



PRAKTIJK ANNO NU
MONDZORG

AVG. Hoe nu verder? (568 dagen na de invoering)

Een samenwerking van

knmt **waar?** **MO** **MedischOndernemen**
Succesvol ondernemen en samenwerken in de eerste lijn



Twitter



Wifi

Agenda

1. Wat is er al gedaan in de praktijk?
2. Een datalek en wat dan?
3. Naleving rechten betrokkenen
4. Bewustwording informatiebeveiliging
5. Veilige e-mail – NTA 7516
6. Vragen



1. Wat is er al gedaan in de praktijk?

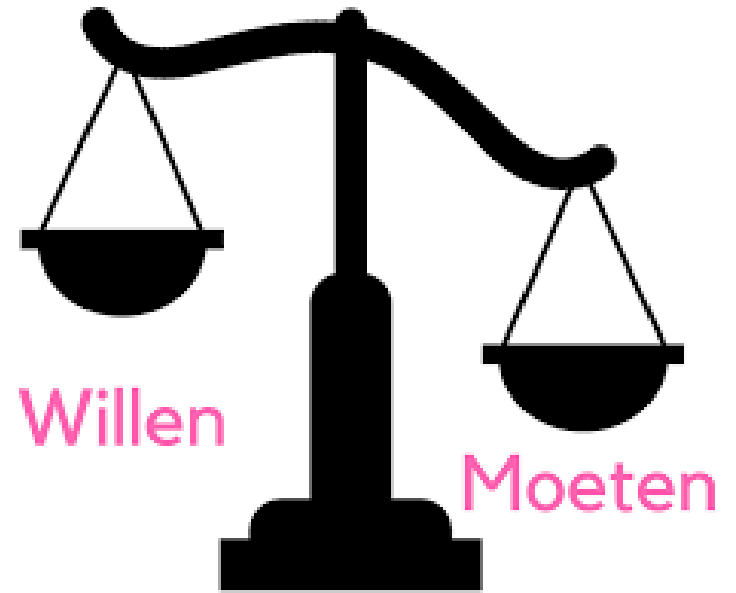
Wie heeft de vereiste documenten opgesteld?

- Een intern privacybeleid?
- Een verwerkings- en datalekkenregister?
- Een privacy- en cookieverklaring?
- Een privacyverklaring werknemers en sollicitanten?
- Verwerkersovereenkomsten gesloten met alle verwerkers?
- Al dan niet verplicht een FG aangesteld?



AVG: van moeten naar willen!

Zie het als een mogelijkheid om wetgeving toe te passen als een meerwaarde voor de praktijk, zodat persoonsgegevens binnen de kaders verwerkt worden, maar dienstverlening en efficiëntie niet uit het oog verloren worden.



Je zou moeten willen 🤔

AVG: gaat niet meer weg!

Quote tandarts: 'Ik heb alle documenten opgesteld en heb verder geen incidenten. Wat nu?'

AVG is continue proces. Wat goed gaat borgen en daarnaast blijven verbeteren.



2. Een datalek, en wat dan?



Datalek: gegevens 10.000 Achmea-klanten op straat

Datalek patientgegevens van 22 kinderen Viecuri ziekenhuis op straat

Sinds nieuwe Europese privacywet achttienduizend datalekken gemeld

21.000 klanten door datalek

13 november 2018 16:20
Laatste update: 1 dag, 2 u

UMC Utrecht stuurt brieven met persoonlijke gegevens naar verkeerde adressen



end klanten van
nkele online
at heeft het

bedrijf gemeld aan de Autoriteit Persoonsgegevens (AP).

Albert Heijn heeft de wachtwoorden van de betrokken klanten uit voorzorg geblokkeerd. De klanten zijn per email op de hoogte gebracht, met het verzoek het wachtwoord opnieuw in te stellen.

Een datalek! Of toch niet..... ? En moet ik die melden?

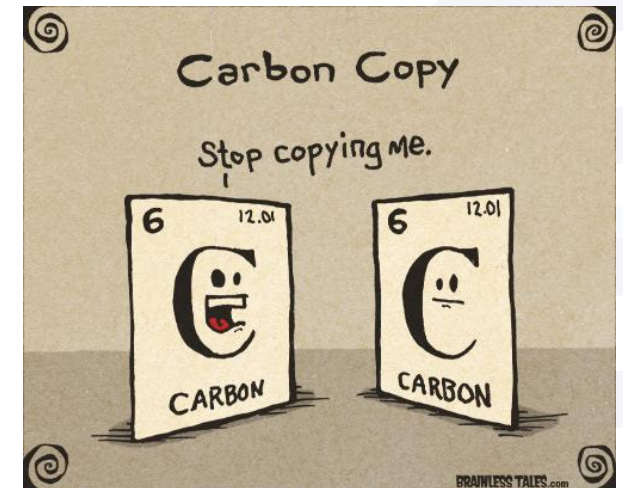


Wat zegt de wet?

In beginsel moet ieder datalek aan de AP worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van melding.

Een aantal voorbeelden uit de praktijk:

1. Vanuit de praktijk zijn er e-mails verzonden waarbij er 95 e-mailadressen voor een infomailing via de CC zijn verzonden en voor anderen zichtbaar waren.



2. Patiënten hebben elkaars recept gekregen. Hierop staan veel persoonsgegevens van de patiënt vermeld (naast NAW ook het Burgerservicenummer).



3. In de online praktijkagenda waren de gegevens (naam + geboortedatum) van andere patiënten een bepaalde tijd zichtbaar.

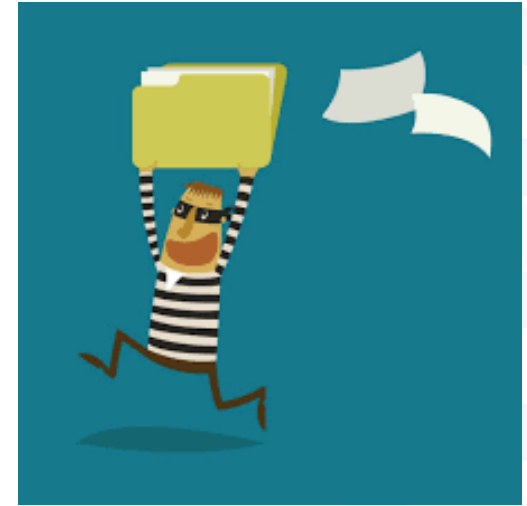
Wachttijd tussen afspraken
15 min

Klik hieronder op de plek waar u de afspraak wilt plaatsen

Datum en tijd	Medewerker	Stoel
di 11-11-2014 11:05 - 11:25 wacht 10 min 11:35 - 12:05	Jan Tandarts	KAMER 01
	Wies Mondhygienist	KAMER 02
do 13-11-2014 11:05 - 11:25 wacht 10 min 11:35 - 12:05	Jan Tandarts	KAMER 01
	Wies Mondhygienist	KAMER 02
di 18-11-2014 11:05 - 11:25 wacht 10 min 11:35 - 12:05	Jan Tandarts	KAMER 01
	Wies Mondhygienist	KAMER 02
do 20-11-2014 11:05 - 11:25 wacht 10 min 11:35 - 12:05	Jan Tandarts	KAMER 01
	Wies Mondhygienist	KAMER 02
ma 24-11-2014 11:05 - 11:25 wacht 10 min 11:35 - 12:05	Jan Tandarts	KAMER 01
	Wies Mondhygienist	KAMER 02
di 25-11-2014 11:05 - 11:25 wacht 10 min 11:35 - 12:05	Jan Tandarts	KAMER 01
	Wies Mondhygienist	KAMER 02
do 27-11-2014 11:05 - 11:25 wacht 10 min 11:35 - 12:05	Jan Tandarts	KAMER 01
	Wies Mondhygienist	KAMER 02

Tips

- Onderzoek het beveiligingsincident/datalek.
- Leg het vast in het datalekkenregister.
- Meld uiterlijk binnen 72 uur bij Autoriteit Persoonsgegevens.
 - Tenzij: lek geen risico's inhoudt voor de rechten en vrijheden van betrokkene
- Melden bij betrokkene.
 - Als: lek waarschijnlijk een hoog risico met zich meebrengt voor hun rechten en vrijheden. Zie voorbeelddocumenten op www.knmt.nl
- Pas beveiligingsmaatregelen aan.



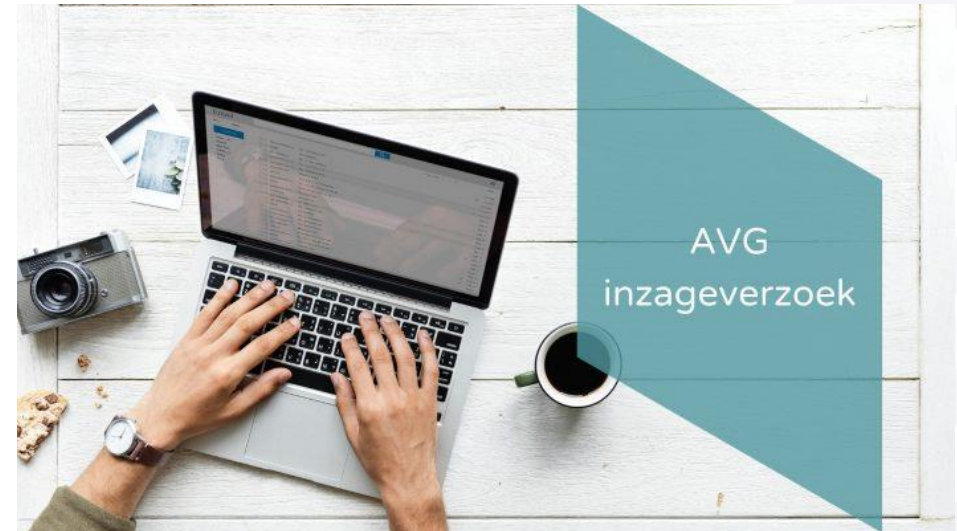
3. Naleving rechten van betrokkenen

- Recht op informatie
- Recht op inzage en afschrift
- Recht op rectificatie / wijziging
- Recht op toevoegen van een verklaring
- Recht op verwijdering en vernietiging
- Recht op beperking van verwerking
- Recht op bezwaar
- Recht op dataportabiliteit



Meest voorkomende rechten binnen de mondzorgpraktijk

Recht op inzage



Recht op verwijdering / vernietiging

Hoe gaat die naleving nu in zijn werk?

- Verzoek patient komt binnen (schriftelijk).
- Controle identiteit.
- Ga na wat de reactietermijn is waaraan je aan het verzoek moet voldoen.
- Vanaf 16 jaar mag iemand zelf een verzoek doen zolang deze niet onder curatele staat. Onder de 16 jaar moet de wettelijk vertegenwoordiger het verzoek doen.
- Wel of niet voldoen?
- Acties indien wel voldoen.
- Tip: wijs iemand in de praktijk hiervoor aan.



4. Bewustwording informatiebeveiliging

- Iedereen krijgt vroeg of laat te maken met Cybercrime. Privé en/of zakelijk!
- Gevolgen: financieel, reputatie, vertrouwen.
- Niet alleen door techniek, maar vaak ook door menselijk handelen.
- Dus bewust omgaan met internet en informatie = security awareness.

Vraag:



Welke vormen van cybercrime zijn bekend?

(On)bekendheid digitale risico's

Kun je aangeven in welke mate je bekend bent met de onderstaande zaken? % Nog nooit van gehoord	NL 16-80 jaar (n=1.004)	Klein MKB (n=290)	Groot MKB (n=293)	Grootbedrijf (n=458)	Ambtenaren (n=274)	Vitale infrastructuur (n=342)
Phishing mails	6%	7%	4%	4%	3%	5%
Identiteitsfraude	6%	8%	4%	3%	2%	3%
Cyberaanval	4%	6%	2%	3%	1%	2%
Datalek	10%	9%	8%	9%	4%	5%
Spyware	13%	11%	8%	6%	10%	8%
DDoS-aanval	20%	16%	16%	15%	13%	14%
Malware	15%	14%	14%	9%	9%	8%
Ransomware	25%	22%	20%	19%	18%	13%
Keylogger	54%	51%	45%	42%	39%	27%
Botnet	62%	54%	57%	51%	53%	39%
Social engineering	51%	45%	47%	42%	43%	28%
Spoofing	66%	60%	57%	56%	59%	43%
Portscan	69%	68%	59%	59%	60%	43%
Juice jacking	79%	80%	68%	72%	68%	54%

Cybersecurity Woordenboek:

<https://www.cybersecurityalliantie.nl/alliantieprojecten/lopende-cybersecurity-alliantieprojecten/cybersecurity-woordenboek>

Phishingmail: hoe te herkennen?



Mailadres van de afzender

Taalgebruik (de toon)/schrijfstijl

Aanhef (persoonlijk)

Logo's

Links

Naam van de afzender

Opmaak

Urgentie

Lettertype

Is de site betrouwbaar

Van: International Card Services <<mailto:helpdesk@identity.com>>

Verzonden: maandag 15 augustus 2016 22:10

Aan: [e-mailadres]

Onderwerp: Verifieer uw identiteit



Geachte kaarthouder,

International Card Services vindt fraudepreventie erg belangrijk. Om fraude te voorkomen, voeren wij dan ook regelmatig de nodige controles uit. Uit deze controles is gebleken dat er mogelijk misbruik van uw creditcard gegevens is gemaakt. Om veiligheidsredenen hebben wij uw creditcard beperkt voor gebruik.

Om de beperking op te heffen dient uw identiteit te verifiëren.

Helaas moeten wij u mededelen dat uw rekening binnen 48 uur om veiligheidsredenen wordt geblokkeerd als u uw identiteit niet verifieert.

Wij adviseren u zo spoedig mogelijk om uw identiteit te verifiëren om weer direct gebruik te kunnen maken van uw creditcard zonder beperkingen.

START VERIFICATIE



Met vriendelijke groeten
International Card Services B.V.

Postadres: Postbus 23225, 1100 DS Diemen

© 2016 International Card Services B.V.



Regio

Algemeen

Sport

Video

Opinie

Koken & Eten



Abonneren



Berichtje van de tandarts? Niet openen, waarschuwt de politie in Altena

ALTENA - Meerdere tandartsen en hun patiënten in Altena zijn de dupe van oplichters, die patiënten een vals bericht sturen over een afspraak 'voor komende zaterdag'. Niet op reageren en nergens op klikken, waarschuwt de politie.

Janneke Boluijt 26-11-19, 10:21 Laatste update: 13:53



Het gaat om een sms-berichtje waarin een afspraak voor zaterdag wordt bevestigd. De meeste tandartspraktijken in Altena zijn gesloten op zaterdag, dus alleen dat al is reden tot wantrouwen. De verzender is dan ook niet de tandarts, maar een crimineel die de persoonlijke gegevens van de patiënt probeert te ontfutselen.

Lees ook

toon alles (3) +



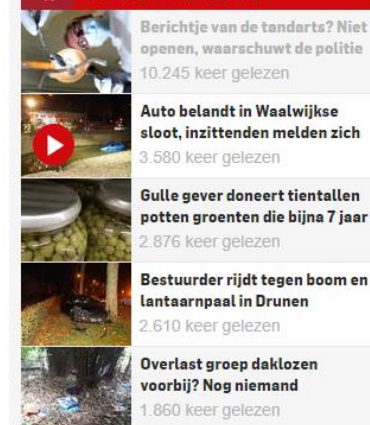
Politie waarschuwt voor phishing via sms: 'Oplichters laten je op link klikken om incasso te stoppen'
[Lees meer](#)

Wie twijfelt en toevallig ook binnenkort naar de tandarts moet, kan beter direct naar de praktijk bellen, is het advies. Het is nog onduidelijk hoeveel mensen zo'n frauduleuze sms hebben gekregen en of er ook slachtoffers zijn gemaakt.



Lees de krant online

MEEST GELEZEN



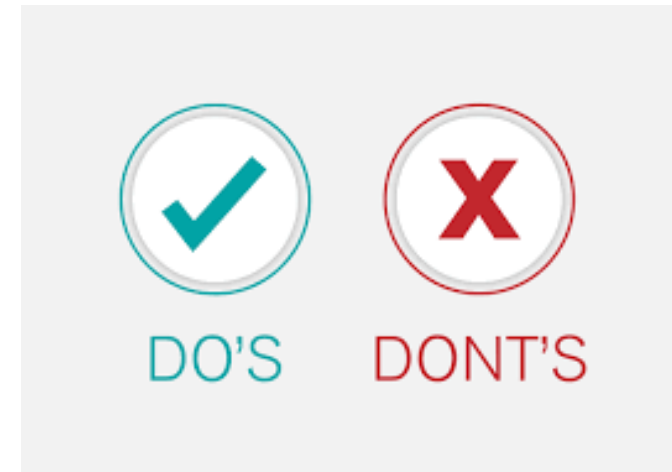
WEBWINKEL



knmt

Tips

- Installeer een spamfilter.
- Controleer de afzender van de e-mail.
- Controleer altijd de links in een e-mail (hoveren = met de muis over de link heengaan, dus zonder te klikken)! Verdachte domeinnaam?
- Controleer de URL van de website.
- Bij twijfel neem contact op met de 'echte' afzender bijv. de bank.
- Is het een phishing e-mail?! Verwijder dan de e-mail uit je mailbox!
- Belangrijk: zorg voor bewustwording!!



Welke maatregelen zijn er te treffen?

Wachtwoorden



- Maak wachtwoorden complexer:
- Gebruik maken van een combinatie van cijfers, letters en speciale tekens
- Gebruik minimaal 8 tekens
- Of gebruik een wachtwoordzin

Moeilijk allemaal te onthouden? Gebruik een wachtwoordmanager

Welke maatregelen zijn er te treffen?

Vertrouwelijkheid

- Deel patiëntgegevens niet met onbevoegden
- Regel de toegangsniveau 's tot de patiënten-informatie
- Kijk niet zomaar in patiëntendossiers (dus zonder noodzaak of bevoegdheid)
- Toegang moet ook worden gelogd (NEN 7513 – Logging)



Welke maatregelen zijn er te treffen?

E-mail

- Link nooit zomaar op vreemde links (zie bij Phishing mail)
- Stuur patiëntengegevens nooit via een onbeveiligde e-mail
- Gebruik alleen de e-mail faciliteiten van de praktijk (niet privé)
- Let **altijd** op dat een bericht naar het juiste e-mail adres wordt gestuurd

E-mailberichten
op de juiste
manier versturen



Welke maatregelen zijn er te treffen?

Veilige hulpmiddelen

- Log in met 2FA door middel van bijvoorbeeld een UZI-pas
- Maak gebruik van encryptie bij het versturen van bestanden
- Maak gebruik van een veilige e-mail applicatie

Leg alle maatregelen vast (in een protocol / praktijkhandboek) en bespreek/check de naleving!



5. Veilige e-mail NTA 7516

Aanleiding project Veilige e-mail



1. Veilig omgaan met patiëntgegevens belangrijk binnen zorg
2. AVG: als je mailt doe het dan veilig! Maar wat is veilig?
3. Toetsingskader gewenst door AP (ook voor handhaving)
4. Bij het veld neergelegd. Opdracht via Informatieberaad aan het NEN
5. Is nu gereed. Nederlandse Technische Afspraak (NTA) 7516

Wat regelt de NTA 7516?

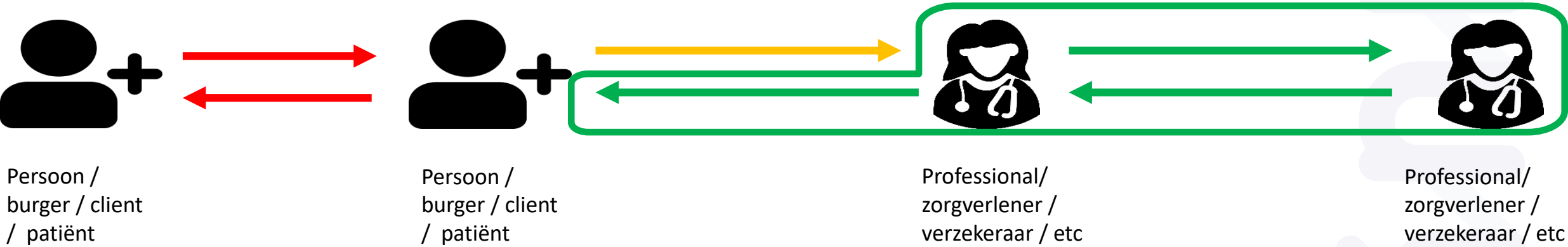
NTA 7516 stelt functionele specificaties vast voor het **veilig uitwisselen van persoonlijke gezondheidsinformatie** tussen *professionals* onderling en tussen *professionals* en *personen/patiënten*, bijvoorbeeld via e-mail. NTA 7516 is van toepassing op **alle vormen** van ad-hoc uitwisseling van *persoonlijke gezondheidsinformatie* tussen twee of meer mensen, waartoe **e-mail, maar ook chatapplicaties** (al dan niet aangeboden binnen een *berichtenportaal* functionaliteit) worden gerekend.



NTA 7516 behandelt niet:

- realtimecommunicatiediensten zoals (beeld)bellen;
- het versturen van berichten via een fax;
- het e-mailen tussen personen/patiënten onderling;
- filetransfer toepassingen als WeTransfer en Dropbox;
- niet-elektronische communicatie, waaronder het uitwisselen van papieren dossiers;
- uitwisseling van gestructureerde informatie (bijvoorbeeld met behulp van IHE -standaarden).

Stelt eisen aan de volgende berichtenstromen



Wat is de grens van veilig mailen vs gewoon mailen?

Moet dit per veilige mail?

Beste Dhr/Mw Jansen,

De openingstijden van onze mondzorgpraktijk zijn gewijzigd. Wij zijn voortaan geopend van 08:30 – 17:30 uur. Voor spoedgevallen kunt u ons altijd bereiken op 0183-485678.

Uw mondzorgpraktijk



Wat is de grens van veilig mailen vs gewoon mailen?

En dit?

Beste Dhr/Mw Jansen,

Hierbij de bevestiging dat u bij ons op 29 oktober 2019 om 09:00 uur een afspraak heeft...

Uw mondzorgpraktijk

Wat is de grens van veilig mailen vs gewoon mailen?

En deze?

Beste Dhr/Mw Jansen,

Hierbij de bevestiging dat u bij ons op 1 november 2019 in de praktijk een afspraak heeft voor het plaatsen van een prothese in de bovenkaak.

Uw mondzorgpraktijk

Wat is de grens van veilig mailen vs gewoon mailen?

En deze dan?

Beste Dhr/Mw Jansen,

Hierbij de bevestiging dat u bij ons op de SOA-polikliniek een afspraak heeft voor het bespreken van uw uitslagen op maandag 20 november a.s. om 09:00 uur.

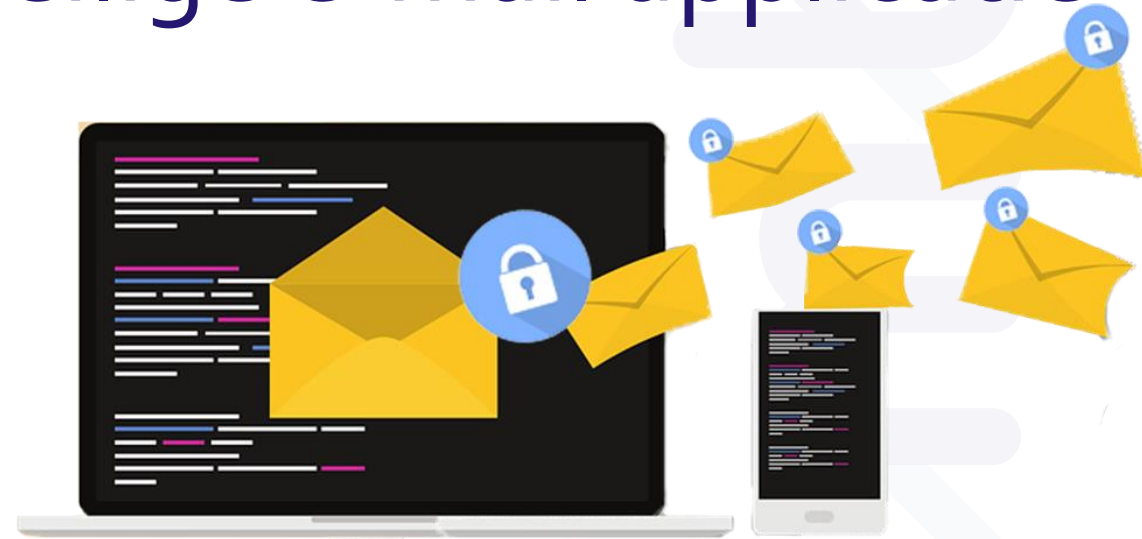
Uw SOA-kliniek

Kan dit helpen?



Sector én contextafhankelijk. Koepels is gevraagd om met richtlijnen te komen.

Eisen aan aanbieders van veilige e-mail applicatie



- Moet inter-operabel zijn
- Moet kenbaar maken hoe de toepassing gebruikt moet worden
- Moet kenbaar maken aan welke criteria applicatie wel/niet voldoet
- Moet gecertificeerd worden voor de NTA 7516 (mei 2020)
- Moet een NEN7510/ISO27001 certificaat hebben

Mogelijke aanbieders van veilige e-mail applicatie



Wat moet er gebeuren?

- Kies een leverancier die voldoet aan NTA 7516
- Faciliteer patiënten in veilig mailen naar de praktijk
- Informeer patiënten
- Stel praktijkregels op en check de naleving daarvan
- ICT beheerder moet enkele aanpassingen doen
- Via tweefactor authenticatie
- VWS komt met een praktische handreiking

ZO

**DAT WAREN
DE REGELS**

**DAN GAAN WE
NU OVER NAAR
DE REALITEIT**

Loesje

Wanneer: In de loop van 2020. De KNMT houdt u op de hoogte!

Vragen?



knmt



PRAKTIJK ANNO NU
MONDZORG

Bedankt

www.mondzorgpraktijkannonu.nl