UNIVERSITEIT GENT

Optimaliseren van veilige,digitale, interdisciplinaire gegevensdeling in de regio

empact

Sibe Samen is beter

Inhoud

Inleiding

In een tijd waarin technologieën zich exponentieel ontwikkelen en waarin de behoefte aan efficiënte informatie-uitwisseling tussen verschillende disciplines steeds groter wordt, rijst de vraag naar het optimaliseren van veilige, digitale, interdisciplinaire gegevensdeling in de regio. De samenwerkingsverbanden geïntegreerde zorg, empact en Sibe, slaan samen de handen in elkaar om met het thema ‘veilige, digitale, interdisciplinaire gegevensdeling’ aan de slag te gaan.

De behoefte aan veilige gegevensuitwisseling komt voort uit een samenleving waarin zorgverleners uit verschillende organisaties en disciplines samenwerken om complexe uitdagingen aan te pakken. Deze samenwerking vereist een naadloze en efficiënte informatie-uitwisseling door middel van digitale tools (platformen, applicaties, …) die voldoen aan de eisen rond de privacy van de patiënt. Het probleem ligt echter in de vaak fragmentarische en inefficiënte manier waarop gegevens worden gedeeld. Traditionele methoden van informatieoverdracht, zoals papieren documenten of verouderde systemen, zijn niet alleen tijdrovend en arbeidsintensief, maar ook vatbaar voor menselijke fouten en beveiligingsrisico's. Dit kan leiden tot vertragingen in dienstverlening, gebrekkige besluitvorming, verminderde kwaliteit van zorg en zelfs inbreuken op de privacy van individuen.

Veilige, digitale, interdisciplinaire gegevensdeling verwijst naar het proces waarbij gegevens elektronisch worden uitgewisseld, rekening houdende met strenge beveiligingsprotocollen en privacyrichtlijnen. Dit omvat onder andere het gebruik van geavanceerde encryptietechnologieën en toegangscontrolemechanismen om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot relevante informatie en dat de integriteit van de gegevens wordt beschermd. Hiernaast dient er voldaan te worden aan de principes van de AVG (Algemene Verordening Gegevensbescherming), ook wel GDPR (General Data Protection Regulation) genoemd.

Het doel van deze studie is om eerst het concept van veilige gegevensdeling in kaart te brengen, inclusief een overzicht van diverse digitale tools die op vandaag gebruikt worden om interdisciplinaire gegevensuitwisseling tussen zorgverleners te faciliteren. Daarnaast is het van cruciaal belang om de bewustwording en kennis van zorgverleners over dit onderwerp te onderzoeken. Hiervoor maakt dit onderzoek gebruik van zowel kwantitatieve als kwalitatieve methoden om inzicht te krijgen in de percepties en kennis van zorgverleners in het werkveld. Op basis van deze bevindingen zal dit rapport de hiaten en behoeften in de regio identificeren, met als uiteindelijk doel bewustwording te bevorderen door middel van een informatieve brochure.

1 Het brede landschap van de digitale tools

1.1 Veiligheid bij digitale gegevensdeling

Digitale tools worden in verschillende vormen ingezet om gezondheidsgegevens te delen in de zorg. Er is een groot aanbod aan applicaties, platformen, … waarmee zorgverleners aan de slag kunnen. Hierbij is het uitermate belangrijk om ervoor te zorgen dat er voorzichtig omgegaan wordt met deze gegevens. Gezondheids- en patiëntengegevens horen onder de gevoelige privégegevens, waardoor digitale tools dienen te voldoen aan de principes van de AVG, ook wel de GDPR. Deze vormen de basis voor de bescherming van persoonlijke gegevens binnen de Europese Unie (Vlaanderen, z.d.). De belangrijkste principes zijn:

Rechtmatigheid, rechtvaardigheid en transparantie: Persoonsgegevens moeten op een rechtmatige, eerlijke en transparante manier worden verwerkt. Dit betekent dat personen moeten worden geïnformeerd over hoe hun gegevens worden gebruikt.
Doelbeperking: Persoonsgegevens mogen alleen worden verzameld voor specifieke, expliciete en rechtmatige doeleinden. Ze mogen niet verder worden verwerkt op een manier die niet verenigbaar is met deze doeleinden.
Gegevensminimalisatie: Organisaties moeten ervoor zorgen dat de persoonsgegevens die ze verwerken, relevant zijn, adequaat zijn en beperkt tot wat nodig is voor de doeleinden waarvoor ze worden verwerkt.
Juistheid: Persoonsgegevens moeten accuraat en actueel zijn. Indien nodig, moeten onnauwkeurige of onvolledige gegevens worden gecorrigeerd of bijgewerkt.
Opslagbeperking: Persoonsgegevens moeten (niet langer dan nodig) worden bewaard in een vorm die identificatie van betrokkenen mogelijk maakt voor de doeleinden waarvoor de gegevens worden verwerkt.
Integriteit en vertrouwelijkheid: Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging ervan waarborgt, inclusief bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
Verantwoordingsplicht: De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de principes van de GDPR en moet kunnen aantonen dat zij in overeenstemming handelen met deze principes.

In wat volgt worden verschillende digitale tools voor veilige interdisciplinaire gegevensdeling beschreven, waarbij indien mogelijk die veiligheid extra wordt beoordeeld aan de hand van de GDPR-normen. Deze oplijsting is niet limitatief.

1.2 Niet-veilige digitale tools voor interdisciplinaire gegevensdeling

Communicatie en gegevensuitwisseling verhogen de kwaliteit van patiëntenzorg en maken administratieve opvolging efficiënter. Doordat gezondheidsgegevens gevoelige informatie bevatten, is het cruciaal om gebruik te maken van beveiligde kanalen. Helaas zijn er nog steeds platformen die niet aan de vooropgestelde veiligheidsnormen voldoen bij het delen van gezondheidsgegevens. In onderstaande beschrijving worden de niet-veilige digitale tools bij interdisciplinaire gegevensdeling beschreven. In volgend onderdeel worden alternatieven hiervoor verder uitgelicht.

Een eerste voorbeeld is **WhatsApp.** Wanneer een WhatsApp-bericht op een telefoon binnenkomt, is het vaak al gedeeltelijk zichtbaar op het vergrendelde startscherm. Dit maakt het voor anderen dan de eigenaar van de telefoon makkelijker om berichten te lezen. Bovendien worden foto's standaard opgeslagen op de telefoon. Op een iPhone worden ze bijvoorbeeld ook nog eens doorgestuurd naar de iCloud. Hierdoor kan er geen controle worden uitgeoefend over wie de berichten ziet, wat de beveiliging van deze gegevens in twijfel trekt. Zorgverleners dienen alle mogelijke maatregelen te nemen om te voorkomen dat patiëntgegevens in handen vallen van onbevoegden. Als zorgverlener zijn zij gebonden aan een beroepsgeheim en mogen zij medische gegevens in principe niet delen met anderen. Wanneer een WhatsApp-bericht wordt gelezen door een onbevoegde persoon, vormt dit een onwettige schending van het beroepsgeheim en een onrechtmatige verwerking van persoonsgegevens (Dutij, 2019; Masoni & Guelfi, 2020).

Een ander voorbeeld is **Dropbox of WeTransfer**. Deze worden gebruikt omwille van de gebruiksvriendelijkheid, maar zijn onvoldoende beveiligd en niet conform de opgelegde GDPR-normen.

Het doorsturen van medische gegevens via een standaard **e-mail** is ten strengste af te raden. Volgens de GDPR is het op zijn minst vereist om een beveiligde e-mailtoepassing en versleuteling te gebruiken. De Orde der Artsen gaat nog een stap verder en adviseert het gebruik van systemen met een zogenaamde multifactorauthenticatie. Zo kan een e-mail zonder enige onderschepping verstuurd worden (Ondernemingsdatabank, 2023). De meeste populaire e-mailproviders, zoals Gmail, Outlook en Yahoo, scannen de inhoud van e-mails en gebruiken een e-mailadres om een gedetailleerd profiel te maken en winst te maken met gegevens. Wel biedt Outlook versleuteld mailen aan waarbij ontvangers eerst een code krijgen, aangezien de mail onleesbaar is zonder deze code.

1.3 Veilige digitale tools bij interdisciplinaire gegevensdeling

Er bestaat een groot aanbod aan digitale portalen, platformen, applicaties, … voor het veilig delen van gezondheidsgegevens en patiëntengegevens, waardoor het overzicht makkelijk verloren gaat. Om die reden is het essentieel hierin structuur te scheppen en het huidige digitale landschap te schetsen. Eerst worden gelijkaardige alternatieven beschreven die veilig zijn voor de eerder beschreven niet-veilige digitale tools. Daarna worden andere veilige tools beschreven.

Doctolib Siilo kan een veiliger alternatief bieden voor WhatsApp. Dit is een gratis Messenger-applicatie voor zorgverleners om onderling tekstberichten, foto's, video's en bestanden uit te wisselen. Door het bureau van de Nationale Raad van de Orde der Artsen wordt deze applicatie bestempeld als een bruikbaar platform voor het delen van gegevens en bestanden. Op de website van het eHealth-platform krijgen ze het label 'recommended'. Het eHealth-platform is gericht op het verbeteren en vereenvoudigen van de uitwisseling van gezondheidsgegevens. Het ondersteunt de samenwerking tussen diverse zorgverleners en instellingen en maakt het voor burgers makkelijker om toegang te krijgen tot hun eigen gezondheidsinformatie (eHealth-platform, z.d.). Het gebruik van een soortgelijk messenger-systeem zoals Doctolib Siilo kan leiden tot snelle interventies, multidisciplinaire discussies over specifieke gevallen en efficiënt werken, zowel individueel als in een bredere groepscontext. Met het oog op gebruik in de zorgsector heeft Siilo extra aandacht besteed aan beveiliging. Gebruikers worden geverifieerd als zorgverleners aan de hand van hun identiteitskaart en RIZIV-nummer. Het datatransport wordt versleuteld en bij het opstarten van de app moet altijd een pincode worden ingevoerd om ongeautoriseerde toegang te voorkomen. In tegenstelling tot WhatsApp waarbij ontvangen data versleuteld en toegankelijk opgeslagen wordt op de ontvangende telefoon, komt bij Siilo de data terecht in een versleutelde kluis (Dutij, 2019; Masoni & Guelfi, 2020).

Toch zijn er belangrijke aandachtspunten voor de gebruiker. Aangezien Siilo niet gekoppeld is aan de beveiligingssystemen van eHealth, wordt geen rekening gehouden met bijvoorbeeld therapeutische relaties en uitsluitingen. Via de app kunnen niet-geanonimiseerde medische gegevens dus worden verstuurd naar een contact die geen behandelende zorgverstrekker is van deze patiënt of zelfs naar een volledige contactgroep. Vanuit dat perspectief draagt de versturende zorgverlener zelf verantwoordelijkheid voor het naleven van de GDPR-regelgeving. Er werden in de app wel extra functionaliteiten geïntegreerd voor de anonimisering van foto's en bestanden, zoals bijvoorbeeld een deel van een foto blurren om de patiënt of patiëntengegevens onherkenbaar te maken (Domus Medica, 2023a).

Als veilig alternatief voor Dropbox en WeTransfer bestaat de **Transferbox**, ontwikkeld door de Orde van Artsen. Dit is een volwaardig, beveiligd en gebruiksvriendelijk alternatief. Deze voorziet voldoende ruimte om digitale medische informatie te delen met collega's, maar ook met derden waaronder experten, advocaten, rechtbanken, … De Transferbox is te vinden op de website van de Orde der artsen (www.ordomedic.be). Na authenticatie via ITSME is het mogelijk om gegevens over te dragen. Deze functie maakt het verzenden van berichten mogelijk met een maximale capaciteit van 250 MB per bericht. Elke individuele arts heeft een totale capaciteit van 2GB, wat significant hoger is dan de limieten van verschillende andere beschikbare platformen (Domus Medica, 2023a). Transferbox ontwikkelde een handleiding over het gebruik ervan, te raadplegen via deze link: https://ordomedic.be/uploads/public-files/Transferbox-Handleiding-NL.pdf

Een gelijkaardig, maar veilig alternatief voor Dropbox en WeTransfer is de **eHealthBox.** Dit is een beveiligde elektronische brievenbus om vertrouwelijke gezondheidsgegevens te delen. Dit werd door het eHealth-platform ontwikkeld en gratis ter beschikking gesteld voor alle Belgische zorgverleners, instellingen en actoren met een RIZIV-nummer. Elke actor in de gezondheidszorg kan vertrouwelijke berichten (document of informatiebrief) verzenden naar elke andere actor in de gezondheidszorg (individu of groep). Elke zorgverlener heeft toegang tot de eigen persoonlijke eHealthBox, waar de ontvangen berichten van andere actoren in de gezondheidszorg teruggevonden kunnen worden. Naast hun persoonlijke eHealthBox kunnen zorgverleners ook de eHealthBox raadplegen die hen is toegekend in het kader van hun functie binnen een ziekenhuis.

De berichten die via de eHealthBox ontvangen of verstuurd worden, kunnen beveiligd worden via het eHealth-certificaat, waardoor een bericht versleuteld kan worden door de afzender en enkel de bestemmeling het kan openen. Zo kunnen op een veilige manier laboresultaten, verwijsbrieven, elektronische formulieren, enzovoort uitgewisseld worden met andere zorgverstrekkers. Bij het eerste gebruik van de online toepassing van de eHealthBox dient het eHealth-certificaat toegevoegd te worden. Dat certificaat moet op de computer geïnstalleerd worden. De eHealthBox wordt gebruikt via het elektronisch patiëntendossier in het softwarepakket (of via de online toepassing) (eGezondheid, z.d.). De eHealthBox is op zichzelf niet erg gebruiksvriendelijk. Daarom hebben private bedrijven betaalde toepassingen ontwikkeld die gekoppeld zijn aan de eHealthBox, zowel voor huisartsen als paramedici. Sommige softwarepakketten hebben hiervoor een eigen toepassing hiervoor geïntegreerd. Deze toepassingen maken de eHealthBox makkelijker te gebruiken en zorgen ervoor dat verslagen en documenten van een patiënt automatisch aan het juiste patiëntendossier binnen de software van de huisart worden gekoppeld (Domus Medica, 2021b).

eHealthBox ontwikkelde ook een handleiding (https://www.ehealth.fgov.be/ehealthplatform/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/90ea90daf44ac689b4c694a31e966b8c9056310e/ehealthbox_nl_21012021.pdf) waarin o.a. volgende zaken worden uitgelegd: hoe aanmelden, eHealth-certificaat configureren, berichten lezen, bijlagen openen, zelf berichten sturen en berichten verwijderen.

Naast deze gelijkaardige veilige alternatieven voor de bovenvermelde onveilige digitale tools, kunnen andere veilige digitale tools beschreven worden. Waar de vorige tools eerder bedoeld zijn voor het actief gebruik (bv. berichten/bestanden delen), zijn de volgende digitale tools eerder bedoeld voor het passief delen. Hiermee wordt bedoeld dat zorgverstrekkers de nodige info kunnen raadplegen en opvragen, gedeeld door andere zorgverstrekkers. Vooraleer hierop verder wordt ingegaan, dienen eerst enkele belangrijke begrippen toegelicht te worden.

In België verzamelt het regionale systeem van eerstelijnskluizen informatie uit de eerstelijnsgezondheidszorg (zie ook onze pagina over Vitalink), terwijl **de hubs of gezondheidsnetwerken** van de ziekenhuizen gegevens uit de tweedelijnszorg toegankelijk maken voor zorgverleners. Deze diverse netwerken (kluizen, hubs, enz.) zijn onderling verbonden. Het eHealth-platform fungeert als een “metahub”, een overkoepelend systeem dat de verschillende hubs met elkaar verbindt en beveiligingscontroles uitvoert. Dankzij deze onderlinge connecties kunnen individuele zorgverleners alle informatie op deze systemen raadplegen via hun eigen software (Domus Medica, 2021c). In België zijn er vier regionale hubs die elk informatie verzamelen van de aangesloten ziekenhuizen, namelijk Collaboratief Zorgplatform (CoZo), Vlaams Ziekenhuisnetwerk KU Leuven (VZN), Brussels GezondheidsNetwerk (Abrumet) en Reseau Santé Wallon (RSW) (CM, 2024). Hierdoor kan een huisarts ook informatie raadplegen uit ziekenhuizen buiten zijn regio. De softwarepakketten van zorgverleners hebben een verbinding met de bestaande hubs, waarbij informatie gekoppeld is aan het specifieke dossier van een patiënt. Via Single Sign On (SSO) kunnen zorgverleners de documenten van een patiënt op de hub bekijken en eventueel downloaden. Sommige verslagen of verwijsbrieven worden door het ziekenhuis of de specialist via de eHealthbox naar het elektronisch medisch dossier van de huisarts gestuurd, waar ze eenvoudig terug te vinden zijn in de documentenlijst van de patiënt (Domus Medica, 2021c).

Naast zorgverleners hebben ook patiënten toegang tot de informatie op de hubs via de eigen patiëntenportalen van de hubs en het overkoepelende federale patiëntenportaal mijngezondheid.belgie.be (Domus Medica, 2021c). **MijnGezondheid** is een nationaal initiatief dat als centrale toegangspoort dient voor Belgische burgers om digitaal hun gezondheidsgegevens te bekijken. Gebruikers kunnen hier hun geïnformeerde toestemming registreren, openstaande medicatievoorschriften bekijken, en links naar andere platformen

vinden waar hun gegevens beschikbaar zijn. Via secties zoals 'Mijn rapporten en resultaten' of 'Links naar andere patiëntenportalen' worden gebruikers doorverwezen naar verschillende hubs (CoZo, z.d.a; Belgium.be, z.d.).

1.3.1 CoZo en nexuzhealth consult (& pro)

Een van deze hubs is het **Collaboratief Zorgplatform (CoZo)**, dat een portaal aanbiedt waarmee zorgverleners gezondheidsgegevens kunnen consulteren en patiënten toegang krijgen tot medische resultaten die worden gedeeld door de instellingen die zijn aangesloten bij CoZo. CoZo is een digitaal samenwerkingsplatform voor ziekenhuizen, psychiatrische instellingen, extramurale laboratoria, radiologiepraktijken en huisartsenkringen in België. Zo is snelle en beveiligde uitwisseling van gezondheidsgegevens mogelijk tussen verschillende zorgverleners (bv. de huisarts, arts-specialist en betrokken specialisten) die een patiënt behandelen (Psychiatrisch Centrum Sint-Hiëronymus, z.d.). CoZo is verbonden met andere hubs in België. Hierdoor kunnen gebruikers ook resultaten die beschikbaar zijn bij andere hubs vinden via CoZo (CoZo, z.d.a).

Naast deze hub bestaat eveneens een andere Vlaamse hub, namelijk **nexuzhealth.** Nexuzhealth ontwikkelde het elektronische patiëntendossier (EPD) voor ziekenhuizen, verpleegkundigen (thuisverpleging), huisartsen en andere zorginstellingen. Dit centraal beheerd dossier is beschikbaar voor meer dan 30 aangesloten ziekenhuizen/zorginstellingen. Elke patiënt van deze ziekenhuizen heeft slechts één dossier, ook al is hij/zij gekend in meerdere ziekenhuizen die het EPD van nexuzhealth gebruiken. In al deze ziekenhuizen kan informatie toegevoegd worden over de patiënt in hetzelfde centrale dossier. Dit omvat eveneens eerdere behandelingen in andere nexuzhealth ziekenhuizen wat een volledig beeld biedt van de patiënt. Zorgverleners uit die ziekenhuizen kunnen gegevens zoals beeldmateriaal, verslagen, medicatieoverzichten en laboresultaten daarna raadplegen via **nexuzhealth consult**. Hiermee kunnen zorgverstrekkers zoals artsen, verpleegkundigen, apothekers, tandartsen, kinesitherapeuten en vroedvrouwen gratis toegang hebben tot alle benodigde informatie voor optimale patiëntenzorg. Naast nexuzhealth consult bestaat er eveneens **nexuzhealth pro**, wat ervoor zorgt dat een huisarts of thuisverpleegkundige ook informatie kan toevoegen (nexuzhealth, z.d.a).

1.3.2 Vitalink

Naast CoZo en nexuzhealth die verbonden zijn aan een hub, bestaat **Vitalink**, een digitale kluis van de Vlaamse overheid voornamelijk gericht op eerstelijns gegevens, zoals die van een huisarts of thuisverpleging. Het is echter belangrijk te vermelden dat Vitalink eveneens gegevens deelt met de tweede lijn, waaronder bijvoorbeeld medicatieschema's. Hierdoor kunnen zorgverleners in de tweede lijn (bijvoorbeeld specialisten in ziekenhuizen) toegang krijgen tot relevante informatie over medicatie die eerstelijnszorgverleners gedeeld hebben via Vitalink. Met Vitalink kunnen zorgverleners naast medicatieschema's onder andere ook informatie over vaccinaties, samenvattingen van medische dossiers (Sumehr), bevolkingsonderzoeken en het dossier van Kind & Gezin delen.

MyHealthViewer is de specifieke viewer van Vitalink, ontworpen om de gegevens die in Vitalink zijn opgeslagen te bekijken. CoZo is gekoppeld aan Vitalink, waardoor via CoZo gegevens geraadpleegd kunnen worden die via Vitalink ter beschikking worden gesteld. Hiernaast zijn er nog andere hubs naast CoZo in België die verbonden zijn met Vitalink. De metahub is een centrale hub die gegevensuitwisseling mogelijk maakt tussen verschillende regionale hubs (de vier Belgische ziekenhuisnetwerken), waardoor deze via de metahub verbonden zijn met Vitalink (CoZo, z.d.a).

Het resultaat is een betere samenwerking en betere continuïteit van zorg, met als gevolg dat de burger meer controle krijgt over de eigen gegevens en behandeling. Er wordt op verschillende manieren gezorgd dat patiëntgegevens veilig zijn. Enkel de patiënt en zorgverleners kunnen gegevens raadplegen. De zorgverleners dienen hiervoor wel eerst toestemming te vragen aan de patiënt en er dient een zorgrelatie te zijn.

Alleen zorgverleners met wie een patiënt een therapeutische relatie of zorgrelatie heeft, kunnen gegevens raadplegen en wijzigen. Hierbij kan de patiënt specifieke zorgverleners uitsluiten van toegang tot zijn gegevens. Wanneer de patiënt toestemming geeft, geldt dit voor de volgende projecten: Vitalink, ziekenhuisnetwerken (hubs), het Gedeeld Farmaceutisch Dossier, gezondheidskluizen van het Réseau Santé Wallon en van het Brussels Gezondheidsnetwerk. De beroepsgroep van een zorgverlener bepaalt welke gegevens hij kan inzien en bewerken. Dit wordt aangegeven door een toegangsmatrix in Vitalink met de opties 'lezen', 'lezen en wijzigen', en 'geen toegang'. Zorgorganisaties kunnen alleen gegevens delen via Vitalink als er maatregelen zijn genomen om privacy en veiligheid te waarborgen. Het systeem van de 'circle-of-trust' ('vertrouwenscirkel') stelt eisen aan zorgorganisaties om de privacy en veiligheid van de patiënt te garanderen. Hierdoor kunnen zorgorganisaties bepaalde controles uitvoeren, zoals de controle op de zorgrelatie, die bij individuele zorgverleners door Vitalink worden uitgevoerd. Om deel te nemen aan de circle-of-trust moet

een organisatie in de gezondheids-, zorg- en hulpverleningssector voldoen aan dertien criteria die zijn vastgesteld door het Beheerscomité van het eHealth-platform. De erkende overheid of de overheid waarmee de organisatie een overeenkomst heeft, registreert de CoT-status zodra de organisatie verklaart aan de criteria te voldoen (Departement Zorg, z.d.c.). Via Vitalink kan informatie gegroepeerd worden en up-to-date gehouden worden door de verschillende zorgverleners die bij deze patiënt betrokken zijn. Door ook apothekers, thuisverpleegkundigen, tandartsen, vroedvrouwen… toegang te geven om gegevens op deze kluis te plaatsen, wordt ervoor gezorgd dat deze info gecentraliseerd en correct blijft (Departement Zorg, 2013a).

1.3.3 Andere digitale tools

- **BeLRAI**

BelRAI is een instrument dat diverse beoordelingshulpmiddelen bundelt en praktische richtlijnen biedt om de zorgkwaliteit voor kwetsbare individuen met complexe zorgbehoeften te verbeteren (Belrai, z.d.).

De elektronische formulieren van BelRAI stellen zorgverleners in staat om gestructureerd en gestandaardiseerd gegevens over zorggebruikers te verzamelen, ongeacht de zorgomgeving. Dit bevordert het gebruik van een gemeenschappelijke taal en vergemakkelijkt zo de coördinatie en continuïteit van zorg, vooral in een tijd waarin zorgtrajecten steeds complexer en kostbaarder worden. Door een holistische (biopsychosociale) en gestandaardiseerde beoordeling van zorgbehoeften ondersteunt BelRAI professionals bij het vaststellen van prioriteiten en bij het opstellen van zorg- en ondersteuningsplannen die nauw aansluiten op de individuele behoeften en levenssituatie van kwetsbare personen (Belrai, z.d.).

De verschillende beoordelingsinstrumenten binnen BelRAI, waaronder uitgebreide instrumenten, screeners en aanvullende tools, zijn ontworpen om rekening te houden met diverse zorgomgevingen, zowel binnen als buiten zorginstellingen. Terwijl BelRAI voornamelijk zorgverleners ondersteunt bij het opstellen van persoonsgerichte zorg- en ondersteuningsplannen, richt MyBelRAI zich op het bieden van tools en richtlijnen aan zorggebruikers zelf. Momenteel zijn de BelRAI-instrumenten beschikbaar in heel België. De BelRAI-screener is beschikbaar voor de diensten gezinszorg, de diensten Maatschappelijk Werk van de ziekenfondsen, de OCMW's en Welzijnsverenigingen. Het BelRAI-sociaal supplement voor de diensten gezinszorg en de Diensten Maatschappelijk Werk van de ziekenfondsen. Sinds 1 juni 2023 volgt BelRAI-Home Care voor de thuiszorg en BelRAI-Long Term Care Facilities voor de ouderzorg (Belrai, z.d.).

- **Alivia**

Alivia is een digitale tool die nog in de pilootfase zit. De eerste versie van Alivia is reeds klaar, waarbij personen met een zorgnood en hun zorgteams in Antwerpen en Zuid-West-Vlaanderen zich voorbereiden om Alivia te gebruiken. In deze twee regio's wordt vanaf april 2024 gedurende zes maanden de werking van Alivia getest en de bijdrage tot het organiseren van een meer doelgerichte manier van zorg in kaart gebracht. (Departement Zorg, z.d.b).

Alivia faciliteert doelgerichte en geïntegreerde zorg. Personen met lange termijn of intensieve zorgnoden krijgen vaak hulp van meerdere zorgaanbieders tegelijk, bijvoorbeeld professionele zorgaanbieders, welzijnswerkers en familieleden. Hierdoor draagt Alivia bij tot een betere samenwerking tussen de leden van het zorg- en ondersteuningsteam aan de hand van een website of app die toelaat om een zorgplan te creëren, taken te verdelen en informatie te delen. Alivia vertrekt van de levensdoelen van de persoon met een zorg- en ondersteuningsnood en bestaat uit vijf start onderdelen: levensdoelen, zorg- en ondersteuningsdoelen, zorgtaken, zorgteam en communicatie (Departement Zorg, z.d.b).

De ontwikkeling van Alivia gebeurt samen met de eindgebruikers: personen met zorg- en ondersteuningsnoden, mantelzorgers, beroepsverenigingen en koepelorganisaties uit zorg en welzijn. Alivia zal integreerbaar zijn in andere softwarepakketten en werken met veilige en internationale FHIR (Fast Healthcare Interoperability Resources) standaarden (Departement Zorg, z.d.b).

Alivia is dus enerzijds een tool die nog in de opstartfase zit vooraleer implementatie kan plaatsvinden, maar anderzijds kan het in de toekomst een gepast platform bieden waarbij interdisciplinaire samenwerking rond en met de patiënt kan plaatsvinden.

1.4 GDPR en digitale tools

Hier volgt een opsomming van de digitale tools, waarbij ze worden beschreven op basis van hun naleving van de GDPR (Algemene Verordening Gegevensbescherming). Tussen haakjes wordt telkens vermeld welk specifiek principe van de GDPR van toepassing is. Vervolgens wordt deze informatie weergegeven in een matrix, waarbij een onderscheid gemaakt wordt tussen veilige en niet-veilige digitale tools voor het delen van gegevens tussen zorgverleners.

Veilige digitale tools:

Nexuzhealth (consult/pro)
Elke patiënt heeft toegang tot de persoonsgegevens die worden verwerkt en heeft recht op inzage in deze gegevens. *(rechtmatigheid, rechtvaardigheid en transparantie)* Nexuzhealth verzamelt en verwerkt persoonsgegevens op basis van gerechtvaardigd belang. De verwerking is noodzakelijk om de goede werking van de applicatie te garanderen, waarbij alleen het minimum aan gegevens wordt verzameld. *(gegevensminimalisatie)* Er bestaat het recht om te verzoeken om de wissing of rectificatie van foutieve, onvolledige, ongepaste of verouderde persoonsgegevens. *(juistheid)* Nexuzhealth zal informatie niet langer opslaan dan nodig is voor de doeleinden waarvoor de informatie wordt verwerkt. De gegevens zullen binnen maximaal één maand worden verwijderd. *(opslagbeperking)* Daarnaast zijn er zijn redelijke fysieke, organisatorische en technische maatregelen getroffen om persoonlijke informatie te beschermen tegen ongeoorloofde toegang, vrijgave of gebruik. *(integriteit en vertrouwelijkheid)* Nexuzhealth beheert zelf geen persoonsgegevens van patiënten of zorgverleners, maar werkt uitsluitend in opdracht van zorginstellingen als verwerker. *(verantwoordingsplicht)* Omdat iedereen in hetzelfde dossier werkt, is de informatie ook volledig en meteen beschikbaar. Aangezien er zo veel informatie in dat centrale dossier zit, moet dit uiteraard zeer goed beveiligd zijn om de gezondheid en privacy van de patiënt en de zorgverlener te beschermen. Het centrale patiëntendossier betekent echter niet dat iedereen zomaar toegang krijgt tot een dossier in de nexuzhealth zorginstellingen. Dit wordt beschermd door strikte toegangsregels, die vertaald kunnen worden naar drie grote principes: *(doelbeperking)* 1) Alleen zorgverleners waarmee de patiënt een therapeutische relatie heeft, krijgen toegang tot het dossier. Deze therapeutische relatie wordt bepaald op basis van geplande of uitgevoerde handelingen zoals consultaties, ingrepen en onderzoeken.

Dit is bovendien beperkt in de tijd, dus het gaat hier enkel over zorgverleners die betrokken zijn bij een lopende behandeling.

2) De functie van een zorgverlener bepaalt hoeveel men kan zien. Een arts zal meer kunnen zien dan een administratief medewerker.
3) Een zorgverlener kan ook zelf toegang vragen tot het patiëntendossier wanneer dit noodzakelijk is. De zorgverlener moet hier verplicht een reden voor geven en de behandelende zorgverleners worden hiervan op de hoogte gebracht. Dit zorgt voor een continue controle op de toegang tot het dossier.

Nexuzhealth zorgt ervoor dat elke inzage of wijziging in het patiëntendossier wordt geregistreerd. De patiënt kan bij zijn/haar zorginstelling inzage vragen tot de audit logs waarin deze acties worden opgelijst. *(integriteit en vertrouwelijkheid)*
Bron: (nexuzhealth, z.d.b; nexuzhealth, z.b.c)

CoZo

De geïnformeerde toestemming ("informed consent") is de toestemming die de patiënt aan zijn zorgverleners geeft om zijn medische gegevens onderling en beveiligd uit te wisselen, met het oog op een optimale kwaliteit en continuïteit van de zorg. De geïnformeerde toestemming geldt nationaal en kan geregistreerd worden op CoZo of het eHealth-platform door de patiënt zelf, de huisarts, een behandelende zorgverlener, het ziekenfonds, de apotheek van de patiënt of de opnamedienst van het ziekenhuis. Registratie gebeurt doorgaans aan de hand van de elektronische identiteitskaart van de patiënt en altijd met toestemming van de patiënt. *(rechtmatigheid, rechtvaardigheid en transparantie)*

Gegevens kunnen enkel worden opgevraagd door zorgverleners die op dat moment betrokken zijn bij de behandeling van de patiënt en enkel indien de patiënt daarvoor zijn geïnformeerde toestemming heeft gegeven. *(doelbeperking)* Enkel zorgverleners die de patiënt behandelen, hebben – na de geïnformeerde toestemming van de patiënt – toegang tot zijn medische gegevens. Een behandelrelatie ("therapeutische relatie") duurt gewoonlijk tot 15 maanden nadat de identiteitskaart van een patiënt bij de betrokken zorgverleners werd ingelezen voor een consultatie. Op CoZo zelf worden geen medische resultaten bewaard. De resultaten blijven te allen tijde in de producerende instelling of bron. *(opslagbeperking)* Alle medische gegevens die nuttig zijn voor de behandeling van de patiënt kunnen gedeeld worden via CoZo, zoals: medische verslagen, resultaten van onderzoeken, medische

beelden, vaccinatie- en medicatieschema's, voorgeschreven medicatie, (ontslag)brieven en beknopt medisch dossier (sumehr). Ook de medische gegevens beschikbaar op de platformen waarmee CoZo integreert, kunnen worden opgevraagd. *(gegevensminimalisatie)*

Indien de patiënt vaststelt dat CoZo verkeerde of onvolledige gegevens over hem/haar verwerkt, heeft hij/zij het recht om aan CoZo te vragen om deze te corrigeren of aan te vullen. Dit verwijst naar het recht op rectificatie. *(juistheid)* Ter bescherming van de persoonsgegevens treft CoZo passende technische en organisatorische maatregelen om persoonsgegevens van patiënten te beschermen tegen verlies, bewerking, ongeoorloofde toegang of misbruik. Deze maatregelen worden tevens opgelegd aan de aangestelde verwerkers. *(integriteit en verantwoordelijkheid)* Voor de verwerking van deze persoonsgegevens, is CoZo verantwoordelijk voor de verwerking. Deze houdt rekening met de AVG-voorwaarden. *(verantwoordingsplicht)*
Bron: (CoZo, z.d.c)

Vitalink

Vitalink heeft een duidelijk gegevensbeschermingsbeleid opgesteld dat voldoet aan de vereisten van de GDPR. Dit beleid beschrijft hoe persoonsgegevens worden verzameld, verwerkt, opgeslagen en beschermd. Vitalink zorgt ervoor dat patiënten transparante informatie ontvangen over hoe hun gezondheidsgegevens worden verwerkt en voor welke doeleinden. Wanneer nodig wordt toestemming verkregen van de patiënten voor de verwerking van hun gegevens. *(rechtmatigheid, rechtvaardigheid en transparantie; doelbeperking)* Vitalink implementeert technische en organisatorische maatregelen om de gegevens te beschermen tegen ongeautoriseerde toegang, manipulatie of vernietiging. Dit omvat het gebruik van versleuteling, toegangscontrole en audits van systeemactiviteiten. *(integriteit en vertrouwelijkheid)* Vitalink sluit gegevensverwerkingovereenkomsten af met zorgverleners en andere betrokken partijen om ervoor te zorgen dat de verwerking van persoonsgegevens in overeenstemming is met de GDPR-normen. *(verantwoordingsplicht)*

Bron: (Departement Zorg, z.d.c)

BeLRAI

Organisaties in de gezondheidssector moeten veiligheid garanderen bij het delen van gezondheidsgegevens. Het 'Circle of Trust'-principe wordt gebruikt om dit te waarborgen. Dit houdt in dat organisaties die gegevens delen, moeten voldoen aan strikte veiligheidsmaatregelen, zodat andere partijen erop kunnen vertrouwen dat deze maatregelen worden nageleefd. Om als 'Circle of Trust' erkend te worden, moeten organisaties voldoen aan 13 criteria, die zijn goedgekeurd door het Beheerscomité van het eHealth-platform en het informatieveiligheidscomité. Deze criteria omvatten onder andere authenticatie van medewerkers en verificatie van zorgrelaties (Departement Zorg, z.d.d).

Om een BelRAI-inschaling te kunnen delen, zijn er binnen het Vlaams IT-platform BelRAI twee essentiële elementen (Departement Zorg, z.d.d):

1) Zorg- of therapeutische relatie: Deze relatie is nodig om een BelRAI-inschaling binnen de organisatie te delen. Een zorgverlener die een persoon met een zorg- en ondersteuningsnood behandelt of verzorgt, heeft een zorg- of therapeutische relatie met die persoon. Een therapeutische relatie geldt wanneer de zorgverlener een gezondheidszorgberoep uitoefent, en een zorgrelatie geldt wanneer de zorgverlener geen gezondheidszorgberoep uitoefent.
2) Geïnformeerde toestemming: Deze toestemming is nodig om een BelRAI-inschaling buiten de organisatie te delen. Het hebben van een zorg- of therapeutische relatie betekent niet automatisch dat men BelRAI-gegevens kan delen met zorgverleners van andere organisaties. Voor het elektronisch delen van gezondheidsgegevens, inclusief BelRAI-inschalingen, met zorgverleners van andere organisaties is de geïnformeerde toestemming van de persoon met een zorg- en ondersteuningsnood vereist. Deze toestemming kan worden gegeven door de persoon zelf via 'Mijngezondheid' of via verschillende zorgverleners zoals huisartsen, thuisverpleegkundigen, ziekenfondsen of de opnamedienst van een ziekenhuis.

BelRAI 2.0 is beoordeeld en goedgekeurd door de Gegevensbeschermingsautoriteit en voldoet aan de GDPR-vereisten (Declercq, 2019).

Doctolib Siilo

Doctolib Siilo voldoet aan de eisen van GDPR (DSGVO/AGD), ISO 27001, HIPAA e-Privacy, NHS DSP Toolkit en Information Governance Toolkit, DCB 0129, en NEN 7510, 7512 & 7513.

Bij doctolib Siilo heeft de gebruiker altijd toegang tot zijn/haar persoonlijke informatie waarvan Siilo in het bezit is. Dit verwijst naar het recht op inzage (artikel 15 van de AVG). *(rechtmatigheid, rechtvaardigheid en transparantie)* De gebruiker kan bezwaar maken tegen de verwerking van zijn/haar persoonsgegevens voor directe marketingdoeleinden en/of kan bezwaar maken tegen verwerking op basis van het gerechtvaardigd belang van Siilo (artikel 21 van de AVG). *(doelbeperking)* De gebruiker kan eveneens verzoeken om zijn/haar persoonsgegevens te wijzigen of te verwijderen. Dit verwijst naar het recht op rectificatie (artikel 16 van de AVG). *(gegevensminimalisatie en juistheid)* Gegevens worden niet langer behouden of bewaard dan wettelijk is toegestaan, wettelijk verplicht is en/of noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt. De gegevens worden verwijderd na beëindiging van de contractuele relatie. De bewaartermijn is afhankelijk van de soort gegevens en de doeleinden van de gegevensverwerking. *(opslagbeperking)* De persoonsgegevens worden beschermd tegen verlies of enige vorm van onrechtmatige verwerking via passende technische en organisatorische maatregelen. *(integriteit en vertrouwelijkheid)* Siilo Holding B.V. of een aangewezen groepsmaatschappij is de Verwerking Verantwoordelijke voor de persoonsgegevens die met name worden verzameld in het kader van de administratie en het beheer van gebruikersaccounts, browsen op de website of de app, het maken van statistieken met betrekking tot het gebruik van de app en diensten, hun berekening en anonimisering, het verzenden van marketingcampagnes naar de gebruikers en prospecten van Siilo. Als Verwerking Verantwoordelijke neemt Siilo passende maatregelen om de bescherming en vertrouwelijkheid te waarborgen van de persoonsgegevens die zij bewaart of verwerkt in overeenstemming met de bepalingen van de AVG. *(verantwoordingsplicht)*

Bron: (Doctolib Siilo, z.d.)

Alivia
De GDPR-normen kunnen voor Alivia enkel bekeken worden voor de pilootprojecten. Het Departement Zorg treedt op als verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens in het kader van deelname aan het Alivia Pilootproject. Alivia handelt steeds in overeenstemming met de AVG 2016/679 van Europa en/of alle nationale wetten met betrekking tot het uitvoeren van de AVG. *(verantwoordingsplicht)* De patiënt heeft het recht om op elk moment toegang te vragen tot zijn/haar persoonsgegevens en om geïnformeerd te worden over het doel van de verwerking door Alivia. *(rechtmatigheid, rechtvaardigheid en transparantie)* Persoonsgegevens worden enkel gebruikt voor de juiste doeleinden, namelijk het ontwikkelen van een systeem dat beter is afgestemd op de unieke behoeften van personen met zorg -en ondersteuningsnood en hun zorgteam. *(doelbeperking)* Alivia zal persoonsgegevens niet langer bewaren en verwerken dan noodzakelijk is voor de beschreven doeleinden. De gegevens zullen maximaal zes maanden na afronding van het pilootproject bewaard worden. Uitgezonderd de statistische gegevens over het gebruik van Alivia die maximaal vijf jaar worden bewaard na afronding van het pilootproject. *(opslagbeperking)* Wanneer de patiënt van mening is dat persoonsgegevens onjuist of niet langer actueel zijn, dan heeft deze het recht om Alivia te vragen die persoonsgegeven te rectificeren. *(juistheid)* Wanneer de gegevens niet langer nodig zijn om de omschreven doeleinden na te streven, kan de patiënt verzoeken om de gegevens te wissen en de verwerking te beperken tot het strikt noodzakelijke om de gegevens gepast te bewaren. *(gegevensminimalisatie)* Alivia heeft beveiligingsmaatregelen genomen, zowel technisch; organisatorisch als fysiek om de vernietiging; verlies; vervalsing; wijziging; ongeoorloofde toegang of onbedoelde kennisgeving van persoonsgegevens aan een derde partij te voorkomen. *(integriteit en vertrouwelijkheid)* Bron: (Departement Zorg, z.d.e)

Onveilige digitale tools:

WhatsApp
WhatsApp is een vaak gebruikte berichtendienst die vaak wordt ingezet door artsen en zorginstellingen om de continuïteit van zorg te bevorderen en efficiënte dienstverlening in de gezondheidszorg te vergemakkelijken. WhatsApp voldoet echter niet aan onder andere de vereisten van de Europese AVG. Het delen van gezondheids- en patiëntinformatie via WhatsApp is daarom niet geschikt en kan leiden tot inbreuken op de privacy en beveiliging van patiëntgegevens. Daarom wordt gekeken naar alternatieven voor WhatsApp die voldoen aan de AVG en de privacy van patiëntgegevens waarborgen. Het doel is zorgorganisaties en zorgverleners zoals artsen te stimuleren om veilige berichten-apps te gebruiken, waarvan sommige gratis zijn (Masoni & Guelfi, 2020).

WeTransfer
WeTransfer wordt niet als veilig beschouwd, omdat er momenten zijn tijdens het overdrachtsproces van bestanden waarop bestanden niet gecodeerd zijn. Hoewel WeTransfer gegevens versleutelt tijdens de overdracht en op hun servers, worden bestanden tijdelijk gedecodeerd bij het wisselen van coderingstype. Dit betekent dat ze leesbaar zijn voor iedereen met toegang tot de servers van WeTransfer, wat een risico vormt voor de veiligheid van gevoelige gegevens (O'Sullivan, 2024).

Dropbox
Dropbox wijst op het feit dat alle beschikbare metadata worden geanalyseerd en verwerkt in het belang van het verbeteren van de algehele gebruikerservaring. In het geval van privégebruik worden opgeslagen gegevens voor andere doeleinden gebruikt, zoals reclame en het verbeteren van de dienstverlening. Hiernaast moet er rekening gehouden worden dat de toegang tot encryptiesleutels (decentraal opgeslagen op verspreide locaties) door Dropbox zelf op ieder moment mogelijk is. De opgeslagen bestanden kunnen in theorie dus door Dropbox gelezen worden. Cloudproviders (bedrijven die via internet IT-diensten aanbieden, zoals opslag, verwerking en netwerken) kunnen theoretisch toegang krijgen tot opgeslagen gegevens door hun technische opzet. Hoewel ze gegevens versleutelen tijdens overdracht en opslag, gebeurt dit niet altijd end-to-end. Hierdoor kunnen gegevens soms in ongecodeerde vorm beschikbaar zijn voor de aanbieder (Lawpilots, 2023).

Naast de argumentatie over veilige en onveilige digitale tools, is er ook het aspect van e-mail via platforms zoals Outlook. E-mailen kan veilig plaatsvinden, indien de e-mails worden versleuteld. Versleuteling zorgt ervoor dat de inhoud alleen leesbaar is voor de geadresseerde. Hiernaast beschermt dit de gegevens tegen ongeautoriseerde toegang tijdens de overdracht via e-mail. Hierdoor kunnen gevoelige informatie en patiëntgegevens veilig worden verzonden als de juiste beveiligingsmaatregelen worden toegepast.

In onderstaande tabel wordt weergegeven hoe de digitale tools al dan niet voldoen aan de principes van de GDPR/AVG:

Digitale tool	**Veiligheid**
nexuzhealth consult & pro	
CoZo	
Vitalink	
Doctolib Siilo	
WhatsApp	
eHealthBox	
BeLRAI	
Alivia (pilootfase)	
WeTransfer	
Dropbox	
Outlook	

1.5 Bewustzijn en gebruik van digitale tools bij zorgverleners

Het gebruik van digitale tools in het Belgische gezondheidssysteem is behoorlijk complex aangezien er enerzijds al veel functionaliteiten goed ingeburgerd raken in de dagelijkse werking en anderzijds nog veel gebrek is aan kennis over de verschillende mogelijkheden. Uit gegevens van de meest recente eHealthMonitor in 2019 blijkt dat er een gebrek aan kennis is bij zowel zorgverleners als burgers. Dit gaat over het digitaal uitwisselen van gezondheidsgegevens, de online inzage van persoonlijke gezondheidsgegevens via een gezondheidsportaal en het bestaan en gebruik van de verschillende gezondheidsapps (Steenberghs et al., z.d.).

Mede door de COVID-19 crisis is het gebruik van digitale tools gestegen. Dit kan gaan over teleconsultaties, nieuwe eGezondheidsdiensten en online communicatiekanalen tussen zorgverleners en patiënten. Zorgverleners hebben dringend behoefte aan ondersteuning en informatie met betrekking tot eHealth. Volgens hen is er te weinig communicatie over welke toepassingen beschikbaar zijn, over hoe nieuwe toepassingen geïmplementeerd kunnen worden, en over welke opleidingen beschikbaar zijn om met deze toepassingen te leren werken. Door meer training en communicatie over de functionaliteiten zou het gebruik ervan ook toenemen, aangezien het niet-gebruik vaak te wijten is aan het gebrek aan kennis over een toepassing of de voordelen ervan. De eHealthMonitor geeft ook aan dat de uitwisseling van gezondheidsgegevens tussen zorgverleners voornamelijk nog schriftelijk en telefonisch gebeurt. Bij de zorgverleners is slechts een minderheid tevreden met het aanbod aan digitale communicatiekanalen voor het uitwisselen van gezondheidsgegevens (Steenberghs et al., z.d.).

Hoewel digitale gezondheidszorg mogelijkheden biedt om de kwaliteit, efficiëntie en veiligheid van gezondheidszorginstellingen te verbeteren, verloopt de adoptie van digitale instrumenten en technologieën in de eerstelijnszorg langzaam. Dit komt deels door een gebrek aan digitale gezondheidsgeletterdheid. Het blijkt dat slechte digitale gezondheidsgeletterdheid de voornaamste belemmering vormt voor de implementatie van digitale gezondheidszorgdiensten. Het belang van het verbeteren van de digitale geletterdheid wordt benadrukt als middel om de acceptatie van nieuwe digitale hulpmiddelen en technologieën onder gezondheidswerkers te bevorderen. Daarom is er een dringende behoefte aan toegankelijke, gestructureerde en uitgebreide training van gezondheidswerkers, zodat zij technologie optimaal kunnen benutten en zo het volledige potentieel op het gebied van kwaliteitszorg kunnen realiseren (Jiménez et al., 2020).

Er dient een grotere focus te liggen op het blootstellen van zorgverleners aan diverse mogelijkheden binnen de digitale gezondheidszorg. Dit is cruciaal om de bekendheid, interesse en gebruikerservaring te vergroten, wat bijdraagt aan het versterken van hun digitale gezondheidsvaardigheden. Bovendien is er behoefte aan meer informatie over de aspecten die de ontwikkeling van deze competenties bij zorgverleners stimuleren (Jarva et al., 2022).

Digitale geletterdheid maakt deel uit van gezondheidsvaardigheden (het vinden, begrijpen, beoordelen en gebruiken van gezondheidsinformatie). Dit bevat drie aspecten, namelijk: functioneel, kritisch en interactief/communicatief. Binnen het functionele aspect zit geletterdheid (lezen, schrijven en rekenen) vervat, maar ook digitale geletterdheid (bv. informatie opzoeken). Die laatste kan gelinkt worden aan digitale inclusie, wat wil zeggen dat iedereen in rekening wordt gebracht om mee te doen op digitaal gebied. E-health is hier een voorbeeld van, waar digitale toepassingen in de zorg zoals gezondheidsportalen en apps onder vallen (Sibe, z.d.).

In de context van beperkte gezondheidsvaardigheden verdienen digitale vaardigheden bijzondere aandacht. Aangezien een groeiend deel van het dagelijks leven zich online afspeelt, wordt het vermogen om te navigeren door digitale gezondheidstools -en diensten steeds belangrijker, zowel voor patiënten als zorgverleners (Heijmans et al., 2020).

Enkele hulpmiddelen om die digitale gezondheidsvaardigheden bij veilige, digitale, interdisciplinaire gegevensdeling te versterken zijn onder andere:

- VIVEL Academie organiseert opleidingen en biedt zorgverleners ondersteuning rond IT en gegevensdeling (eGezondheid). Hiernaast worden de activiteiten van éénlijn.be verder gezet. VIVEL Academie biedt handige toolboxen met tools, methodieken en relevante informatie. Voorbeelden hiervan zijn: e-learning: 'Hoe veilig communiceren in de zorg?' en Webinar: 'Veilig digitaal communiceren' (VIVEL, z.d.).
- CoZo biedt een opleiding aan: 'Algemene verkenningstocht eGezondheid in ziekenhuizen'. Het doel van de opleiding is diverse functies binnen het ziekenhuis (en andere instellingen) samen laten ontdekken en wat zorgverleners en vooral de patiënten te winnen hebben bij een vlotte en efficiënte digitale samenwerking. De opleiding kan plaatsvinden in het ziekenhuis of op een locatie naar keuze, zowel overdag als 's avonds. Meerdere sessies op één dag zijn mogelijk (aaneensluitend) en vanaf 15 deelnemers kan de sessie doorgaan. De opleiding is volledig kosteloos, enkel een geschikt lokaal met beamer en internet dient te worden voorzien (TransEL-Éénlijn.be, z.d.).

Naast de kennis en vaardigheden en het gebrek hieraan op vlak van digitale tools voor veilige gegevensdeling, kan het gebruik en voorkeur ervan belicht worden. Er zijn geen specifieke cijfers voorhanden, maar wel enkele gegevens. Zo werd CoZo vooral druk bezocht door huisartsen en zorgverleners in ziekenhuizen. Via CoZo worden maandelijks talloze resultaten opgevraagd uit Vitalink, waarbij vooral de COVID-19 vaccinatiegegevens en sumehr vaak worden opgevraagd (CoZo, z.d.b). Het meest gebruikte gezondheidsportaal is NexuzHealth waarbij meer dan 113.600 zorgverleners aangesloten zijn (nexuzhealth, z.d.). De hubs, vitalink en het eHealth platform in het algemeen zijn in Vlaanderen/België de systemen van voorkeur voor het veilig uitwisselen van zorggegevens. Documenten van de ziekenhuizen worden ter beschikking gesteld via de hub en de eerstelijnszorgverstrekkers gebruiken vitalink voor het delen van gegevens. Ook de eHealthBox is een vaak gebruikt systeem, maar dan voor punt-tot-punt communicatie, wat betekent dat er communicatie plaatsvindt tussen twee actoren (Raeymaekers et al., 2020).

1.6 Probleemstelling

In de huidige gezondheidszorg is digitale gegevensdeling een cruciaal aspect geworden voor het leveren van effectieve zorg en het bevorderen van patiëntveiligheid. Echter, ondanks de voordelen van digitale tools voor gegevensuitwisseling, blijven zorgverleners vaak platforms en applicaties gebruiken die niet adequaat zijn beveiligd.

Het gebrek aan bewustzijn en kennis bij zorgverleners over veilige praktijk voor digitale gegevensdeling draagt bij aan het blijvende gebruik van tools die niet conform zijn met de GDPR. Mogelijk zijn veel zorgverleners niet op de hoogte van de risico's die verbonden zijn aan het delen van gevoelige informatie via onvoldoende veilige platformen of het verzenden van onbeveiligde e-mails en berichten. Bovendien kan het ontbreken van richtlijnen en standaarden het voor zorgverleners moeilijk maken om de juiste tools te kiezen en veiligheidsmaatregelen te nemen. Op die manier wordt er gekozen voor wat men gewoon is met als gevolg dat veiligheid niet meer prioritair is.

Het huidige landschap van digitale gegevensdeling in de zorg wordt dus gekenmerkt door een paradox: hoewel de beschikbaarheid van digitale tools de efficiëntie van zorgverlening kan verbeteren, blijft het gebruik van onveilige platformen en het gebrek aan bewustzijn over veilige gegevensdeling een aanzienlijk obstakel vormen voor het realiseren van een veilige en effectieve digitale gegevensuitwisseling.

Deze bevindingen maken het essentieel om bewustzijn te creëren bij zorgverleners over het belang van veilige, digitale gegevensuitwisseling tussen zorgverleners en wat dit dan precies inhoudt. Op die manier kan volgende onderzoeksvraag opgesteld worden:

“Hoe kan het bewustzijn rond het belang van veilige gegevensuitwisseling tussen zorgverleners vergroot worden?”

2 Methode

Om een meer uitgebreid begrip van veilige, digitale, interdisciplinaire gegevensdeling te verkrijgen, is het voor de hand liggend om een mixed-method onderzoeksmethode te hanteren. Dit betekent om zowel kwantitatieve als kwalitatieve methoden voor dataverzameling te gebruiken.

Voor het verzamelen van kwantitatieve data wordt er gebruikgemaakt van een online vragenlijst. Zo kan er een ruime doelgroep van zorg -en welzijnsverleners aangesproken worden en neemt dit hiernaast niet veel tijdverlies of verplaatsing in beslag. Deze resultaten geven het algemeen beeld weer, maar eveneens de belangrijke zaken om aandacht aan te besteden. De semi-gestructureerde enquête bestaat uit open en gesloten vragen, waaronder schaalvragen (5-puntenschaal) en meerkeuzevragen. De vragenlijst werd gedurende drie weken (eind april - midden mei 2024) opengesteld voor respondenten via de nieuwsbrief van de samenwerkingsverbanden geïntegreerde zorg, empact en Sibe.

Voor het verzamelen van kwalitatieve data hanteert dit onderzoek focusgroepen. Op die manier kunnen meer diepgaande inzichten verkregen worden. Er worden drie focusgroepen georganiseerd, waarvan twee fysiek en één digitaal. De twee fysieke focusgroepen vinden plaats in de Empact-regio (ELZ Westhoek, ELZ Midden-West-Vlaanderen, ELZ RITS) en in de Sibe-regio (ELZ Westkust&Polder, Houtland en Polder en Oostende-Bredene). De digitale focusgroep vindt dus online plaats en zorgt ervoor dat zorgaanbieders uit het ruime zorglandschap van West-Vlaanderen kunnen deelnemen. De verwerking van de gegevens gebeurt anoniem. Voor de focusgroepen werd gemikt op een omvang van 6 tot 12 deelnemers voor de focusgroepen, maar dit werd niet bereikt vanwege de korte tijdspanne bij de rekrutering van deelnemers. Hierdoor kan er eerder gesproken worden van interviews met meerdere deelnemers.

Enerzijds is het dus van belang om via de online bevraging een duidelijk beeld te krijgen van hoe de zorgverleners kijken naar en staan tegenover veilige, digitale, interdisciplinaire gegevensdeling. Anderzijds bieden mondelinge gesprekken een aanvullende meerwaarde hierop.

3 Resultaten

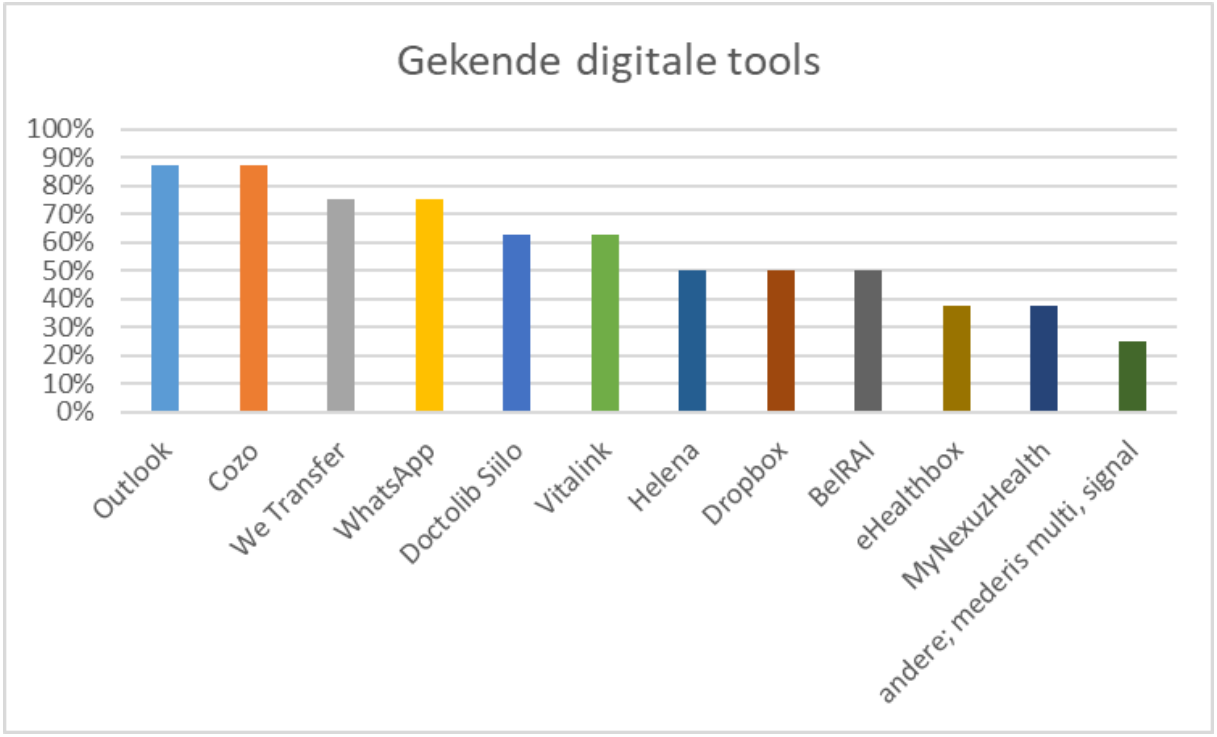
3.1 Kwantitatief onderzoek: online bevraging

Algemene informatie

Acht respondenten vulden de enquête in rond veilige, digitale, interdisciplinaire gegevensdeling. De jobs/functies van de respondenten zijn heel divers. Zo is er een medewerker sociale dienst, directie, ziekenhuisapotheker, coach van community health workers en (zelfstandig) verpleegkundigen. De respondenten zijn ongeveer gelijk verdeeld volgens de regio waarin ze werkzaam zijn, namelijk regio empact en regio Sibe.

Digitale tools

Er zijn twee opvallende zaken bij de **bekendheid** van onderstaande digitale tools. Enerzijds valt op welke digitale tools het meest gekend zijn, namelijk Vitalink, Cozo, Outlook, WhatsApp, Doctolib Siilo, BelRAI en WeTransfer. Dit staat bij deze vraag los van de functionaliteit waarvoor het gebruikt wordt. Anderzijds springt in het oog dat er ook tools zijn die bijna tot niet gekend zijn bij werknemers. Deze zijn onder andere MyNexuzHealth, eHealthBox en Transferbox.



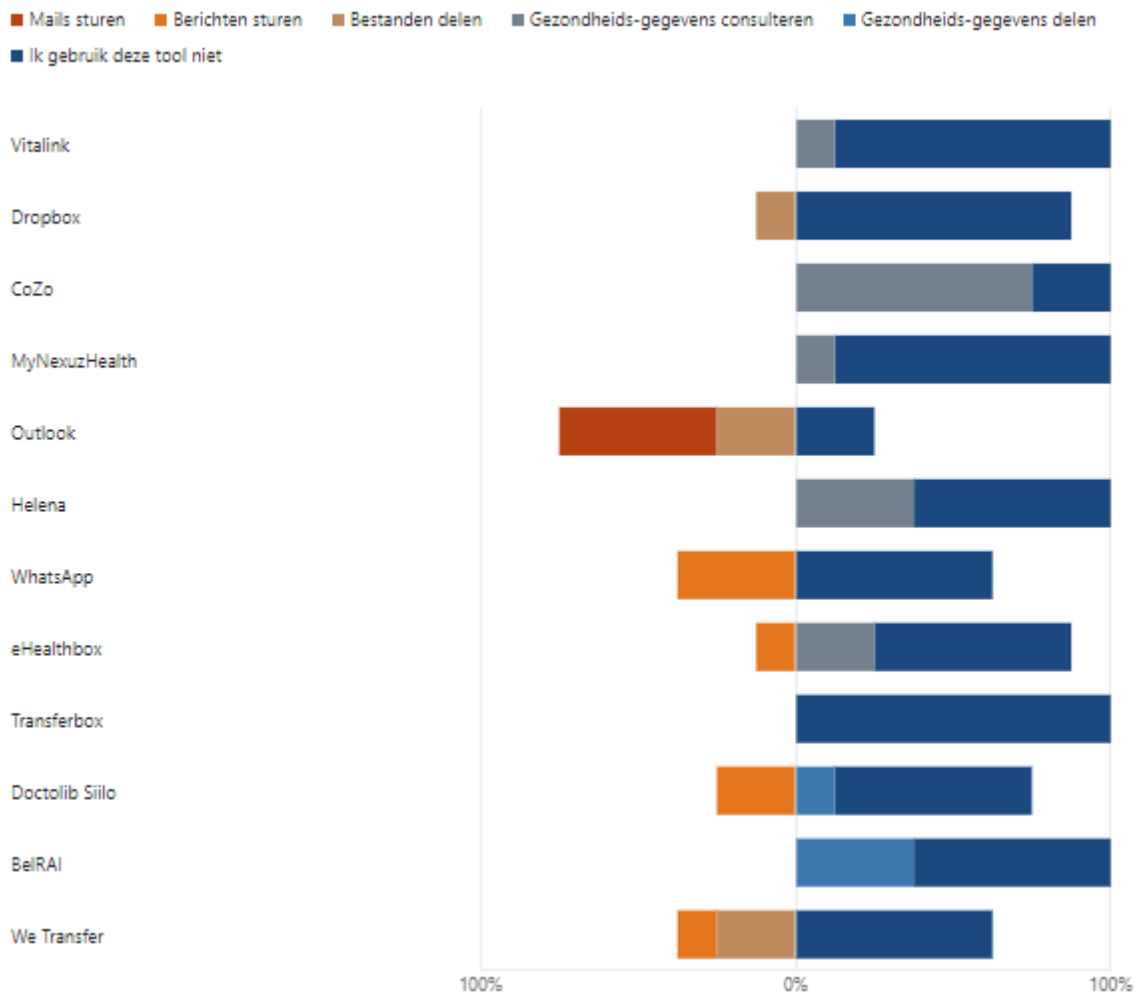
Figuur 1: gekende digitale tools bij de responderende zorgverleners

Voor **welk aspect van gegevensdeling** de digitale tools worden gebruikt, kan onderverdeeld worden in verschillende categorieën:

- *mails sturen:* Outlook
- *berichten sturen:* WhatsApp, eHealthbox, Doctolib Siilo
- *bestanden delen:* Dropbox, Outlook, WeTransfer
- *gegevens consulteren:* Vitalink, CoZo
- *gegevens delen:* BelRAI, Doctolib Siilo

Andere digitale tools die door respondenten werden opgegeven om gezondheidsgegevens te delen met andere zorgverleners zijn Mederis Multi en via mail met Ziiver als beveiliging.

Onderstaande figuur geeft dit weer door voor de verschillende digitale tools in een balk te schetsen voor welk aspect van gegevens delen ze gebruikt worden.



Figuur 2: Aspect van gegevensdeling waarvoor digitale tools gebruikt worden door responderende zorgverleners

Hiernaast werd de **gebruiksvriendelijkheid** van digitale tools bevraagd bij de respondenten. Dit kan opgedeeld worden in de meest gebruiksvriendelijke en de minst gebruiksvriendelijke tools.

Meest gebruiksvriendelijk	*Minst gebruiksvriendelijk*
Doctolib Siilo - makkelijk andere zorgverleners terugvinden - beschikbaarheid huisartsen - zichtbaar wanneer info gelezen is - snelle respons - vlug en gemakkelijk zonder storen	Doctolib Siilo - gevaarlijk voor het missen van (belangrijke) info bij verlof of afwezigheid - omslachtig om screenshots van de inhoud aan je verpleegdossier toe te voegen
Outlook - voor berichten	Mail via Virtu
WhatsApp - voor berichten	CoZo/vitalink - zelf geen gegevens aanpassen - geen datum beschikbaar van update laatste info
MyNexuzHealth - gezondheidsinfo consulteren	Dropbox/WeTransfer - lukt niet altijd - linken vervallen binnen x aantal dagen

Hiernaast werd bevraagd **hoe** de respondenten de digitale tools hebben **leren kennen en gebruiken**. Hieruit blijkt dat alle respondenten in aanraking komen met de digitale tools op de werkplaats. Bijkomend één iemand via een opleiding en een andere respondent via persoonlijk gebruik en via familie die in de zorg werkt. Eveneens gaven de respondenten hetzelfde antwoord bij de manier waarop ze ermee leren werken, namelijk dat ze dit zelf uitgezocht hebben. Eén respondent gaf bijkomend aan dat dit ook via een opleiding en handleiding gebeurde.

Als laatste vraag bij dit onderdeel werd gevraagd naar de **tevredenheid met het huidige aanbod** aan digitale tools voor digitale gegevensdeling. De meerderheid, namelijk acht respondenten, gaf aan neutraal te zijn. Dit betekent dat hun tevredenheid met de beschikbare digitale tools voor gegevensdeling gemiddeld is, dus niet echt positief of negatief. Twee respondenten zijn over het algemeen tevreden. Opvallend is dat één respondent zeer ontevreden is met het huidige aanbod, wat betekent dat het helemaal niet voldoet aan de behoeften van de respondent voor gegevensdeling.

Veiligheid

Alle respondenten geven aan vertrouwd te zijn met de principes van de GDPR. Wanneer er wordt gevraagd naar de veiligheid blijkt dat de meeste respondenten niet alle digitale tools veilig vinden die ze gebruiken. Zo wordt gewoon mailverkeer waar Outlook onder valt, beschouwd als onveilig. Doctolib Siilo is dan wel als veilig beschreven. Hierbij wordt ook aangegeven dat het handiger zou zijn moest er één tool zijn, als iedereen met dezelfde tool zou werken en als het snel en efficiënt werkt.

Alle respondenten vinden het belangrijk tot zelfs zeer belangrijk dat digitale gegevensdeling tussen zorgverleners op een veilige manier verloopt. De meeste, respectievelijk vijf van de acht respondenten, maken zich dan ook wel soms zorgen dat het delen van gegevens met anderen niet veilig verloopt. Hiervoor zijn er verschillende redenen, namelijk: het gevaar dat dit door de verkeerde persoon wordt gelezen, via cyberaanvallen op het internet terecht komt, door het weten van praktijken die gegevens delen via niet geschikte tools, … Eveneens wordt hier vermeld dat er vaak specifiek wordt gevraagd om via mail te sturen waardoor er geen andere optie is dan om via deze weg gegevens te delen. Twee respondenten gaan ervan uit dat dit sowieso veilig verloopt vanuit de eigen werkplek.

De zaken die worden aangegeven om veiliger digitaal gegevens te delen kunnen gegroepeerd worden in drie categorieën, namelijk: eenzelfde systeem/platform voor alle zorgverleners, gebruiksvriendelijkheid en bewustwording. Hiernaast worden nog enkele maatregelen genomen, namelijk beveiligd versturen van mails en opletten met phishingberichten door de afzender te controleren. Hiernaast vinden alle respondenten het belangrijk tot zeer belangrijk dat zorgverleners geïnformeerd of opgeleid worden om op een veilige manier gegevens digitaal te delen met andere zorgverleners.

3.2 Aanvullend kwalitatief onderzoek

De bovenstaande resultaten kunnen aangevuld worden met informatie uit kwalitatief onderzoek. Er zijn drie interviews afgenomen met actoren die werkzaam zijn in de zorg. Uit deze interviews blijkt dat zij bekend zijn met commerciële digitale tools zoals WeTransfer, WhatsApp en Outlook. Hoewel veilige alternatieven vaak wel bekend zijn, is er weinig inzicht in de gebruiksvriendelijkheid en bruikbaarheid binnen de softwarepakketten van de zorginstellingen. Hierdoor maken zorginstellingen vaak gebruik van eigen digitale tools om gegevens te delen. Hiernaast voelt het vaak als een grote taak voor zorgverleners om rekening te houden met het veilig delen van gegevens, aangezien dit vaak snel moet gebeuren tussen bijvoorbeeld consultaties of patiënten bezoeken. Dit wordt als een extra belasting ervaren.

Uit de interviews kwam naar voren dat er behoefte is aan meer gebruiksvriendelijkheid en een minder grote verscheidenheid aan digitale tools. Zorgverleners zouden liever één systeem of platform gebruiken. Als voorbeeld werd de eHealthBox genoemd als een veilige manier om interdisciplinair gegevens te delen. Bij het bespreken van veiligheid en maatregelen werd benadrukt dat bewustwording en duidelijke richtlijnen belangrijk zijn. Dit omvat niet alleen wat zorgverleners moeten doen, maar ook wat ze zeker niet mogen doen bij het delen van gezondheidsgegevens. Een van de geïnterviewden gaf aan dat het van belang is om op een creatieve, aantrekkelijke en gericht manier te communiceren, zodat de boodschap duidelijk en begrijpelijk is voor zorgverleners.

4 Discussie en aanbevelingen

Wanneer er met een kritische blik teruggekeken wordt, kunnen enkele discussiepunten geformuleerd worden. Eerst en vooral was het grootste gebrek bij dit project de tijd. Aangezien de brochure en poster in één maand tijd diende gemaakt te worden, was er weinig tijd om een bevraging op te zetten. Op die manier waren er weinig respondenten op de online bevraging en weinig deelnemers aan de focusgroepen. Omwille van de beperkte respons werd dit gereduceerd tot drie individuele interviews. Hierdoor was er minder interactie mogelijk tussen zorgverleners waarbij de ervaringen en kennis gedeeld kunnen worden. Aangezien er een zeer ruim landschap is aan digitale tools lijkt vervolgonderzoek aangewezen. Zo kan er meer onderzoek verricht worden naar welke digitale tools het meest en liefst gebruikt worden, aangezien hier nu zeer weinig cijfers over beschikbaar zijn.

Een kritische opmerking bij de digitale tools is dat het gebruik en de bekendheid ervan afhankelijk kan zijn van de voorkeuren van zorgverleners en zorginstellingen en de regionale richtlijnen. Daarnaast worden bepaalde platformen maar gebruikt binnen bepaalde netwerken. Welke digitale tools het meest gebruikt worden en de voorkeur genieten van zorgverleners kunnen afhankelijk zijn van verschillende factoren zoals de locatie, het type zorginstelling, de functie van de zorgverlener en individuele voorkeuren. Dit soort informatie kan verzameld worden door bijvoorbeeld enquêtes, gegevensverzameling in zorginstellingen of aan de hand van interviews en focusgroepen met zorgverleners in de regio.

Een eerste aanbeveling voor de praktijk is een verbeterde communicatie en ondersteuning voor zorgverleners. Hierbij kunnen trainingen en workshops voor zorgverleners omtrent eHealth-toepassingen georganiseerd worden, inclusief informatie over beschikbare tools, implementatiestrategieën en voordelen. Hiernaast kunnen online platforms of communities opgericht worden waar zorgverleners ervaringen kunnen delen en elkaar kunnen ondersteunen bij het gebruik van eHealth-tools. Als tweede is het blijven promoten van bewustwording en begrip een belangrijke aanbeveling. Campagnes die zich richten op bewustwording en educatie van veilige eHealth-toepassingen om gezondheidsgegevens te delen zijn en blijven nodig. Het is hierbij van belang om informatie over eHealth toepassingen en hun functionaliteiten gemakkelijk toegankelijk te maken via online bronnen, brochures of informatieve sessies. Een derde, maar niet minder belangrijke aanbeveling richt zich op de overheid. Dit kleinschalig onderzoek toont een behoefte aan gebruiksvriendelijkere digitale tools en meer eenheid. Het komen tot één digitaal platform voor het veilig delen van gezondheidsgegevens is nodig, omdat de huidige veelheid aan digitale tools eerder hindert dan helpt.

5 Ontwikkeling brochure en poster

Op basis van de bovenstaande literatuurstudie en de antwoorden van de respondenten is besloten om een **brochure** te ontwikkelen om bewustwording te creëren over veilige digitale gegevensuitwisseling (zie bijlage 1 en bijlage 2).

De brochure bevat volgende elementen:

1. **Doelpubliek:** De brochure richt zich specifiek op zorgverleners en zorginstellingen.
2. **Informatie over veilige digitale gegevensdeling:** Er wordt uitgelegd wat 'veilige, digitale, interdisciplinaire gegevensdeling' inhoudt en waarom het belangrijk is.
3. **Praktijkvoorbeelden:** Voorbeelden van onveilige en veilige manieren om gezondheidsgegevens digitaal uit te wisselen met andere zorgverleners worden gegeven.
4. **Tips voor veilige gegevensdeling:** Op de laatste pagina worden praktische tips gegeven om zorgverleners te helpen veilige digitale gegevensuitwisseling te bevorderen.

Bij het ontwikkelen van de **affiche** is de focus gelegd op de belangrijkste tips uit de brochure, omdat deze de bewustwording het meest bevorderen (zie bijlage 3).

6 Online terugkoppelingsmoment

Na de inhoudelijke uiteenzetting tijdens het online terugkoppelingsmoment werden verschillende vragen gesteld aan de deelnemers waarbij volgende antwoorden werden gegeven:

Wat is veilige, digitale, interdisciplinaire gegevensdeling volgens jou?

Veilige, digitale, interdisciplinaire gegevensdeling houdt in dat enkel de informatie die relevant is voor het traject en het behandelproces van de patiënt of cliënt wordt gedeeld.

Het gaat om het veilig versturen van gezondheidsinformatie, waarbij de privacy en vertrouwelijkheid van de zorgvrager worden beschermd.

Waarom denk je dat veilige gegevensdeling belangrijk is?

- **Vertrouwensrelatie:** Patiënten verwachten dat hun gegevens niet onnodig gedeeld worden. Vertrouwen in de zorgverlener is essentieel voor een goede zorgrelatie.
- **Privacybescherming:** De privacy van de zorgvrager moet te allen tijde beschermd worden.
- **Datalekken voorkomen:** Het voorkomen van datalekken is essentieel om gevoelige informatie te beschermen.
- **Betrouwbare Zorg:** Een vertrouwensband opbouwen is de basis voor goede zorg. Dit kan alleen wanneer de zorgvrager weet dat zijn persoonsgegevens en gezondheidsgegevens veilig worden behandeld.

Kun je een voorbeeld geven van een situatie waarin veilige gegevensdeling belangrijk is?

Bij ontslagmanagement, waar een patiënt terug naar huis gaat en ondersteuning nodig heeft, is het cruciaal dat er veilig en efficiënt informatie wordt gedeeld. Dit voorkomt miscommunicatie en zorgt voor een naadloze overgang van zorg.

Wat is de grootste hindernis volgens jou bij het veilig delen van gegevens?

Een belangrijke hindernis is het gebruiksgemak. Veel veilige systemen, zoals de eHealthbox, vereisen RIZIV-nummers en certificaten, terwijl onveilige alternatieven zoals WhatsApp veel toegankelijker zijn. Daarnaast werken verschillende zorgverleners op uiteenlopende manieren, wat de koppeling van patiëntendossiers bemoeilijkt en leidt tot onveilige praktijken zoals het delen van informatie via de telefoon of e-mail.

Hoe denk je dat we bewustzijn kunnen vergroten over het belang van gegevensbeveiliging?

- **Overheidsinformatie:** De overheid kan een rol spelen in bewustwording of bijvoorbeeld via conventies of beroepsverenigingen.
- **Gebruiksvriendelijke oplossingen:** Het aanbieden van gebruiksvriendelijke middelen voor veilige gegevensuitwisseling, want nu wordt WhatsApp vaak gebruikt door de gebruiksvriendelijkheid.
- **Educatie:** Mensen leren hoe ze veilig e-mails met gevoelige informatie kunnen versturen door middel van versleutelen.

Gemeenschappelijke standpunten en nieuwe inzichten

Er is een grote vraag naar één uniform platform of systeem. Momenteel bestaat er een tweedeling tussen gezondheidszorg en welzijnszorg, hoewel samenwerking, met name in de thuiszorg, essentieel is. Alivia zou hier mogelijk een rol in kunnen spelen.

Aanvullingen bij de brochure

- **Veilig mailen:** Naast het niet vermelden van patiëntengegevens in het onderwerp van een e-mail ervoor zorgen dat de mail versleuteld is.
- **Transparantie naar patiënt:** Informeer de patiënt altijd wanneer hun gegevens met externe zorgpartners worden gedeeld.

Aanbevelingen en (eigen) rol

- **Bewustwording:** Collega's aanspreken op het niet delen van patiëntgegevens via onveilige kanalen.
- **Ziekenhuisbeleid:** Meer bewustwording creëren binnen ziekenhuis (door de dienst beleidsinformatie samen met de DPO).
- **Overheidsplatform:** De overheid zou een platform kunnen voorzien voor interdisciplinaire gegevensdeling tussen verschillende zorgberoepen zoals ze met Vitalink deden voor de eerstelijnszorgverleners.
- **Zorgforum:** In het najaar een zorgforum van ELZ Westhoek om met (zelfstandige) zorgverleners te bespreken wat veilige gegevensdeling is voor hen en welke noden er in de regio zijn, maar ook bewustwording creëren.
- **Educatie:** Mensen leren hoe ze hun e-mails moeten versleutelen.

Met de verkregen feedback werd de brochure/affiche verder gefinaliseerd. Hiernaast kunnen andere initiatieven rekening houden met bovenstaande inzichten en aanbevelingen.

7 Besluit

Dit rapport benadrukt de dringende behoefte aan bewustwording en kennis over veilige, digitale gegevensuitwisseling in de zorgsector. Uit de resultaten blijkt dat zorgverleners baat hebben bij betere communicatie en ondersteuning. Trainingen en sensibiliseringscampagnes zijn essentieel om hen bewust te maken van de mogelijkheden en veiligheidsaspecten van digitale tools.

Er is een aanzienlijke variatie in het gebruik en de voorkeuren voor digitale tools, afhankelijk van de zorginstelling, de functie van de zorgverlener en regionale richtlijnen. Vervolgonderzoek is nodig om beter inzicht te krijgen in de meest gebruikte en geprefereerde tools.

Veiligheid en privacy van patiëntgegevens blijven van groot belang. Het delen van gezondheidsinformatie moet altijd plaatsvinden met strikte veiligheidsmaatregelen om de vertrouwelijkheid en integriteit van de gegevens te waarborgen. Om bewustwording te vergroten, zijn een brochure en affiche ontwikkeld. Deze materialen bevatten informatie over het belang van veilige gegevensdeling, praktijkvoorbeelden en praktische tips voor zorgverleners.

Een belangrijke aanbeveling is dus om de communicatie en ondersteuning voor zorgverleners te verbeteren via trainingen, workshops en duidelijke informatie over het gebruik van digitale tools en veiligheidsmaatregelen. Door voortdurende educatie en ondersteuning kan een veilige en efficiënte digitale gegevensuitwisseling worden gewaarborgd, wat zal bijdragen aan verbeterde zorgkwaliteit en patiëntveiligheid.

Bronvermelding

Belgium.be. (z.d.). *MijnGezondheid.* www.belgium.be. https://www.belgium.be/nl/online_dienst/mijngezondheid#:~:text=Mijngezondheid%20is%20een%20online%20gezondheidsportaal,over%20gezondheid%20in%20het%20algemeen

Boodts, N. (2021). *Nieuw project in de kijker: VIDIS – Symbiose.* https://smalssymbiose.be/nl/2021/02/09/nieuw-project-in-de-kijker-vidis/

CM. (2024). *Patiëntengegevens delen.* www.cm.be. https://www.cm.be/nl/zorgverleners/artsen/patientengegevens#:~:text=Een%20hub%20is%20een%20regionaal,ziekenhuis%20als%20in%20een%20priv%C3%A9praktijk

CoZo. (z.d.a). *Wat is het verschil tussen CoZo en andere portalen zoals MijnGezondheid en Vitalink?* www.cozo.be. https://www.cozo.be/ehealthportalen

CoZo. (z.d.b). *EHealth*. www.cozo.be. https://www.cozo.be/ehealth

CoZo. (z.d.c). *Privacyverklaring Collaboratief Zorgplatform Vlaanderen – CoZo VZW*. www.cozo.be. https://www.cozo.be/cozo-privacypolicy

Declercq, A. (2019). *Opent BelRAI de doos van computergestuurde zorgplanning?* Sociaal.Net. https://sociaal.net/achtergrond/belrai-computergestuurde-zorgplanning/

Departement Zorg. (2013a). Vitalink - veilig delen van zorg- en welzijnsgegevens [Video]. YouTube. https://www.youtube.com/watch?v=zysHmAUKY70

Departement Zorg. (z.d.b). *Alivia: uw digitaal zorg- en ondersteuningsplan.* www.zorg-en-gezondheid.be. https://www.zorg-en-gezondheid.be/alivia-uw-digitaal-zorg-en-ondersteuningsplan

Departement Zorg. (z.d.c). *Zo garandeert Vitalink je privacy*. www.vitalink.be. https://www.vitalink.be/gegevens/zo-garandeert-vitalink-je-privacy

Departement Zorg. (z.d.d). *Digitaal gebruik van BelRAI*. www.zorg-en-gezondheid.be. https://www.zorg-en-gezondheid.be/beleid/ezorgzaam-vlaanderen/belrai/digitaal-gebruik-van-belrai

Departement Zorg. (z.d.e). *Privacyverklaring voor gebruik van Alivia in pilootprojecten*. www.zorg-en-gezondheid.be. https://www.zorg-en-gezondheid.be/privacyverklaring-voor-gebruik-van-alivia-in-pilootprojecten

Doctolib Siilo. (z.d.). *Privacybeleid van Siilo*. www.siilo.com. https://www.siilo.com/nl/privacy

Domus Medica. (2023a). *Veilige communicatie en gegevensdeling via Siilo en Transferbox.* www.domusmedica.be. https://www.domusmedica.be/actueel/veilige-communicatie-en-gegevensdeling-siilo-en-transferbox

Domus Medica. (2021b). *Digitale communicatie, rechtstreeks met de eHealthbox.* www.domusmedica.be. https://www.domusmedica.be/expertisedomein/ict/digitale-communicatie-rechtstreeks-met-de-ehealthbox

Domus Medica. (2021c). *Digitale communicatie met de ziekenhuizen: Hubs.* www.domusmedica.be. https://www.domusmedica.be/expertisedomein/ict/digitale-communicatie-met-de-ziekenhuizen-hubs

Dutij, N. (2016). WhatsApp in de gezondheidszorg, gemak voor de zorgverlener of rampzalig voor de privacy? *ICTRecht.* https://www.ictrecht.nl/blog/whatsapp-in-de-gezondheidszorg-gemak-voor-de-zorgverlener-of-rampzalig-voor-de-privacy

eGezondheid. (z.d.). *EHealthBox*. www.ehealth.fgov.be. https://www.ehealth.fgov.be/nl/beroepsbeoefenaars-in-de-gezondheidszorg/diensten/ehealthbox

eHealth-platform. (z.d.). *Wie zijn wij?*. www.ehealth.fgov.be. https://www.ehealth.fgov.be/ehealthplatform/nl/wie-zijn-wij

Heijmans, M., Rademakers, J., Nederlands instituut voor onderzoek van de gezondheidszorg, & CAPHRI/Maastricht University. (2020). Gezondheidsvaardigheden en de mismatch tussen de patiënt en de zorgomgeving. *LEREN IN DE EDUCATIE, LESGEVEN, BEGELEIDEN & FACILITEREN*, 3–16. https://www.nivel.nl/sites/default/files/bestanden/7486.pdf

Jarva, E., Oikarinen, A., Andersson, J., Tuomikoski, A., Kääriäinen, M., Meriläinen, M., & Mikkonen, K. (2022). Healthcare professionals' perceptions of digital health competence: A qualitative descriptive study. *Nursing Open*, *9*(2), 1379–1393. https://doi.org/10.1002/nop2.1184

Jiménez, G., Spinazze, P., Matchar, D. B., Huat, G. K. C., Van Der Kleij, R., Chavannes, N. H., & Car, J. (2020). Digital health competencies for primary healthcare professionals: A scoping review. *International Journal Of Medical Informatics (Print)*, *143*, 104260. https://doi.org/10.1016/j.ijmedinf.2020.104260

Lawpilots. (2023). *Cloud storage: OneDrive, Google Drive, and Dropbox*. Lawpilots. https://lawpilots.com/en/blog/data-protection/google-drive-dropbox-onedrive-gdpr-compliant/

Masoni, M., & Guelfi, M. R. (2020). WhatsApp and other messaging apps in medicine: opportunities and risks. *Internal And Emergency Medicine*, 15(2), 171–173. https://doi.org/10.1007/s11739-020-02292-5

nexuzhealth. (z.d.a). *Waarom nexuzhealth consult.* www.nexuzhealth.com. https://www.nexuzhealth.com/nl/waarom-nexuzhealth/zorgprofessional/andere-zorgverleners

nexuzhealth. (z.d.b). *Het centraal patïentendossier*. www.nexuzhealth.com. https://www.nexuzhealth.com/nl/het-centrale-patientendossier

nexushealth. (z.d.c). *Privacyverklaring.* www.nexuzhealth.com. https://www.nexuzhealth.com/nl/over-ons/privacyverklaring

Ondernemingsdatabank. (2023). *Een laboresultaat of verslag vlug even mailen: mag dat?* ondernemingsdatabank.indicator.be. https://ondernemingsdatabank.indicator.be/medisch_recht___privacy/een_laboresultaat_of_verslag_vlug_even_mailen__mag_dat_/VLTAAWAR_EU33090401/related

O'Sullivan, F. (2024). *Is WeTransfer safe?* Proton. https://proton.me/blog/is-wetransfer-safe

Psychiatrisch Centrum Sint-Hiëronymus. (z.d.). *Het elektronisch delen van je gezondheidsgegevens: enkel met jouw toestemming.* https://www.hieronymus.be/wp-content/uploads/2016/02/Folder-CoZo.pdf

Raeymaekers, P., Balthazar, T., Denier, Y. (2020). *Big data in de gezondheidszorg. Technische, juridische, ethische en privacy-gerelateerde randvoorwaarden voor (her)gebruik van gezondheidsgegevens voor onderzoek.* Brussel: Zorgnet-Icuro

RIZIV. (z.d.a). *VIDIS: elektronisch delen van gegevens over geneesmiddelen.* www.riziv.fgov.be.https://www.riziv.fgov.be/nl/thema-s/egezondheid/vidis-elektronisch-delen-van-gegevens-over-geneesmiddelen

RIZIV. (z.d.b). *Info over de geneesmiddelen van uw patiënt consulteren via ProGezondheid*. www.riziv.fgov.be.https://www.riziv.fgov.be/nl/professionals/info-voor-allen/info-over-de-geneesmiddelen-van-uw-patient-consulteren

Sibe. (z.d.). *Gezondheidsvaardigheden voorstelling*.
Steenberghs, E., Gilles Wuyts, Sofie De Lancker, & Keshia Vleminx. (z.d.). imec.ehealthmonitor | Samenvatting. In *Imec.Ehealthmonitor*. https://drupal.imec.be/sites/default/files/2021-03/ehealthmonitor_V10F_NL.pdf

TransEL- Éénlijn.be. (z.d.). *Algemene Verkenningstocht "eGezondheid" in ziekenhuizen*. https://www.cozo.be/data/files/Algemene%20verkenningstocht%20eGezondheid%20in%20ziekenhuizen.pdf

UZ Gent. (z.d.). *Zivver: veilig privacygevoelige informatie delen*. www.uzgent.be. https://www.uzgent.be/over-uz-gent/zivver-veilig-privacygevoelige-informatie-delen

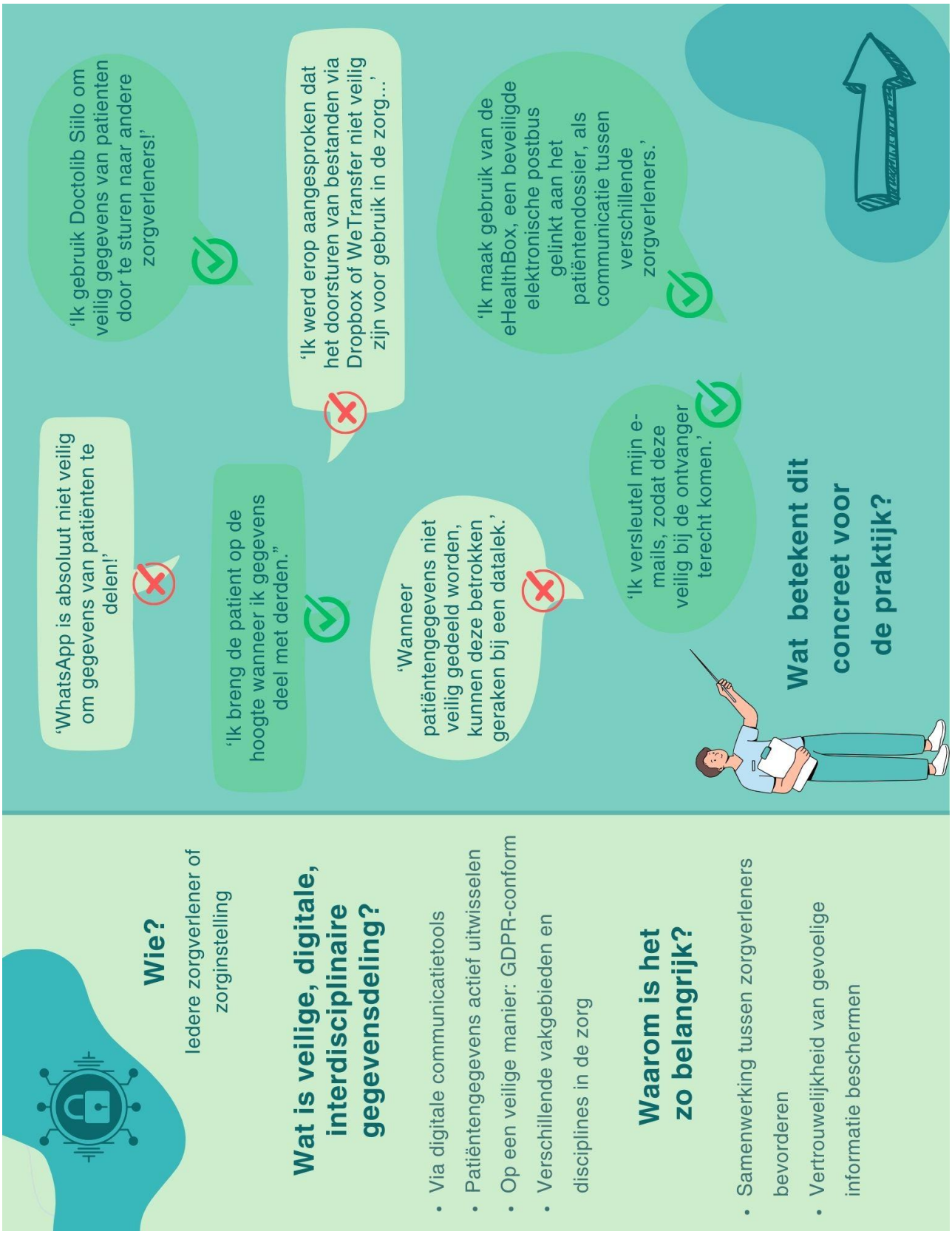
VIVEL. (z.d.). *Cursus: Hoe veilig communiceren in de zorg?* www.vivelacademie.be. https://www.vivelacademie.be/course/view.php?id=37

Vlaanderen. (z.d.). *Beheer en beveiliging van persoonlijke gegevens van Europese burgers (GDPR of AVG).* www.vlaanderen.be. https://www.vlaanderen.be/uw-overheid/werking-en-structuur/hoe-werkt-de-vlaamse-overheid/beheer-en-beveiliging-van-persoonlijke-gegevens-van-europese-burgers-gdpr-of-avg

Bijlagen

Bijlage 1: Buitenzijde brochure

Bijlage 2: Binnenzijde brochure



Bijlage 3: Affiche