Format

Plan van aanpak eOverdracht

Samenwerken aan eOverdracht

Versie 1.1

20 feb 2024

Documentbeheer

|  |  |
| --- | --- |
| Documentnaam | Plan van aanpak eOverdracht |
| Versienummer definitief document |  |
| Datum definitief document |  |
| In opdracht van |  |
| Auteur |  |

Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Auteur/review | Samenvatting van de wijzigingen |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distributielijst

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versie | Datum | Naam | Functie | Bedrijf |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Inhoudsopgave

[1 Omschrijving project 4](#_Toc145427008)

[1.1 Aanleiding en achtergrond 4](#_Toc145427009)

[1.2 Probleemstelling 4](#_Toc145427010)

[1.3 Projectdoel 5](#_Toc145427011)

[1.4 Projectscope 5](#_Toc145427012)

[1.5 Gewenste resultaten 5](#_Toc145427013)

[1.6 Betrokken partijen 5](#_Toc145427014)

[1.7 Relaties met andere projecten 6](#_Toc145427015)

[1.8 Uitgangspunten 6](#_Toc145427016)

[1.9 Randvoorwaarden 7](#_Toc145427017)

[2 Projectaanpak 7](#_Toc145427018)

[2.1 Projectfasering 7](#_Toc145427019)

[2.2 Planning van beslismomenten 7](#_Toc145427020)

[3 Projectbeheersing 8](#_Toc145427021)

[3.1 Planning 8](#_Toc145427022)

[3.2 Projectorganisatie 8](#_Toc145427023)

[3.3 Projectrisico’s 8](#_Toc145427024)

[4 Informatiebeveiliging en privacy 10](#_Toc145427025)

[4.1 Stap 1 Strategie 10](#_Toc145427026)

[4.2 Stap 2 Risico’s in kaart brengen 11](#_Toc145427027)

[4.3 Stap 3 Maatregelen 11](#_Toc145427028)

[4.4 Stap 4 Bewaking 13](#_Toc145427029)

[5 Begroting 14](#_Toc145427030)

[6 Communicatie 15](#_Toc145427031)

[7 Opleidingen en scholing 16](#_Toc145427032)

# Omschrijving project

Met dit template kunt u een plan van aanpak maken voor de implementatie van de Informatiestandaard eOverdracht. In het plan van aanpak staan de stappen die nodig zijn om de eOverdracht te implementeren en tot een goed einde te brengen. Alle voorbeeldtekst uit het plan kunt u naar eigen inzichten aanpassen/verwijderen; het dient slechts als handvat.

Kijk gerust ook de website [Samenwerkenaaneoverdracht](https://www.samenwerkenaaneoverdracht.nl) voor meer informatie.

* Voor vragen of ondersteuning kan direct contact worden opgenomen via [eOverdracht@ictu.nl](mailto:eOverdracht@ictu.nl).

## Aanleiding en achtergrond

Ondanks dat gegevens steeds meer digitaal worden vastgelegd, kunnen verpleegkundigen en verzorgenden nog onvoldoende gebruikmaken van de voordelen van digitale vastlegging. Denk aan hergebruiken van gegevens, efficiënt uitwisselen en minder registratielast. Gegevens worden in gescheiden systemen opgeslagen en zijn bovendien niet eenduidig. Hierdoor is er geen uitwisseling tussen systemen en moeten verpleegkundigen extra registraties uitvoeren. En moeten ze hun gegevens nog handmatig overtypen als een cliënt wordt overgeplaatst. Daarnaast is de verpleegkundige overdracht niet volledig en kan zelfs ontbreken. De verpleegkundige overdracht is dan ook een kwetsbaar onderdeel in het zorgproces. Hierdoor ontstaan risico’s in de zorg voor de cliënt.

Om de kwaliteit van de overdracht tussen verpleegkundigen en verzorgenden te verbeteren, is door het Informatieberaad Zorg een Informatiestandaard voor de verpleegkundige overdracht vastgesteld: eOverdracht. Dit is een verzameling afspraken die ervoor moet zorgen dat de zorginformatie met de juiste kwaliteit van de ene naar de andere zorginstelling wordt overgedragen. Zodat de kwaliteit en continuïteit van de informatie in de verpleegkundige overdracht wordt verbeterd.

## Probleemstelling

De implementatie en borging van de verpleegkundige overdracht wordt verschillend en niet volledig opgepakt. Dit heeft gevolgen voor de:

* continuïteit en kwaliteit van zorg. De overdracht wordt vaak in papieren vorm met de cliënt meegegeven of wordt nagestuurd. Verpleegkundigen moeten de gegevens handmatig invoeren in hun systeem. Dat betekent dat zij navraag moeten doen bij de patiënt of mantelzorger en bedenken hoe de informatie moet worden omgezet naar gegevens in hun systeem. Verschil van interpretatie en verlies van informatie kunnen voorkomen. Hierdoor kunnen fouten ontstaan en wordt de zorg niet altijd even goed uitgevoerd.
* registratielast (uitvoerend niveau). Verpleegkundigen zijn veel tijd kwijt aan het omzetten van informatie in hun systeem. Gegevens moeten vaak nog handmatig worden ingevoerd omdat gegevens niet kunnen worden hergebruikt
* belemmering van het overdrachtsproces (beleidsniveau). Verpleegkundigen, transferverpleegkundigen en wijkverpleegkundigen houden zich bezig met de overdracht van een cliënt. Aangenomen wordt dat verpleegkundigen gemiddeld minimaal 20 minuten bezig zijn met een overdracht en dat er ongeveer 500.000 verpleegkundige overdrachten per jaar zijn.

## Projectdoel

Verpleegkundigen in de regio dragen gegevens van een cliënt digitaal, gestandaardiseerd, beveiligd en met toestemming van de cliënt, over aan verpleegkundigen die de zorg overnemen in een andere zorginstelling. Het gaat hier om gegevens die nodig zijn voor continuïteit en kwaliteit van de zorg. De effecten zijn zichtbaar op uitvoerend niveau en op organisatieniveau.

## Projectscope

De scope van het project is de overdracht door verpleegkundigen van cliënten naar een andere zorginstelling of zorgsetting.

Besloten is om de volgende use case(s) te gebruiken.

De volgende use cases kunnen worden geïmplementeerd:

* Uitwisseling gegevens van ziekenhuis naar thuiszorg.
* Uitwisseling gegevens van thuiszorg naar ziekenhuis.
* Uitwisseling gegevens van ziekenhuis naar verpleeghuis.
* Uitwisseling gegevens van verpleeghuis naar ziekenhuis.
* Uitwisseling gegevens van ziekenhuis naar gehandicaptenzorg.
* Uitwisseling gegevens van gehandicaptenzorg naar ziekenhuis.
* …

## Gewenste resultaten

De gewenste resultaten zijn (hieronder is het interoperabiliteitsmodel van Nictiz als handvat gebruikt):

* Op het niveau van organisatiebeleid: [vul aan, denk aan beleidsafstemming: bestuurlijk commitment, rollen en verantwoordelijkheden, veranderen werkwijze]
* Op het niveau van zorgproces: [vul aan, denk aan samenwerking; (aan)meld-, overdrachts- en afrondingsfase]
* Op het niveau van informatie: [vul aan, denk aan het groeimodel; fasering van zibs.]
* Op het niveau van applicatie: [vul aan, denk aan koppelen van systemen; gebruiken van FHIR profielen]
* Op het niveau van IT-infrastructuur: [vul aan, denk aan de wijze waarop de berichten worden verzonden, ‘de snelweg’]

## Betrokken partijen

Benoem hier de zorginstellingen en eventuele ICT-leveranciers uit uw samenwerkingsverband. Zie ook het format voor de stakeholdersanalyse om de betrokken partijen te benoemen.

## Relaties met andere projecten

Benoem hier andere projecten van implementatie van gegevensuitwisseling die van invloed zijn op de implementatie van de eOverdracht.

## Uitgangspunten

Vul hieronder eventueel aan met uitgangspunten uit de eigen organisatie en/of het samenwerkingsverband.

**Proces- en informatieniveau**

* Het overdrachtsproces bestaat uit:
  + een (aan)meldfase;
  + een overdrachtsfase;
  + een afrondingsfase.
* Alle inhoudelijke zorggegevens die worden vastgelegd in het elektronisch zorgdossier[[1]](#footnote-2) zijn de bron.
* De basis van de verpleegkundige overdracht is het direct uitwisselen van de standaard (zibs) tussen het elektronisch zorgdossier van zorginstelling A en B.
* Zowel de zibs voor de aanmelding als die voor de overdracht zijn gebaseerd op de informatiestandaard eOverdracht.
* De zibs uit de informatiestandaard eOverdracht worden met een zogenoemd groeimodel stap voor stap geïmplementeerd.
* Eventueel gebruik van een makelaarsfunctie (transfersysteem) is alleen voor het ondersteunen van het overdrachtsproces zodat vraag en aanbod op elkaar kunnen worden afgestemd. Dit betekent dat alleen de minimale gegevens om de cliënt te kunnen volgen in het overdrachtsproces worden vastgelegd.
* Het (extern gehoste) transfersysteem heeft geen zorg-/medisch inhoudelijke dossierfunctie en in dit systeem worden geen zibs opgeslagen.
* Indien binnen de organisatie dataverwerking, -opslag plaatsvindt door middel van een makelaar/integratieoplossing, dan kan deze ook zibs verwerken/opslaan; ook hier geldt dat de makelaar geen functie als zorg-/ medisch inhoudelijk dossier heeft.

**Technisch niveau**

* Voor het uitwisselen van gegevens wordt gebruik gemaakt van HL7 FHIR profielen, voor zowel de aanmeldings- als overdrachtsfase.
* Het elektronisch zorgdossier moet vanuit een ander systeem een HL7 FHIR profiel kunnen ontvangen. De ontvangen gegevens moeten kunnen worden verwerkt in het eigen systeem.
* Uitwisseling van gegevens is nadrukkelijk een proces van zowel ziekenhuis naar VVT als van VVT naar ziekenhuis.
* De gebruikte infrastructuur voor berichtuitwisseling sluit aan bij en is afgestemd op de oplossingen die op landelijk niveau zijn of worden vastgesteld.

## Randvoorwaarden

* De deelnemende zorginstellingen zijn verantwoordelijk voor de interne projectorganisatie
* De deelnemende zorginstellingen hebben bestuurlijke commitment om deel te nemen aan het project.
* De ICT-leveranciers van de deelnemende zorginstellingen zijn betrokken bij het project.
* V&VN is verantwoordelijk voor de ontwikkeling en het actueel houden van de Informatiestandaard.
* Nictiz is verantwoordelijk voor het opleveren en actueel houden van de technische standaarden, zoals van HL7 FHIR, de zibs en het functioneel ontwerp.

# Projectaanpak

## Projectfasering

De projectaanpak bestaat uit de volgende fasen:

* Voorbereidingsfase.
* Test- en acceptatiefase.
* Realisatiefase.
* Evaluatie- en borgingsfase.

Werk elke fase uit. In Bijlage 1 ziet u hiervan een voorbeeld. Vermeld hierbij ook expliciet de startdatum en de einddatum van het project.

## Planning van beslismomenten

Om deze planning te maken kunt u het schema hieronder invullen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Beslismoment | Onderwerp | Wie | Wanneer | Hoe |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Projectbeheersing

## Planning

Maak een planning voor de hele looptijd van het project.

## Projectorganisatie

Zo ziet de projectorganisatie eruit: [voeg een organogram in]

Beschrijf de projectorganisatie en ga daarbij uit van:

* Opdrachtgever.
* Opdrachtnemer.
* Organisatie van het samenwerkingsverband (het projectteam).
* Organisatie van het project binnen uw instelling (het projectteam).

### Rollen en verantwoordelijkheden

Vul hieronder van alle partijen uit uw projectorganisatie de personen, rollen en verantwoordelijkheden in. Beschrijf ook hoe de besluitvorming is belegd en het zogenoemde escalatiepad.

|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Functie/rol en organisatie | Verantwoordelijkheid | Intern/Extern |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Projectrisico’s

Beschrijf welke mogelijke risico’s aanwezig zijn die belemmerend werken voor de aanpak van het project. Beschrijf ook welke maatregelen kunnen worden genomen. Hieronder zijn voorbeelden ingevuld.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Beschrijving projectrisico | Kans | Impact | Te nemen maatregel |
| 1. | Geen overeenstemming binnen project over aanpak en werkwijze. | Klein | Groot | Overleg over te nemen maatregel. |
| 2. | Onvoldoende draagvlak van beroepsgroep binnen zorgorganisaties. | Midden | Groot | * Probleemanalyse. * Betrekken van gebruikers bij implementatie. * Breed inzetten op communicatie. |
| 3. | Het niet kunnen waarmaken door leveranciers van inbouwen van (een deel van) eOverdracht volgens de specificaties. | Groot | Groot | Escaleren. |
|  |  |  |  |  |
|  |  |  |  |  |

# Informatiebeveiliging en privacy

Goede informatiebeveiliging en privacy is onlosmakelijk verbonden met het leveren van goede zorg. Bepaalde wetgeving en regels helpen ons hierbij, zie bijlage 2. Bij deze wetgeving wordt verwezen naar de NEN7510, NEN7512 en NEN7513. Als zorgorganisatie zijn we verplicht om te voldoen aan deze normen. De belangrijkste normen zijn:

* NEN 7510: Zorgdragen dat het elektronisch uitwisselingssysteem voldoet aan de veiligheids- en zorgvuldigheidseisen, zoals het vastleggen van beleid, procedures en verantwoordelijkheden rondom gebruikte elektronische uitwisselingssystemen en interne zorginformatiesystemen.
* NEN 7512: Zorgdragen dat gebruik wordt gemaakt van veilige verbindingen, zoals specificeren van de plichten en de daaraan verbonden vereisten in de zorgprocessen van alle organisaties in de keten.
* NEN 7513: Zorgdragen dat een betrouwbaar overzicht geleverd kan worden van de gebeurtenissen waarbij persoonlijke gezondheidsinformatie is verwerkt en dat deze informatie bijgehouden wordt.

**Wie?**

De Informatieveiligheidsprofessional in de organisatie, zoals de Chief Information Security Officer (CISO) of Functionaris Gegevensbescherming (FG) kan hierover advies geven.

**Hoe?**

Volg de volgende vier stappen om een goede start te maken met informatiebeveiliging en privacy bij de eOverdracht. Maak daarbij gebruik van dit format Plan van aanpak. Afhankelijk van de huidige situatie zullen eventueel extra acties uitgevoerd moeten worden. Neem hiervoor contact op met Bureau eOverdracht via [eOverdracht@ictu.nl](mailto:eOverdracht@ictu.nl).

De genoemde punten onder elke stap zijn voorbeelden/stappen om te komen tot meer informatieveiligheid. Beoordeel aan de hand van de behoeftes en context van jouw organisatie welke aanvullende acties nodig zijn om te voldoen aan bovenstaande normen.

## Stap 1 Strategie

Het helpt om in kleine stappen gestructureerd toe te werken naar meer informatieveiligheid. In deze stap start je met bewustzijn in de gehele zorgorganisatie. Daarnaast is het van belang om een centraal beleid omtrent informatiebeveiliging op te stellen. Wederom is bewustzijn en informatieveilig gedrag daarbij cruciaal. Kies, afhankelijk van jouw situatie, één of meerdere van de volgende stappen:

### Awareness sessie Informatiebeveiliging bij eOverdracht Neem contact op met Bureau eOverdracht voor het inplannen van de Awareness sessie.

### Opstellen beleid informatieveiligheid

### Borgen van de gedragscode gegevensuitwisseling in de organisatie Zie [Gedragscode Elektronische gegevensuitwisseling in de zorg](https://nictiz.nl/publicaties/gedragscode-elektronische-gegevensuitwisseling-in-de-zorg-egiz/)

**Hoe?**

### Denk bij het opstellen van het beleid informatieveiligheid aan onder meer de kenmerken van de organisatie (missie, visie), geldende wet- en regelgeving, risicobereidheid, beleidsuitgangspunten, verantwoordelijkheden, verbetercyclus en het informatiebeveiligingsmanagementforum.

## Stap 2 Risico’s in kaart brengen

Bij de start van elk nieuw project, verwerking en/of applicaties die een (beoogde) verwerking van persoonsgegevens in zich hebben, is het nodig om in het beginstadium (tijdig) advies in te winnen bij de FG (privacy) en de CISO (informatiebeveiliging). Dat geldt dus ook voor de start van het project eOverdracht.

Indien deze functies niet beschikbaar zijn in de organisatie, neem dan contact op met Bureau eOverdracht voor informatie en ondersteuning.

Bij het in kaart brengen van de risico's van het project helpt het om een DPIA uit te voeren. Op dat moment is het namelijk nog mogelijk om met open blik na te denken over de effecten en bestaat er nog voldoende gelegenheid om de uitgangspunten van het projectvoorstel zonder grote nadelige consequenties te herzien. Dit voorkomt ook latere, kostbare aanpassingen in processen, herontwerp van systemen of zelfs het stopzetten van het project.

Je kunt hiervoor het format DPIA gebruiken.

* Zie format DPIA eOverdracht op website samenwerkenaaneoverdracht   
  (is nog in ontwikkeling en volgt spoedig)

### Voor een overzicht met actuele bedreigingen op het gebied van informatiebeveiliging in de zorg, zie onder meer de website [Z-Cert](https://www.z-cert.nl/).

## Stap 3 Maatregelen

Nadat de DPIA is uitgevoerd, ligt de focus op het verlagen van de in kaart gebrachte risico's tot het gewenste risiconiveau (risicobereidheid). Om dit te realiseren dienen maatregelen conform de NEN7510, NEN7512 en NEN7513 opgesteld en geborgd te worden in de organisatie. Gebruik hiervoor het format Context analyse waarbij de huidige – en gewenste situatie in kaart wordt gebracht, zie de website samenwerkenaaneoverdracht.nl

Deze normen schetsen de veiligheidsmaatregelen waaraan uw organisatie dient te voldoen. Stem bij deze implementatie van de maatregelen in de organisatie af wie voor elk risico en maatregel de eigenaar is en leg dit vast in het ISMS (Information Security Management System). Dit ISMS wordt meestal uitgewerkt door de ICT-afdeling van organisatie in samenwerking met de Informatieveiligheidsprofessionals, met formele goedkeuring door de directie.

Indien hier vragen over zijn, neem dan contact op met [eOverdracht@ictu.nl](mailto:eOverdracht@ictu.nl) voor informatie en ondersteuning.

De bovengenoemde NEN-normen bevatten beheersmaatregelen die in het ISMS geborgd worden. Vanuit de processtappen van de eOverdracht gaat het om onder meer om de volgende acties:

1. Inloggen EPD/ECD[[2]](#footnote-3)
   1. Zorg voor veilige en betrouwbare aanmeldprocedures voor gebruikers (inloggen, identificatie en authenticatie).
   2. Zorg voor logging van alle gebeurtenissen in het EPD/ECD en controle op deze logging.[[3]](#footnote-4)
2. Aanmelden vervolgzorg
   1. Classificeer de gegevensuitwisseling rondom de drie zekerheidsaspecten (beschikbaarheid, integriteit en vertrouwelijkheid)
   2. Stel een uitwisselovereenkomst op met de communicerende partijen waarin deze zekerheidsaspecten geborgd zijn.
   3. Zorg dat de gegevens beschikbaar gesteld in het aanmeldbericht niet herleidbaar zijn tot een persoon.
   4. Zorg dat de encryptie conform de NEN7510 is toegepast
3. Versturen eOverdracht
   1. Maak gebruik van de juiste identificatie en authenticatie hulpmiddelen om de identiteit van de verzender vast te stellen[[4]](#footnote-5)
4. Verwerken eOverdracht
   1. Zorg dat er een controle op behandelrelatie bij raadpleging en verwerken van de overdracht (grondslag)

Ook is het van belang om informatieveilig gedrag van medewerkers te stimuleren.

* Workshop: Informatieveilig gedrag in de zorg

Vragen hierover, neem contact op met [eOverdracht@ictu.nl](mailto:eOverdracht@ictu.nl) voor het inplannen van de workshop Informatieveilig gedrag in de zorg.

## Stap 4 Bewaking

Zodra alle risico's en maatregelen voldoende geborgd zijn is het belangrijk om te zorgen dat deze maatregelen ook effectief blijven. Er zijn verschillende zaken van belang in het bewaken van je organisatie. Zo is het handig om een meerjarig intern auditprogramma in te stellen, zodat je als organisatie zicht blijft houden op de staat van informatiebeveiliging. Deze audits leveren namelijk inzicht in hoeverre je je op het gewenste niveau bevindt. Daar waar nodig is het zo ook mogelijk om verbeteringen uit te voeren. Door het vastleggen van de risico’s, incidenten, maatregelen en audits in het informatiebeveiligingsmanagementsysteem behoud je grip en overzicht over de voortgang van het continue verbeterproces.

Bij een positieve uitkomst van de interne audit kan de volgende stap zijn om een collegiale review uit te voeren. Vervolgens kan je je als zorgorganisatie certificeren. Indien afwijkingen worden gevonden dienen corrigerende maatregelen te worden geïmplementeerd. Bovendien is het van belang om te blijven controleren op de naleving van de maatregelen, zoals een jaarlijkse interne audit.

**Hoe?**

Er zijn verschillende manieren om interne audits uit te voeren. Allereerst kan door uw organisatie zelf worden gekeken naar aan welke eisen u moet voldoen, te onderzoeken in hoeverre u hier nu al aan voldoet, en zo een fit-gap analyse uit te voeren. Het is ook mogelijk om een collegiale review te doen, waarbij een collega-organisatie een audit uitvoert. Daarnaast is het mogelijk om deze taak uit te besteden aan een van de vele commerciële audit partijen. Mocht er uit deze analyse blijken dat er tekortkomingen bestaan in de huidige informatiebeveiliging, dan kan vervolgens worden gekeken hoe deze hiaten kunnen worden opgevuld met corrigerende maatregelen.

Hoewel het als zorginstelling niet verplicht is om je te certificeren voor de NEN-normen en andere beveiligingsstandaarden, moet u wel aantoonbaar voldoen aan de NEN7510. U kunt daarom overwegen om u te laten certificeren. Er zijn verschillende marktpartijen die certificeringsdiensten aanbieden.

# Begroting

Hierbij kun je het format voor de begroting gebruiken dat je kunt vinden op de pagina Instrumenten en downloads op deze website.

# Communicatie

Hierbij kun je het format voor de communicatie gebruiken dat je kunt vinden op de pagina Instrumenten en downloads op deze website.

# Opleidingen en scholing

Hierbij kun je het format voor een opleidingsplan gebruiken dat je kunt vinden op de pagina Instrumenten en downloads op deze website.

Bijlage 1: Voorbeeld projectaanpak eOverdracht

1. **Voorbereidingsfase**

Voorbereiding van het proces

* U maakt een draaiboek voor de overgang naar de nieuwe werkwijze.
  + Opzetten van de testfase: bepalen van de criteria en de cliëntengroep die in de testfase wordt overgedragen.
  + Bepalen wie de testfase uitvoert en waar deze plaatsvindt.
  + Bepalen wanneer de testfase start.
  + Vastleggen van afspraken over de overgang van de oude naar de nieuwe werkwijze.
  + Beschrijven van de taakverdeling van betrokken medewerkers.
  + In kaart brengen van aanwezige ondersteuning vanuit ICT en beleid in de verschillende fases van de implementatie.
* U zorgt voor de interne communicatie.
  + Presenteren van het project aan (teams van) de zorginstellingen.
  + Informeren van de cliënten- en patiëntenraad en de Verpleegkundige en/of Verzorgende Adviesraad.
  + Maken van informatiemateriaal voor betrokken cliënten/patiënten.
* U bereidt de organisatie voor.
  + Uitwerken van de nieuwe werkwijze voor de wijkverpleegkundige en de (transfer)verpleegkundige.
  + Opzetten van werkgroepen en zogenoemde superusers voor begeleiding en aanspreekpunten.
* U past de werkinstructie of het protocol aan.
  + Beschrijven van de nieuwe werkinstructie of het nieuwe protocol voor de eOverdracht.
  + Beschrijven van de werkinstructie voor aanpassingen in het elektronisch zorgdossier (zowel ECD als EPD).
* U maakt afspraken over feedback over de kwaliteit van de ontvangen overdracht.
  + Bijhouden of en wanneer een overdracht is verstuurd en ontvangen.
  + Bijhouden of een aanmelding overeenkomt met de zorgvraag.
  + Bijhouden of de gegevens van een overdracht volledig en eenduidig zijn.
* U stelt een digitaal logboek op om de feedback bij te houden.

Voorbereiding van de techniek

* U maakt gebruik van een technisch ontwerp voor de overgang naar de nieuwe werkwijze.
  + [Specificaties](https://www.nictiz.nl/standaardisatie/informatiestandaarden/verpleegkundige-overdracht/) van de nieuwe overdrachtsroute: HL7 FHIR profielen en koppelingen. Dat doet u samen met informatieanalisten van de zorginstellingen, ICT-leveranciers en de regionale samenwerkingsorganisatie (RSO).
  + Specificaties van de route via infrastructuur met RSO en betrokken leveranciers.
  + Opzet van HL7 FHIR profielen (volgens eerdergenoemde specificaties) voor de overdracht.
  + Planning van de implementatie van de zibs voor eOverdracht.
  + Specificaties voor het rechtstreeks kunnen uitwisselen van berichten tussen ziekenhuis en thuiszorg.
  + Specificaties voor de makelaar (het transfersysteem); alleen te gebruiken voor capaciteitsplanning en procesondersteuning.
* U past de inrichting van het elektronisch zorgdossier van de thuiszorg aan.
* Specificeren hoe de aanmelding in thuiszorg na ontslag van patiënt uit het ziekenhuis wordt ontvangen in het elektronisch zorgdossier.
* Specificeren hoe gegevens uit een overdrachtsbericht worden ontvangen vanuit het ene in het andere elektronisch zorgdossier.
* Specificeren hoe gegevens uit een overdrachtsbericht worden gevalideerd en geïmporteerd in het elektronisch zorgdossier.
* Melding maken in het elektronisch zorgdossier van de thuiszorg als cliënt wordt opgenomen in het ziekenhuis.
* Specificeren welke gegevens uit de bron moeten worden geselecteerd voor een overdrachtsbericht van het ene naar het andere elektronisch zorgdossier.
* Specificeren van de wijze van versturen van HL7 FHIR profielen naar het ziekenhuis.
* U past de inrichting van het elektronisch zorgdossier van het ziekenhuis aan.
  + Specificeren welke gegevens uit de bron moeten worden geselecteerd voor aanmelding van patiënt voor vervolgzorg (via het tussensysteem naar het elektronisch zorgdossier).
  + Specificeren welke gegevens uit de bron moeten worden geselecteerd voor een overdrachtsbericht van het ene naar het andere elektronisch zorgdossier.
  + Specificeren van de wijze van versturen van HL7 FHIR profielen naar de thuiszorg.
  + Specificeren hoe gegevens uit een overdrachtsbericht worden ontvangen vanuit het ene in het andere elektronisch zorgdossier.
  + Specificeren hoe gegevens uit een overdrachtsbericht worden gevalideerd en geïmporteerd in het elektronisch zorgdossier.
* **Te behalen mijlpaal: er is een draaiboek voor de realisatie.**

1. **Test- en acceptatiefase**

* U start de testprocedure van een berichtuitwisseling tussen zorginstellingen. Daarna zet u de berichtuitwisseling klaar voor productie.
* **Te behalen mijlpaal: de systemen zijn klaar voor het in productie nemen van gegevensuitwisseling volgens het technisch ontwerp.**

1. **Realisatiefase**

In de realisatiefase wordt dat wat in de testfase is getest daadwerkelijk uitgevoerd.

Realisatiefase proces eOverdracht

* U organiseert een kick-off bijeenkomst voor de start van de implementatie.
* De implementatie start volgens het eerder gemaakte draaiboek.
* Cliënten zijn geïnformeerd en hebben toestemming gegeven voor uitwisseling van gegevens volgens eOverdracht.
* Er is regionale afstemming over de voortgang.
* U gebruikt het digitale logboek bij knelpunten.

Realisatiefase techniek eOverdracht

* De aanpassingen in het elektronisch zorgdossier (volgens het technisch ontwerp) worden in productie genomen.
* Tijdens de realisatiefase wordt de kwaliteit van de gegevensuitwisseling bewaakt.
  + U controleert of de gegevens volgens de afgesproken techniek worden uitgewisseld.
  + U gebruikt het digitale logboek bij knelpunten.
  + U evalueert wekelijks tot de gegevensuitwisseling goed verloopt.
* **Te behalen mijlpaal: gegevens worden volgens de gemaakte afspraken van eOverdracht uitgewisseld.**

1. **Evaluatiefase**

* U beschrijft de resultaten van de realisatiefase en de zogenoemde lessons learned. Ook benoemt u adviezen voor het vervolg.
* **Te behalen mijlpaal: de evaluatie van de realisatiefase is beschikbaar** **en als dat nodig is, wordt er bijgesteld. Verder zijn er afspraken gemaakt om de implementatie te borgen.**

Bijlage 2: Gerelateerde wetgeving

Zorgorganisatie dienen voor de eOverdracht te voldoen aan de volgende– niet uitputtende lijst met - wetgeving, zoals:

* Algemene verordening gegevensbescherming (AVG), daarbij gaat het om rechtmatig omgaan met persoonsgegevens
* De Wet elektronische gegevensuitwisseling in de zorg (Wegiz) verplicht dat gegevensuitwisseling tussen zorgaanbieders elektronisch verloopt
* WGBO (Wet op de geneeskundige behandelingsovereenkomst) – zorgverlener moet verantwoord omgaan met patiëntgegevens (medisch beroepsgeheim) en zorgverlener heeft een dossierplicht.
* Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz): waarborgen voor cliënten bij elektronische gegevensuitwisseling.
* Besluit elektronische gegevensverwerking door zorgaanbieders – verplichting om te voldoen aan NEN 7510 en NEN 7512 in het kader van de verwerking van het burgerservicenummer.
* WDO - Wet Digitale Overheid regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij publieke organisaties. Zorgaanbieders die op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, burgerservicenummers verwerken zijn zogenaamde ‘aangewezen organisatie’ en vallen onder deze wet.
* Network and Information Systems Directive (NIS2) – Deze toekomstige wet schrijft regels en voorschriften voor met betrekking tot cyber security. Deze nieuwe richtlijn wordt omgezet in Nederlandse wetgeving en zal van toepassing zijn op zorgaanbieders (afhankelijk van omzet en aantal medewerkers), waarbij de Raad van Bestuur hoofdelijk aansprakelijk is voor informatiebeveiliging.

**Dit is een uitgave van V&VN**

Juni 2022

1. Elektronisch zorgdossier is een overkoepelende term voor EPD, ECD en professioneel dossier. [↑](#footnote-ref-2)
2. [NEN7510, met name H9 Toegangsbeveiliging](https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg)  [↑](#footnote-ref-3)
3. [NEN7513 Logging](https://www.nen.nl/en/nen-7513-2018-nl-245399)  [↑](#footnote-ref-4)
4. [Opbouw informatie van het aanmeldbericht en overdrachtsbericht](https://informatiestandaarden.nictiz.nl/wiki/vpk:V4.0_Opbouw_eOverdracht_algemeen)   [↑](#footnote-ref-5)