorgt ervoor dat berichten in-transit (tijdens het transport over het internet of tussen cliënt en servers) beschermd tegen ongeautoriseerde toegang.	Eis
6.1.13	Leverancier geeft aan hoe berichten die buiten de EER (Europees Economische Ruimte) komen worden beschermd.	Eis
6.1.14	Leverancier geeft aan hoe ontvanger via de e-maildienst veilig een bericht terugstuurt. (Opmerking: de ontvanger heeft dan zelf geen NTA 7516 product anders mag de leverancier niet de eigen veilige e-maildienst tonen).	Eis
6.1.15	Leverancier geeft aan hoe de ontvanger via de e-maildienst een bericht veilig doorstuurt naar derden en/of hoe wordt de ontvanger erop geattendeerd dat een bericht niet veilig kan worden doorgestuurd (Opmerking: de ontvanger heeft dan zelf geen NTA 7516 product anders mag de leverancier niet de eigen veilige e-maildienst tonen).	Eis
6.1.16	Leverancier geeft aan op welke wijze 'Security by default' binnen de veilige e-maildienst is geïmplementeerd.	Eis
6.1.17	Leverancier geeft aan op welke wijze een ontvanger een bericht kan lezen of bijlagen kan openen die met de veilige e-maildienst zijn verstuurd zonder een account aan te maken.	Eis
6.1.17	Leverancier heeft de veilige e-maildienst gebruiksvriendelijk gemaakt en mogelijkheden geïmplementeerd om ook voor personen met visuele hulpmiddelen gebruikt te worden.	Eis
6.1.17	Leverancier geeft aan op welke webpagina de toegankelijkheidsverklaring rondom de WCAG-2.0 richtlijnen te vinden is.	Eis
6.1.17	Leverancier geeft aan welke handelingen een patiënt moet doorlopen als zij/hij een bericht via de veilig e-maildienst ontvangt. Nb de patiënt moet zich authentiseren met een authenticatiemiddel eIDAS niveau substantieel.	Wens, maar wel goed om te weten bij het selecteren van een veilige e-maildienst.
6.1.18	Leverancier geeft aan op welke manieren de ontvanger en/of professional berichten inclusief bijlagen kan downloaden en opslaan op een zelfgekozen locatie.	Eis
6.1.19	Leverancier geeft aan of met een eenvoudige handeling het bericht veilig in het EPD/ECD/Dossier te kunnen opnemen en met welke applicaties ervaringen zijn. Nb informeer ook of uw EPD/ECD/Dossierapplicatie in staat is met een NTA 7516 veilige e-maildienst te koppelen.	Wens, veel zorgverleners vinden het slim, veilig en snel overnemen van relevante informatie wel wenselijk.
7.1	Leverancier publiceert transparant in welke onderdelen uit NTA 7516 de veilige e-maildienst wel of niet voorziet.	Eis
7.2	De veilige e-maildienst kan koppelen met andere NTA 7516 diensten waardoor ontvangers zonder extra handelingen een bericht kunnen bekijken en de ontvanger een bericht van een ander product direct kan bekijken (in de norm heet dit interoperabel/multikanaalcommunicatie)?	Eis
7.3	Leverancier vermeld met welke andere veilige e-maildiensten koppelingen zijn.	Eis
7.4	De gehele keten van ontwikkelaars, datacenters en andere onderliggende partners van de dienst ISO27001/NEN 7510 is gecertificeerd voor die onderdelen waar de leverancier van de veilige e-maildienst de partner voor betrekt.	Wens, zo ver gaat de norm niet maar hiermee heb je meer zekerheden over de kwaliteit op het gebied van informatiebeveiliging in de gehele keten die voor de veilige e-maildienst nodig is.

Onderdeel NTA 7516	Element	Eis/wens
7.5	Leverancier heeft een ISO27001 en/of NEN 7510 certificering.	Eis
Bijlage A	De leverancier heeft een functie waarmee een patiënt een veilige e-mail kan initiëren (bijvoorbeeld een veilig formulier, portaal of iets anders).	Wens, je mag dit ook zelf oplossen bijvoorbeeld in een portaal van uw ECD/EPD
Certificering	Leverancier is gecertificeerd voor NTA 7516 (mogelijk vanaf ca Q1 2020) Totdat certificering mogelijk is heeft de leverancier de intentieverklaring van VWS rondom veilige e-mail getekend.	Eis
Certificering	Leverancier geeft de garantie om interoperabiliteit uiterlijk 1 januari 2020 geregeld te hebben, zodat voldaan kan worden aan de eisen van de WvGGZ.	Eis, indirect. Het niet kunnen voldoen hieraan betekent dat de dienst niet voldoet aan NTA 7516
Certificering	Leverancier ondersteunt alle standaarden uit de door VWS opgestelde technische handreiking (CaDES, s/mime, DANE, etc.).	Eis
Overige	Leverancier ondersteunt bij een incident met (veilige) e-mail en bekend is op welke wijze.	Wens, leveranciers kunnen echter wel ondersteunen in incidentmeldingen (incident-response)
Overige	Leverancier heeft een voorbeeld communicatieplan voor uw patiënten/cliënten.	Wens, je kunt dit ook zelf regelen
Overige	Leverancier biedt inzicht in aanvullende productmogelijkheden.	Wens
Overige	Leverancier garandeert updates van de software als dat nodig is.	Eis, zeker op het gebied van beveiliging moet een leverancier het product actueel houden. Dit volgt mede uit de NEN 7510
Overige	Leverancier biedt het opleiden en testen met eindgebruikers aan als onderdeel van de dienstverlening.	Wens, je kunt dit ook zelf regelen
Overige	Leverancier levert een plug-in voor Outlook/Office365/G-suite/etc. (selecteren wat relevant is).	Wens, echter gebruik in bestaande mailapplicaties is vaak wel handig
Overige	Leverancier geeft aan wat de maximale grootte is van een bericht inclusief bijlagen en een eventuele (online) mailbox.	Wens
Overige	Leverancier levert ook een app voor mobiel gebruik (iPhone/Android).	Wens
Overige	Leverancier kan een API/plug-in leveren voor online web omgevingen waarin de toepassing geïntegreerd kan worden.	Wens
Overige	Leverancier biedt een functie aan om berichten in te trekken en een nieuwe versie van een bericht te sturen.	Wens

Het is voor een leverancier niet verplicht om aan alle elementen van het PvE te voldoen. Let er wel altijd op dat alle onderdelen uiteindelijk wel ingevuld zijn. Je kunt er ook voor kiezen verschillende elementen zelf in te richten.

Let op: er zijn meerdere leveranciers die de intentie hebben hun veilige e-maildienst te laten voldoen aan NTA 7516. Dit is pas mogelijk als er een formele certificering mogelijk is. Deze wordt in 2020 verwacht. Totdat certificering mogelijk is, geldt dat:

- een leverancier formeel niet kan aangeven te voldoen aan NTA 7516.
- leveranciers die actief participeren in het leveranciersoverleg van VWS rondom het opstellen van de technische uitwerking van de norm te vinden zijn op de website van het Informatieberaad Zorg (https://www.informatieberaadzorg.nl/over-het-informatieberaad/het-project-veilige-mail).
- leveranciers in ieder geval geheel transparant moeten zijn in welke onderdelen van NTA 7516 hun dienst ondersteunt. Zorg dat leveranciers antwoorden onderbouwen. Een enkel 'ja/nee' of 'volstaat/volstaat niet' is in veel gevallen onvoldoende.
- leveranciers in veel gevallen hun dienst moeten aanpassen om ook berichten van andere veilige e-maildiensten (NTA 7516-proof) direct te kunnen ontvangen. Informeer actief of de leverancier de opgestelde technische handreiking ondersteunt, deze is te vinden op de website over veilige mail van het informatieberaad.

Tips voor de implementatie

De implementatie van veilige mailen is in de praktijk een beperkt technisch project. Het is veel meer een proces-, organisatie-, communicatie- en veranderproject. Daarom is het verstandig al voor het selecteren van een veilige e-maildienst na te denken over de implementatie ervan.

Denk hierbij aan:

- Waaraan moet de veilige e-maildienst nog meer aan voldoen dan enkel NTA 7516?
- Welke impact heeft veilig mailen op de werkwijzen van de praktijk?
- Welke impact heeft het op de communicatie met andere collega zorgverleners?
- Welke bedreigingen en risico's zijn er bij het niet of niet volledig voldoen aan NTA 7516?
- Wanneer willen wij veilige e-mail inzetten? Is dit enkel voor communicatie tussen professionals of willen we een vorm van e-mail (dan wel veilig) naar onze cliënten/patiënten inzetten?
- Welke communicatiemogelijkheden heeft ons EPD/ECD of een eventueel persoonlijke gezondheidsomgeving (PGO) en hoe past hier een veilige e-maildienst in?
- Hebben we al een oplossing die ook ad-hoc veilige e-mail kan ondersteunen?
- Het kan zijn dat je praktijk al meerdere oplossingen gebruikt. Hoe zorg je er dan voor dat je geen e-mails over het hoofd ziet?
- Willen wij ook op andere manieren (zoals veilige chat) veilig kunnen communiceren?
- Hoe gaan we om met onze cliënten/patiënten die mogelijk niet de digitale vaardigheden hebben om via verschillende digitale communicatiemedia met sms-codes, wachtwoorden of andere mechanismen kunnen werken?
- Op welke wijze willen wij ondersteuning krijgen van de leverancier bij de implementatie, verwachten we een kant en klare implementatie aanpak inclusief communicatie-uitingen?

Hou na de selectie van een veilige e-maildienst en bij het opstellen van een implementatieplan rekening met de volgende onderdelen:

Domein	Elementen
Communicatie	• Hoe betrek ik, en informeer ik collega's dat we anders gaan werken met veilige e-mail (en soms ook chat)? • Hoe informeer ik mijn cliënten/patiënt dat er een verandering aanstaande is en dat ik niet meer onveilig zal/kan/mag communiceren via email? • Welke andere partijen zullen geen NTA 7516 product hebben en zullen een verandering merken? • Hoe zorg ik ervoor dat op mijn website de mogelijkheden om veilig te communiceren duidelijk zijn voor personen?
Eigen processen	• Hoe zorg ik ervoor dat ik authenticatiemiddelen uitreik en voldoe aan de eIDAS vereisten (laat ik aan de balie telefoonnummers registreren, heeft mijn leverancier een handige oplossing)? • Waar kom ik allemaal veilige e-mail tegen (inkomend en uitgaand) en welk effect heeft het werken met een aanvullende applicatie? • Gaan we als praktijk in 1x over of doen we dit gefaseerd?
Koppelingen	• Welke koppelingen heb ik nu vanuit de e-mail (denk aan koppelingen met/vanuit HIS/ECD) en blijven deze werken? • Wil ik een integratie met het ECD en veilige e-mail en kan mijn ECD-leverancier dit aan? • Zijn er andere mailkoppelingen die veranderen?
Techniek	• Hoe gaan we om met veilige e-mail en smartphonegebruik, is dit ook veilig? • Hoeveel tijd verwacht ik nodig te hebben om de technische zaken (zie checklist techniek) te laten regelen.

Communicatietoolkit

Communicatie over veilig mailen is essentieel. We geven in dit hoofdstuk een aantal suggesties op welke manieren je kunt informeren.

Tijdens het selecteren en testen van de dienst is het ook belangrijk goed contact te houden met patiënten en medewerkers. Vraag hen naar hun wensen, verwachtingen en ervaringen.

Communicatie naar patiënten

Manieren om patiënten te informeren zijn:

- door onderaan iedere veilige e-mail te vermelden:
  Voor het versturen van deze e-mail maken we gebruik van een veilige e-maildienst. Hierdoor zorgen we ervoor dat de medische gegevens die we met u delen beveiligd zijn. Alleen u kunt deze e-mail inzien. Wilt u er meer over weten? Ga dan naar onze website voor meer informatie.
- via een informatiefolder in de wachtkamer of op de balie.
- als informatieblok op de website van de praktijk.
- in de nieuwsbrief.
- per post. Bijvoorbeeld de folder bij de uitnodiging van de griepprik voegen.

Beschrijf in de uitgebreide informatie – bijvoorbeeld op de website – onder andere:

- de voordelen van het gebruik van een veilige e-maildienst.
- waarom het gebruik verplicht is voor het delen van persoonlijke gezondheidsinformatie.
- hoe de veilige e-maildienst werkt.
- wanneer je het moet gebruiken.

Communicatie naar collega's buiten de praktijk

Manieren om collega zorgverleners te informeren zijn:

- per e-mail.
- via de post.
- op informatieavonden.
- via een belrondje.

Communicatie naar medewerkers

Manieren om je medewerkers te informeren zijn:

- organiseer informatieworkshops. Doe dit gedurende het hele project zodat je medewerkers altijd op de hoogte zijn.
- organiseer testuurtjes waarin medewerkers de veilige e-maildienst uitproberen.
- zorg voor een handleiding hoe de veilige e-maildienst gebruikt moet worden.

Checklist techniek (voor je ICT beheerder)

Deze checklist is voor je ICT-beheerder. E-mails worden vanuit een emaildomein@zorgpraktijk.nl gestuurd. In de techniek is een (vaak kleine) aanvulling nodig in de emailomgeving. Deze aanvulling wordt vaak door de ICT-beheerder doorgevoerd. In dit hoofdstuk wordt ingegaan op deze aanpassing

De ICT-beheerder mag onderstaande wijzigingen alleen doorvoeren als de zorgverlener kan aantonen aan elementen van NTA 7516 te kunnen voldoen (beleid, multifactor, etc etc). Het is aan de zorgverlener zelf om te verklaren hieraan te voldoen. De zorgverlener zal om te voldoen aan NTA 7516 de techniek veelal bij een veilig e-mailleverancier inkopen, maar een deel ook zelf moeten verzorgen zoals het opstellen van beleid. In dit handboek staat in het hoofdstuk "voldoen aan NTA 7516" dit uitgebreider beschreven.

Veilige mailen - volgens NTA 7516 - zorgt ervoor dat verzenders van veilige e-mail de ontvangers van veilige e-mail moeten kunnen herkennen. Hiermee wordt ervoor gezorgd dat de veilige e-mail direct in de veilige e-maildienst van de ontvanger terecht kan komen. Het zogenaamde multikanaalcommunicatie (zie NTA 7516 paragraaf 7.2). De leverancier van de veilige e-maildienst moet hier wat voor regelen, maar ook de (zorg)praktijk die verantwoordelijk is voor het maildomein zoals jansen@zorgpraktijk.nl.

Om veilige e-mails te kunnen ontvangen moet de eigenaar (die de beheerder opdracht geeft) het domein '...@zorgpraktijk.nl' een aantal zaken regelen. Op de website van het Informatieberaad Zorg is voor verdere beschrijving van de techniek een technische handreiking voor leveranciers beschikbaar op de website over veilige mail van het informatieberaad. Veel zaken moeten belegd worden bij een ICT-beheerder, zoals:

- Er moet in de DNS-server een TXT-record worden toegevoegd. De specificatie hiervan staat in de technische handreiking.

- De domeinregistratie moet met DNSSec beschermd zijn. Is dit niet het geval, laat dit activeren of verhuis de domeinregistratie naar een partij die dit wel aanbiedt. De kosten en inspanningen hiervan zijn vaak beperkt. Het verhuizen van een domein heeft geen effect op de werking van je website of applicaties.
- Zorg dat ook de gewone e-mail beschermd is middels SPF; START-TLS; DKIM; DMARC; DANE. Dit zijn technische standaarden die zeer wijdverbreid in gebruik zijn en de beveiliging van e-mail allemaal sterk vergroten.

Daarnaast bieden veel veilige e-maildiensten een plug-in om geïntegreerd te worden in het huidige mailprogramma om het gebruikersgemak te verhogen. Hiervoor is het nodig om aanvullende software op de werkplek in de praktijk te installeren. Dit moet in overleg met de ICT beheerder van de werkplek. Dit geldt ook voor een eventuele app van de veilige e-mail die op een smartphone of tablet kan worden gebruikt.

Gebruik de volgende checklist verder als hulpmiddel voor het technische gedeelte van de inrichting van veilige mailen volgens NTA 7516:

Item	Aantekening
Mijn domein @zorgpraktijk.nl wordt beheerd door?	
Mijn domein, @zorgpraktijk.nl is beschermd met DNS Sec?	
Mijn huidige mailserver is beschermd met SPF; Start-TLS; DKIM; MDARC; DANE Gebruik hiervoor de test op internet.nl 'test je email'. Laat de beheerder een reactie geven op de uitkomsten.	
Mijn normale emailprogramma wordt beheerd door?	
Als ik Office 365, G-suite of een andere cloudapplicatie gebruik voor mijn e-mail dan is hier de implementatiepartner?	
Als mijn leverancier een 'veilige e-mail plugin' levert dan wordt deze door de beheerder van mijn normale emailprogramma (op de werkplek of in de Cloud) ondersteunt?	
Zakelijke apps op de smartphone/tablet kunnen medewerkers zelf installeren of worden beheerd door?	

Ben je ICT beheerder van een e-mailserver en wil je zonder aanvullende toepassingen de mailserver laten voldoen aan NTA 7516 en zo een eigen veilige e-maildienst aanbieden? Dan moet je voldoen aan alle vereisten uit de technische handreiking en onderdelen uit NTA 7516.

Evaluatietoolkit

Een vereiste van NTA 7516 is dat je de e-maildienst jaarlijks moet evalueren. Doel van die evaluatie is vast te stellen of de dienst nog voldoet aan de eisen van NTA 7516. Dit is meteen ook een mooi moment om andere zaken te evalueren:

- Sluit het nog aan bij de werkwijzen van de praktijk?
- Wat is het daadwerkelijke gebruik?
- Hoe evalueren patiënten het?
- Sluiten de praktijkafspraken nog voldoende aan?

Om je hierbij te ondersteunen hebben we voor medewerkers en patiënten voorbeeldvragen opgesteld.

Voorbeeldvragen voor medewerkers

- Ben je bekend met het gebruik van de veilige e-maildienst?
- Gebruik je de dienst ook of zijn er redenen ook wel eens gewone e-mail te gebruiken bij persoonlijke gezondheidsinformatie? Toelichting...
- Ondervind je problemen bij de acceptatie van veilige e-mail bij ontvangers (zowel professionals als patiënten)?
- Heb je nog tips en aanbevelingen?

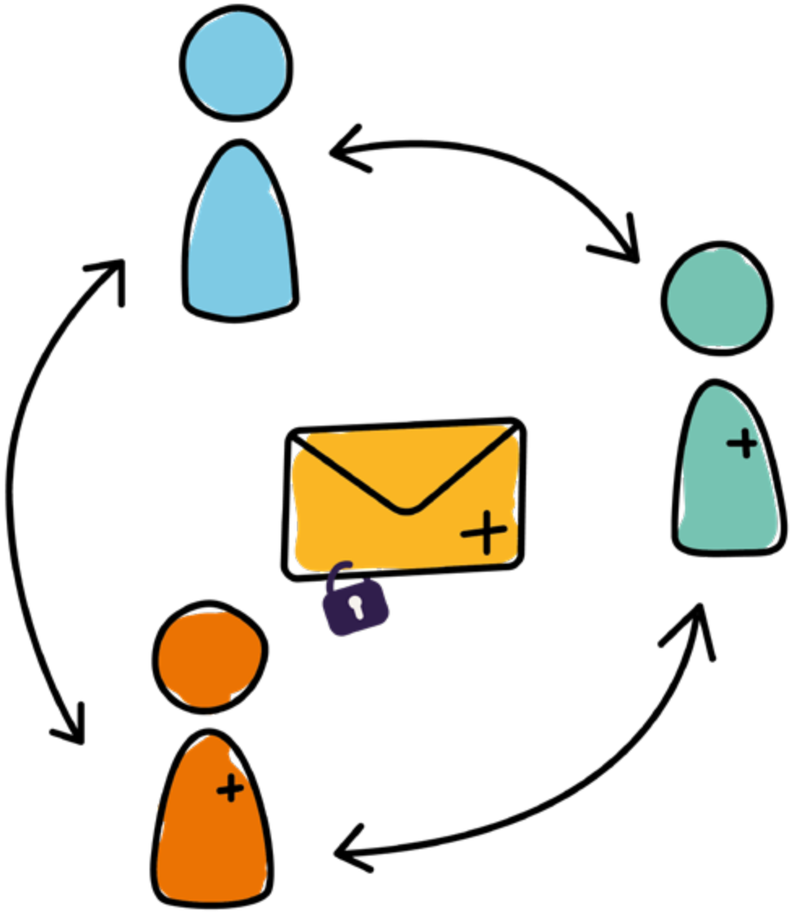
Voorbeeldvragen voor patiënten

Sinds een aantal maanden gebruiken we een veilige e-maildienst in de praktijk, [naam van de dienst]. Zo zorgen we ervoor dat de persoonlijke gezondheidsinformatie die we via e-mail met je delen veilig wordt verstuurd. We zijn erg benieuwd wat je vindt van de verandering en vragen graag naar je mening. Zo kunnen we onze dienstverlening verbeteren.

- Ken je [de veilige e-maildienst]?
- Heb je een keer een e-mail van ons ontvangen via [de veilige e-maildienst]?
- Heb je ons een keer gemaild via [de veilige e-maildienst]?
- Als je een veilig bericht ontvangt, was deze eenvoudig te bekijken?
- Er is ook toegang tot informatie via ons ‘zorgportaal’, gebruik je deze ook om met ons te communiceren?
- Maak je al gebruik van een persoonlijke gezondheidsomgeving (PGO) zoals ...?
- Onze praktijk maakt het mogelijk om via een PGO (met MedMij-keurmerk) veilig te communiceren. Maak je daar gebruik van?
- Heb je nog tips en aanbevelingen?
- Bedankt voor het invullen van de vragen!

Manieren om de vragenlijsten te verspreiden onder je patiënten.

- Neerleggen in de wachtkamer. Vraag je baliemedewerkster om patiënten te wijzen op de vragenlijst.
- Meegeven aan het eind van een consult en vragen of de patiënt het direct in wil vullen.
- Maak de vragenlijst digitaal, bijvoorbeeld via Microsoft Forms of Surveymonkey. De link kun je vervolgens delen via e-mail.



Colofon

Het handboek ‘Veilig mailen, hoe regelen we dat?!’ is een uitgave van Informatieberaad Zorg en Nictiz.

December 2019

Het handboek bestaat uit drie delen:
1. Stappenplan
2. Toolkit
3. Praktijkscenario’s

Bij deze ‘Toolkit’ horen het ‘Stappenplan’ en de ‘Praktijkscenario’s’.

Auteurs
Charlotte Schreuder | Nictiz
Ralph Wagter | Ministerie van Volksgezondheid, Welzijn en Sport
Beer Franken

INFORMATIE BERAAD

Meer informatie: www.informatieberaadzorg.nl