Aanleiding

In mei 2019 is de norm voor veilige ad hoc communicatie van gezondheidsinformatie in werking getreden. Deze norm is gemaakt door de NEN, in opdracht van het ministerie van VWS, het Informatieberaad Zorg en gemeenten. Deze norm maakt het mogelijk dat gecertificeerde communicatiediensten op een veilige wijze met elkaar kunnen communiceren.

De eerste aanbieders van “veilig e-mailen” zijn inmiddels gecertificeerd conform deze norm. Dit heeft gevolgen voor de gebruikers. Zij zullen ook moeten voldoen aan een aantal vereisten. Daarnaast moet de aanbieder aan kunnen tonen dat zij haar gebruikers heeft gewezen op de vereisten uit de NTA.

Scope

Momenteel zijn een groot aantal praktijken benaderd door Enovation, de organisatie achter Zorgmail Secure e-mail. Enovation is één van de eerste aanbieders die NTA 7516 gecertificeerd is. De overige aanbieder (Secumail, Ezorg, Zivver en anderen) zullen op korte termijn gaan volgen. De NTA 7516 certificering is een verplichting voor alle aanbieder van veilig e-mailen.

Ondersteuning vanuit ZIO

De aanbieder van veilig e-mailen in de zorg stelt een aantal vereisten aan de huisartspraktijken die gebruik maken van hun dienst. Deze vereisten zijn normerend en dus verplicht, echter zijn ze door het technische taalgebruik lastig te implementeren. De bestuursgroepvoorzitters hebben ZIO verzocht om een kort en duidelijk stappenplan te maken om huisartspraktijken te ondersteunen om te kunnen voldoen aan de vereisten. Dit korte stappenplan en een voorbeeld beleidsverklaring vindt u in dit document.

Vereisten voor de huisartsenpraktijk

De vereisten die de aanbieder aan de praktijk stelt staan gelijk aan een aantal normonderdelen aan de NTA 7516. Per normonderdeel geven we in onderstaand aan wat er geregeld moet worden, inclusief suggesties hoe.

6.1.1 Algemene criteria

In deze paragraaf staat beschreven dat de praktijk gebruik maakt van de mogelijkheid tot veilig mailen. Dit dient opgenomen te worden in het kwaliteitsmanagementsysteem, waarbij wordt beschreven hoe aan bepaalde normen wordt voldaan. Een voorbeeld van een beleidsstuk over veilig e-mail is te vinden in bijlage 1.

6.1.8 Autorisatie verzender

Wat bij 6.1.8 in de norm staat is dat de organisatie van de verzender garandeert dat de verzender is geautoriseerd om een mail aan een ontvanger te sturen. Dit kan ingeregeld worden door middel van een twee stapsverificatie. Hoe dit ingeregeld moet worden, is afhankelijk van de wijze waarop het veilig mailen is geïmplementeerd in de praktijk.

Wijze 1; via webmail/zimbra

De praktijk gebruikt waar mogelijk de optie om een toegangscode per SMS aan de ontvanger te

verzenden. Dit doet men door de onderwerkregel te starten met: SMS 06….. Dit geldt voor ontvangers die niet in het zorgmail-adresboek staan.

Wijze 2; bij integratie in outlook (“groene veilig verzenden knop”)

Er dient een 2e factor op de werkplek/mailclient geïmplementeerd te worden. Dit geldt voor de interne werkplek, thuiswerkplek en mobiele werkplek; voor zover deze werkplekken worden gebruikt om veilig te mailen met ZorgMail Secure e-mail. Dit kan op twee manieren:

- *Via digitale middelen*
  Het is mogelijk om een 2e factor toe te voegen door middel van een applicatie op gsm’s. Dit kan gerealiseerd worden door de applicatie “Microsoft Authenticator”. Dit is kostentechnisch voordeliger dan het inrichten van een 2e factor middels van hardware. Iedere medewerker die toegang nodig heeft tot de veilig mailen applicatie, dient wel in het bezit te zijn van een smartphone.
- *Middels hardware*
  Een aantal systeembeheerders bieden de mogelijkheid om de 2e factor toe te voegen door middel van een vingerafdruklezer.

De praktijk dient een keuze te maken tussen beide wijzen van 2e factor. Als u deze keuze heeft gemaakt, kun u contact opnemen met uw systeembeheerder. Deze kan u ondersteunen bij het implementeren van de 2e factor.

Nadat bovenstaande 2e factor is ingevoerd, moet de knop “veilig verzenden” een update krijgen. Uw aanbieder van veilige e-mail ondersteunt u hierbij. Voor zorgmail is de update hier te vinden. Selecteer de optie ‘*Veilig verzenden add-in Outlook voor de 1e lijn’*.

6.1.12 Verzendingsgrond

In deze norm staat beschreven dat de focus voor veilig verzenden bij de verzender ligt en niet bij de ontvanger. Door de werkwijze behorende bij norm 6.1.8 te implementeren, voldoet de praktijk automatisch aan deze norm.

6.2.2.1 Veilige connectie

De in de technische infrastructuur aanwezige verzendende server (die verbinding maakt met de verzendende client-software) moet de in de technische infrastructuur aanwezige ontvangende e-mailserver (die verbinding maakt met de ontvangende client-software) controleren op de mogelijkheid tot het veilig ontvangen van ad-hocberichten[1]. Als de ontvangende server niet aan de benodigde veiligheidseisen voldoet, mag de verzendende server het ad-hocbericht niet met (directe

[1] E-mailverkeer en chatberichten worden in de NTA norm gedefinieerd als ad-hocberichten.

toegang tot) persoonlijke gezondheidsinformatie aanbieden. Dit wordt automatisch ingeregeld als er gebruik wordt gemaakt van de veilig e-mail aanbieder.

6.3 Gebruik

De huisartsenpraktijk moet regels vaststellen (beleid) over hoe hij en degenen die voor hem werken, gebruik mogen maken van geïmplementeerde communicatiemogelijkheden. Dit is terug te vinden in het voorbeeld beleidsstuk in bijlage 1.

6.4 Toezicht/naleving

De praktijk moet vaststellen hoe er wordt bekeken of de gekozen applicatie voor veilig e-mailen in de zorg nog passend is voor de eisen die de praktijk stelt. De wijze waarop dit gebeurd, wordt opgenomen in het beleidsstuk. (bijlage 1) Daarnaast moet er per praktijk 1 persoon voor deze controle aangewezen worden. Dit moet vermeld worden op de zelfverklaring.

6.5 Door personen geïnitieerd ad-hoc berichtenverkeer

De praktijk moet aan patiënten, zorgpartners en anderen bekend maken dat ze gebruik maken van een applicatie voor veilig e-mailen. Dit kan door middel van het vermelden van het veilige e-mailadres op de website. Onderstaande voorbeeldtekst kan gebruikt worden:
Huisartsenpraktijk [naam invullen] hecht er veel waarde aan dat er op een juiste manier met persoonlijke informatie omgegaan wordt. Daarom kiezen we voor de mogelijkheid tot het veilig verzenden van e-mails. Onze aanbieder [naam aanbieder] conformeert zich aan de wettelijke eisen hiervoor. U kunt ons veilig bereiken via [e-mailadres].

Zelfverklaring

De aanbieder voor veilig e-mailen verzoekt de huisartsenpraktijk om de zelfverklaring in te vullen en te retourneren. Door het ondertekenen van deze zelfverklaring, geeft de praktijk aan bovenstaande normonderdelen geïmplementeerd te hebben. Daarnaast wijst de praktijk een verantwoordelijke medewerker aan voor de controle en implementatie van de vereisten. De kolom “Opmerking professional” mag leeg gelaten worden. Deze kolom heeft vooral een checklist functie.

Bijlage 1

Beleidsverklaring Veilig e-mailen in de zorg

Huisartsenpraktijk *[naam invullen]* maakt gebruik van de diensten van *[naam leverancier veilig mailen]* om de digitale ad-hoc communicatie op een veilige wijze vorm te geven. *[Naam leverancier]* is gecertificeerd conform NTA7516.

Alle medewerkers in de huisartsenpraktijk conformeren zich aan de vastgestelde eisen in deze beleidsverklaring.

Criteria NTA 7516

Onderstaande criteria uit de NTA 7516 zijn vastgesteld en geïmplementeerd in de praktijk. De eisen in de praktijk berusten op de onderwaardes, vastgesteld door de NEN.

Groep	**Criterium**	**Herleidbaarheid in de praktijk**
Beschikbaarheid	Minimale beschikbaarheid (6.1.2)	De minimale beschikbaarheid van de applicatie is 99.8% per jaar. In het geval van uitval wordt niet overgegaan op een onbeveiligde wijze voor ad-hoc communicatie.
	Maximale uitvalduur (6.1.3)	De hoogst aanvaardbare aaneengesloten uitvalduur van ad-hocberichtenverkeer is 24 uur. Gerekend over de aan de praktijk toe te rekenen software & technische infrastructuur.
	Maximaal gegevensverlies (6.1.4)	Tenzij de verzender binnen 24 uur na verzending wordt geïnformeerd over (mogelijk) gegevensverlies, is geen enkel gegevensverlies vanaf de praktijk acceptabel. De praktijk zal ook direct een melding maken van dit datalek bij de AP.
Integriteit	Herkomstbevestiging (6.1.5)	De authenticatiemethode moet minimaal een betrouwbaarheidsniveau met het niveau ‘substantieel’ hebben conform UeIDAS. In de praktijk is dit ingericht middels 2 factor identificatie.
	Data-integriteit (6.1.6)	Wijziging van de inhoud van een ad-hocbericht tussen verzending en ontvangst is niet toegestaan. Tussenliggende componenten noch eventueel betrokken personen/professionals mogen de inhoud van een ad-hocbericht wijzigen.
	Onweerlegbaarheid verzender (6.1.7)	Het veilige e-mailadres van de is herkenbaar voor de ontvanger en is te relateren aan de praktijk.
	Autorisatie verzender (6.1.8)	De praktijk garandeert dat de verzender geautoriseerd is om een ad-hocbericht aan een ontvanger te

Groep	Criterium	Herleidbaarheid in de praktijk
		sturen. Dit is geregeld middels de 2 facter identificatie.
Vertrouwelijkheid	Gegevensvertrouwelijkheid (6.1.9)	Door professionals opgeslagen ad-hocberichten mogen niet in handen van onbevoegden komen. Dat geldt zowel voor opgeslagen ad-hocberichten in de technische infrastructuur als die in de client-software. De praktijk regelt dit door middel van 2 factor identificatie.
	Toegangsvertrouwelijkheid (6.1.10)	Toegang tot ad-hocberichten is niet toegestaan met authenticatiemiddelen lager dan 'substantieel' voor personen en 'hoog' voor gegevens waarop het wettelijk beroepsgeheim van de professional berust. Waar mogelijk wordt gebruik gemaakt van een sms-verificatie van de ontvanger. Indien het veilig e-mail adres gebruikt wordt voor een koppeling met edifact, wordt deze toegangsvertrouwelijkheid geborgd door het HIS.
	Communicatievertrouwelijkheid (6.1.11)	Toegang tot ad-hocberichten door partijen die daartoe geen geldige grond hebben, moet onmogelijk zijn. Dit is geregeld door *[naam leverancier]*.
	Verzendingsgrond (6.1.12)	De praktijk heeft vastgesteld dat medewerkers met bepaalde functies veilige ad-hoccommunicatie mogen gebruiken ten behoeve van patiëntenzorg. De praktijk ziet toe dat de praktische uitvoering van deze afspraak wordt gehonoreerd.
	Internationaal ad-hocberichtenverkeer (6.1.13)	Indien ad-hoccommunicatie noodzakelijk is buiten de grenzen van de EER, mag dit alleen indien er een grondslag is conform AVG.
Gebruiksvriendelijkheid	Continuïteit van ad-hocberichtenverkeer – beantwoorden (6.1.14)	De berichten die veilig worden verzonden vanuit de praktijk, bieden de mogelijkheid om beantwoord te worden door de ontvanger.
	Continuïteit van ad-hocberichtenverkeer – doorsturen (6.1.15)	De berichten die veilig worden verzonden vanuit de praktijk, bieden de mogelijkheid om door de ontvanger te worden doorgestuurd.
	Veiligheid als gemak (6.1.16)	De optie “veilig verzenden” staat standaard aan bij het gebruik van de applicatie.

Groep	Criterium	Herleidbaarheid in de praktijk
	Leesbaarheid (6.1.17)	De hoofdtekst van het ad-hocbericht (de 'body') is zonder additionele viewer te lezen.
	Eigen kopie (6.1.18)	De hoofdtekst van het ad-hocbericht (de 'body') is na opslag zonder additionele viewer te lezen.
Interoperabiliteit	Dossierkoppeling (6.1.19)	Verzonden berichten kunnen ten alle tijden gekoppeld worden aan het HIS.

Gebruik

De huisartsenpraktijk heeft duidelijke afspraken/regels gemaakt over het gebruikmaken van de veilig e-mailen applicatie. Onderstaand een korte weergave van de gemaakte regels:

- Praktijk vult aan: *stel vast hoe omgegaan wordt met veilig mailen tijdens waarneming/vervanging. Krijgt de waarnemer ook toegang tot de applicatie? Zorg dan voor 2 factor identificatie.*
- De huisarts is primair eindverantwoordelijk voor de ad-hoc communicatie, echter zijn taken gedelegeerd naar de [benoemen functies];
- Er is altijd sprake van een directe behandelrelatie tussen de huisarts en diegene waar de ad-hoccommunicatie over gaat;
- Het adresboek dat beschikbaar wordt gesteld door [naam leverancier] wordt alleen gebruikt voor zakelijke doeleinden;
- Het intrekken/wijzigen van een reeds verzonden ad-hocbericht, is niet toegestaan zonder expliciete toestemming van de huisarts. Deze wijziging/intrekking wordt ten allen tijde gedocumenteerd in het HIS;
- Er wordt gebruik gemaakt van de afwezigheidsassistent, indien de mailbox doordeweeks langer dan 24 uur niet wordt gelezen;
- De praktijk houdt zich aan de wettelijk geldende bewaartermijnen en bewaart ad-hoccommunicatie niet langer dan strikt noodzakelijk;
- De praktijk informeert de patiënt over de mogelijkheid tot het veilig verzenden van ad-hocberichten;
- *Evt. aanvullen met praktijkeigen afspraken.*