Authenticatie risicoanalyse

Situatie

Fictieve case: huisartsen inzage geven in cliëntdossiers van cliënten wijkverpleging van een VVT-organisatie, met als doel verbetering van wijkzorg waarbij zowel de huisarts als de zorgorganisatie zijn betrokken. Deze risico-inventarisatie gaat alleen in op de risico’s rondom het type gegevensverwerking ‘inzage’.

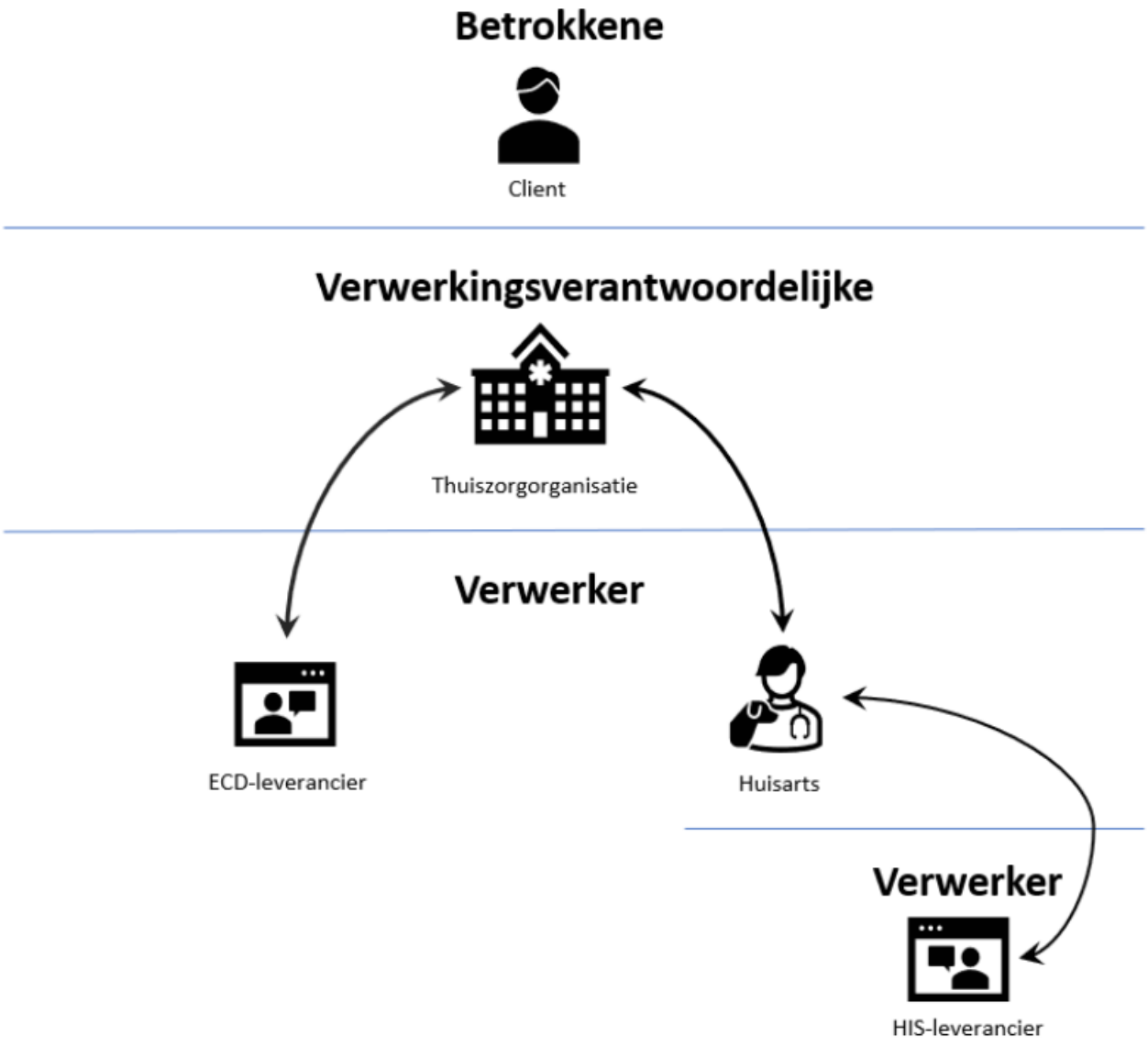
Scope van de risicoanalyse

Deze risicoanalyse geeft een overzicht van verschillende risico’s, bekeken vanuit het oogpunt van compliancy, security en privacy en is bedoeld als input voor de verdere uitwerking van project(en) rondom netwerkzorg en specifiek rondom gegevensontsluiting van VVT-organisaties met huisartsen.

Bij de uiteindelijke keuze voor een bepaalde techniek tellen verschillende aspecten mee:

- Aansluiting bij relevante wet- en regelgeving
- Aansluiting bij het werkproces van zowel de VVT-organisatie als van de huisartsenpraktijk.
- Aansluiting bij de visie van de betrokken partijen op het gebied van netwerkzorg en gegevensontsluiting.
- Aansluiting bij bewaken van belangen van de betrokken cliënten.

Partijen en rollen rondom dataverwerkingsproces



Relevante reguleringskaders

De kenmerken van de use case bepalen welke kaderstellende wet-regelgeving/normering van belang is rondom het in kaart brengen van risico's. Hieronder is per kenmerk te vinden welke wet-regelgeving/normering van belang is.

Kenmerk van use case	Kaderstellende wet-regelgeving/normering
Het werkveld: de gezondheidszorg	Wgbo, NEN7510, -12 en -13
Het beoogde doel: elektronische gegevensuitwisseling in de zorg (via inzage in extern ECD)	Begz, Wabpvz
Het type informatie: gevoelige persoonlijk identificeerbare informatie (PII)	Avg

Context en aandachtspunten

AVG: Rechten van de Betrokkene in acht nemen

De AVG geeft aan dat de cliënt als betrokkene een aantal rechten heeft, die nagevolgd moeten worden door de partij die de gegevens van de betrokkene verwerkt. Rondom de verwerking Inzage door de huisarts zijn met name de onderstaande rechten relevant:

- Recht op inzage wie het cliëntdossier ingezien heeft
- Recht om bezwaar te maken

Wgbo: Vanuit Betrokkene toestemming voor inzage door huisarts

In het verleden heeft de cliënt ingestemd met de verwijzing naar de thuiszorgorganisatie door de huisarts. Ook is de huisarts nog betrokken bij de zorg voor de thuiszorg-cliënt. De Wgbo stelt dat er vanuit die gedachte sprake is van een vorm van gedeelde of ketenzorg: huisarts en VVT-organisatie verlenen samen zorg aan dezelfde patiënt. Hiermee is de huisarts te beschouwen als medebehandelaar. Daarmee heeft de huisarts veronderstelde toestemming van de cliënt voor inzage van het dossier. Belangrijk: dit geldt alleen voor de huisarts zelf. Andere zorgverleners of medewerkers van een huisartsenpraktijk hebben dit dus niet zomaar ook.

> **Discussie**: Verder specificeren wat ‘Inzage’ hier precies inhoudt en onderbouwen of deze inzage ook echt ‘Inzage’ inhoudt, of alleen bijvoorbeeld het regelmatig delen van updates/brieven met de huisarts.

Vanuit zorgvuldigheid is het wel verstandig om de toestemming, ook al is die verondersteld, toch expliciet op te nemen, bijvoorbeeld door in de zorgovereenkomst met de cliënt op te nemen dat de zorgorganisatie met elke zorgverlener gegevens mag delen, mocht dat voor een goede zorgverlening noodzakelijk zijn.

AVG: Afspraken tussen Verwerkingsverantwoordelijke en Verwerker

De AVG schrijft specifieke rollen en verantwoordelijkheden voor rondom het verwerken van gegevens van een persoon. Bij inzage door de huisarts in het thuiszorg-cliëntdossier, is een logische rolstructuur rondom dataverwerking de volgende: de VVT-organisatie is Verwerkingsverantwoordelijke; de huisarts is Verwerker. De Verwerkingsverantwoordelijke bepaalt de grondslag (het waarom) en op welke wijze de huisarts als Verwerker de verwerkingsactiviteit Inzage mag uitvoeren.

De VVT-organisatie geeft als Verwerkingsverantwoordelijke de huisarts als Verwerker instructies hoe de gegevens uit het cliëntdossier te verwerken zijn (vaak via een Verwerkersovereenkomst). Het is goed om daarbij rekening te houden met bestaande kaders en cliëntafspraken. Andere aspecten die hierin rondom de use case van belang kunnen zijn:

- Specifiek vastleggen wie de huisarts is (op persoonsniveau)
- Hoe om te gaan met allerlei soorten wijzigingen
- Hoe om te gaan met (tijdelijke) vervanging van de huisarts
- Hoe om te gaan met evt. delegering van de inzagebevoegdheid door de huisarts binnen de praktijk

Concreet betekent dit dat de technische authenticatie-opzet mogelijk ingericht moet worden op twee niveaus, verschillend per leverancier:

1. Herkenning op organisatieniveau: tussen het ECD-systeem van de thuiszorgorganisatie en het HIS-systeem van de huisarts. Hiertussen is mogelijk alleen identificatie tot op organisatieniveau mogelijk, bijvoorbeeld via een api-endpoint. Wellicht zijn er ook mogelijkheden te verkennen die wel herkenning tot op persoonsniveau mogelijk maken, maar bij de voorgestelde api-endpoint is dit lastig.
2. Identificatie/autorisatie op persoonsniveau: Binnen het HIS-systeem van de huisarts. Binnen dit systeem is in te richten, vast te leggen en te loggen wie gebruik mag maken en heeft gemaakt van de koppeling met het ECD-systeem. De logging moet voldoen aan de NEN7513.

> **Discussie**: Gecertificeerd zijn op de NEN7513 zou het risico op niet afdoende logging afdekken. Hoe wordt er gecertificeerd voor de NEN7513? Dus hoe kun je aantonen dat je hieraan voldoet? En is dat dan voldoende ‘risico-afdekking’ voor het risico dat de logging mogelijk niet specifiek genoeg is, of is dat een te zwakke mitigering en is meer nodig dan ‘NEN7513’ gecertificeerd zijn?

> **Discussie**: Een alternatieve opzet zou ook kunnen zijn om zowel de VVT-organisatie als de huisarts beide als Verwerkingsverantwoordelijke te zien en om vanuit die case samen te bepalen wat het doel van de verwerking gaat zijn, maar dit is voor deze concrete use case wellicht te uitgebreid. Kan wel relevant zijn bij andere cases rondom netwerkzorg.

Technisch en organisatorische aspecten

De informatie hierboven laat zien dat de risico’s die bij de inzage door de huisarts van een thuiszorg-cliëntdossier komen kijken, niet zwart-wit zijn en ook niet volledig technisch te borgen zijn. Goede keuzes, afspraken en instructies zijn daarom belangrijk om risico’s zoveel mogelijk te beheersen en te beperken.

Overzicht van mogelijke risico’s

Een overzicht van een aantal mogelijke risico’s rondom deze use case staat in de volgende tabel:

Situatie	Risico	Oorzaak risico	Mitigeringsoptie

Verkeerde huisarts bij cliënt vastgelegd	Verkeerde huisarts krijgt inzage	Organisatorisch	VVT-organisatie: In eigen werkprocessen zorgvuldig inregelen
Geen expliciete toestemming van cliënt voor inzage	Niet echt risico, wel ‘grijs gebied’ en ruimte voor verschil van opvattingen van VVT versus cliënt.	Organisatorisch	VVT-organisatie: Toestemmingen vooraf duidelijk in zorgovereenkomst vastleggen
Onzekerheid over sterkte en correcte inzet van authenticatiemiddel (b.v. UZI)	Risico dat het authenticatiemiddel niet identificeert dat de persoon die inzage vraagt, niet de feitelijke persoon is die inzage mag hebben (middel is niet sterk genoeg, middel wordt misbruikt, etc.) Hieruit volgt mogelijk onrechtmatige inzage.	Technisch Organisatorisch	VVT-organisatie: Een sterk authenticatiemiddel op persoonsniveau inzetten
Middelen om organisatie achter inzage-vragende zorgverlener te identificeren, zijn niet adequaat genoeg. Daarom vertrouwt men nu: • op een verklaring van een leverancier over de identiteit van de klant en; • op de door de leveranciers ingerichte processen over de kwaliteit van die bewering.	Risico dat niet gesignaleerd wordt dat het verzoek afkomstig is van een vertegenwoordiger van een organisatie zonder behandelingsovereenkomst met de client. Hieruit volgt mogelijk onrechtmatige inzage.	Technisch Organisatorisch	Technisch en organisatorisch: • Technische afdichting door werken met gezamenlijke technische infrastructuur • Afspraken met aansluitcriteria opstellen
Afhankelijkheid van de kwaliteit van en de opzet van de interne organisatie binnen huisartsenpraktijk	Allerlei risico’s	Organisatorisch	VVT-organisatie: Duidelijke instructie aan huisarts om belangrijkste mogelijke risico’s rondom afhankelijkheid van diens bedrijfsvoering te beperken.

Cliënt wil recht als betrokkene uitoefenen om te weten wie cliëntdossier heeft ingezien.	VVT-organisatie: risico dat de gevraagde gegevens niet adequaat opgeleverd kunnen worden, door: • afhankelijkheid van kwaliteit van logging van HIS • geen directe toegang/inzage/invloed op logging door HIS	Technisch, Organisatorisch	VVT-organisatie: Afhankelijkheid van HIS inperken door als VVT-organisatie zelf iets anders te regelen op technisch én/of organisatorisch gebied. Certificering voor NEN7513 op orde hebben
Inzage-opzet generiek uit willen breiden naar (veel) huisartsen uit de regio.	Opzet is mogelijk niet makkelijk schaalbaar naar eenzelfde opzet voor allerlei verschillende huisartspraktijken in de regio. • Ingewikkeld • Papierwerk op orde • Afspraken per huisartsenpraktijk lastig te ‘generaliseren’	Technisch (verschillende HIS’sen), Organisatorisch	Technisch en organisatorisch: • Technische afdichting door werken met gezamenlijke technische infrastructuur • Afspraken met aansluitcriteria opstellen

Revision #2
Created 2024-03-12 08:51:19 UTC by Steven van der Vegt
Updated 2024-12-06 09:27:43 UTC by Steven van der Vegt