adapta
mét lef, uit liefde

WHITEPAPER

FEB 2025

(on)zin van veilig mailen

NTA 7516 ontleed tot de essentie

inhoudsopgave

“Ik hoop dat er een oplossing komt die goed werkt”

1 inleiding

Als het om persoonsgegevens gaat, lijkt het logisch dat e-mails “veilig” verstuurd moeten worden. Maar wat betekent “veilig mailen” eigenlijk? Vraag het aan tien personen en je krijgt tien verschillende antwoorden. Dat is problematisch, want e-mail is voor bijna alle organisaties het primaire communicatiekanaal. Dat geldt ook voor de zorgsector, waar bovendien sprake is van een complicerende factor: vaak bevatten e-mails privacygevoelige gezondheidsgegevens.

Zorgen over de veiligheid van e-mail zijn niet nieuw. Al bij de introductie van het protocol in de jaren ‘60 speelde het veiligheidsthema op. Dit is logisch, want e-mail is niet specifiek ontworpen met het oog op veiligheid. En massale adoptie was evenmin voorzien. Het was simpelweg een protocol om digitale berichten te versturen. Je kunt dus stellen dat e-mail onveilig by design is. Uiteraard zijn er later een enorme hoeveelheid extra beveiligingslagen en toepassingen ontwikkeld die de veiligheid opvoerden. Maar welke je als organisatie toe wilt passen, dat is aan jou. Dat brengt ons tot de kernvraag: als er zo veel mogelijkheden zijn, wat is dan de juiste combinatie van veiligheidsmaatregelen? En, nog belangrijker, wanneer kun je de conclusie trekken dat de inrichting van de e-mailomgeving veilig genoeg is?

Om tot handvatten voor “veilig mailen” te komen, heeft de Nederlandse zorgsector in mei 2019 het NTA 7516-normenkader geadopteerd. Vijf jaar later blijkt dat echter te zijn uitgemond in een ***“veilig mailen”-pandemie***. Symptomen zijn:

- **Een wildgroei aan “veilig mailen”-software/appjes/extensies. Soms meerdere per zorginstelling;**
- **Gesloten infrastructuren uit commercieel belang;**
- **Gefrustreerde zorgprofessionals door slecht functionerende applicaties;**
- **Verwarring bij security officers en IT-beheerders door onduidelijke eisen;**
- **Torenhoge kostenposten door dure implementatie en licenties.**

En of e-mailverkeer echt veiliger is geworden valt te betwijfelen...

1.1 deze whitepaper

Samen met zes zorginstellingen hebben we onderzocht hoe deze situatie kon ontstaan. En of het mogelijk is om “bekende” e-mail oplossingen (zoals Gmail en Microsoft Outlook) zo in te richten dat zelfs gezondheidsgegevens “veilig” kunnen worden uitgewisseld.

Wij hebben KPMG opdracht gegeven:

- Een objectief raamwerk op te stellen waarin eisen aan “veilig mailen” worden geconcretiseerd op basis van de meeste gangbare technieken;
- Gmail te toetsen in het licht van dit raamwerk;

Er is voor Gmail gekozen omdat deelnemende zorginstellingen Gmail als primaire e-mailoplossing inzetten. Het OCF kan in de toekomst echter ook gebruikt worden om andere oplossingen te toetsen, zoals Microsoft Outlook.

Deze whitepaper bevat:

- **Achtergrond bij het thema “veilig mailen”**
- **Op hoofdlijnen de structuur van het Objective Control Framework (OCF);**
- **De uitkomsten van de uitgevoerde beoordeling van Gmail tegen het OCF;**

1.2 contact en meer informatie

Vragen of opmerkingen over dit onderzoek? Behoefte aan meer informatie? Of andere vragen over informatieveiligheid in de zorg? Wij helpen je graag verder!!

Matthias van Alphen
Founder & CEO

E matthias@adapta.nl
L LinkedIn

2 achtergrond bij “veilig mailen”

2.1 Project: Veilig Mailen van Informatieberaad Zorg (2018)

De bedoelingen waren goed. Om “veilig mailen” in de zorgcontext te standaardiseren, startte Informatieberaad Zorg in 2018 het Project Veilige Mail. Dit heeft op hoofdlijnen geleid tot het opstellen van vijf documenten:

document	inhoud
Intentieverklaring	Een document waarin deelnemende partijen (zorginstellingen, leveranciers van communicatieoplossingen) verklaren te willen komen tot een breed gedragen consensus, waaraan alle partijen zich zullen houden.
Normenkader NTA 7516	Het centrale normenkader met eisen aan “veilig mailen”. Gericht op zowel zorginstelling als toeleveranciers van communicatieoplossingen. Belangrijkste pijlers zijn: beschikbaarheid, integriteit, vertrouwelijkheid, gebruiksvriendelijkheid en interoperabiliteit.
Implementatiehandboek NTA 7516	Een implementatiehandboek NTA 7516 voor kleine zorgpraktijken, bestaande uit een stappenplan, toolkit en praktijkvoorbeelden.
Technische handreiking NTA 7516	Technische handreiking met suggesties voor technieken om NTA 7516 in praktijk te brengen.
Certificatieschema NCS 7516	Een certificatieschema voor leveranciers van communicatieoplossingen, belicht vanuit het NTA 7516-normenkader. Dit certificatieschema is per mei 2022 vervallen

2.2 de praktijk van Veilig Mailen (2023)

Het doel van Veilig Mailen was nobel, maar (zeer) ambitieus. De uitdagingen op veilig mailen gebied zijn namelijk niet zorgspecifiek. Bijna alle organisaties worstelen met het onderwerp, en er bestaat geen wereldwijde consensus over best practices, laat staan dat die een-op-een kunnen worden overgenomen vanuit andere sectoren. Dat ook de projectgroep hier lastig grip op kreeg, blijkt onder andere uit:

- Het centrale document (NTA 7516) bevat vooral algemeenheden en geen concrete implementatie criteria;
- De technische handreiking voor leveranciers bestaat grotendeels uit suggesties en heeft geen verplichtend karakter;
- Zowel de NTA 7516 als de technische handreiking zijn op onderdelen niet praktisch toepasbaar. Bijvoorbeeld op het gebied van authenticatie en de toepassing van technische protocollen;
- Het certificeringsmechanisme voor leveranciers blijkt in de praktijk niet goed te werken en is uiteindelijk (in mei 2022) zelfs ingetrokken;
- Bij de ontwikkeling van de NTA 7516 zijn vooral specialistische Nederlandse leveranciers betrokken. De oplossingen en visie van internationale e-mail giganten, zoals Google en Microsoft, zijn niet of nauwelijks meegewogen.

Deze pijnpunten maken het zorginstellingen erg lastig om te doorgronden wat er precies van ze wordt verwacht. Vaak leidt dit ertoe dat zij zich wenden tot (niche) aanbieders van e-mail oplossingen. Aanbieders die hierdoor vrij baan hebben gekregen om hun oplossingen te pushen en die vaak niet of nauwelijks worden gechallenged op kwaliteit en kostenefficiency. De gevolgen:

- Kostbare, soms langlopende implementatieprojecten;
- Hoge licentiekosten;
- Gebrekkige implementaties, bijvoorbeeld omdat oplossingen niet voldoende goed aansluiten op de manier waarop zorg wordt georganiseerd;
- Zorgprofessionals die niet weten wat ze met alle apps, extensies en tooltjes aan moeten;
- Zorgprocessen die zich aan de toepassingen moeten conformeren, in plaats van andersom (“techniek dicteert de manier van werken”);
- Een gebrek aan interoperabiliteit tussen “veilig mailen”-oplossingen onderling en in relatie tot de overige zorginformatiesystemen.

Ondanks alle goede bedoelingen, is de stip op de NTA 7516 horizon dus niet bereikt. Sterker; die lijkt alleen maar verder weg. Een conclusie die des te wranger is, indien wordt meegewogen dat de huidige aanpak het eigenlijk zorgproces (soms in ernstige mate) frustreert en hoge kosten met zich meebrengt.

3

project: objectieve beoordeling mail-oplossingen

Dat de huidige aanpak om e-mail veilig in te richten mank gaat, is alle projectdeelnemers duidelijk. Er bestaat dan ook behoefte aan een andere, beter werkbare en effectievere oplossing voor alle partijen. Vooral de NTA 7516 doelstellingen gebruiksvriendelijkheid en interoperabiliteit blijven ver uit zicht. En dat terwijl zorgorganisaties hoge implementatie- en licentiekosten maken. Veel voor weinig dus.

Hoewel het verleidelijk is om streng naar aanbieders van e-mail oplossingen te wijzen, is dat te kort door de bocht. Ook zorgorganisaties kunnen veilig en gebruiksvriendelijk e-mailen bevorderen, bijvoorbeeld door oplossingen goed binnen het zorgproces te integreren, tot gedegen beleid te komen en het veiligheidsbewustzijn van medewerkers te stimuleren. Het is echter wel een feit dat het toevoegen van steeds meer appjes en tooltjes de “veilig mailen” ambitie geen stap dichterbij brengt. Pleisters plakken is soms zinvol, maar niet als de patiënt kampt met hartfalen.

Waarom zijn al die tooltjes eigenlijk nodig? Wat maakt mailen met al deze extra oplossingen veiliger dan via de eigen, reguliere mailoplossing? En zijn ze überhaupt veiliger dan correct ingerichte Gmail of Microsoft Outlook omgevingen? Indien het antwoord op die laatste vraag ‘nee’ is, zou het de voorkeur kunnen hebben om dergelijke standaardoplossingen te omarmen. Die worden namelijk al door de meeste zorgprofessionals gebruikt. En zijn vele malen eenvoudiger binnen het zorgproces te integreren dan maatwerkoplossingen.

3.1 Kaders project

3.1.1 Onderzoeksvraag

Hoe kunnen we op een gedegen, toekomstbestendige en praktische manier toetsen of de reguliere mailoplossing van een zorgorganisatie voldoet aan eisen voor “veilig mailen”?

3.1.2 Projectgroep

Deelnemende zorginstellingen

Opdrachtgever	adapta
Opdrachtnemer	KPMG
Partner	Google

organisatie	deelnemer	functie
Adapta Security	Nick Zuiderwijk	Business Coordinator
Adapta Holding	Matthias van Alphen Joep Kleinmeulman	CEO Chief Product Officer
RDIT	René Dissel	Senior Consultant
KPMG Nederland	Peter Kits Sara van Lieshout Jasper Oomen	Partner Digital Law Senior Consultant Digital Law Consultant Digital Law
Google	Jerome Tabak Luc de Jager	Head of Global Strategic Deal Leads Customer Engineer
Stichting Laurens	Marije Brugman Chris Kunkeler Armit den Drijver	CIO / Manager I&A Senior Informatiemanager Information Security Officer
Stichting Amstelring Groep	Yoanette den Boer	CIO
Stichting Altrecht	Dieter van Grinsven Jeroen Bakker Paul Blok	Projectmanager Innovatie Coördinator Servicedesk ICT Teammanager ICT & FB
Stichting BrabantZorg	Ellen van den Brand	Teammanager Ondersteuning & Advies
Stichting Buurtzorg Nederland	Joost de Blok	Projectmedewerker
Stichting Zorggroep de Betuwe	Christiaan van Driel Mark van Reenen	Adviseur ICT Adviseur ICT

3.2 Onderzoek KPMG: Objective Control Framework (OCF)

3.2.1 Aanpak

Na de algemene onderzoeksvraag binnen de projectgroep te hebben vastgesteld, heeft KPMG de aanpak als volgt gedefinieerd:

Onderzoeken:

- **of en hoe,**
- **binnen de kaders van de technologische mogelijkheden en (aanstaande) wet- en regelgeving, organisaties aan de NTA 7516 norm kunnen voldoen, en,**
- **op leveranciers- en technologie onafhankelijke wijze gezondheidsgegevens via e-mail interoperabel uitgewisseld kunnen worden.**

Wij doen dit op basis van een beproefde aanpak die bij eerdere onderzoeken is gehanteerd met behulp van een Objective Control Framework ('OCF').

Het OCF is een beproefd raamwerk dat KPMG ook voor andere, vergelijkbare onderzoeken inzet. Het fundament van dit raamwerk bestaat uit:

- **Marktpraktijken en capaciteiten**: wat wordt binnen de industrie als standaard praktijken of afspraken op het gebied van "veilig mailen" beschouwd?
- **Wet- en regelgeving**: welke wettelijke en regelgevende bronnen stellen eisen aan "veilig mailen" en wat zijn die eisen?
- **Industriestandaarden**: welke industriestandaarden zijn er rondom "veilig mailen", en welke eisen vloeien hieruit voort?

Voor het uitgevoerde onderzoek betekent dit dat KPMG in eerste instantie – specifiek voor het beoordelen van mailoplossingen in de zorg – een OCF heeft ontwikkeld. In tweede instantie heeft KPMG Gmail tegen dat OCF beoordeeld. Daarbij werd dus niet alleen tegen het NTA 7516-normenkaders getoetst, maar ook tegen de onderliggende wet- en regelgeving, andere relevante industriestandaarden en marktpraktijken. Het OCF is er dan ook op gericht en in staat om objectief te beoordelen in welke mate een mailoplossing (al dan niet) aan de eisen voldoet, waar 'gaps' zitten en op welke punten zorgaanbieders, leveranciers of beiden nadere technische, organisatorische of juridische maatregelen moeten treffen om aan bepaalde vereisten te kunnen voldoen.

3.2.2 Bronnen

Voor het vaststellen van controls (“maatregelen”) maakte KPMG gebruik van de bronnen:

Wet- en regelgeving	Industriestandaarden	Marktpraktijken / capaciteit
Algemene verordening gegevensbescherming (AVG)	NTA 7516 (2019)	Intentieverklaring NTA 7516
Wet aanvullende bepalingen verwerking persoonsgegevens (Wabpvz)	Technische handreiking NTA 7516 (v1.3)	Praktijkvoorbeelden
Wet verplichte GGZ (Wvggz)	NEN 7510 (2017)	Voorbeelden buitenland
Wet Digitale Overheid (WDO)	NEN 7512 (2015 en 2022)	
Wet op de geneeskundige behandelingsovereenkomst (WGBO)	NEN 7513 (2018)	
Wet kwaliteit, klachten en geschillen zorg (Wkkgz)	ETSI	
Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)	Enisa	
European Health Data Space (EHDS)		
Wet langdurige zorg (Wlz)		
Wet maatschappelijke ondersteuning 2015 (Wmo 2015)		
Wet elektronische gegevensuitwisseling in de zorg (Wegiz)		

3.2.3 Controls en structuur

In totaal werden **84** controls geïdentificeerd.
Dit is binnen het OCF als volgt gestructureerd:

Wet- en regelgeving	Industriestandaarden
Control	Gedetailleerde uitwerking van de control inclusief vindplaats
Categorie	i) beschikbaarheid, ii) integriteit, iii) vertrouwelijkheid, iv) gebruiksvriendelijkheid, v) interoperabiliteit, vi) personen & governance, vii) overig
Herkomst	Wet- en regelgeving, industriestandaard of marktpraktijk
Domein	Proces, technologie of mens
Adressant	Zorginstelling, leveranciers of beide
Observatie	incl. aangeleverde documentatie
Beoordeling	Zie tabel onder 3.2.4 Wijze van beoordeling
MoSCoW	Must have, Should have, Could have, Would have

3.2.4 Wijze van beoordeling

Voor beoordeling van een mailoplossing tegen
het OCF wordt het volgende model gehanteerd:

✅	**Score 2** - Control volledig geïmplementeerd(*). Geen verbeteringen benodigd.
⚠️	**Score 1** - Control gedeeltelijk geïmplementeerd. Verdere verbeteringen benodigd. Aanbevelingen hiertoe worden binnen de beoordeling vastgelegd.
🚩	**Score 0** - Control niet geïmplementeerd. Verdere verbeteringen benodigd. Aanbevelingen hiertoe worden binnen de beoordeling vastgelegd.
nntb	**Nog niet te beoordelen**, bijvoorbeeld omdat het toekomstige wet- en regelgeving betreft.
nvt	**Niet van toepassing**. Bijvoorbeeld bij vervallen normeisen of wanneer normeisen alleen van toepassing zijn op zorginstellingen (en dus niet op toeleveranciers).

(*) Controls zijn in "opzet" getoetst. Dit betekent dat KPMG heeft geconstateerd dat een control in de praktijk aanwezig is, of kan worden ingericht door een zorginstelling. "Bestaan" en "werking" over langere tijd zijn niet getoetst.

3.3 Onderzoek KPMG: Beoordeling Gmail tegen OCF

3.3.1 Uitkomsten beoordeling

Categorie	Uitkomsten op hoofdlijnen
Beschikbaarheid	• Controls betreffende beschikbaarheid zijn goed op orde binnen Google Workspace (inclusief Gmail); • Google Workspace (inclusief Gmail) levert de hoogste standaard voor beschikbaarheid door High Availability en overtreft de grenswaarde; • Openstaande vraag is of Service Continuity en Availability conform ISO/IEC 20000 is ingericht. Achterliggende eis is echter dat Google zorginstelling hiertoe zelf in staat stelt, en niets duidt erop dat dit niet het geval is.
Integriteit	• Google hanteert een hoge standaard op het gebied van zowel fysieke als digitale beveiliging van haar systemen; • Zorginstelling wordt gefaciliteerd om zelf ook een hoog niveau van beveiliging te bereiken; • Google claimt compliance met de AVG binnen Google Workspace (inclusief Gmail) • Het is niet aannemelijk dat Google gevolg zal geven aan de jaarlijkse controleverplichtingen die volgen uit de NTA 7516.
Vertrouwelijkheid	• Google voldoet aan de meeste eisen met betrekking tot AVG, authenticatie en implementaties; • Google heeft de verplichte DNS records niet ingericht. Echter hangen deze nauw samen met de vervallen certificering en worden daarom momenteel niet relevant geacht; • DNSSEC is ingeschakeld op Google-webservices maar niet op Google-mailservers. De NTA 7516 staat op dit vlak echter ook een alternatieve inrichting toe om bescherming te garanderen. Wij zijn van mening dat Google door middel van deze alternatieve inrichting voldoet aan de gestelde eis.
Gebruiks-vriendelijkheid	• Google scoort hoog op gebruiksvriendelijkheid, met Gmail als een handige tool die goed integreert met andere Workspace-diensten (inclusief Gmail) en diensten van derde partijen/zorginstellingen; • Gmail biedt veelzijdige ondersteuning voor bijlagen in verschillende formaten, die ontvangers gemakkelijk kunnen exporteren zonder speciale software; • Zorginstellingen kunnen de beveiligingsinstellingen van Gmail aanpassen tijdens configuratie en ze hebben de vrijheid om te kiezen waar gegevens worden opgeslagen, met de EU als standaardlocatie als er geen specifieke keuze wordt gemaakt.
Interoperabiliteit	• Google toont sterke interoperabiliteit, met Gmail als handige tool voor gegevensuitwisseling met andere systemen; • We voorzien dat de kosten bij Google waarschijnlijk lager zullen uitvallen dan bij alternatieve zorgmail aanbieders; • Het is vooralsnog onduidelijk welke verdere technische specificaties zullen volgen op basis van EHDS en Wegiz. Deze kunnen wij daarom nog niet beoordelen; • Gmail voldoet ruimschoots aan eisen op het gebied van gegevensuitwisselingen in standaardformaat; • Door Google's gebruik van open standaarden wordt bijgedragen aan één van de beoogde doelen van de NTA 7516, namelijk standaardisering. Standaardisering is een belangrijke basis voor interoperabiliteit.
Personen, governance en overig	• Google ondersteunt zorginstellingen bij het naleven van normen, waaronder Data Loss Prevention (DLP) voor geautomatiseerde datamonitoring; • Google streeft naar naleving van wet- en regelgeving en biedt ondersteuning voor zorgspecifieke normen zoals NEN en NTA

Strikt kijkend naar de individuele controls scoort Gmail als volgt:

Score		Uitkomst beoordeling Gmail tegen OCF
✅	**Score 2**	67 controls voldoen volledig
⚠️	**Score 1**	6 controls voldoen gedeeltelijk
🚩	**Score 0**	0 controls voldoen niet
nntb	**Nog niet te beoordelen**	4 controls zijn (nog) niet te beoordelen
nvt	**Niet van toepassing**	7 controls zijn niet van toepassing

3.3.2 Duiding uitkomsten beoordeling

De conclusie is dat Gmail in het algemeen voldoet aan de vereisten voor “veilig mailen” zoals die in de Nederlandse zorgsector worden gehanteerd. Er werden immers geen grote belemmeringen aangetroffen. Wel is sprake van (gedeeltelijke) afwijkingen rondom de administratieve inrichting van de NEN 7510 en NTA 7516, en de beschikbaarheid/werking van technische richtlijnen.

Betekent dit dat Gmail “veilig” is?

Eigenlijk dient iedere zorgorganisatie daar zelf een antwoord op te formuleren. Waarbij het er niet zozeer om gaat om ‘maximale veiligheid’ te bereiken, maar om tot een acceptabel (en werkbaar) veiligheidsniveau te komen. Vergelijk het met de fysieke wereld: een pand zonder deuren en ramen is goed bestand tegen inbrekers, maar levert geen prettige werkomgeving op. Ook de NEN 7510 en NTA 7516 gaan uit van een door zorgorganisaties zelf te maken risico-inschatting. Er is geen checklist die je kunt afvinken. Laat staan dat je het predicaat “veilig mailen” verdient als je genoeg vinkjes hebt geplaatst. Elke organisatie heeft dus de vrijheid (en de opdracht!) om alle factoren mee te wegen en daar een onderbouwde conclusie aan te verbinden. De vraag is dus: wat vind je, gegeven de bedrijfsprocessen, veilig genoeg en hoe kun je dat niveau van veiligheid bereiken en borgen? Het OCF en de bijbehorende beoordeling van Gmail bieden daartoe een stevig fundament.

Wel geven wij nog deze punten mee ter overweging:

- **Staar je niet blind op technische richtlijnen**. Deze hebben geen verplichtend karakter, en vinden hun oorsprong in normenkaders die alweer enkele jaren oud zijn. Alternatieve (nieuwere) maatregelen kunnen en moeten ook worden overwogen.
- **Denk na over de inrichting van het eigen beleid** (inclusief implementatie van een bewustwording programma) en de integratie binnen de bedrijfsvoering. Ook dit is vanuit NEN 7510 en NTA 7516 een verplichting voor de organisatie zelf.
- **Het inzetten van Gmail en Outlook als oplossing voor "veilig mailen" draagt mogelijk bij aan het behalen van doelstellingen voor informatiebeveiliging**, zoals genoemd in de inleiding van de NEN 7510 norm:
  - Door de omvang en kennis van de Security-teams van Microsoft en Google worden actuele best practices op het gebied van beveiliging gevolgd. (doelstelling b)
  - Gmail en Microsoft Outlook worden al jarenlang gebruikt door zorgprofessionals (zakelijk en privé). Deze oplossingen zijn dus goed bekend. Dit maakt rekenschap eenvoudiger (doelstelling c) en zorgt er bovendien voor dat collega's hun (beveiligings) behoeftes makkelijker kunnen formuleren (doelstelling e).
  - De exploitatiekosten worden substantieel verlaagd (doelstelling f).
  - Google en Microsoft maken graag en vaak gebruik van open standaarden (= interoperabel!) (doelstelling j).
- **Implementatie van oplossingen die zorgprofessionals al kennen, verlaagt de drempel, vereenvoudigt het zorgproces en bevordert eenduidigheid.** Zorgprofessionals houden hierdoor tijd over voor hun kernactiviteiten.
- **De inzet van aanvullende tools en software beperkt het overzicht en de grip op informatiebeveiliging.** Er is dan namelijk sprake van aanvullende verwerkingen in de zin van de AVG. Gevoelige informatie verlaat het vertrouwde netwerk en wordt soms zelfs volledig aan het interne zicht onttrokken. Bovendien dienen er meer leveranciers beoordeeld en gemonitord te worden op hun aanpak van informatiebeveiliging.

3.4 Vervolgstappen

Het is aan de zorgsector om deze inzichten om te zetten naar actie. Dat vraagt om bestuurlijke wil en om sectorbrede samenwerking. Alleen dan kunnen noodzakelijke veranderingen in gang worden gezet en adoptie geaccelereerd. En ja, er zal mogelijk sprake zijn van een drempel: de zorgsector is immers geconditioneerd om ‘in aanvullende tools’ te denken. Toch zijn wij van mening dat objectiviteit een koerswijziging dicteert: als tools niet of nauwelijks meerwaarde hebben of zelfs belemmerend werken, schaadt dat de beoogde efficiëntie en veiligheid.

Adapta roept zorgorganisaties dan ook op om deze barrière te overwinnen. Het is tijd dat zorgorganisaties hun collectieve ‘inkoopkracht’ benutten om leveranciers te challengen om nut en noodzaak van hun productaanbod te onderbouwen. Tegelijkertijd is het cruciaal dat zorgprofessionals worden toegerust met de kennis en vaardigheden om Gmail “veilig” te gebruiken..

Samenwerking op bestuurlijk niveau, geïnspireerd door een gemeenschappelijke ambitie, zal de weg vrijmaken voor een gestroomlijnde en kosteneffectieve communicatie-infrastructuur, waarbij technologie de zorgprofessional ondersteunt in plaats van belast.

Adapta zelf blijft zich inzetten om zorgorganisaties op veiligheidsgebied te ondersteunen en te faciliteren. Bijvoorbeeld door het ontwikkelen van een technische implementatiegids, het opstellen van beknopte, gerichte stakeholdercommunicatie en via trainingen.

Meer weten? Hulp nodig bij de configuratie van Gmail?
Een andere vraag?

Wij helpen graag!
Je kunt contact opnemen via:

A [Boek een digitale kennismaking]
E info@adapta.nl
T +31 (0) 85 060 6119
W adapta.nl

4 hartenkreten

Voor dit project hebben we natuurlijk ook gesproken met de mensen om wie het echt gaat: de zorgprofessionals zelf. En de aan zorgprofessionals ondersteunende diensten. Want nog belangrijker dan de wereld van governance en compliance is dat het zorgproces goed functioneert.

Hieronder staan een aantal veelgehoorde uitspraken. Onafhankelijk van organisatie of gebruikte oplossing. Ter herinnering waarom dit project zo belangrijk is.

Ik moet telkens in mijn verzonden items kijken om te controleren of het bericht wel echt verzonden is

Berichten met een BSN erin worden geblokkeerd, terwijl ik dit nodig heb voor mijn werk

In ons team werkt onze veilig mailen oplossing maar goed bij één collega, dus zij deelt cliëntdossiers namens het hele team

Wij ontvangen de code om berichten veilig te openen op een teamtelefoon, dus we kunnen alleen berichten openen met deze collega in de buurt

Wanneer een “veilig bericht” zich eenmaal in de keten van een bepaalde leverancier bevindt krijg je deze er ook bijna niet meer uit

Het systeem van huisartsen kan niet communiceren met onze veilig mailen oplossing

De titels en inhoud van “veilige berichten” zijn niet doorzoekbaar, waardoor we regelmatig oudere communicatie niet kunnen terugvinden

5 over adapta

adapta
mét lef, uit liefde

De missie van Adapta is het **verrijken van het werkzame leven van zorgprofessionals door oplossingen te bieden die hun dagelijkse taken leuker, beter en makkelijker maken.**

Wij geloven dat technologie een cruciale rol speelt bij het realiseren van onze ‘triple aim’:

- het leveren van betere zorg;
- het verhogen van de tevredenheid onder zorgprofessionals en cliënten;
- het reduceren van de kosten binnen de gezondheidszorg.

Adapta streeft ernaar om het beste uit de markt te halen; indien de markt niet voorziet, nemen we het heft in eigen handen door zelf innovatieve oplossingen te ontwikkelen.

5.1 Onze labels

adapta hello,	Hello is (maar vooral jullie!) superapp die het organiseren van de zorg eenvoudiger, schaalbaarder en efficiënter maakt. Door telefoonverkeer slimmer te verdelen. Door zorgtechnologie signalen geautomatiseerd te ontsluiten. En door handwerk bij innovatieteams weg te nemen.
adapta workspace	Door het in de tech-wereld populaire keep it simple, stupid, mantra te adopteren. Oftewel: door alle collega’s laagdrempelige digitale werkplekken te bieden. Powered by Google. Maar dan wel volledig toegespitst op de actuele zorgrealiteit en unieke wensen en eisen van jouw zorgorganisatie.