zivver

Praktische handleiding NTA 7516

Ontdek wat de nieuwe norm voor veilige ad hoc communicatie inhoudt en hoe jouw organisatie er snel aan voldoet

☐ Checklist

→

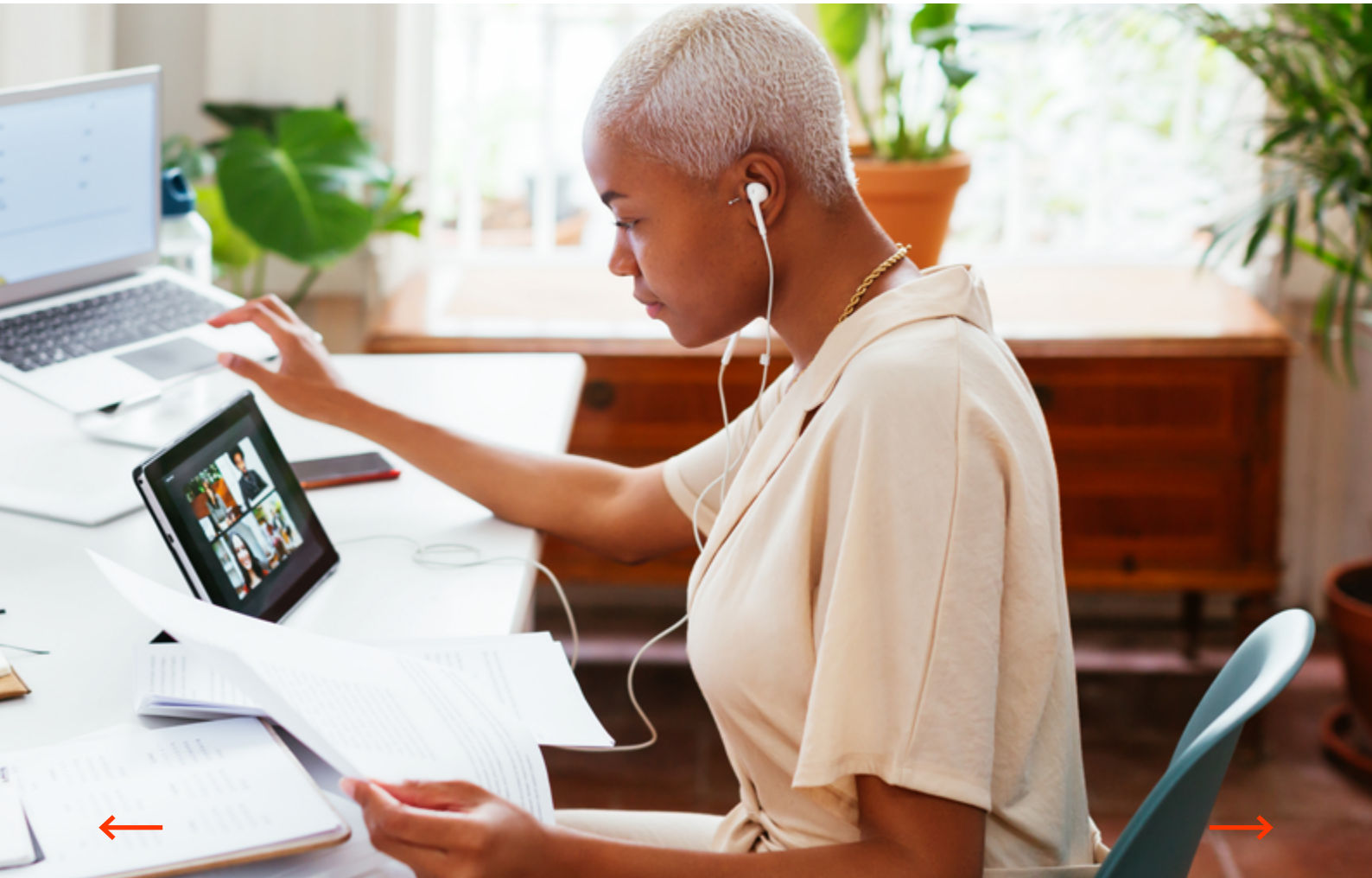
Inhoudsopgave

Introductie

In september 2018 kreeg de NEN de opdracht van het ministerie van VWS en het Informatieberaad Zorg om de NTA 7516 te ontwikkelen. De aanleiding was enerzijds een verzoek van de Autoriteit Persoonsgegevens (AP).

Die constateerde namelijk dat de meeste datalekken ontstonden bij de uitwisseling van persoonsgevoelige, vaak gezondheidsgerelateerde, informatie.
De AP had dus behoefte aan een toetsingskader, zodat zij kon handhaven op compliance aan de nieuwe Europese privacywetgeving GDPR (General Data Protection Regulation, ook wel Algemene Verordening Gegevensbescherming of AVG genoemd) en andere relevante wetten en normen, zoals de NEN 7510, 7512, 7513, WGBO.

Anderzijds vroeg ook het veld om duidelijkheid over wanneer communicatie zoals e-mail veilig ingezet kon worden en om de mogelijkheid om verschillende oplossingen met elkaar te koppelen. De NTA 7516 biedt het kader voor veilige ad hoc communicatie en aan welke eisen die moet voldoen.



Wat is de NTA 7516?

De NTA 7516 is de norm voor veilige ad hoc communicatie van gezondheidsinformatie. Deze norm is gemaakt door de NEN, in opdracht van het ministerie van VWS, het Informatieberaad Zorg en gemeenten. Onder ad hoc communicatie vallen naast e-mail ook chat, portalen en messengers. Oftewel: alle vormen van communicatie die tussen mensen plaatsvindt. De norm beschrijft aan welke ruim twintig eisen organisaties en de oplossingen die zij gebruiken moeten voldoen als ze willen claimen veilig te zijn. Dit zijn eisen ten aanzien van beschikbaarheid, integriteit, vertrouwelijkheid, gebruiksvriendelijkheid, interoperabiliteit, beleid en logging.

De NTA 7516 heeft twee belangrijke doelstellingen:

- Ad hoc communicatie van gezondheidsinformatie gaat altijd veilig:
  De NTA 7516 is bedoeld om het gebruik van e-mail en chatapplicaties (al dan niet aangeboden via een berichtenportaal) te voorzien van randvoorwaarden. Zo borgt de norm veilige en betrouwbare uitwisseling van persoonlijke gezondheidsinformatie.
- Verschillende oplossingen worden gekoppeld:
  De NTA 7516 heeft als doel dat er tussen de verschillende oplossingen die er voor professionals beschikbaar zijn, onderling berichten uitgewisseld kunnen worden, ongeacht hun leverancier.

Voldoen aan de NTA 7516 is niet verplicht, je hoeft immers niet ad hoc te communiceren. Er bestaan al veel koppelingen tussen systemen van verschillende (zorg)organisaties en deze vallen onder de NEN 7512.

Als jouw organisatie wel ad hoc communiceert, moet elke medewerker die omgaat met gezondheidsinformatie (professional) zich aan de eisen van de NTA 7516 houden. Niet omdat de norm verplicht is, maar omdat de eisen allemaal voortvloeien uit andere wetgeving en richtlijnen.

Voor wie is de NTA 7516?

De NTA 7516 geldt voor alle organisaties die gebruikmaken van ad hoc communicatie voor het delen van gezondheidsinformatie.

Dus bijvoorbeeld het e-mailen van afspraak-bevestigingen of onderzoeksuitslagen aan patiënten, chatten met collega's, of het delen van medische gegevens via e-mail voor een verzekering of beschikking. Verder vormt de NTA 7516 de basis voor informatieuitwisseling in de keten van de Wet verplichte ggz (Wvggz). Hiermee geldt de NTA 7516 dus niet alleen voor ziekenhuizen, GGZ-instellingen, ouderenzorgorganisaties, huisartsen en andere zorgorganisaties en -professionals, maar ook voor gemeenten, het openbaar ministerie (OM), juridische dienstverleners en verzekeraars.

Hoewel organisaties moeten voldoen aan de NTA 7516, kunnen ze dat alleen als ze gebruik maken van NTA 7516-gecertificeerde oplossingen.

Daarmee geldt (een groot deel) van de norm ook voor leveranciers van oplossingen die zich willen kwalificeren als oplossing voor veilige e-mail of veilige chat. We raden je aan gebruik te maken van onze checklist voor leveranciers. Hiermee bereik je dat jouw organisatie en de leveranciers waarmee je samenwerkt voorbereid zijn op de nieuwe norm die binnenkort door de Autoriteit Persoonsgegevens zal worden gehandhaafd.

Vooralsnog is de NTA 7516 een Nederlandse norm. De NEN heeft laten weten dat zij de intentie heeft om een traject te starten om van deze norm een Europese CEN-norm te maken. Nederland is namelijk het eerste land dat een dergelijke norm voor veilige ad hoc communicatie heeft opgesteld. Vaak worden dit soort normen centraal of decentraal overgenomen door andere bij de CEN aangesloten landen, waaronder alle 28 Europese lidstaten.

Checklist: Bereid je voor op de NTA 7516

In het volgende deel vind je twee checklists die je helpen om jouw organisatie aan de NTA 7516 te laten voldoen:

- Allereerst een handige checklist op basis van de vereisten waaraan de organisatie moet voldoen;
- Daarnaast een checklist die je aan relevante leveranciers kunt verstrekken om zeker te zijn dat de digitale ecosystemen van jouw organisatie aan de norm voldoen.

Checklist: Bereid je voor op de NTA 7516

Zivver heeft een handige checklist opgesteld, waarin de verschillende vereisten worden samengevat die nodig zijn om de norm na te leven. Deze checklist helpt je te bepalen welke zaken jouw organisatie nog moet regelen om te voldoen aan de NTA 7516 en veilig te mailen. Bij de verschillende punten staat tussen haakjes aangegeven om welke onderdelen van de NTA 7516 het gaat, zodat je de achtergrondinformatie bij dit onderdeel kunt opzoeken.

Vastleggen minimale eisen (6.1.1)

- [ ] Wij hebben voor onze organisatie minimale eisen en onderbouwing daarvan vastgelegd voor alle normatieve criteria.

Minimale beschikbaarheid (6.1.2)

- [ ] Wij hebben in de SLA met onze leveranciers voor het versturen van veilige e-mail en leveranciers voor het ontvangen van e-mail, heldere en meetbare afspraken gemaakt over een beschikbaarheid van >99.8%, met duidelijke gevolgen bij het niet halen van deze afspraken.
- [ ] Alle relevante leveranciers bieden actueel, verifieerbaar en objectief inzicht in de beschikbaarheid van de afgelopen 12 maanden (bij voorkeur real-time via een zogenaamde statuspagina).

Je kunt de norm hier downloaden: https://www.nen.nl/nta-7516-2019-nl-254878

Maximaal gegevensverlies (6.1.4)

- [ ] Wij hebben in de SLA met onze leveranciers voor het veilig versturen en ontvangen van e-mail heldere en meetbare afspraken gemaakt over het voorkomen van gegevensverlies en garantie op het informeren van de verzender binnen 24 uur als informatie niet kan worden afgeleverd, met duidelijke gevolgen bij het niet halen van deze afspraken.

Herkomstbevestiging (6.1.5)

- [ ] Wij hebben geregeld dat toegang tot een mailbox vanaf elke cliënt (bijvoorbeeld Outlook vanaf de werkplek, een app vanaf mobiel of webmail vanaf thuis) alleen maar mogelijk is na inloggen met (geverifieerde) 2FA. Toegang tot gevoelige informatie met alleen een wachtwoord is dus niet mogelijk.
- [ ] We hebben gewaarborgd dat al onze e-mails met persoonlijke gezondheidsinformatie worden verstuurd met DKIM-ondertekening op de wijze die in de betreffende passages uit de 'Technische handreiking NTA 7516 voor e-mail dienstenleveranciers' is toegelicht.
- [ ] We hebben gewaarborgd dat al onze e-mails met persoonlijke gezondheidsinformatie digitaal worden ondertekend door middel van CaDES op de wijze die in de betreffende passages van de technische handreiking is toegelicht.

Data-integriteit (6.1.6)

- [ ] Wij hebben geregeld dat communicatie tussen alle e-mailclients en onze mailserver beveiligd is met de juiste waarborgen (TLS 1.2 of hoger en certificaatvalidatie).

Onweerlegbaarheid verzender (6.1.7)

- [ ] Wij hebben DKIM, DMARC en SPF ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van de technische handreiking is toegelicht.
- [ ] Wij hebben gewaarborgd dat bij de ontvanger zichtbaar gemaakt wordt welke persoon vanuit een functionele mailbox een e-mail heeft verstuurd. Deze moet bij de ontvanger zichtbaar zijn.
- [ ] Wij hebben gewaarborgd dat de ontvanger (visueel) kan vaststellen dat een bericht veilig is verstuurd.

Autorisatie verzender (6.1.8)

- [ ] Wij hebben beleid opgesteld over welke (soorten) zorgverleners geautoriseerd zijn tot het inzien van en communiceren met of over patiënten/cliënten. We hebben dit beleid vertaald in de technische toegang tot functionele (voor een team) of gedelegeerde mailboxen.
- [ ] Wij hebben logging van de toegang van individuele medewerkers tot e-mailboxen en specifieke gevoelige e-mail gewaarborgd.

Gegevensvertrouwelijkheid (6.1.9)

- [ ] Wij hebben gewaarborgd dat berichten versleuteld opgeslagen worden op zowel de e-mailservers van onze leveranciers als op de servers van de cliëntsoftware binnen GDPR-compatibele jurisdicties.
- [ ] Wij hebben gewaarborgd dat onbevoegden geen toegang hebben tot de data of de sleutels die toegang geven tot de informatie.
- [ ] Wij weten welke mogelijkheden onze leverancier van veilige e-mail biedt om gegevensvertrouwelijkheid te garanderen als een bericht onverhoopt wordt verstuurd aan iemand die daartoe geen geldige grond heeft.
- [ ] Wij hebben met alle leveranciers die betrokken zijn bij het verzenden en ontvangen van e-mail met persoonlijke gezondheidsinformatie een verwerkersovereenkomst afgesloten.

Toegangsvertrouwelijkheid (6.1.10)

- ☐ Wij hebben gewaarborgd dat toegang tot een mailbox vanaf elke cliënt (bv Outlook vanaf werkplek, app vanaf mobiel, webmail vanaf thuis) alleen maar mogelijk is na inloggen.
- ☐ Wij hebben gewaarborgd dat de toegang tot ontvangen berichten door eigen medewerkers op persoonsniveau wordt gelogd.
- ☐ Wij hebben gewaarborgd dat verstuurde e-mails met persoonlijke gezondheidsinformatie voor ontvangers die niet voldoen aan de NTA alleen maar toegankelijk zijn nadat de ontvanger zich heeft geauthenticeerd met (geverifieerde) 2FA, bijvoorbeeld via een SMS naar een geverifieerd telefoonnummer.

Communicatievertrouwelijkheid (6.1.11)

- ☐ Wij hebben gewaarborgd dat berichten in-transit (tijdens het transport over het internet of tussen cliënt en servers) zijn beschermd tegen ongeautoriseerde toegang.
- ☐ Wij hebben gewaarborgd dat e-mails alleen maar worden verstuurd als 'notificatie e-mails' in het geval ze worden gestuurd aan een ontvanger die niet voldoet aan de NTA. Waarbij het bericht alleen toegankelijk is met een geverifieerde 2FA of, als de ontvanger wel voldoet (claimt te voldoen), dit alleen gebeurt conform de eisen die staan beschreven in de technische handreiking. E-mails met persoonlijke gezondheidsinformatie worden niet meer als 'gewone' e-mail verstuurd.

Verzendingsgrond (6.1.12)

- ☐ Wij hebben beleid hebben opgesteld waarbij voor de verzendende professional duidelijk is beschreven aan welke regels hij/zij zich moet houden. Het beleid geeft onder meer duidelijkheid over de afwegingen rondom geheimhouding die moeten worden gemaakt. Hier is in beschreven welke professionals welke verzendingsgronden mogen hanteren en wie moet toezien op de uitvoering van het beleid.

Internationale ad-hocberichtenverkeer (6.1.13)

- ☐ Wij hebben gewaarborgd dat berichten die onder onze verantwoordelijkheid vallen, opgeslagen worden binnen de EER (Europees Economische Ruimte).
- ☐ Wij hebben gewaarborgd dat berichten die buiten de EER (Europees Economische Ruimte) komen passend worden beschermd.

Continuïteit van communicatie: beantwoorden (6.1.14)

- ☐ Wij hebben gewaarborgd dat een ontvanger die niet aan de NTA voldoet via onze veilige e-maildienst een veilig bericht kan terugsturen zonder dat hij/zij een account hoeft aan te maken.

Continuïteit van communicatie: doorsturen (6.1.15)

- ☐ Wij hebben gewaarborgd dat een ontvanger die niet aan de NTA voldoet via onze e-maildienst een bericht veilig kan doorsturen naar derden waarbij, als hierbij de veiligheid niet kan worden gewaarborgd, de ontvanger hierop wordt geattendeerd.

Veiligheid als gemak (6.1.16)

- ☐ Wij hebben gewaarborgd dat, als er persoonlijke gezondheidsinformatie wordt verstuurd, de 'normale' verzendknop resulteert in veilig versturen conform de NTA en dat gebruikers niet op een andere verzendknop hoeven te drukken.

Leesbaarheid (6.1.17)

- [ ] Wij hebben gewaarborgd dat ontvangers van veilige berichten geen account bij onze veilige e-maildienst hoeven aan te maken alvorens een bericht te lezen, te beantwoorden, door te sturen of te downloaden.
- [ ] Wij hebben gewaarborgd dat ontvangers van veilige berichten met visuele hulpmiddelen kunnen lezen, beantwoorden, etc. door te zorgen dat onze oplossing voor veilige e-mail voldoet aan de relevante eisen van de WCAG 2.0.
- [ ] Wij hebben gewaarborgd dat onze leverancier voor veilige e-mail een toegankelijkheidsverklaring rondom de WCAG 2.0-richtlijn op zijn website heeft gepubliceerd.

Eigen kopie (6.1.18)

- [ ] Wij hebben gewaarborgd dat ontvangers van veilige e-mailberichten het bericht veilig en eenvoudig kunnen opslaan op een zelf gekozen locatie in een formaat dat met reguliere clientsoftware leesbaar is. Bijvoorbeeld door het te downloaden als een .eml-bestand.

Dossierkoppeling (6.1.19)

- [ ] Wij hebben gewaarborgd dat medewerkers met een eenvoudige handeling het bericht veilig in het EPD/ECD/ dossier kunnen opnemen.

6.2 Implementatie-eisen

Wij hebben één of meerdere oplossingen voor veilige e-mail en chat applicaties geselecteerd op basis van de eisen in 6.1. Daarbij hebben wij gedocumenteerd hoe deze aanbieder(s) deze eisen waarborgen.

De implementatie-eisen zijn gedocumenteerd voor:

- [ ] e-mail (6.2.2) Hierbij gaat het om het bewerkstelligen van een veilige connectie (6.2.2.1) en moeten metadata worden beperkt tot uitsluitend het noodzakelijke of beschermd worden (6.2.2.2)
- [ ] veilige chatapplicaties (6.2.3)

Beleid over gebruik (6.3)

Wij hebben regels (beleid) vastgesteld over de wijze waarop binnen onze organisatie gewerkt mag worden met de geïmplementeerde communicatiemogelijkheden, met ten minste regels over:

- [ ] het waarnemen van collega's tijdens hun afwezigheid;
- [ ] het mandateren en delegeren van toegang tot adhocberichten;
- [ ] de toegang tot informatie zonder een directe behandelrelatie (in zorginstellingen);
- [ ] de toegang tot functionele berichtenboxen (bijvoorbeeld orthopedie@voorbeeld.nl);
- [ ] het gebruik van een adresboek;
- [ ] het gebruik van functies die kunnen resulteren in het intrekken of wijzigen van ad-hocberichten;
- [ ] het gebruik van geautomatiseerde functies bij ontvangst van ad-hocberichten (waaronder maar niet uitsluitend: autoreply bij afwezigheid, leesbevestiging);
- [ ] bewaartermijnen;
- [ ] sleutelbeheer indien van toepassing, de mogelijkheden voor forensisch onderzoek (zie NEN 7510 2:2017, 16.1.1) en 'key escrow' regeling;
- [ ] verantwoordelijkheden;
- [ ] verzendingsgronden;
- [ ] het continueren van de dienstverlening bij faillissement van de communicatie dienstenaanbieder;
- [ ] het informeren van de persoon over de veilige e-mailvoorziening.

Programma over toezicht en naleving (6.4.1)

Wij hebben een programma vastgesteld waarmee

- ☐ i) continu de naleving van de gebruiksregels wordt gemonitord.
- ☐ ii) jaarlijks de geschiktheid van de geselecteerde en geïmplementeerde communicatiemogelijkheden wordt vergeleken met de criteria die daarvoor zijn vastgelegd en.
- ☐ iii) we elke twee jaar de vastgelegde criteria beoordelen op geschiktheid en passendheid.

Vereiste logging van handelingen en gebeurtenissen (6.4.2)

Categorieën van gebeurtenissen die moeten worden gelogd:

- ☐ alle gebeurtenissen met betrekking tot het versturen van berichten;
- ☐ het intrekken van verzonden berichten;
- ☐ het wijzigen van verzonden berichten;
- ☐ het verwijderen (bij de verzender) van verzonden berichten;
- ☐ alle gebeurtenissen met betrekking tot het ontvangen van berichten;
- ☐ het raadplegen van ontvangen berichten;
- ☐ het verwijderen van ontvangen berichten;
- ☐ het doorsturen van ontvangen berichten;
- ☐ het aanmaken en opheffen van een e-mail- en/of chat-account;
- ☐ het toekennen, wijzigen en intrekken van rechten aan/van een e-mail en/of chat-account;
- ☐ alle gebeurtenissen met betrekking tot authenticatie van gebruikers voor het uitvoeren van;
- ☐ handelingen op berichten;
- ☐ de toegang tot loggegevens;
- ☐ het wijzigen of verwijderen van loggegevens.

Door personen geïnitieerde communicatie (6.5)

- ☐ Wij hebben op brede schaal aangekondigd, bijv. op onze website, op welke eenvoudige manier personen op hun eigen initiatief veilig kunnen communiceren met onze organisatie.

Zekerheden (7.1)

- ☐ Wij werken alleen met leveranciers voor veilige e-mail die in een publiek toegankelijk register publiceren aan welke criteria deze oplossing wel en niet voldoet.

Multikanaalcommunicatie (7.2)

- ☐ Wij hebben gewaarborgd dat onze veilige e-maildienst kan koppelen met andere NTA 7516-diensten op basis van de standaarden en vereisten zoals beschreven in de technische handreiking.

Implementatie (7.3)

- ☐ Wij hebben gewaarborgd dat onze leverancier(s) voor veilige e-mail transparant publiceert in welke onderdelen uit de NTA 7516 de veilige e-maildienst voorziet, en op welke manier.

Gebruiksregels communicatiedienstenaabieder (7.4)

- ☐ Wij hebben gewaarborgd dat onze leveranciers voor veilige e-mail regels hebben vastgesteld over hoe zij en degenen die voor hen werken, gebruik mogen maken van bevoegdheden ten aanzien van de verwerking van ad-hocberichtenverkeer die passen bij de eisen van ISO 27001, NEN 7510 en NEN 7513.

Toezicht/naleving (7.5)

- [ ] Wij werken alleen met communicatie dienstenaanbieders voor veilige e-mail die over een geldig NEN-ENISO/IEC 27001-certificaat of een geldig NEN 7510-certificaat beschikken waarbij de onderdelen van NTA 7516 zijn opgenomen binnen de scope van het certificaat.
- [ ] Wij hebben vastgesteld dat onze leveranciers een programma hebben waarmee zij continu de werking van gepubliceerde criteria vaststellen. Jaarlijks wordt de passendheid van de gepubliceerde implementatievoorschriften en de naleving van de gebruiksregels getoetst en de resultaten worden gedocumenteerd.

Certificering (7.6)

- [ ] Wij werken alleen met communicatie dienstenaanbieders die garanties geven over het feit dat zij zich zo snel mogelijk officieel laten certificeren op het voldoen aan de eisen van de NTA 7516 die op hen van toepassing zijn.

Zijn je leveranciers klaar voor de NTA 7516?

Zoals je hierboven ziet zijn leveranciers erg belangrijk om als organisatie aan de NTA 7516 te kunnen voldoen. Om zeker te zijn dat de digitale ecosystemen van jouw organisatie klaar zijn voordat de norm daadwerkelijk gehandhaafd wordt, heeft Zivver een handige checklist voor leveranciers ontwikkeld. Deze uitkomsten kunnen jouw organisatie houvast geven bij het bepalen of je organisatie al voldoet aan specifieke onderdelen van bovenstaande checklist waar jouw organisatie afhankelijk is van leveranciers.

We raden aan dat je deze checklist zo snel mogelijk laat invullen door alle leveranciers waarmee je samenwerkt. Door de checklist volledig in te vullen wordt duidelijk of er aanvullende maatregelen nodig zijn om te voldoen aan de NTA 7516, of dat er gezocht moet worden naar alternatieven.

Waarom het belangrijk is dat je leveranciers voldoen aan de eisen van de NTA 7516:

- De reputatie van jouw organisatie is ten dele afhankelijk van het gebruik van andere systemen. Als er een datalek plaatsvindt, is het klanten en contactpersonen om het even wie hier technisch verantwoordelijk voor is.
- Partijen waar jij privacygevoelige informatie mee uitwisselt moeten er altijd op kunnen vertrouwen dat hun gegevens met uiterste zorgvuldigheid worden behandeld.
- Datalekken, ook onbedoeld, kunnen leiden tot financiële boetes en andere schadelijke gevolgen voor jouw organisatie.

Praktische stappen, beleid en tijdslijnen

De implementatie van de NTA 7516 heeft mogelijk gevolgen voor verschillende onderdelen van je organisatie. Om je te helpen bij het voorbereidingsproces en de identificatie van eventuele noodzakelijke wijzigingen, hebben we een overzicht gemaakt van de aanbevolen acties. Als je deze richtlijnen volgt, bereid je de organisatie voor op volledige compliance aan de nieuwe norm. Bespaar jezelf tijd met behulp van de handige checklists en overzichten die we in deze handleiding delen.

Overzicht van praktische stappen

1. Stel beleid op
2. Zorg voor goede beveiliging van de mailserver met opgeslagen e-mails
3. Implementeer een dienst om veilig e-mails te ontvangen
4. Implementeer een oplossing die uitgaande communicatie naar niet NTA-ontvangers beveiligt
5. Implementeer een oplossing die interoperabiliteit naar NTA-ontvangers waarborgt
6. Implementeer een voorziening waarmee derden veilig contact kunnen initiëren
7. Overweeg een oplossing waarmee e-mails eenvoudig opgenomen kunnen worden in het medisch dossier

Stap 1

Stel beleid op over:

- het waarnemen van collega's tijdens afwezigheid;
- mandatering en delegatie van toegang tot berichten;
- de toegang tot informatie zonder een directe behandelrelatie (in zorginstellingen);
- de toegang tot functionele berichtenboxen (bijvoorbeeld orthopedie@voorbeeld.nl);
- het gebruik van een adresboek;
- het gebruik van functies die kunnen resulteren in het intrekken of wijzigen van berichten;
- het gebruik van geautomatiseerde functies bij ontvangst van berichten (bijvoorbeeld een autoreply of leesbevestiging);
- bewaartermijnen;
- sleutelbeheer indien van toepassing, de mogelijkheden voor forensisch onderzoek en key escrow-regeling;
- verantwoordelijkheden;
- verzendingsgrond (hoe weet de ontvanger zeker dat de afzender gerechtigd was om het ad hoc bericht te versturen?);
- de continuïteit van de dienstverlening bij faillissement van de veilige e-mailvoorziening.

Stap 2

Zorg voor goede beveiliging van de mailserver met opgeslagen e-mails. Dit houdt in:

- Toegang medewerkers tot gevoelige informatie mag alleen met twee-factor-authenticatie
- Toegang tot gevoelige informatie moet gelogd worden
- Zorg voor de juiste waarborgen over beschikbaarheid en bereikbaarheid

Stap 3

Implementeer een dienst om veilig e-mails te ontvangen. Dit houdt in:

- De dienst moet DANE ondersteunen of certificaat moet te valideren zijn op basis van PHIX
- Zorg voor de juiste waarborgen over beschikbaarheid en bereikbaarheid

Stap 4

Implementeer een oplossing die uitgaande communicatie naar niet NTA-ontvangers beveiligt. Deze oplossing moet

- Sterke authenticatie van ontvangers waarborgen
- Berichten sterk versleutelen zonder toegang voor onbevoegden
- Security by default bieden
- Ontvangers niet dwingen een account aan te maken
- Ontvangers de mogelijkheid geven veilig te antwoorden
- Ontvangers de mogelijkheid geven veilig door te sturen
- ISO 27001/NEN 7510 gecertificeerd zijn
- Handelingen medewerkers en toegang tot informatie voor gasten loggen
- De juiste waarborgen over beschikbaarheid en bereikbaarheid bieden

Stap 5

Implementeer een oplossing die interoperabiliteit naar NTA-ontvangers waarborgt

- Let op hoe integratie met oplossing naar niet NTA-ontvangers gebeurt
- Zorg voor logging van alle transacties en acties
- Zorg voor juiste waarborgen over beschikbaarheid en bereikbaarheid

Stap 6

Implementeer een voorziening waarmee derden veilig contact kunnen initiëren. Dit houdt in:

- Derden moeten veilig contact kunnen opnemen met de organisatie
- Ontvangers hebben geen account nodig
- Vermeld de voorziening duidelijk op de eigen website

Stap 7

Overweeg een oplossing waarmee e-mails snel opgenomen kunnen worden in het medisch dossier

- Met minimale inspanning van de professional kan een ad hoc bericht geschikt worden gemaakt voor koppeling en veilig worden gekoppeld aan het juiste dossier.

Tijdslijnen

Organisaties (professionals) moeten zelf zorgen dat ze voldoen aan de NTA 7516, waarbij ze een of meer gecertificeerde leveranciers selecteren waarmee informatie-uitwisseling veilig kan plaatsvinden. Hieronder geven we een indicatie van de benodigde tijd voor de activiteiten die nodig zijn om aan de NTA 7516-norm te voldoen.

Indicatie benodigde tijd	Activiteiten
Circa 1 maand	• Inventarisatie huidige ad hoc communicatiestromen • Bepalen 'gaten' ten opzichte van vereisten van de NTA 7516 • Bepalen hoe gaten te dichten (beleid, huidige of nieuwe leverancier)
Circa 1 maand	• Marktonderzoek afronden naar mogelijkheden van leveranciers • Contractering met nieuwe leveranciers afronden • Nieuw/aanvullend beleid uitwerken
Circa 1,5 maand	• Starten met voorbereiding implementatie nieuwe leveranciers • Starten met voorbereiding nieuw beleid
Circa 1 maand	• Technische implementatie nieuwe leverancier(s) • Introductie nieuwe leverancier(s) en nieuw beleid onder medewerkers • Inregelen monitoring rondom naleving

Zivver
Kon. Wilhelminaplein 30
1062 KR Amsterdam

085 016 0555
contact@zivver.com

www.zivver.nl