smartlockr

Met Smartlockr in een paar stappen NTA 7516-compliant

Checklist

Wat moet ik als organisatie doen om NTA 7516-compliant te kunnen zijn?

Het is een vraag die we vaak horen. Veel organisaties weten dat NTA 7516 er is, maar zijn vaak nog niet volledig op de hoogte van wat er precies moet worden gedaan om als organisatie compliant te kunnen zijn.

- *Wat zijn de eisen waar een organisatie aan moet voldoen?*
- *Waar kan een leverancier bij helpen en wat moet er als organisatie zelf worden geregeld?*
- *Hoeveel tijd kost het om aan de eisen te voldoen en in hoeverre zal dit binnen de organisatie een verandering in de werkwijze brengen?*

Om je meer duidelijkheid te geven over wat er geregeld moet worden, hebben we een stappenplan opgesteld dat wij verderop uitgebreid met je zullen doorlopen:

Stap 1. Bekijk welke eisen er voor je organisatie gelden.

Stap 2. Maak inzichtelijk welke eisen er door een leverancier moeten worden ingeregeld.

Stap 3. Stel een plan op voor de organisatorische maatregelen waar jij zelf verantwoordelijk voor bent.

Stap 1: Wat zijn de eisen waar ik als organisatie aan moet voldoen?

NTA 7516 is een norm die bestaat uit een aantal onderdelen. Als organisatie moet je rekening houden met het volgende:

- **De 18 normatieve criteria** waar de organisatie minimale eisen voor moet vastleggen. Binnen NTA 7516 zijn deze criteria vastgelegd onder *6.1.2 - 6.1.19*. (tabel 1.1.)
- **Additionele eisen** die je moeten helpen om met de introductie van de e-mailoplossing veilig te blijven communiceren in overeenstemming met NTA 7516. Deze maatregelen dienen te worden vastgelegd in een beleid of programma en moeten constant worden gemonitord en geëvalueerd. Dit zijn punten *6.3 (Gebruik), 6.4.1 (Toezicht/naleving)* en *6.4.2 (Logging)* die in de norm beschreven staan.

Beschikbaarheid

6.1.2. Minimale beschikbaarheid
6.1.3 Maximale uitvalduur
6.1.4 Maximaal gegevensverlies

Integriteit

6.1.5 Herkomstbevestiging
6.1.6 Data-integriteit
6.1.7 Onweerlegbaarheid verzender
6.1.8 Autorisatie verzender

Vertrouwelijkheid

6.1.9 Gegevensvertrouwelijkheid
6.1.10 Toegangsvertrouwelijkheid
6.1.11 Communicatievertrouwelijkheid
6.1.12 Verzendingsgrond
6.1.13 Internationaal ad-hocberichtenverkeer

Gebruiksvriendelijkheid

6.1.14 Continuïteit van ad-hoc berichtenverkeer – beantwoorden
6.1.15 Continuïteit van ad-hoc berichtenverkeer – doorsturen
6.1.16 Veiligheid als gemak
6.1.17 Leesbaarheid
6.1.18 Eigen kopie

Interoperabiliteit

6.1.19 Dossierkoppeling

Tabel 1.1 - De 18 normatieve eisen van NTA 7516

Er bestaat in het veld nog onduidelijkheid over de eisen waaraan moeten worden voldaan. De norm beschrijft namelijk zowel normatieve als additionele eisen - iets wat vaak voor verwarring zorgt.

Een goed uitgangspunt is het volgende:

Elke zorgorganisatie die de uitwisseling van gezondheidsinformatie via e-mail wil laten verlopen, hoort te voldoen aan de 18 normatieve eisen (6.1.2 - 6.1.19) die de NTA 7516 stelt. Deze norm brengt richtlijnen waar veilige communicatie en de uitwisseling van deze specifieke data aan moet voldoen. Ter aanvulling zal er aan een aantal eisen moeten worden voldaan om de veilige uitwisseling ook op lange termijn te kunnen waarborgen. Hier is een intern beleid voor nodig met belangrijke organisatorische maatregelen. Indirect heb je als organisatie dus met meer eisen te maken dan 18 normatieve eisen.

"NTA 7516: niet alleen omdat het moet, maar je doet jezelf er ook een plezier mee"

- Stanley van der Straten, ICT-regisseur en Security Officer Gemeente Zeist

Stap 2: Waar kan Smartlockr mij bij helpen?

Van de normatieve eisen die er worden gesteld, **moeten er 16 door de leverancier worden ingeregeld.** Dit zijn de technische eisen. Dit betekent dat er voor jou nog twee eisen overblijven die je zelf moet inregelen: *6.1.8 Autorisatie verzender* en *6.1.12 Verzendingsgrond*. Bij stap drie zullen we daar meer uitleg over geven.

Het is belangrijk om te kijken welke leverancier of combinatie van leveranciers voldoet aan het maximaal aantal punten. Het is mogelijk om voor meerdere leveranciers te kiezen, maar uit ervaring blijkt dat dit ten koste gaat van het gebruiksgemak en de kwaliteit van de werkprocessen.

Smartlockr is één van de weinige leveranciers die volledig NTA 7516-compliant is op de 17 uitgangspunten (met aanvulling van 7.2 Multi-kanaal communicatie), die gelden voor leveranciers. Dit betekent dat Smartlockr dus zorgt voor zowe de normatieve eisen als de additionele eisen.

NEN NTA 7516 VEILIGE MAIL (1)

"NTA 7516, daar moet je als organisatie gewoon aan voldoen en die kun je invullen met techniek. [...] Ik heb gezocht naar een pakket dat alles op groen licht heeft staan. [...] De eindgebruikers hebben de oplossing makkelijk omarmd. Dus als je me vraagt of ik helemaal tevreden ben, dan kan ik daar positief op antwoorden."

- Stefan Gensen, IT-Manager Novadic-Kentron

Deze organisaties blijven straks veilig en eenvoudig werken binnen het NTA 7516-netwerk:

Het Zand Zorgspectrum · gemeente Alkmaar · Novadic Kentron NK Nieuwe Kansen · Flevoziekenhuis · meppel.nl

Dit betekent het volgende:

NORMATIEVE EISEN

Beschikbaarheid

- ✓ 6.1.2. Minimale beschikbaarheid
- ✓ 6.1.3 Maximale uitvalduur
- ✓ 6.1.4 Maximaal gegevensverlies

Integriteit

- ✓ 6.1.5 Herkomstbevestiging
- ✓ 6.1.6 Data-integriteit
- ✓ 6.1.7 Onweerlegbaarheid verzender
- ~ 6.1.8 Autorisatie verzender

Vertrouwelijkheid

- ✓ 6.1.9 Gegevensvertrouwelijkheid
- ✓ 6.1.10 Toegangsvertrouwelijkheid
- ✓ 6.1.11 Communicatievertrouwelijkheid
- ~ 6.1.12 Verzendingsgrond
- ✓ 6.1.13 Internationaal ad-hocberichtenverkeer

Gebruiksvriendelijkheid

- ✓ 6.1.14 Continuïteit van ad-hoc berichtenverkeer – beantwoorden
- ✓ 6.1.15 Continuïteit van ad-hoc berichtenverkeer – doorsturen
- ✓ 6.1.16 Veiligheid als gemak
- ✓ 6.1.17 Leesbaarheid
- ✓ 6.1.18 Eigen kopie

Interoperabiliteit

- ✓ 6.1.19 Dossierkoppeling

ADDITIONELE EISEN

- ✓ 6.3. Gebruik
- ✓ 6.4.1 Toezicht/naleving
- ✓ 6.4.2 Logging

EIS VOOR LEVERANCIERS

- ✓ 7.2 Multi-kanaal communicatie

✓ Smartlockr voldoet

✓ Additionele eis voor organisatie,Smartlockr kan helpen

~ Normatieve eis voor organisatie,Smartlockr kan helpen

Stap 3: Wat moet ik zelf nog regelen en hoe?

Voor de overige normatieve eisen ben je zelf verantwoordelijk - hier moet je organisatorische maatregelen voor te nemen. Vaak hebben organisaties dit al geregeld. Is dit niet het geval, dan zijn kleine aanpassingen voldoende:

6.1.8 Autorisatie verzender

Je moet kunnen garanderen dat de verzender binnen de organisatie geautoriseerd is om een bericht te versturen. Belangrijk is dat de afzender daarbij altijd vermeld is, zodat de ontvanger geen twijfel heeft over de afkomst van een bericht.

Enkele tips voor de maatregelen:

- Het klinkt misschien logisch, maar zorg ervoor dat de afzender altijd duidelijk herkenbaar is in een e-mailadres;
- Deactiveer oude e-mailaccounts van ex-werknemers, om te voorkomen dat accounts die inactief lijken, toch gebruikt worden.

6.1.12 Verzendingsgrond

Mag de verzender informatie sturen naar een bepaalde ontvanger? Door een communicatiebeleid op te stellen, weten je werknemers wat er mag worden gedeeld en met wie. Zo kun je voorkomen dat er informatie wordt gedeeld met ontvangers die hier niet voor gemachtigd zijn.

Wat hierbij niet mag worden vergeten:

- Eventuele geheimhoudingsplicht. Is er bepaalde informatie die niet met bepaalde personen/afdelingen/relaties mag worden gedeeld? Leg dit dan vast in het beleid, om te voorkomen dat er communicatie ontstaat die niet gewenst is;
- Duidelijkheid onder de werknemers over wanneer iets wel of niet mag/kan worden gedeeld. De menselijke fout is een grote bedreiging voor informatieveiligheid - voorkomen is daarom nog altijd beter dan genezen.

Additionele eisen

Heb je alles ingeregeld voor de normatieve eisen? Dan zijn er nog enkele aanvullende eisen waar Smartlockr je kan ondersteunen:

6.3 Gebruik

Er moet een beleid worden opgesteld over hoe iedereen binnen de organisatie gebruik mag maken van geïmplementeerde communicatiemogelijkheden.

Denk hier bijvoorbeeld aan:

- het waarnemen van collega's tijdens afwezigheid;
- het gebruik van een adresboek;
- toegang tot functionele inboxen.

6.4.1 Toezicht/naleving

Met een programma moet de naleving van de norm worden gemonitord. Zullen alle aanpassingen in een aantal jaar nog relevant zijn en kan naleving worden gegarandeerd?

6.4.2 Logging

Voor de uitwisseling van gezondheidsinformatie moet er ook worden voldaan aan NEN 7513:2018. Daarvoor moeten er verschillende gebeurtenissen worden gelogd.

Smartlockr logt alle gegevens volgens NEN 7513:2018 en NTA 7516:2019. Hierdoor kunnen alle gebeurtenissen die je moet loggen, ook op de juiste manier worden bijgehouden.

Voor alle bovengenoemde punten geldt dat Smartlockr je ondersteunt met o.a. advies bij het inrichten van het beleid en kwaliteitsprogramma's om de naleving van de norm te waarborgen.

Tot Slot

Als aan alle eisen is voldaan, ben je als organisatie compliant aan NTA 7516. In tegenstelling tot leveranciers, is er momenteel nog geen officiële certificering voor organisaties. Dit neemt niet weg dat het belangrijk is om aan te kunnen tonen dat je als organisatie de juiste organisatorische maatregelen hebt genomen.

Smartlockr zorgt daarom niet alleen dat je voldoet aan de verplichte eisen voor leveranciers. Wij denken vooral met je mee en bieden hulp en advies om ook te kunnen voldoen aan de overige eisen.

We kunnen je ook assisteren bij:

- Advies op maat voor het opstellen van een intern communicatiebeleid;
- Advies bij het opstellen van een programma om jaarlijks de geschiktheid van Smartlockr te evalueren;
- Een overzicht van de maatregelen die je nog moet nemen en hoe hier invulling aan kan worden gegeven.

Ook jouw organisatie is in slechts enkele stappen klaar voor NTA 7516. Eenvoudig, met Smartlockr

Ben je benieuwd hoe dit er voor je uit komt te zien? Of wil je graag met een van onze specialisten kijken wat dit voor je organisatie betekent? Onze ervaren adviseurs zitten klaar om je vragen te beantwoorden.

Plan je adviesgesprek

WEBSITE
https://smartlockr.io/nl/

E-MAIL ADDRESS
sales@smartlockr.eu

TELEFOON
+31 (0) 20 244 03 50