TRUSTCENTRE · DOCUMENTEN

DPIA-template voor zorgorganisaties

Een vertrekpunt voor de eigen beoordeling van je organisatie.

DOCUMENT-ID D08 | VERSIE 4.1.6 | TEKSTREVISIE 4 november 2026

VASTGESTELD 4 november 2026 | VORM Template

Over deze tekst. Je leest de juridische tekst, versie 4.1.6. Deze legt afspraken vast. De publicatie van een afspraak is geen afzonderlijk bewijs dat de technische uitvoering is gecontroleerd. De documentgegevens staan bovenaan.

DPIA-template voor zorgpraktijken en zorginstellingen

Tekstrevisie	4 november 2026. Versie 4.1.6.
Revisie-ID	D08-4.1.6
Tekstdatum	4 november 2026.
Versie	4.1.6, document 08
Documentdatum	4 november 2026
Ingangsdatum	de datum waarop Hysio deze versie in het TrustCentre publiceert
Voorgangers	versie 4.1.5 en versie 4.0, tekstdatum 15 september 2026, gepubliceerd op 16 september 2026 (Revisie-ID D08-PUB-20260915)
Taal	Nederlands
Uitgever	Hysio B.V.

Gegevensbeschermingseffectbeoordeling voor de inzet van Hysio binnen je organisatie. Onderdeel van de juridische set Hysio Zorg, versie 4.1.6, en van de bijstand uit artikel 16 van de Verwerkersovereenkomst. Begrippen met een hoofdletter hebben de betekenis uit artikel 1 van de Algemene Voorwaarden.

Deze template bevat leveranciersinformatie en invulonderdelen voor je eigen organisatie. Zij is een informatief document bij de Verwerkersovereenkomst. De normen voor de dienstverlening van Hysio in deze template zijn verplichtingen van Hysio uit de Verwerkersovereenkomst en de Regeling Datatoegang; bij verschil gaan die documenten voor. Per maatregel staat in 3.3 of die bij de ingangsdatum van deze versie is ingericht of een toezegging is die vanaf een genoemde mijlpaal geldt. Wat jij zelf regelt, staat bij de invulvelden en in 3.4. Deze template is een hulpmiddel voor jouw

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

eigen beoordeling en vervangt die beoordeling niet. Bij de onderdelen waarvoor je aanvullend bewijs nodig hebt, staat vermeld wat je bij Hysio kunt opvragen; beveiligingsgevoelige gegevens worden onder geheimhouding verstrekt.

Je kunt deze template ook als Word-document downloaden: DPIA-template voor zorgpraktijken, versie 4.1.6. Het Word-document heeft dezelfde tekst en indeling als deze pagina, met daarnaast ruimte om je eigen antwoorden en keuzes in te vullen. Bij verschil geldt deze pagina.

Voor wie is deze template?

Deze template is bestemd voor organisaties en zelfstandige beroepsbeoefenaars die Hysio gebruiken voor verwerking van gegevens over patiënten, cliënten, medewerkers of andere betrokkenen. De toepasselijke regels hangen af van de werkzaamheden en rol van je organisatie. Een beroepsprofiel in Hysio bepaalt die rol of bevoegdheid niet.

Hysio levert ingevulde informatie over het platform, de onderzochte functies en de gekozen dienstverlening. Je organisatie beschrijft de eigen doeleinden, grondslagen, bevolking, werkprocessen, apparatuur, ontvangers en beslissingen. Zij maakt de lokale risicoanalyse en neemt het eindbesluit. Als je zelf als verwerker handelt, moet de feitelijke verwerkingsverantwoordelijke bij de beoordeling en besluitvorming worden betrokken.

De template is geen reeds vastgestelde DPIA van je organisatie. De eigen interne Hysio-DPIA vervangt haar evenmin. Andersom ontslaat jouw beoordeling Hysio niet van haar eigen verplichtingen of van het leveren van juiste, toereikende leveranciersinformatie. Ontbrekend bewijs over Hysio hoef je niet zelf te verzinnen of als bevestigd te beschouwen.

Zo gebruik je deze template.

1. Bepaal met 0.5 of een DPIA voor jou verplicht is. Werk je als individuele zorgprofessional, lees dan ook 0.5.1. Hysio raadt een DPIA ook aan als die niet verplicht is.
2. Neem de informatie over Hysio over uit 1.2, 1.4, 1.9, 1.10 en 3.3.
3. Vul de velden [organisatie vult in] in voor de functies die je echt gebruikt. Wat niet op jou van toepassing is, markeer je met een korte reden. De onderdelen 2.8 tot en met 2.11 vul je alleen in als die context bij jou voorkomt.
4. Beoordeel de risico's in 3.2, leg je eigen maatregelen vast in 3.4 en neem je besluit in 4.5.

Houd daarbij de Verwerkersovereenkomst met Bijlage 1, 2 en 3, de Regeling Datatoegang en de openbare samenvatting van de DPIA van Hysio bij de hand. Vragen over je DPIA stel je via privacy@hysio.nl.

Sectie 0: methodologie, scope en DPIA-plicht

0.1 Methodologie en bewijsstatus

De opbouw volgt de vereisten van AVG artikel 35 lid 7: systematische beschrijving, noodzaak en evenredigheid, risico's voor betrokkenen en de maatregelen om die risico's te behandelen. Je kunt een andere geschikte methode gebruiken als dezelfde onderdelen aantoonbaar worden beoordeeld.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Leg schaal, uitgangssituatie, beslisregels en eventuele afwijkingen vast.

Deze template gebruikt een eigen kwalitatieve methode. Eerst wordt onderzocht of de verwerking zelf rechtmatig, nodig en evenredig is. Daarna worden risico's van het voorziene gebruik én risico's door fouten, misbruik en uitval beoordeeld. Een gunstige beveiligingsscore maakt een onrechtmatig doel niet rechtmatig.

Leg bij elke feitelijke onderbouwing vast: bron, datum, betrokken dienst en omgeving, onderzochte gegevens en beperkingen. Gebruik de volgende statussen:

Status	Betekenis voor de beoordeling
Technisch aangetroffen	De implementatie bevat de beschreven mogelijkheid. Activering en werking in de gebruikte omgeving zijn daarmee nog niet vastgesteld
Configuratie bevestigd	De relevante instelling is voor de genoemde omgeving en datum gecontroleerd; werking en volledige dekking kunnen daarnaast bewijs vragen
Uitvoering waargenomen	De beschreven handeling is onder vastgelegde omstandigheden uitgevoerd; dit bewijst niet automatisch ieder ander pad of toekomstige uitvoering
Verklaring of contract ontvangen	De partij verklaart een feit of aanvaardt een verplichting. Beoordeel of aanvullend uitvoeringsbewijs nodig is
Gekozen beleidsnorm	De norm is door Hysio gekozen; invoering en naleving moeten afzonderlijk blijken
Gedeeltelijk bevestigd, tegenstrijdig of onbekend	De betrokken onzekerheid blijft zichtbaar en verlaagt niet zonder onderbouwing de risicowaardering

De stand die Hysio in 3.3 per maatregel opgeeft, is een verklaring van Hysio. Neem die over als verklaring en beoordeel zelf of je aanvullend uitvoeringsbewijs nodig hebt. Zo neem je de stand over: bij Ingericht noteer je de bewijsstatus Verklaring of contract ontvangen en beoordeel je zelf of je de maatregel als ingevoerd aanmerkt; een toezegging noteer je als gepland.

Noteer voor maatregelen afzonderlijk: **gepland**, **gedeeltelijk ingevoerd** of **ingevoerd en op effectiviteit gecontroleerd**. Een contractuele verplichting kan betekenis hebben, maar telt niet als bewijs van technische verwijdering, versleuteling of menselijke controle.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Het EDPB-sjabloon voor een DPIA (versie 1, vastgesteld op 10 maart 2026, met een consultatie tot 9 juni 2026) is als aanvullende volledigheidscontrole gebruikt. In oktober 2026 is er nog geen eindversie; het is geen verplicht voorgeschreven formulier. De relevante principes zijn verwerkt in deze Hysio-template; je hoeft niet ook een tweede identiek formulier in te vullen.

Onderzoek ook of de verantwoordelijke of een betrokken verwerker een op grond van AVG artikel 40 goedgekeurde gedragscode naleeft. Artikel 35 lid 8 verlangt dat deze naleving bij de effectbeoordeling naar behoren wordt meegewogen. Leg vast welke activiteiten en partijen onder de goedkeuring vallen en welk bewijs de daadwerkelijke naleving ondersteunt. Een gewone beroepscode, een beveiligingsnorm of een voornemen om zich aan te sluiten is niet vanzelf zo'n goedgekeurde gedragscode.

Goedgekeurde gedragscode: [naam, versie, goedkeuringsbesluit, scope, betrokken partijen en bewijs van naleving; of gemotiveerd niet van toepassing]. **Gevolgen voor deze beoordeling:** [organisatie vult in].

Eigen methode, aanvullingen en motivatie: [organisatie vult in].

0.2 Afbakening van de beoordeling

De beoordeling omvat de daadwerkelijk gekozen keten: invoer, lokale herstelopslag, upload, transcriptie, tekstverwerking, tijdelijke opslag, bewerking, levering, gebruik in een ander systeem, bewaring en verwijdering. Neem ook ondersteunende verwerking mee, zoals toegang, foutafhandeling, relevante logging, ondersteuning en back-ups.

Beoordeel ten minste de routes die je gebruikt:

- vrije tekst, vragen, cliëntcontext en documenten;
- opnemen of uploaden van audio, segmenteren en transcriberen;
- brongebonden conceptverslagen, samenvattingen en communicatie;
- Werkstromen met aanvullende overwegingen, hypotheses, vragen, scores of voorstellen;
- gezamenlijke besprekingen waarin meerdere betrokkenen voorkomen;
- kopiëren, downloaden, delen, koppelingen en automatische teruglevering;
- beëindiging, export, rechtenverzoeken en verwijdering.

Een aangrenzend EPD, cliëntportaal, mailkanaal of ontvangend systeem kan niet buiten de analyse blijven wanneer de risico's van de Hysio-route daarvan afhangen. Gebruik een verwijzing naar een bestaande eigen DPIA waar de verwerking aantoonbaar gelijk is en voeg de verschillen toe.

Dat een functie in de catalogus, in een beroepsprofiel of in een testomgeving staat, betekent niet dat zij voor jouw organisatie aan staat of geschikt is. Leg vast welke functies en versies je echt gebruikt. Deze versie geldt voor het webplatform. Voordat een mobiele app algemeen beschikbaar komt, maakt Hysio de opslag op het toestel en de bewaartermijnen daarvan bekend.

Eigen account-, factuur-, website- en bedrijfsverwerkingen van Hysio worden in de Privacyverklaring en de eigen DPIA van Hysio onderscheiden; van die DPIA staat een openbare samenvatting bij de juridische documenten. Neem hun raakvlakken met jouw verwerking wel mee, bijvoorbeeld wanneer

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

een supportbericht toch cliëntgegevens bevat.

Eigen scope, uitgesloten onderdelen en reden; gekoppelde beoordelingen: [organisatie vult in].

0.3 Vooraf ingevulde leveranciersinformatie

De Hysio-informatie staat in §1.2, de routebeschrijving in §1.4, de gegevensinventaris in §1.6, de dienstverleners en doorgiften in §1.9, de bewaartermijnen in §1.10 en de maatregelen in §3.3. Zij sluit aan op versie 4.1.6 van de Verwerkersovereenkomst met haar bijlagen en op de Regeling Datatoegang. De ketenopgave per overeenkomst, de doorgiftebeoordeling en de samenvatting van het beveiligingsbeleid ontvang je op verzoek. Hysio publiceert daarnaast een samenvatting van haar eigen DPIA bij de juridische documenten. Gebruik die als leveranciersinput bij 1.9, sectie 3 en 3.3; zij vervangt jouw eigen beoordeling niet.

Hysio bevestigt op verzoek, met datum, welke dienstverleners, instellingen, uitgerolde versies en maatregelen gelden voor de functies die jouw organisatie gebruikt, en bij een nieuwe route vóór de eerste verwerking voor jouw organisatie. Een algemene verklaring over het platform vervangt die bevestiging niet.

Voor je eigen beoordeling, je risico-inventarisatie en het toezicht op de invoering van AI in de zorg levert Hysio op verzoek de volgende vaste leveranciersinformatie:

- bekende foutsoorten en beperkingen per functie;
- informatie over wijzigingen in het model of de instructies die de uitkomst merkbaar raken;
- de incidentroute;
- haar beoordeling van de ingezette AI-dienst, ook van de rechtmatige ontwikkeling van het model, voor zover bekend;
- input voor je risico-inventarisatie en je programma van eisen;
- DPIA-input per toepassing;
- informatie voor de beoordeling onder de AI-verordening die je samen met Hysio maakt;
- de verwijzing naar de bewaartermijnen in Bijlage 1 van de Verwerkersovereenkomst.

Beoordeel een functie in haar concrete gebruikscontext.

Vraag deze informatie op via privacy@hysio.nl. Vertrouwelijke stukken, zoals de doorgiftebeoordeling en de samenvatting van het beveiligingsbeleid, vraag je op via legal@hysio.nl (zie ook 6.4). Hysio verstrekt standaarddocumentatie zonder onnodige vertraging en uiterlijk binnen twintig Werkdagen na een voldoende bepaald verzoek; bij een incident of een wettelijke termijn eerder (Bijlage 4 van de Verwerkersovereenkomst).

0.4 Door je organisatie in te vullen

De velden met **[organisatie vult in]** betreffen jouw omstandigheden: identiteit en rollen, concrete doelen, grondslagen, schaal, Werkstromen, gegevens en ontvangers, lokale maatregelen, eigen risico-inschatting, raadpleging en besluit. Verwijs naar bewijs of bestaande interne documenten en voeg de relevante versie toe.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Maak voor iedere afwijking van leveranciersinformatie onderscheid tussen een eigen aanvullende maatregel en een wijziging van de Hysio-dienstverlening. Een lokaal gekozen kortere termijn werkt pas als je die ook kunt uitvoeren of Hysio de daarvoor benodigde instructie uitvoert. Vraag bij onduidelijkheid feitelijke bijstand via privacy@hysio.nl.

0.5 Trigger-checklist en AP-schaalmatrix

Een DPIA is verplicht wanneer de verwerking waarschijnlijk een hoog risico inhoudt voor rechten en vrijheden, gelet op aard, omvang, context en doeleinden. AVG artikel 35 lid 3 noemt bijzondere gevallen. Het Nederlandse AP-besluit bevat daarnaast specifieke verwerkingen waarvoor een DPIA verplicht is. Toets beide en documenteer de uitkomst vóór de verwerking.

0.5.1 Grootschaligheid in de zorg

Context	Beoordeling
Ziekenhuis, huisartsenpost of zorggroep	De AP beschouwt de verwerking van patiëntgegevens in deze contexten altijd als grootschalig, ongeacht het aantal patiënten
Alle overige zorgaanbieders, waaronder huisartsenpraktijken, fysiotherapie, apotheken en medisch-specialistische instellingen die geen ziekenhuis zijn	De AP hanteert meer dan 10.000 ingeschreven patiënten óf gemiddeld meer dan 10.000 behandelde patiënten per jaar, én hun gegevens in één informatiesysteem
Overige zorgaanbieder die niet aan deze schaalomschrijving voldoet	De genoemde AP-schaalgrond is niet vastgesteld. Beoordeel daarnaast de concrete risico's en eventuele andere gronden voor een DPIA of een FG

Deze matrix volgt de AP-uitleg van 11 december 2018. De AP heeft daarmee haar eerdere uitleg verbreed en de behandeling van apotheken genuanceerd. De getalsgrens is uitleg van de toezichthouder, geen getal uit de AVG en geen algemene vrijstelling voor organisaties onder die grens. Leg ook gegevensvolume, verscheidenheid, duur en geografische reikwijdte vast en onderzoek afwijkende verwerkingen.

De schaaltoets voor jouw organisatie en die voor Hysio als dienstverlener hebben een eigen scope. Tel niet zonder toelichting alle Hysio-klanten bij jouw praktijk op; beschouw de omvang van de leverancierskete wel bij afhankelijkheid, concentratie en mogelijke gevolgen van incidenten. Een kleine organisatie is geen algemene uitzondering op artikel 35 lid 1.

Het AP-besluit over verplichte DPIA's zegt: "individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de Algemene verordening gegevensbescherming uitgezonderd van de verplichting een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren". Deze uitzondering

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

gaat over de individuele beroepsbeoefenaar; een praktijk met meerdere zorgverleners of een instelling valt er niet vanzelf onder.

Los van dit AP-besluit adviseert Hysio een eigen afweging. Bij nieuwe technologie en bijzondere persoonsgegevens kan artikel 35 lid 1 alsnog een DPIA vragen. Hysio raadt daarom een DPIA aan, ook als die voor jou niet verplicht is.

Eigen aantallen, gegevensvolume, duur, bereik en conclusie: [organisatie vult in].

0.5.2 WP248-criteria en aanvullende Nederlandse triggers

Criterium	Toets voor je concrete gebruik
1. Evaluatie of scoretoekenning	Onderzoekt of beoordeelt de gekozen functie persoonlijke aspecten? Denk ook aan hypotheses, functioneren, gezondheid, gedrag en scores
2. Geautomatiseerde besluiten met rechtsgevolg of vergelijkbaar wezenlijk gevolg	Onderzoek de feitelijke invloed en menselijke tussenkomst; een contractuele reviewplicht beantwoordt deze vraag niet
3. Stelselmatige monitoring	Worden personen structureel gevolgd, gecontroleerd of geobserveerd? Een losse notitie bewijst dit niet, een ingerichte reeks kan anders uitpakken
4. Gevoelige of zeer persoonlijke gegevens	Gezondheid, zorginhoud, strafrechtelijke gegevens, gezin, financiën en andere vertrouwelijke informatie kunnen relevant zijn
5. Grootschalige verwerking	Gebruik de afzonderlijke schaalbeoordeling hierboven
6. Combineren van datasets	Beschrijf welke bronnen, doelen en verantwoordelijken worden gecombineerd en wat betrokkenen redelijkerwijs verwachten
7. Kwetsbare betrokkenen	Beoordeel afhankelijkheid en mogelijkheden om rechten uit te oefenen, bijvoorbeeld bij patiënten, kinderen, werknemers of gedwongen zorg
8. Innovatieve toepassing	Beoordeel de nieuwe verwerking en gevolgen van generatieve functies in de concrete context

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Criterium	Toets voor je concrete gebruik
9. Belemmering van rechten, diensten of overeenkomsten	Wordt toegang tot zorg, ondersteuning, werk of een ander wezenlijk belang afhankelijk van de verwerking of output?

Twee toepasselijke criteria wijzen doorgaans op de noodzaak van een DPIA. Dit is een beoordelingshulp, geen mechanische wettelijke optelsom. Eén criterium kan voldoende zijn. Motiveer een conclusie dat ondanks meerdere criteria geen DPIA nodig is. Doorgifte naar een derde land is geen tiende WP248-criterium, maar hoort wel in de inhoudelijke analyse.

Toets in Nederland daarnaast de precieze omschrijvingen van het AP-besluit. Naast categorie 7 over grootschalige gezondheidsgegevens kunnen onder meer samenwerkingsverbanden in het sociaal domein, controle van werknemers en systematische uitgebreide profilering relevant zijn. Een losse beroepsnaam of de aanwezigheid van AI is niet hetzelfde als voldoen aan alle voorwaarden van zo'n categorie. Er zijn voorstellen voor lijsten met verwerkingen waarvoor geen DPIA nodig is. Die gelden nu niet.

Voor nieuwe generatieve functies op gezondheidsgegevens is het werkadvies van Hysio daarom: voer de beoordeling uit, ook als nog onzeker is of die wettelijk verplicht is. Daarmee verklaart Hysio niet dat iedere klant dezelfde DPIA-plicht heeft.

Uitkomst: [ ] verplicht [ ] vrijwillig uitgevoerd [ ] gemotiveerd niet verplicht. **Bepalingen, criteria, motivering en FG-advies indien aangewezen:** [organisatie vult in].

0.6 Beroepscategorie en toepasselijke regimes

Leg de feitelijke werkzaamheden vast, niet alleen de naam van het geselecteerde profiel. Een beroepsgroep kan onder verschillende regels werken. Hysio biedt op dit moment geen Familiemodules aan; deze template geldt voor alle beroepen. Een keuze voor een beroepsprofiel in het platform bepaalt je rol of bevoegdheid niet. Let in elk geval op de scheiding van medische en werkgeversinformatie (2.10), kinderen en vertegenwoordiging (2.8), gegevens over dieren (2.11) en het ontbreken van gedeelde toegang in een wijkteam of multidisciplinair overleg (1.3 en 1.7).

Context	Ten minste te bepalen
Behandeling van mensen	Toepasselijkheid WGBO, beroepsgeheim, titel en bekwaamheid, dossier- en gegevensuitwisselingsregels
Jeugd, maatschappelijke ondersteuning en sociaal werk	Wie de taak uitvoert, sectorale grondslag, ontvangers, vertegenwoordiging en eigen dossierregels

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Context	Ten minste te bepalen
Arbeid, bedrijfsgezondheid en keuringen	Opdracht, onafhankelijke medische rol, werkgeversschot, doel van de rapportage en eventuele keuringsrechten
Verplichte of onvrijwillige zorg, forensische context	Toepasselijke bijzondere wet, bevoegdheden en welke documenten juridische gevolgen hebben
Veterinaire werkzaamheden	Persoonsgegevens van eigenaren, medewerkers en derden; diergeneeskundige inhoud is niet uitsluitend door haar medische karakter een gezondheidsgegeven van een mens
Beroepsnorm voor AI en opname	Wat je beroepsorganisatie of toezichthouder zegt over AI bij verslaglegging en opname; zie het overzicht in hoofdstuk 4 van de Disclaimer. Voor jeugdhulp bestaan volgens de IGJ nog geen veldnormen voor digitale zorg; gebruik dan de normen voor zorgaanbieders als referentie
Cyberbeveiligingswet	Valt je organisatie eronder? Dat hangt af van de sector uit de bijlagen van de wet, voor de zorg de zorgaanbieder in de zin van de Wkkgz, en van de omvang: vanaf 50 fte, of jaaromzet én balanstotaal boven 10 miljoen euro, met verbonden organisaties meegeteld. Een aanwijzing als kritieke entiteit geldt altijd. Zo ja: verbind deze DPIA met je ketenbeveiligingsbeleid; de DPIA blijft een AVG-instrument
Meldroute bij een incident of calamiteit	Datalekken aan de Autoriteit Persoonsgegevens (AVG artikel 33 en 34); calamiteiten volgens de Wkkgz, de Jeugdwet of de Wmo 2015 aan de Inspectie Gezondheidszorg en Jeugd of de bevoegde gemeentelijke toezichthouder; waar van toepassing significante incidenten onder de Cyberbeveiligingswet

Werkzaamheden, beroepsbevoegdheid, regime en beroepsnorm voor AI en opname: [organisatie vult in].

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

0.7 DPIA-team

Rol	Eigen invulling en taak
Verwerkingsverantwoordelijke en bevoegde besluitvormer	[organisatie vult in]; bepaalt doelen, maatregelen en besluit
Privacycoördinator	[organisatie vult in]; verzamelt en onderhoudt de analyse
FG, indien aangewezen	[organisatie vult in]; onafhankelijk advies en toezicht, geen vervanging van de besluitvormer
Informatiebeveiliging en ICT	[organisatie vult in]; architectuur, toegang, instellingen en bewijs
Professioneel inhoudsverantwoordelijke	[organisatie vult in]; bevoegdheid, betekenisvolle controle en gevolgen voor de zorg of ondersteuning
Vertegenwoordiging van betrokkenen	[organisatie vult in]; zie §4.2
Externe adviseur, indien ingeschakeld	[organisatie vult in]; exacte opdracht en beoordeelde versie vastleggen
Hysio	Levert leveranciersinformatie en redelijke verwerkersbijstand; neemt het klantbesluit niet over

0.8 Peildata en versie

Vastlegging	Waarde
Naam van de verwerking en koppeling aan je verwerkingsregister	[organisatie vult in]
Eigen DPIA-versie en eerdere besluiten	[organisatie vult in]
Begin onderzoek en feitelijke peildatum	[organisatie vult in]
Gecontroleerde Hysio-documenten, versies en brondata	[organisatie vult in]
Omgeving, actieve functies en gekoppelde systemen	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Vastlegging	Waarde
Beoogde start of materiële wijziging	[organisatie vult in]
Formele vaststelling en eventuele voorwaarden	[organisatie vult in]
Eerstvolgende controle en verantwoordelijke	[organisatie vult in]

0.9 IGJ-toetsingskader Digitale Zorg en landelijk modelplan

Als zorgaanbieder blijf je verantwoordelijk voor een zorgvuldige invoering en een zorgvuldig gebruik van AI. De Inspectie Gezondheidszorg en Jeugd toetst dat aan het Toetsingskader Digitale Zorg; sinds de update van juli 2026 geldt dat kader ook voor jeugdhulpaanbieders. De tabel laat zien waar de relevante normen in deze template terugkomen (stand oktober 2026, niet uitputtend).

Norm uit het toetsingskader	Waar in deze template
1.1 Vastgelegd beleid voor digitale zorg en 1.3 proces voor keuzes over digitale zorg	0.7 en 4.5
1.4 Risico's van de ICT-omgeving	Sectie 3
2.1 en 2.2 Aanschafproces en programma van eisen	0.3, 3.3 en 3.4
3.1 tot en met 3.3 Patiënten betrekken, een geïnformeerde keuze en alternatieven	2.4, 2.12 en 4.2
5.1 Informatiebeveiliging	3.3 en 3.4

Volgens de IGJ doe je bij de invoering van generatieve AI het volgende:

- je stelt het doel vast;
- je maakt een risico-inventarisatie;
- je zorgt dat medewerkers risico's kunnen inschatten en uitkomsten op hun waarde kunnen schatten;
- je volgt of de toepassing in de praktijk goed werkt;
- je regelt het melden van fouten en incidenten;
- je bevraagt de leverancier over risico's en validatieresultaten;
- je let op informatiebeveiliging;
- je bepaalt of de MDR van toepassing is.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Gebruik die punten als controlelijst naast deze template.

Het landelijke modelplan Spraakgestuurd rapporteren noemt als maatregel een DPIA per toepassing. Leg in deze template daarom per toepassing vast welke Werkstroom, welke invoer en welke ontvanger je beoordeelt.

Eigen koppeling aan het toetsingskader, controlelijst en verantwoordelijke: [organisatie vult in].

Sectie 1: systematische beschrijving van de verwerking

1.1 Identiteit van de Verwerkingsverantwoordelijke

Veld	Waarde
Juridische naam, rechtsvorm, adres en KvK-nummer waar van toepassing	[organisatie vult in]
Werkende praktijken, locaties en organisatorische eenheden	[organisatie vult in]
Bevoegde vertegenwoordiger en privacycontact	[organisatie vult in]
FG-contact en beoordeling van de aanstellingsplicht	[organisatie vult in]
Contact voor incidenten, ook bij afwezigheid van het gewone contact	[organisatie vult in]
Eventuele mede-verantwoordelijken of opdrachtgever	[organisatie vult in]
AGB-, BIG- of andere beroepsregistratie voor zover relevant	[organisatie vult in]

1.2 Identiteit van Hysio

Veld	Leveranciersinformatie
Naam	Hysio B.V.
KvK-nummer	98649744
Vestigingsadres	De Aak 11, 7908 EL Hoogeveen
Privacy en feitelijke bijstand	privacy@hysio.nl

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Veld	Leveranciersinformatie
Vertrouwelijke juridische documentatie	legal@hysio.nl
Subverwerkerwijzigingen en bezwaar	compliance@hysio.nl
Rol voor inhoud op klantinstructie	Verwerker, of subverwerker als de opdrachtgever zelf verwerker is; de feitelijke verhouding is bepalend
Eigen verwerkingen	Afzonderlijk beschreven in de Privacyverklaring; geen algemene vrijbrief voor eigen gebruik van cliëntinhoud
Privacytoezicht Hysio	Hysio heeft geen functionaris gegevensbescherming aangesteld; privacyvragen stel je via privacy@hysio.nl. De eigen verplichtingen van je organisatie blijven gelden.

1.3 Feitelijke rolconstellatie

Een behandelpraktijk kan zelf doelen en wezenlijke middelen bepalen. Een medewerker handelt doorgaans onder haar gezag. Een zelfstandige professional kan in de ene opdracht verantwoordelijke en in een andere opdracht onder het gezag van een instelling werkzaam zijn. Een technisch beheerder is door die functie niet bevoegd tot alle dossiers.

Als meerdere partijen doelen en wezenlijke middelen gezamenlijk bepalen, beoordeel je gezamenlijke verantwoordelijkheid en leg je de taakverdeling volgens AVG artikel 26 vast. Het delen van een platform, dezelfde database of een technische koppeling maakt partijen niet op zichzelf gezamenlijk verantwoordelijk. Een ontvangende zorgverlener kan voor de ontvangen gegevens zelfstandig verantwoordelijk zijn.

Werk je in een Team, dan is ieder Teamlid voor de eigen Sessies en Klantdata de Klant en Verwerkingsverantwoordelijke, tenzij schriftelijk anders is overeengekomen. Wie feitelijk verwerkingsverantwoordelijke is, volgt uit de feiten en niet alleen uit deze afspraak (artikel 1.4 van de Algemene Voorwaarden). Een Team is geen praktijkorganisatie: wil een praktijk of instelling zelf verwerkingsverantwoordelijke zijn voor de Sessies van haar zorgverleners, bijvoorbeeld omdat die in loondienst werken, dan sluit zij de overeenkomst met Hysio als organisatie (artikel 1.5ter van de Verwerkersovereenkomst). Beoordeel in je rolkaart wie feitelijk verwerkingsverantwoordelijke is. De Teambeheerder krijgt geen toegang tot Sessies en Klantdata van Teamleden, tenzij dat schriftelijk anders is overeengekomen; welke beheer- en factuurgegevens de Teambeheerder ziet, staat in de Privacyverklaring. Hysio is niet ingericht als systeem waarmee zelfstandige zorgaanbieders dossiers voor elkaar raadpleegbaar maken. Deel je via Hysio met een andere zelfstandige zorgaanbieder, ook in een Team, dan is daarvoor een aparte schriftelijke afspraak met Hysio en je eigen beoordeling nodig. Maakt je inrichting dossiers of gegevens uit dossiers raadpleegbaar voor een andere

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

zorgaanbieder, dan kan dat een elektronisch uitwisselingssysteem zijn in de zin van de Wabvpz. Dan is onder meer vooraf uitdrukkelijke toestemming van je patiënt of cliënt nodig (artikel 15a Wabvpz) en heeft die recht op elektronische inzage en afschrift (artikel 15d Wabvpz). Gebruik binnen één zorgaanbieder valt daar niet onder.

Beschrijf voor iedere schakel: entiteit, feitelijke rol, doel, instructiebevoegdheid, autorisatie, ontvangers en relevante overeenkomst. Vermijd dat een integratiepartner zich als verantwoordelijke voordoet zonder het benodigde mandaat.

Eigen rolkaart en afspraken; maakt je inrichting via Hysio dossiers raadpleegbaar voor een andere zorgaanbieder? [organisatie vult in].

1.4 Doel, aard en gegevensstroom

Route	Hysio-verwerking en relevante begrenzing	Eigen doel en inrichting
Tekstinvoer en cliëntcontext	Ontvangen en verwerken van ingevoerde inhoud in de gekozen Sessie; context kan ook worden gebruikt in volgende bewerkingen binnen de route	[organisatie vult in]
Audio	Opname of upload, tijdelijke opslag, eventueel segmentering, transcriptie en verdere gekozen tekstverwerking	[organisatie vult in]
Document	Ontvangen, opslaan en waar ondersteund ontsluiten van inhoud; invoer en metadata kunnen gegevens van derden bevatten	[organisatie vult in]
Concept	Structureren of genereren van verslagen, samenvattingen, vragen, brieven en andere gekozen Output; de toegestane inhoudelijke ruimte verschilt per Werkstroom	[organisatie vult in]
Bewerking	Aanpassen van concepten; de oorspronkelijke inhoud verdwijnt niet noodzakelijk door een bewerking	[organisatie vult in]
Kopiëren en download	Levering van geselecteerde gegevens; controle van juiste persoon, versie, context en ontvanger blijft nodig	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Route	Hysio-verwerking en relevante begrenzing	Eigen doel en inrichting
API, gedeelde of gehoste Sessie, postback	Start, raadpleging en eventuele automatische teruglevering aan een vooraf toegelaten ontvanger; conceptlevering en definitieve vaststelling zijn verschillende momenten	[organisatie vult in]
Ondersteuning	Minimale gegevens op instructie voor een concreet probleem; geen standaard volledige dossierkopie per e-mail. Supportberichten met persoonsgegevens lopen alleen via de toegelaten supportroute uit Bijlage 3 van de Verwerkersovereenkomst; stuur geen zorginhoud die voor de vraag niet nodig is	[organisatie vult in]
Rechten, exit en verwijdering	Selectie, veilige teruggave, correctie, beperking, verwijdering en beperkte verantwoording volgens de overeengekomen route	[organisatie vult in]

Leg ook frequentie, aantallen betrokkenen, gemiddelde en maximale inhoud, landen, locaties, apparaten, beschikbaarheidsbehoefte en eventuele seizoens- of piekbelasting vast. Een technisch verbruiksmaximum vervangt geen noodzakelijkheidstoets.

1.4.1 Stroomschema per geactiveerde route

Gebruik per route het volgende invulmodel en voeg vertakkingen toe:

bron en bevoegde invoerder → apparaat/lokale opslag → beveiligde ontvangst → validatie en autorisatie → gekozen dienstverlener → resultaat en opslag → bewerking en controle → bevoegde ontvanger → gebruik in primair dossier → retentie en verwijdering.

Teken daarnaast de fout- en herstelroute, tijdelijke bestanden, logging, ondersteuning, back-ups en de gegevens die bij het uitvallen van een schakel achterblijven. Vermeld op ieder overdrachtspunt welke inhoud meegaat en wie die inhoud mag ontvangen.

Eigen routebeschrijving, systeemnamen en bewijs: [organisatie vult in].

1.4.2 Zo werkt de AI-ondersteuning

Hysio zet spraak om in tekst via een transcriptiedienst en maakt met een tekstverwerkingsdienst een concept van het gekozen verslag of document (zie 1.9). Het resultaat is een concept dat jij controleert, aanpast en vaststelt voordat je het gebruikt (zie 2.7). AI kan feiten verzinnen, informatie weglaten, betekenis veranderen, een ontkenning verliezen, een uitspraak aan de verkeerde persoon toeschrijven of een onzekere bevinding te stellig formuleren (zie R4 tot en met R6 en R30). De Verwerkersovereenkomst sluit modeltraining op Klantdata uit. De bekende foutsoorten en beperkingen per functie kun je opvragen (zie 0.3).

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

1.5 Familie- en Werkstroominventaris

1.5.1 Beroepsfamilie

Selecteer de werkelijk gebruikte contexten: [ ] Paramedie [ ] Huisarts [ ] Specialist [ ] Mentale Zorg [ ] Verpleegzorg [ ] Mondzorg [ ] Geboortezorg [ ] Jeugd & Sociaal Werk [ ] Arbeid & Gezondheid [ ] Andere zorgprofessional. Algemene Werkstromen worden aan hun concrete gebruik gekoppeld.

1.5.2 Functiechecklist

Maak voor iedere gebruikte Werkstroom een record met onderstaande velden. Je mag gemeenschappelijke onderdelen hergebruiken, mits de overeenkomst is gemotiveerd en iedere afwijking wordt onderzocht.

Veld	Vastlegging per Werkstroom
Identiteit	Code, naam, profiel, versie en datum
Beschikbaarheid	Ontworpen, gebouwd, geactiveerd en daadwerkelijk gebruikt; omgeving afzonderlijk
Doel en doelgroep	Concrete taak, bevoegd beroepsbeoefenaar en betrokken persoon
Invoer	Tekst, audio, bestand, cliëntcontext, herkomst en noodzakelijke gegevens
Inhoudelijke ruimte	Alleen bronweergave, selectie, berekening, interpretatie, hypothese, aanbeveling of andere invloed
Uitvoer	Volledige tekst, geselecteerde velden, bijlagen, samenvatting en context die verloren kan gaan
Controle	Wie controleert welke inhoud, met welke bron en vóór welk gebruik?
Ontvanger	Eigen dossier, andere zorgverlener, cliënt, werkgever, verzekeraar of andere partij
Bijzondere beoordeling	Privacy, beroepsregels, MDR/IVDR waar relevant, AI-verordening en bronrechten. Heb je vóór invoering beoordeeld of een risicoanalyse of prospectieve risico-inventarisatie nodig is, en heb je bij Hysio per Werkstroom de stand van de screening opgevraagd (zie het MDR-positiedocument)?

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Veld	Vastlegging per Werkstroom
Resultaat	Toelaatbare scope, maatregelen, resterende voorwaarden en besluit

Let op bij eigen AI-inhoud. Een Werkstroom kan wat in de bron staat combineren met eigen aanvullingen van Hysio, zoals een werkhypothese. Ga er niet van uit dat alle eigen AI-inhoud onder het kopje Hysio Aanvullend staat. Laat je dat blok weg uit een uitvoerformaat, dan kan de overige tekst nog steeds inhoud bevatten die Hysio heeft toegevoegd. Controleer daarom het hele resultaat.

Wanneer een uitvoerformaat waarschuwingen, bronverwijzingen, ontbrekende onderzoeksdelen of onzekerheid weglaat, moet de ontvangende professional toch over de noodzakelijke context beschikken. Test dat vóór gebruik. Een werkende gegevensoverdracht is nog geen inhoudelijk veilige overdracht.

Een DPIA geeft geen MDR-kwalificatie, medische validatie of vrijgave onder de AI-verordening. Onderzoek invloed op diagnose, behandeling, triage, functioneren, score, codering en toegang tot diensten in samenhang met de betreffende positiedocumenten. Een label als concept en menselijke controle geven geen automatische wettelijke vrijstelling.

1.6 Categorieën gegevens

Categorie	Mogelijke inhoud en noodzakelijkheidstoets
Identificatie	Naam, pseudoniem, intern nummer, geboortedatum, adres of contactgegevens voor zover ingevoerd. Met initialen of een intern nummer kan iemand nog steeds herleidbaar zijn
Gezondheid en zorg	Klachten, anamnese, onderzoek, diagnose, medicatie, behandeling, metingen, functioneren, prognose en eerdere zorginformatie
Audio	Stem, inhoud, achtergrondgesprekken en andere aanwezigen; een stemopname is niet alleen vanwege het stemgeluid automatisch biometrische identificatie
Transcript en output	Bronweergave, correcties, hypotheses, voorstellen, samenvattingen en relevante oorspronkelijke versies
Bestanden	Inhoud, bestandsnaam, auteur, datum en andere metadata. Een document kan meer bevatten dan de zichtbare relevante passage

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Categorie	Mogelijke inhoud en noodzakelijkheidstoets
Andere gevoelige gegevens	Gezin, seksualiteit, afkomst, geloof, schulden, werk, geweld, strafrechtelijke gegevens of andere categorieën die in de bron voorkomen
Derden	Familieleden, mantelzorgers, medebetrokken cliënten, verwijzers, medewerkers en andere in de bron genoemde personen
Toegang en verwerking	Account, rol, organisatie, Sessie, tijdstip, verwerkings- en afleverstatus, beperkte technische loggegevens
BSN	Geen algemeen noodzakelijk invoergegeven. Beoordeel een afzonderlijke wettelijke bevoegdheid en noodzaak; een vrij tekstveld verleent geen bevoegdheid
Beroepsidentificatie	AGB-, BIG- of andere registratie voor zover noodzakelijk voor de betreffende professional of communicatie

Werkelijk gebruikte categorieën, rechtvaardiging en weggelaten gegevens: [organisatie vult in].

1.6.1 Cliëntcontext

Leg vast welke achtergrondinformatie aan een Sessie wordt toegevoegd en hoe relevantie, juistheid en actualiteit worden gecontroleerd. Onderscheid bekende feiten, een vermoeden, een historische situatie en informatie over een andere persoon. Afwezigheid van informatie betekent niet automatisch afwezigheid van een klacht, risico of behandeling.

Het beleid van Hysio verlangt dat gegevens en onzekerheden niet ongefundeerd worden aangevuld of als vaststaand worden gepresenteerd. Toets per Werkstroom of dat lukt. Een invoerinstructie of schema bewijst niet dat iedere generatie en export deze grens bewaart.

1.7 Categorieën betrokkenen

Beschrijf patiënten of cliënten, minderjarigen, personen met verminderde beslisvaardigheid, vertegenwoordigers, familieleden, andere aanwezigen, medewerkers en professionele ontvangers. Beoordeel per groep afhankelijkheid, machtsverhouding, taal, digitale toegankelijkheid en mogelijkheid om bezwaar of andere rechten uit te oefenen.

Een gecombineerde bespreking kan meerdere cliënten betreffen. Selecteer bij overname naar één dossier alleen de relevante rechtmatig te delen gegevens. Een volledige vergaderingsexport is uitsluitend passend voor een ontvanger die tot de volledige inhoud bevoegd is.

Eigen groepen en bijzondere kwetsbaarheid: [organisatie vult in].

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

1.8 Ontvangers en externe routes

Geef voor iedere ontvanger de identiteit of duidelijk omschreven categorie, rol, doel, benodigde inhoud, grondslag, geheimhouding, land, beveiliging en bewaartermijn op. Een beheer-, betaal- of contractrol geeft geen vanzelfsprekende toegang tot cliëntinhoud.

Bronrechten, gegevensbeschermingsgrondslag en bevoegdheid van de ontvanger moeten al vóór iedere verstrekking zijn geregeld. Professionele inhoudscontrole vóór definitieve vaststelling is een aanvullende stap. Een vooraf geautoriseerde automatische conceptlevering aan een afgeschermde werkvoorraad is alleen passend als zij de benodigde context bewaart en niet ongemerkt leidt tot een vastgesteld dossier, beslissing of cliëntbericht.

Eigen ontvangersmatrix en geteste terugleverroute: [organisatie vult in].

1.9 Dienstverleners en doorgiften

Onderstaande tabel geeft per dienst aan wat je voor je eigen beoordeling vastlegt. Bijlage 3 van de Verwerkersovereenkomst vermeldt de partijen, functies en toelatingsvoorwaarden. Neem in je eigen register alleen de feitelijk gebruikte diensten, partijen en locaties op die voor jouw Werkstroom zijn bevestigd. Noteer in 0.8 de versie en datum van de ketenopgave die je hebt ontvangen. Vraag ontbrekende gegevens bij Hysio op. De voorwaarden voor aankondiging en bezwaar bij een nieuwe of vervangende Subverwerker staan in de artikelen 11.2 en 11.3.

Dienst	Waar de entiteit staat	Wat je voor deze DPIA vastlegt
Hosting	Bijlage 3 van de Verwerkersovereenkomst	De overeengekomen locatie in Duitsland binnen de EER, de toegangsroute, de back-upcyclus en de herstelprocedure
Tekstverwerking	Bijlage 3 van de Verwerkersovereenkomst	Welke route je Werkstromen daadwerkelijk gebruiken volgens de ketenopgave en hoe de route voldoet aan de contractuele norm van verwerking binnen de Europese Unie, de uitsluiting van modeltraining op Klantdata, en de bewaartermijn per verwerkingsfunctie
Transcriptie	Bijlage 3 van de Verwerkersovereenkomst	De contracterende entiteit, de verwerkingslanden, de doorgiftewaarborg per stap met doorgiftebeoordeling, en de retentie-instelling op het gebruikte account

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Dienst	Waar de entiteit staat	Wat je voor deze DPIA vastlegt
Supportberichten	Bijlage 3 van de Verwerkersovereenkomst, onderdeel A	Dat supportberichten met persoonsgegevens alleen via de toegelaten supportroute lopen, en dat je geen zorginhoud meestuurt die voor de vraag niet nodig is
Transactionele e-mail	Privacyverklaring, paragraaf 5.4 (eigen verwerking van Hysio)	Dat account- en dienstberichten geen cliëntinhoud bevatten
Betaling	Mollie B.V., zelfstandig verwerkingsverantwoordelijke	Dat de betaalroute geen bestemming is voor zorginhoud. Deze verwerking valt niet onder de klantverwerkersketen

Verwerking of toegang buiten de EER kan voorkomen bij tekstverwerking, transcriptie en ondersteuning per e-mail. Transcriptie kan ook in de Verenigde Staten plaatsvinden. Bevestig per dienst en Werkstroom de feitelijke verwerking, toegang en toepasselijke doorgiftewaarborg voordat je die route gebruikt. Artikelen 11 en 15 en Bijlage 3 van de Verwerkersovereenkomst beschrijven de voorwaarden.

Een Europese opslaglocatie bewijst niet dat toegang of doorgifte vanuit andere landen is uitgesloten. Een doorgiftewaarborg maakt een anderszins verboden of onnodige verwerking niet toegestaan. Een adequaatheidsbesluit en een passend instrument uit AVG artikel 46 vragen een verschillende beoordeling. Waar het gekozen instrument dat vergt, worden ook het recht en de praktijk in het bestemmingsland en aanvullende maatregelen onderzocht. Vraag de onderbouwing van een concrete route op via legal@hysio.nl en leg vast welk bewijs je hebt ontvangen.

Ook waar het EU-VS Data Privacy Framework beschikbaar is, legt Hysio voor de betrokken stap vooraf vast welk ander passend doorgifte-instrument, met een doorgiftebeoordeling, als terugval geldt (artikel 15.5 van de Verwerkersovereenkomst). Beantwoord de onderstaande vragen aan de hand van de ontvangen stukken en noteer ontbrekende onderbouwing.

Doorgiftevraag	Eigen vastlegging
Steunt een stap in de keten op het EU-VS Data Privacy Framework, en welke terugvalwaarborg geldt dan?	[organisatie vult in]
Is de doorgiftebeoordeling herzien na een relevante wijziging in het recht of de praktijk van het derde land?	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Doorgiftevraag	Eigen vastlegging
Op welk instrument steunt per stap de doorgifte, ook vanuit het Verenigd Koninkrijk?	[organisatie vult in]
Heb je rekening gehouden met de geldigheid van het adequaatheidsbesluit voor het Verenigd Koninkrijk, dat geldt tot 27 december 2031?	[organisatie vult in]

De keuze in deze versie is dat een route via een dienstverlener voor gezondheidsgegevens pas wordt vrijgegeven na controle van de werkelijke dienstvoorwaarden, rol, instructie, retentie, doorgifte en instellingen. Voor hosting geldt als norm dat de verwerking binnen de Europese Economische Ruimte blijft; voor tekstverwerking geldt de Europese Unie. Het invullen van deze template verleent geen tijdelijke uitzondering op een verbod om een dienstverlener in te schakelen.

1.10 Bewaartermijnen en verwijdering

De bewaarinstructies voor wat Hysio in opdracht verwerkt, staan in Bijlage 1, onderdeel C, van de Verwerkersovereenkomst. Leg de toepasselijke instructies en termijnen met versie en datum vast in je eigen beoordeling. Hysio zorgt ervoor dat bij iedere opruimronde wordt vastgelegd hoeveel gegevens per soort zijn verwijderd, zonder inhoud, en levert dat overzicht op verzoek. Verwijderen heeft de betekenis van Verwijdering uit artikel 1 van de Algemene Voorwaarden: definitief uit de actieve opslag halen, met de bijbehorende bestanden. Kopieën in back-ups verdwijnen binnen de back-uptermijn uit de Verwerkersovereenkomst.

Hysio verzorgt geen zorgtoegangslogging in de zin van artikel 5 van het Besluit elektronische gegevensverwerking door zorgaanbieders, tenzij je dat vóór de eerste verwerking schriftelijk met Hysio afspreekt (Bijlage 1, onderdeel C, van de Verwerkersovereenkomst). Zonder zo'n afspraak regel je die logging in je eigen dossiersysteem. Beoordeel zelf of de loggingplicht ook geldt voor wat je in Hysio verwerkt. Leg in je DPIA vast hoe je de toegang tot Sessies in Hysio verantwoordt zolang dat niet is beslist.

1.10.1 Actieve verwerking

Overgenomen termijnen, versie en datum van Bijlage 1: [organisatie vult in].

Pas een kortere termijn toe wanneer het doel is vervallen of een rechtmatige instructie dit vergt. Een wettelijke uitzondering wordt per gegevenslaag, doel, bevoegdheid en termijn vastgelegd. Zij rechtvaardigt geen onbeperkte bewaring van een volledige Sessie.

Controleer behalve de klok ook de uitvoering: alle kopieën en bijlagen, mislukte taken, nieuwe pogingen, bewerkte Output, browsergegevens, kopieën bij dienstverleners en herstel uit back-ups. Een verborgen item, weergavefilter of soft-delete is geen definitieve verwijdering. Tel een niet-bevestigde maatregel niet als gerealiseerde risicobeperking.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Eigen noodzakelijke termijn per doel, overeengekomen afwijkingen en uitvoeringsbewijs:
[organisatie vult in].

1.10.2 Beëindiging en gegevensverzoeken

De Regeling Datatoegang voorziet in een beperkte continuïteitsperiode van drie kalendermaanden voor raadpleging, export en afwikkeling. Zij verlengt niet automatisch een eerder verstreken bewaartermijn van audio, uploads of andere gegevens. Alleen nog rechtmatig aanwezige gegevens kunnen worden teruggegeven. Bij een overstap gelden daarnaast de rechten uit de Regeling Datatoegang: opzegtermijn, overgangsperiode, ophaaltermijn, de vastgelegde formaten en geen overstapkosten. Een volledige kopie van je gegevens vraag je tijdens het gebruik aan via privacy@hysio.nl als integrale archiefkopie; Hysio stelt die voor je samen. Bij beëindiging of een overstap verloopt de teruggave als integrale overdracht. Beide routes volgen de Regeling Datatoegang (zie HM10).

Een tijdig verzoek wordt ook bij het naderen van het einde van die periode behoorlijk afgehandeld. Registreer ontvangst, geverifieerde scope, aflevering, eventuele gebreken en de daarop volgende verwijdering. Een onbetaalde factuur is geen algemene grond om gegevensrechten of de overeengekomen eindoverdracht te blokkeren. Gewone export-, overstap- en rechtenverzoeken kunnen verschillende termijnen en regels hebben; volg de toepasselijke route uit de Regeling en de Verwerkersovereenkomst.

Veiligstellen van het primaire dossier begint tijdens gebruik. Wacht niet tot beëindiging met het overbrengen van noodzakelijke gecontroleerde informatie. Test de volledigheid van de overdracht; een geslaagde export van één Sessie bewijst geen volledige account- of dossierscope.

1.10.3 Dossierbewaring van je organisatie

Wanneer de WGBO van toepassing is, geldt voor het dossier in beginsel twintig jaar vanaf de laatste wijziging, of langer voor zover de zorg van een goed hulpverlener dat redelijkerwijs verlangt. Vernietiging op verzoek en de wettelijke uitzonderingen moeten afzonderlijk worden beoordeeld. Buiten de jeugdgezondheidszorg geldt geen algemene regel dat de termijn voor ieder minderjarigendossier pas op achttienjarige leeftijd begint.

Onder de Jeugdwet geldt voor het jeugdhulpdossier in beginsel twintig jaar; onder de Wmo 2015 bewaren college en aanbieder persoonsgegevens vijftien jaar vanaf de laatste wijziging, met vernietiging binnen drie maanden na een schriftelijk verzoek. Onder de WGBO en de Jeugdwet geldt voor vernietiging op verzoek geen eigen wettelijke termijn; dan geldt de reactietermijn van AVG artikel 12 lid 3. De KNMG-richtlijn Omgaan met medische gegevens (2024) noemt langere termijnen, zoals minimaal tot het 39e levensjaar bij gegevens over vermoedens van kindermishandeling; in de jeugdgezondheidszorg begint de termijn gebruikelijk bij 18 jaar. Bij verplichte ggz en onder de Wzd gelden eigen termijnen.

Voor andere regimes, bijvoorbeeld arbeid, archivering of veterinaire werkzaamheden, stel je de toepasselijke bewaarbepaling per documentsoort vast. Een fiscale plicht voor facturen of een wettelijke logtermijn is geen grond om alle tijdelijke zorginhoud even lang te bewaren. Hysio is geen vervanging voor het enige primaire dossier of iedere sectorale archiefvoorziening.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Een Sessie in Hysio is een werkkopie voor de verslaglegging en vervangt je dossier niet. Neem het gecontroleerde verslag tijdig op in je eigen dossier en laat de Sessie daarna verwijderen. Zolang gegevens nog in Hysio staan, vallen ze onder het recht op inzage en verwijdering van je patiënt of cliënt, en helpt Hysio je die rechten uit te voeren.

Eigen bewaartabel, vernietigingsprocedure en primaire dossierlocatie; waar staat het enige primaire dossier? [organisatie vult in].

Sectie 2: noodzaak, rechtmatigheid en evenredigheid

2.1 Grondslagketen per doel

Leg voor ieder afzonderlijk doel een grondslag uit AVG artikel 6 vast. Beoordeel daarnaast een uitzondering uit artikel 9 wanneer bijzondere persoonsgegevens worden verwerkt en het toepasselijke regime voor strafrechtelijke gegevens onder artikel 10. Een beroepsgeheim, verwerkersovereenkomst of artikel 9-uitzondering vervangt de artikel 6-grondslag niet.

Voor verwerking die objectief nodig is voor een behandelingsovereenkomst kan artikel 6 lid 1 onder b relevant zijn. Voor het wettelijk vereiste dossier kan artikel 6 lid 1 onder c in samenhang met BW artikel 7:454 relevant zijn. De dossierplicht verplicht niet tot audio, AI of iedere aangeboden Werkstroom. Bij gezondheidsgegevens kan artikel 9 lid 2 onder h met lid 3 en UAVG artikel 30 relevant zijn binnen de toepasselijke zorg-, taak- en geheimhoudingsvoorwaarden. Pas deze route niet automatisch toe op iedere coach, werkgever, gemeente of andere opdrachtgever.

Een publiekrechtelijke taak verlangt de toepasselijke wettelijke basis. Bij een gerechtvaardigd belang leg je doel, noodzaak en belangenafweging vast, en beoordeel je of deze grondslag in die hoedanigheid beschikbaar is. Als toestemming de grondslag is, moet zij vrij, specifiek, geïnformeerd, aantoonbaar en intrekbaar zijn. Voor bijzondere gegevens is waar die route wordt gebruikt uitdrukkelijke toestemming nodig. De afhankelijke positie van patiënten of werknemers vraagt daarbij aandacht.

Een doelwijziging, bijvoorbeeld onderzoek, evaluatie van medewerkers of modelverbetering, volgt niet stilzwijgend uit toestemming tot behandeling of uit het contract met Hysio. Onderzoek de nieuwe verwerking afzonderlijk. De gekozen verwerkersinstructie sluit training op Klantdata en algemene productverbetering met zorginhoud uit; de leveranciersvoorwaarden en instellingen moeten dat ondersteunen.

Doel	Gegevens en betrokkenen	Artikel 6	Artikel 9 of 10 indien relevant	Concrete noodzaak, wet of andere onderbouwing
Dossiervorming	[organisatie vult in]	[invullen]	[invullen]	[invullen]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Doel	Gegevens en betrokkenen	Artikel 6	Artikel 9 of 10 indien relevant	Concrete noodzaak, wet of andere onderbouwing
Audio en transcriptie	[organisatie vult in]	[invullen]	[invullen]	[invullen]
Conceptcommunicatie	[organisatie vult in]	[invullen]	[invullen]	[invullen]
Hypothese, voorstel, score of andere inhoudelijke ondersteuning	[organisatie vult in]	[invullen]	[invullen]	[invullen]
Koppeling of verstrekking aan een andere partij	[organisatie vult in]	[invullen]	[invullen]	[invullen]
Eigen aanvullend doel	[organisatie vult in]	[invullen]	[invullen]	[invullen]

2.2 Doelbinding per functie

Beschrijf wat de gekozen functie moet bereiken en hoe je vaststelt dat zij daarvoor geschikt is. Een algemene verwachting van tijdwinst bewijst niet dat alle gegevens noodzakelijk zijn of dat de uitkomst voldoende betrouwbaar is. Gebruik geschikte testgevallen, professionele beoordelingscriteria en controle van fouten en ontbrekende informatie.

Maak onderscheid tussen bronweergave, selectie, interpretatie en nieuwe voorstellen. Een gewenste hypothese kan volgens ontwerp worden gegenereerd en toch een risico voor de betrokkene veroorzaken, bijvoorbeeld door verankering van een vermoeden in het dossier. Dat risico valt ook binnen de DPIA als er geen technische fout optreedt.

Beoordeel misbruik en voorzienbaar gebruik buiten de afgesproken functie. Een verbod in een contract is een maatregel, maar maakt een feitelijk mogelijk en voorzienbaar schadelijk gebruik niet irrelevant. Koppel de functionele begrenzing aan instructies, autorisaties, opleiding en zo nodig technische beperkingen.

Doel, geschiktheidsbewijs, toegestane en uitgesloten handelingen per functie: [organisatie vult in].

2.3 Dataminimalisatie

Gebruik alleen gegevens die nodig zijn voor de gekozen taak en ontvanger. Beoordeel vóór verzending of een beperkte passage, samenvatting of pseudoniem volstaat. Controleer ook bestandsnamen, bijlagen, metadata, vrije feedback en achtergrondgesprekken. Het vervangen van

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

een naam laat de overige herleidbaarheid onverlet. Pseudonimiseren verlaagt het risico. Gegevens die met redelijkerwijs beschikbare middelen tot iemand te herleiden zijn, blijven persoonsgegevens.

Voor BSN-gebruik stel je een wettelijke bevoegdheid en noodzaak vast. De technische mogelijkheid om een BSN in vrije tekst in te voeren is geen rechtvaardiging. Een AGB- of BIG-nummer heeft een andere functie en wordt niet automatisch onder dezelfde regels gebracht.

Gegevens over derden kunnen voor de zorg of ondersteuning nodig zijn, maar worden niet onbeperkt meegenomen omdat zij in een bron staan. Beoordeel noodzaak, geheimhouding, informatieplicht en eventuele beperking ter bescherming van anderen. Toestemming van iedere genoemde derde is niet zonder meer de enige mogelijke grondslag.

Invoerregels, controles, uitzonderingen en verantwoordelijke: [organisatie vult in].

2.4 Audio: afzonderlijke noodzakelijkheidstoets

Beoordeel opname en bewaring na transcriptie afzonderlijk. De behandelingsovereenkomst en het belang van goede verslaglegging maken een volledige opname niet automatisch noodzakelijk. Leg vast welk probleem audio oplost, wie hoorbaar is, hoe lang wordt opgenomen, wie kan luisteren en waarom een minder ingrijpend alternatief niet volstaat.

Je vertelt je cliënt of patiënt dat je Hysio gebruikt en volgt daarbij je eigen beroepsnormen. Jij bepaalt de toepasselijke AVG-grondslag en, voor gezondheidsgegevens, de uitzondering die de verwerking toestaat. De keuze over opname bepaalt die grondslag op zichzelf niet. Leg in je DPIA vast welke grondslag en, waar nodig, welke uitzondering voor gezondheidsgegevens van toepassing zijn. Toestemming voor een geneeskundige verrichting onder BW artikel 7:450 is op zichzelf geen opnamegrondslag.

Een niet-opnemenroute moet daadwerkelijk bruikbaar zijn. Weigering van optionele audio mag niet ongemerkt tot weigering van noodzakelijke zorg leiden. In een bijzondere situatie waarin opname op een andere wettelijke taak berust, onderzoek je die uitzondering afzonderlijk en presenteer je haar niet als vrije toestemming.

Hysio bewaart het audiobestand op haar servers beveiligd in Duitsland. De nachtelijke opruimtaak selecteert transcriptietaken zodra die ouder zijn dan 90 kalenderdagen, gerekend vanaf de aanmaak van de taak. Voor spraak-naar-tekst kan verwerking buiten de EER plaatsvinden. Bijlage 1 beschrijft de bewaarinstructie. Langer bewaren kan alleen bij een concrete wettelijke bewaarplicht of een rechtsgeldige bewaarinstructie, voor de noodzakelijke gegevens met een vastgelegd eindcriterium.

Audio-keuze	Vastlegging
Doel, noodzaak en alternatief	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Audio-keuze	Vastlegging
Personen die hoorbaar kunnen zijn en informatie vooraf	[organisatie vult in]
Grondslag en toestemming waar vereist door wet of beroepsnorm	[organisatie vult in]
Afhandeling van bezwaar of intrekking, waar toepasselijk	[organisatie vult in]
Duur, apparaat en lokale herstelgegevens	[organisatie vult in]
Opruimtaak en afzonderlijke bewaarlagen	[organisatie vult in]
Bevoegde luisteraar en correctie van sprekerverwisseling	[organisatie vult in]
Dienstverlener- en verwijderroute	Bijlage 3 noemt de beoogde transcriptiedienst. Bij de transcriptiedienst staat de instelling voor zero data retention aan. Per route moeten het toepasselijke account, de gegevens waarop dit geldt, de uitzonderingen en de contractuele en technische werking nog worden bevestigd. Leg ook het opruimoverzicht uit 1.10 vast.
Toepasselijk beroepsadvies en beoordeling van de opnameketen	[organisatie vult eigen beroepscontext en eventuele voorwaarden in]

2.5 Alternatieven en privacy by design

Behoud een open vergelijking. Vul vooraf geen conclusie in dat lokale verwerking, handmatig werken of een andere leverancier slechter is. Onderzoek functionele geschiktheid, nauwkeurigheid, gegevensvolume, locatie en toegang, leveranciersketen, beveiliging, kosten, beheercapaciteit, continuïteit en gevolgen voor betrokkenen.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Alternatief	Onderzoek en bewijs	Voordelen en nadelen voor betrokkenen	Keuze en reden
Handmatige dossiervorming zonder AI	[organisatie vult in]	[invullen]	[invullen]
Lokale of organisatiebeheerde spraak-naar-tekst	[organisatie vult in]	[invullen]	[invullen]
Andere leverancier of andere verwerkingsroute	[organisatie vult in]	[invullen]	[invullen]
Hysio met uitsluitend tekst en zonder audio	[organisatie vult in]	[invullen]	[invullen]
Hysio met minder gegevens of beperktere functies	[organisatie vult in]	[invullen]	[invullen]
Hysio zonder automatische koppeling	[organisatie vult in]	[invullen]	[invullen]
Gekozen inrichting	[organisatie vult in]	[invullen]	[invullen]

Concludeer per doel of de gekozen inrichting geschikt, nodig en evenredig is. Noteer ook gevolgen als de verwerking precies werkt zoals ontworpen: ontstaat nieuwe gevoelige informatie, extra zichtbaarheid binnen een organisatie, een gevoel van voortdurende registratie of afhankelijkheid van een leverancier? Een gunstige uitkomst voor de organisatie alleen is onvoldoende.

2.6 Declaratie, codering en administratieve stelsels

Onderscheid een uit de bron overgenomen code, een berekende score, een kandidaatcode en een inhoudelijke classificatie. Laat de bevoegde professional de juistheid, bronversie, toepasselijke regels en ontvanger controleren. Een voorgestelde code is geen bewezen diagnose of garantie op vergoeding.

Beschrijf waarom de gegevens noodzakelijk zijn voor de concrete declaratie of rapportage. Een zorgverzekerings- of contractuele declaratieregel is geen algemene opdracht om de volledige bron of alle medische gegevens te verstrekken. Beoordeel welke inhoud de ontvanger daadwerkelijk nodig heeft.

Controleer ook rechten op meetinstrumenten, richtlijnen en codestelsels. Een openbare bron of professionele toegang geeft niet automatisch toestemming voor ieder commercieel hergebruik. Een onzekerheid over gebruiksrechten wordt vóór het betrokken gebruik opgelost; een disclaimer of

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

menselijke controle vervangt die toestemming niet.

Gebruikte stelsels, versies, rechten, controle en minimale verstrekking: [organisatie vult in].

2.7 Betekenisvolle menselijke controle en AVG artikel 22

De gekozen gebruiksgrens verlangt dat een bevoegde professional de relevante bron en Output beoordeelt, afwijkingen kan herkennen en de inhoud kan corrigeren of verwerpen. Zorg voor voldoende tijd, deskundigheid, informatie en beslisruimte. Alleen klikken op bevestigen of routinematig overnemen is geen betekenisvolle tussenkomst.

Deze beoordeling vindt plaats vóór vaststelling in het primaire dossier, een professionele beslissing, declaratie of cliëntcommunicatie. Een vooraf geautoriseerde automatische levering van een herkenbaar concept aan een afgeschermde werkvoorraad is niet hetzelfde als definitieve aanvaarding. Leg vast waar de controle in de keten plaatsvindt en hoe het ontvangende systeem onbedoelde vaststelling voorkomt.

Voor gegevens die al vóór deze inhoudscontrole worden overgedragen, moeten grondslag, noodzakelijkheid, bronrechten en ontvangerbevoegdheid vooraf kloppen. Het conceptkarakter verruimt die voorwaarden niet.

Onderzoek de werkelijke invloed op besluiten die rechtsgevolgen hebben of iemand vergelijkbaar wezenlijk treffen. Als menselijke beoordeling ontbreekt of slechts formeel is, moet de toepasselijkheid van AVG artikel 22 opnieuw worden onderzocht, inclusief eventuele uitzonderingen en waarborgen. De enkele aanwezigheid van een professional sluit artikel 22, de MDR of verplichtingen uit de AI-verordening niet uit.

Controleprocedure, bevoegde functies, afwijsmogelijkheid, bewaard bewijs en ontvangende systeemstatus: [organisatie vult in].

2.8 Jeugd, gezag en vertegenwoordiging

Leeftijd, wilsbekwaamheid, gezag, opdracht en het concrete recht worden afzonderlijk vastgesteld. Een begeleidende volwassene, ouder, accountbeheerder of betaler is niet automatisch bevoegd tot iedere beslissing of alle gegevens. Leid gezag of toestemming niet uit een profielnaam of familievermelding af.

Voor behandeling en dossier gelden waar toepasselijk de bijzondere WGBO-regels. Onderscheid onder meer de positie beneden twaalf jaar, de gedeelde positie van twaalf tot zestien jaar en de zelfstandige positie vanaf zestien jaar, met de wettelijke uitzonderingen en de beoordeling van wilsbekwaamheid. Toegang tot gegevens van derden vraagt een eigen afweging.

De algemene UAVG-regels zijn per september 2026 gewijzigd. Maak bij gegevensbeschermingsrechten onderscheid tussen vertegenwoordiging beneden twaalf jaar, de positie van kind én vertegenwoordiger van twaalf tot zestien jaar en zelfstandige uitoefening vanaf zestien jaar. De regels voor op toestemming gebaseerde verwerking en intrekking zijn niet identiek aan die voor rechtenverzoeken. Curatele, bewind en mentorschap vragen beoordeling van de concrete bevoegdheid en taak. Een bijzondere wettelijke regeling kan voorgaan.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Controle	Eigen vastlegging
Betrokkene, leeftijd en relevante beslisvaardigheid	[organisatie vult in]
Wettelijke regeling voor de concrete handeling of het recht	[organisatie vult in]
Vertegenwoordiger en geverifieerde bevoegdheid	[organisatie vult in]
Instemming, informatie, bezwaar of geheimhoudingsbelang van de jeugdige	[organisatie vult in]
Selectie van gegevens, ook over ouders en andere derden	[organisatie vult in]
Wie ontvangt welk deel en waarom?	[organisatie vult in]

2.9 Wvggz, Wzd en documenten met bijzondere rechtsgevolgen

De wettelijk bevoegde actoren behouden hun eigen rollen bij verplichte en onvrijwillige zorg. Een concepttekst van Hysio beslist geen zorgmachtiging, crisismaatregel, ernstig nadeel, onvrijwillige zorg of wettelijke stappenplanuitkomst.

Beoordeel een medische verklaring of andere rapportage met wettelijke eisen aan onafhankelijkheid, deskundigheid en besluitvorming afzonderlijk. Leg actor, bron, verplichte inhoud, beoordeling, ondertekening, eventuele inzage en wederhoor, ontvanger en gevolgen vast. Een generieke beschikbaarheid van een Werkstroom is hiervoor geen vrijgave.

Voorkom dat automatische levering leidt tot een als definitief aangemerkt document of een procedurele beslissing zonder de vereiste beoordeling. Beoordeel daarnaast productkwalificatie, de AI-verordening en de privacyrisico's van de precieze functie. Neem slechts de werkelijk benodigde persoonsgegevens op.

Documentcategorie, wettelijke rol, vereiste controle en besluit over inzet: [organisatie vult in].

2.10 Werkgeversschot, keuring en rapportage aan derden

Scheid medische informatie van de functionele informatie die een werkgever of andere opdrachtgever rechtmatig mag ontvangen. Deel geen diagnose, testuitslag of medische privégegevens met een werkgever uitsluitend omdat deze opdrachtgever of betaler is. De bevoegde professional bepaalt de toegestane minimale terugkoppeling vanuit de concrete rol en wettelijke regeling.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Onderdeel	Eigen vastlegging
Opdracht, wettelijke taak en onafhankelijke professionele positie	[organisatie vult in]
Scheiding medisch dossier en werkgeversinformatie	[organisatie vult in]
Toegestane functionele informatie en uitgesloten inhoud	[organisatie vult in]
Ontvanger, autorisatie en verzendcontrole	[organisatie vult in]
Eventuele inzage, correctie of blokkering bij een keuring	[organisatie vult in]
Toegangslogging en bewaartermijn per dossier	[organisatie vult in]

Voor verzekeraar, gemeente, jeugdbescherming, rechterlijke actor of een andere derde wordt dezelfde concrete toets uitgevoerd. Toestemming in een afhankelijke arbeidsverhouding is niet vanzelfsprekend vrij.

Wanneer personeelsgegevens naar een Amerikaanse ontvanger gaan en het Data Privacy Framework als waarborg wordt gebruikt, moet de specifieke dekking voor die gegevens en verwerking zijn onderzocht. De ontvanger moet weten dat de overdracht zulke gegevens omvat. Een gewone vermelding van een actieve certificering beantwoordt deze vraag niet. Voor doorgiften in de keten van Hysio geldt de terugvalwaarborg uit 1.9; de doorgiftebeoordeling vraag je op via legal@hysio.nl.

2.11 Veterinaire variant

Onderscheid diergegevens, persoonsgegevens van eigenaar of houder, gegevens van medewerkers en eventuele informatie over andere mensen. Humane gezondheidsgegevens die toevallig in de bron staan, houden hun eigen bescherming. Gegevens over een dier zijn niet vanzelf persoonsgegevens, maar kunnen door hun koppeling informatie over een persoon opleveren.

Pas humane WGBO-, Wet BIG-, Wkkgz- of artikel 9-aannames niet automatisch toe op diergeneeskundige werkzaamheden. Bepaal de toepasselijke veterinaire beroeps-, dossier- en andere regels afzonderlijk en leg de relatie met de eigenarencommunicatie vast.

Gegevenslaag, doel, grondslag waar nodig, bewaartermijn en ontvanger: [organisatie vult in].

2.12 Transparantie, rechten en raadpleegbaarheid

Informeer betrokkenen begrijpelijk en tijdig over de relevante verwerking: doel, verantwoordelijke, gegevens, AI- en audio-inzet waar relevant, ontvangers, doorgifte, termijn, rechten en contactroute. Gebruik passende taal en vorm. Een algemeen informatieblad is niet voldoende als het de gekozen bijzondere functie of ontvanger niet beschrijft. Hysio stelt een invulbaar cliëntinformatieblad beschikbaar op de pagina met juridische documenten; vul het aan met je eigen gegevens en de functies die je gebruikt.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Richt een uitvoerbare route in voor inzage, correctie, verwijdering, beperking, bezwaar en waar toepasselijk overdraagbaarheid. Niet ieder recht geldt op dezelfde grondslag of zonder uitzondering. Onderscheid een commerciële accountexport, overstappen en het recht van een individuele betrokkene. Een accountbeheerder heeft geen onbeperkt recht op alle cliëntinhoud.

Controleer identiteit en bevoegdheid proportioneel. Vraag niet standaard meer gezondheidsgegevens of een volledige identiteitskopie dan nodig. Selecteer relevante oorspronkelijke en bewerkte informatie en noodzakelijke metadata; alleen het laatste zichtbare concept kan onvoldoende zijn. Bescherm rechten van anderen en motiveer een eventuele beperking. Zolang gegevens nog in Hysio staan, gelden de rechten op inzage en verwijdering ook voor die gegevens; Hysio helpt je ze uit te voeren.

Voor AVG-verzoeken geldt in beginsel reactie binnen één maand, met alleen de toepasselijke wettelijke verlenging en tijdige uitleg. De gewone commerciële exportplanning verlengt deze termijn niet. De eerste kopie en gewone rechtsuitoefening zijn in beginsel kosteloos; uitzonderingen worden alleen toegepast wanneer de wettelijke voorwaarden werkelijk gelden. Beoordeel daarnaast bijzondere dossierregels. Een verzoek wijs je alleen af als het kennelijk ongegrond of buitensporig is (AVG artikel 12 lid 5). Je moet dat aantonen en legt het bewijs vast. Een geschonden inzagerecht kan tot schadevergoeding leiden.

Informatievoorziening, verzoekenprocedure, uitvoerders, termijnen en tests: [organisatie vult in].

2.13 AI-verordening

De AI-verordening geldt naast de AVG. Zij geeft jou en Hysio elk eigen verplichtingen. Hysio zorgt voor uitleg bij elke functie, voor instructie van de eigen medewerkers en voor actualisering bij wijzigingen. Jouw organisatie zorgt voor passende instructie van iedereen die namens jou met Hysio werkt. Leg je antwoorden op de volgende vragen vast.

Vraag	Eigen vastlegging
Welke rol heb jij? Jij of je organisatie bent gebruiksverantwoordelijke voor je eigen inzet van Hysio. Werk je onder het gezag van een organisatie, dan is die organisatie gebruiksverantwoordelijke en ben jij geen afzonderlijke gebruiksverantwoordelijke. Hysio biedt de AI-functies van het platform onder eigen naam aan en is daarom aanbieder van dit AI-systeem in de zin van de AI-verordening, ook waar het onderliggende model van een andere partij komt (artikel 13.2 van de Algemene Voorwaarden). Deze rolverdeling is geen conclusie dat een functie een hoogrisicosysteem is en ligt voor ter externe validatie (zie Open punten)	[organisatie vult in]
Welke maatregelen neem je voor de AI-geletterdheid van wie namens jou met Hysio werkt (artikel 4)?	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Vraag	Eigen vastlegging
Publiceer je met Hysio gemaakte tekst om het publiek te informeren over een onderwerp van algemeen belang, zoals gezondheid, bijvoorbeeld op je website? Wie beoordeelt die inhoudelijk en wie is redactioneel verantwoordelijk (artikel 50 lid 4)? Zonder die beoordeling en verantwoordelijkheid vermeld je dat de tekst met AI is gemaakt. Een verslag in een dossier, een brief aan een verwijzer of een bericht aan een cliënt is geen publicatie	[organisatie vult in]
Welke informatie vraag je bij Hysio op, zoals de rolverklaring? Het AI-label is de zichtbare melding bij AI-Output, de AI-markering de machineleesbare aanduiding; de stand van beide per uitvoerkanaal staat in hoofdstuk 5 en 6 van de AI Act-transparantieverklaring	[organisatie vult in]

Kwalificeert een functie ooit als hoog risico en is een grondrechteneffectbeoordeling nodig, dan kan die naar deze DPIA verwijzen.

Sectie 3: risico's en maatregelen

3.1 Waarderingsmethode

Beoordeel gevolgen voor mensen, zoals gezondheidsschade, verlies van vertrouwelijkheid, discriminatie, onjuiste beslissingen, sociale of financiële schade en belemmering van rechten. Een financieel of reputatierisico voor de organisatie is niet de maatstaf voor de betrokkene.

Gebruik de volgende vier niveaus en motiveer ze per scenario:

Niveau	Impact	Waarschijnlijkheid
1	Beperkte, eenvoudig herstelbare gevolgen	Onder de beschreven omstandigheden niet waarschijnlijk, met onderbouwing
2	Merkbare gevolgen of herstel dat extra inspanning vraagt	Reëel mogelijk
3	Ernstige, langdurige of moeilijk herstelbare gevolgen	Waarschijnlijk of herhaaldelijk mogelijk
4	Zeer ernstige of mogelijk onomkeerbare gevolgen	Voortdurend, zeer waarschijnlijk of reeds herhaaldelijk aangetroffen

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

De vermenigvuldiging van impact en waarschijnlijkheid helpt prioriteren: 1 tot en met 3 laag, 4 tot en met 7 midden, 8 tot en met 11 hoog en 12 tot en met 16 zeer hoog. **Deze rekenregel is geen juridische beslisregel.** Beoordeel bij impact 4 altijd afzonderlijk of de mogelijke schade ook bij een lage kans onaanvaardbaar blijft. Verlaag een ernstig risico niet door alleen naar het product van twee cijfers te kijken. Motiveer iedere afwijking en onzekerheid; onbekend is geen kans 1.

Beoordeel elk risico in drie toestanden:

1. **Referentierisico zonder de te beoordelen beperkende maatregelen.** Noteer welke normale procesvoorwaarden wel zijn aangenomen. Dit maakt de uitgangssituatie reproduceerbaar.
2. **Huidig restrisico.** Alleen de werkelijk ingevoerde en voldoende onderbouwde maatregelen tellen mee voor de gebruikte omgeving en route. Geef aan wat gedeeltelijke invoering wel en niet afdekt.
3. **Verwacht restrisico na aanvullende maatregelen.** Dit is een voorwaardelijke prognose. Vermeld maatregel, eigenaar, termijn, test en vereiste uitkomst. Gebruik haar niet als bewijs dat de huidige verwerking al voldoende is beschermd.

Een maatregel moet het concrete scenario beïnvloeden. Verwijdering van audio herstelt bijvoorbeeld geen verkeerde sprekerstoewijzing in een al vastgesteld dossier. Een AI-label vervangt geen professionele beoordeling. Een overeenkomst sluit het risico van een feitelijk onjuiste configuratie niet uit.

3.2 Zorgbrede risicomatrix

De identificaties R1 tot en met R28 zijn gelijk aan die in eerdere versies van deze template. De omschrijving is waar nodig geactualiseerd. R29 tot en met R32 zijn in versie 4.0 toegevoegd, R33 tot en met R36 in deze versie. Voor iedere toepasselijke rij wordt het beoordelingsrecord onder de tabel ingevuld; neem geen rij zonder motivering als niet van toepassing aan.

ID	Scenario en mogelijke gevolgen	Relevante beheersing om te onderzoeken
R1	Gestolen toegang, te ruime rollen of gebrekkige uitdienstprocedure onthult gevoelige gegevens	Persoonlijke accounts, minimale rechten, sessiebeveiliging, intrekking, apparaatbeheer, logcontrole
R2	Te lange bewaring of onvolledige verwijdering vergroot blootstelling en belemmert rechten	Retentie per laag, uitvoeringsbewijs, lokale opslag, kopieën bij dienstverleners, tijdelijke bestanden en back-upherstel
R3	Onjuiste dienstverlener, verboden dienstgebruik of onvoldoende doorgiftewaarborgen leidt tot onrechtmatige verwerking	Werkelijke entiteit en dienst, voorwaarden, instellingen, register, passend instrument en routebeoordeling

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Scenario en mogelijke gevolgen	Relevante beheersing om te onderzoeken
R4	Transcriptiefout, ontkenningsverlies of ontbrekende context vervalst zorginformatie	Brontoegang, controle van vaktaal en ontkenningen, correctie vóór definitieve vaststelling
R5	Verzonnen, onjuiste of weggelaten inhoud beïnvloedt dossier of besluit	Functiegrenzen, onderscheid bron en voorstel, professionele controle en ontvangst van volledige context
R6	Inhoud of besluit wordt aan de verkeerde persoon toegeschreven	Spreker- en cliëntcontrole, bronattributie, scheiding van meerdere cliënten
R7	Onnodige identificatoren, derdegegevens of volledige documenten worden verwerkt	Invoerselectie, audioafbakening, metadata- en bijlagecontrole, beperkte supportinformatie
R8	Ontwerp, interface, productuitingen of feitelijk gebruik overschrijden de beoordeelde functie	Afstemming beoogd doel, individuele werkstroomtoets, opleiding, autorisaties en wijzigingsbeheer
R9	Noodzakelijke gegevens ontbreken in het primaire dossier of kunnen bij exit niet worden veiliggesteld	Tijdige overname, complete exporttest, continuïteit, ontvangst- en volledigheidscontrole, overstaprechten uit de Regeling Datatoegang
R10	Incident wordt te laat herkend of gemeld en veroorzaakt vermijdbare vervolgschade	Bereikbare incidentcontacten, detectie, ketenmelding, eigen meldbeslissing en oefeningen
R11	Onvoldoende informatie verhindert een vrije keuze of effectieve rechtsuitoefening	Contextgerichte uitleg, toegankelijke informatie, werkbaar alternatief en verzoekenroute
R12	Activering of wijziging van een dienstverlener voldoet niet aan de voorafgaande voorwaarden	Wijzigingsbericht, bezwaarroute, volledige voorwaarden, actueel configuratie- en verkeersbewijs
R13	Beroepsgeheim wordt doorbroken door onbevoegde inzage, verstrekking of supportgebruik	Taakgebonden toegang, geheimhouding, minimale ontvangersscope en veilige ondersteuning

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Scenario en mogelijke gevolgen	Relevante beheersing om te onderzoeken
R14	Cliëntcontext leidt volgens ontwerp of door fouten tot stereotypering, ongewenste afleiding of schijnzekerheid	Noodzaak van context, onderscheid feit en onzekerheid, test op ongegronde aanvulling en discriminatie
R15	Genetische of voortplantingsinformatie onthult gevoelige gegevens over meer personen	Beperkte gegevens- en ontvangersscope, extra professionele afweging, vertegenwoordiging
R16	Medische inhoud komt ten onrechte bij werkgever of opdrachtgever	Gescheiden dossiers, rolcontrole, minimale functionele rapportage, controle vóór verzending
R17	Onjuiste leeftijds-, gezags- of bevoegdheidsaanname schendt rechten en vertrouwelijkheid	Toepasselijk regime, concrete handeling en geverifieerde vertegenwoordiging
R18	Concept wordt gebruikt als dwangbesluit of wettelijke verklaring zonder vereiste bevoegdheid	Afzonderlijke wettelijke en professionele toets, ondertekening en blokkade tegen ongemerkte vaststelling
R19	Rapportage gaat naar een verkeerde autoriteit of bevat meer dan de opdracht toestaat	Opdracht, grondslag, ontvanger, minimale inhoud, inzage of wederhoor waar toepasselijk
R20	Diergegevens en menselijke persoonsgegevens krijgen ten onrechte dezelfde grondslag of rechtenroute	Gescheiden gegevenslagen, veterinaire context en beoordeling van eventuele humane gezondheidsgegevens
R21	Triage- of spoedfunctie beïnvloedt urgentie onjuist of vertraagt hulp	Werkelijke functie-invloed, bevoegde beoordeling, noodprocedure en geen afhankelijkheid van Hysio voor spoedhulp
R22	Interpretatie, hypothese, score, code of behandelvoorstel wordt onveilig of als vaststaand gebruikt	Individuele kwalificatie, bron-versus-voorstel, medische beoordeling, rechten op bronnen en volledige uitvoercontext

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Scenario en mogelijke gevolgen	Relevante beheersing om te onderzoeken
R23	Automatische conceptlevering wordt definitief dossiergebruik of bereikt een onbevoegde ontvanger	Voorafgaande ontvangerbevoegdheid, afgeschermde werkvoorraad, conceptstatus en controle vóór vaststelling
R24	Te ruime API-rechten, tweede omzetting of verkeerde veldmapping verandert inhoud of scope	Beperkte rechten, validatie, herkomst, schematests en semantische controle in het ontvangende systeem
R25	Feedback of een Sessiereferentie brengt zorginhoud in een ongeschikte e-mailroute	Minimale berichten, passende dienstvoorwaarden, beveiligde inhoudsroute en roltoets
R26	Routinematige bevestiging maakt een wezenlijk besluit feitelijk automatisch	Tijd, deskundigheid, onafhankelijkheid, afwijsmogelijkheid en onderzoek van de werkelijke beslispraktijk
R27	Een universele WGBO-aanname geeft verkeerde bewaar-, vernietigings- of vertegenwoordigingsregels	Regimematrix per taak, document en betrokkene; juridisch gecontroleerde uitzonderingen
R28	Strafrechtelijke of forensische gegevens worden zonder passende wettelijke basis verwerkt	Artikel 10-regime, concrete taak, beperkte personen en ontvangers, geheimhouding
R29	Lokale herstelkopieën blijven op een gedeeld, verloren of afgedankt apparaat staan	Werkelijke browseropslag, bruikbaarheidsgrens, opruimtrigger, apparaatbeveiliging en wissen bij afstoten
R30	Uitvoer laat een waarschuwing, onzekerheid of ontbrekend onderdeel weg terwijl de overblijvende conclusie overtuigend lijkt	Test ieder uitvoerpad op inhoud en context; ontvanger kan ontbrekende beoordeling herkennen
R31	Nieuwe hypotheses en brede contextregistratie vergroten de privacy-inbreuk terwijl het systeem volgens ontwerp werkt	Noodzaak van afleiding, transparantie, beperkte scope en verwerking van correctie of betwisting

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Scenario en mogelijke gevolgen	Relevante beheersing om te onderzoeken
R32	Uitval, leveranciersafhankelijkheid of overname maakt noodzakelijke informatie onbereikbaar	Terugvalproces, bestaande dossiers, geteste export, herstel en contractuele continuïteit, overstaprechten uit de Regeling Datatoegang
R33	Een Sessie in Hysio gaat dienen als schaduwdossier of dubbel dossier naast het eigen dossier	Tijdig overzetten naar het eigen dossier, Sessie laten verwijderen na overzetten, waarschuwing vóór verwijdering
R34	Een medewerker voert cliëntgegevens in een ander, niet overeengekomen AI-hulpmiddel in	Afspraken, beperking tot het overeengekomen platform, opleiding
R35	Het onderliggende AI-model is ontwikkeld met onrechtmatig verwerkte gegevens	Informatie van Hysio over haar beoordeling van de modelaanbieder en de herkomst van trainingsgegevens
R36	Een doorgiftewaarborg in de keten valt weg	Terugvalroute per doorgifte, controle van de doorgiftebeoordeling, aankondiging door Hysio
RX	Aanvullend lokaal scenario	[organisatie vult in]

Beoordelingsrecord, herhalen per risico:

Onderdeel	Vastlegging
Risico-ID, betrokkene, Werkstroom en route	[organisatie vult in]
Gebeurtenis of voorziene werking; oorzaak en mogelijke schade	[organisatie vult in]
Blootstelling, kwetsbaarheid en onderbouwde uitgangssituatie	[organisatie vult in]
Referentie-impact, kans en beoordeling	[organisatie vult in]
Bestaande maatregelen met status en bewijs	[organisatie vult in]
Huidige impact, kans, restrisico en motivering	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Onderdeel	Vastlegging
Extra maatregelen, eigenaar, datum en acceptatietest	[organisatie vult in]
Verwacht restrisico na uitvoering, met voorwaarden	[organisatie vult in]
Ernstige gevolgen ondanks lage kans en samenloop met andere risico's	[organisatie vult in]
Besluit: beperken, anders inrichten, niet starten of artikel 36-route	[organisatie vult in]
Reviewer, datum en volgend controlemoment	[organisatie vult in]

3.3 Technische en organisatorische maatregelen van Hysio

Hieronder staan de maatregelen die Hysio treft, met per onderwerp wat je voor je eigen beoordeling bij Hysio kunt opvragen. De contractuele basis staat in Bijlage 2 van de Verwerkersovereenkomst. Beveiligingsgevoelige gegevens verstrekt Hysio onder passende geheimhouding, zonder een noodzakelijke controle onmogelijk te maken. Vraag de opgave altijd op voor de omgeving en de datum die voor jouw organisatie gelden, en leg die datum in je beoordeling vast. De stukken uit de rechterkolom vraag je op via de adressen in 6.4.

De kolom Stand bij de ingangsdatum zegt per maatregel of die op de ingangsdatum van deze versie is ingericht, of een toezegging is die vanaf of vóór de genoemde mijlpaal geldt. Een toezegging is een verplichting van Hysio, maar nog geen uitvoering; neem haar in je beoordeling op als geplande maatregel. De stand komt overeen met de stand van dezelfde maatregel in Bijlage 2 van de Verwerkersovereenkomst; bij verschil geldt de stand in Bijlage 2.

ID	Maatregel van Hysio	Stand bij de ingangsdatum	Wat je voor je eigen beoordeling opvraagt
HM01	Wachtwoorden worden gehasht opgeslagen en het aantal inlogpogingen wordt begrensd	Ingericht	De instellingen die voor jouw omgeving gelden, en de datum waarop je die hebt gecontroleerd
HM02	Toegang verloopt via rollen en autorisatiecontroles per Account, Sessie en koppeling, met controle op de eigenaar van de Sessie	Ingericht	Een proef op iedere voor jou relevante scope, inclusief de afwijzing van onbevoegde toegang
HM03	Toegang is in tijd begrensd en kan worden ingetrokken.	Contractuele maatregel. Vraag	Welke authenticatie-, sessieduur-,

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Maatregel van Hysio	Stand bij de ingangsdatum	Wat je voor je eigen beoordeling opvraagt
	Beheer- en productietoegang is beperkt tot benoemde personen, verloopt via persoonlijke accounts met een tweede factor en wordt ten minste ieder kwartaal gecontroleerd	bewijs voor je eigen route op	verlengings- en intrekkingsinstellingen voor jouw omgeving gelden
HM04	Publieke diensten en verbindingen met dienstverleners zijn alleen bereikbaar via beveiligd transport (TLS). Voor beheerverbindingen geldt dit vanaf de ingangsdatum van deze versie	Ingericht; beheerverbindingen: Toezegging vanaf de ingangsdatum van deze versie	De dekking van de transportketen, inclusief beheerverbindingen, interne verbindingen en verbindingen met dienstverleners
HM05	De inhoudsvelden van Sessies in de database (ingevulde antwoorden, transcript en uitvoer) worden versleuteld opgeslagen. Sessietitels en bestandsnamen bevatten geen ingevulde antwoorden	Eerste zin: Ingericht. Tweede zin: Toezegging vanaf de vooraf schriftelijk vastgelegde datum voor de betrokken functie	Welke andere lagen versleuteld zijn, zoals titels, bestandsnamen en audio- en uploadbestanden op schijf, en hoe sleutelbeheer, sleutelback-up en rotatie zijn geregeld
HM06	Sessiedocumenten worden alleen via een beveiligde route met eigendomscontrole geleverd	Ingericht	Hoe oudere bestanden, downloads en tijdelijke objecten in alle omgevingen zijn afgedekt
HM07	Om onderbroken werk te kunnen herstellen, kan het platform gegevens tijdelijk in de browser van de Gebruiker bewaren, binnen de termijn uit Bijlage 1 van de Verwerkersovereenkomst. Het platform ruimt ze op na veilige	Contractuele maatregel. Vraag bewijs voor je eigen route op	De bewaarduur, de opruimroute en de instructie voor gedeelde of offline apparaten; dit is een verwerking op jouw apparaten die je in je eigen beoordeling meeneemt. De opslag

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Maatregel van Hysio	Stand bij de ingangsdatum	Wat je voor je eigen beoordeling opvraagt
	verwerking, bij uitloggen, bij een verlopen inlogsessie en bij de eerstvolgende opening van het platform op dat apparaat, en toont bij herstel de bewaarduur		per item staat in hoofdstuk 8 van de Privacyverklaring
HM08	Audio, transcriptietaken en foutmeldingen op de servers van Hysio worden verwijderd binnen de termijnen uit Bijlage 1 van de Verwerkersovereenkomst	Contractuele maatregel. Vraag bewijs voor je eigen route op	Het opruimoverzicht met aantallen over een recente periode en de dekking van alle opslaglagen
HM09	Voor Sessies, bijlagen, logs en back-ups geldt een vastgelegde verwijder- en herstelprocedure; je kunt de datum en uitkomst van de laatste hersteltest opvragen. Back-ups zijn versleuteld en toegangsbeperkt	Contractuele maatregel. Vraag bewijs voor je eigen route op	De procedure en de meest recente verwijder- en hersteltest per laag
HM10	Het verslag van een afgeronde Sessie is te downloaden als TXT, PDF of DOCX, met de titel, de Werkstroom, het tijdstip van afronding en de actuele versie van het verslag; zolang de titel van de Sessie je antwoorden in de intake bevat, staan die ook in het bestand. Uploads download je per Sessie apart. Transcript, nog aanwezige audio, overige invoer en de oorspronkelijke versie naast een bewerking krijg je via de begeleide integrale archiefkopie uit de Regeling Datatoegang, voor zover die gegevens binnen de	Ingericht	De omvang van de begeleide route, inclusief bron, bewerkingen, onderlinge relaties en de juiste ontvanger

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Maatregel van Hysio	Stand bij de ingangsdatum	Wat je voor je eigen beoordeling opvraagt
	termijnen uit Bijlage 1 van de Verwerkersovereenkomst nog bestaan		
HM11	Concepten kunnen door de professional worden bewerkt en vastgesteld	Ingericht	Hoe je de professionele controle vóór teruglevering of gebruik in je eigen werkwijze organiseert; Hysio dwingt die controle niet af
HM12	Gestructureerde uitvoer en postback zijn beschikbaar voor overeengekomen routes	Ingericht	Mapping, conceptstatus, minimale rechten en het ontvangstgedrag van de ontvangende omgeving, en of de afgeleverde gegevens een machineleesbare aanduiding van AI-herkomst en conceptstatus dragen
HM13	De Verwerkersovereenkomst beperkt de inschakeling van Subverwerkers tot Bijlage 3. Met iedere Subverwerker uit Bijlage 3 geldt een verwerkersafspraak die modeltraining op Klantdata uitsluit	Contractuele maatregel. Vraag bewijs voor je eigen route op	De leveranciersspecificatie uit Bijlage 3 en de ketenopgave per overeenkomst, met entiteit, dienst, landen, bewaring en doorgiftewaarborg
HM14	Support- en incidentverwerking is beperkt tot het noodzakelijke en in beleid vastgelegd	Ingericht	De contactroute, bereikbaarheid, veilige inhoudsroute en de instructie aan medewerkers, en hoe de toegelaten supportroute uit Bijlage 3 voorkomt dat zorginhoud als vrije

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Maatregel van Hysio	Stand bij de ingangsdatum	Wat je voor je eigen beoordeling opvraagt
			tekst in interne e-mail terechtkomt
HM15	Hysio meldt een datalek zonder onredelijke vertraging en uiterlijk vierentwintig uur na eigen kennisneming. Een beveiligingsincident zonder datalek dat de dienst voor je organisatie wezenlijk aantast of kan aantasten, meldt Hysio zonder onredelijke vertraging (artikel 13bis van de Verwerkersovereenkomst); valt je organisatie onder de Cyberbeveiligingswet, dan levert Hysio de informatie die je voor je meldingen nodig hebt	Ingericht	De ketenbereikbaarheid buiten Werkdagen en de meest recente oefening of evaluatie
HM16	De juridische set bevat de informatie en gebruiksinstructies voor professionals en betrokkenen	Ingericht	Hoe je die informatie tijdig bij je eigen betrokkenen en professionals krijgt
HM17	Hysio houdt een verwerkingsregister, een risicoregister en een leveranciersregister bij. Wijzigingen per functie en versie legt Hysio vast vanaf de vooraf schriftelijk vastgelegde datum voor de betrokken functie	Eerste zin: Ingericht. Tweede zin: Toezegging vanaf de vooraf schriftelijk vastgelegde datum voor de betrokken functie	De aansluiting van die registratie op de functies die voor jou daadwerkelijk zijn geactiveerd
HM18	Hysio heeft een door het bestuur vastgesteld beveiligingsbeleid; de samenvatting kun je opvragen. Hysio werkt conform de AVG en volgens de werkwijze van	Ingericht	Welke certificaten, assurance-rapporten en samenvattingen van beveiligingstests er zijn, met uitgever, scope en

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Maatregel van Hysio	Stand bij de ingangsdatum	Wat je voor je eigen beoordeling opvraagt
	ISO 27001 en NEN 7510; de certificeringstrajecten zijn in aanloop.		datum; zolang er geen zijn, vermeldt Hysio dat
HM19	Hysio verzorgt geen zorgtoegangslogging in de zin van artikel 5 van het Besluit elektronische gegevensverwerking door zorgaanbieders, tenzij je dat vóór de eerste verwerking schriftelijk met Hysio afspreekt; anders regel je die logging in je eigen dossiersysteem (zie 1.10). Vastlegging van toegang door medewerkers van Hysio tot sessie-inhoud geldt vanaf de vooraf schriftelijk vastgelegde datum voor de betrokken functie	Toezegging vanaf de vooraf schriftelijk vastgelegde datum voor de betrokken functie	Hoe je zorgtoegangslogging in je eigen dossiersysteem borgt; zodra de vastlegging bij Hysio er is, de reikwijdte, de bescherming tegen wijziging, de toegangsrechten en de bewaartermijn
HM20	Gegevensrechten en eindoverdracht zijn contractueel uitgewerkt in de Regeling Datatoegang	Ingericht	Een proef op de volledige scope en de termijnen met geschikte testgegevens
HM21	Ontwikkel- en productieomgevingen zijn gescheiden. Testen gebeurt met synthetische testgegevens of gegevens waarvan de onherleidbaarheid is getoetst. Kopieën van productiegegevens buiten de productieomgeving bestaan alleen versleuteld, doelgebonden en in tijd begrensd voor een vastgelegd incident	Contractuele maatregel. Vraag bewijs voor je eigen route op	Het register van kopieën buiten productie, met doel, versleuteling en verwijderdatum

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

ID	Maatregel van Hysio	Stand bij de ingangsdatum	Wat je voor je eigen beoordeling opvraagt
HM22	Hysio deelt bekende beveiligingsrisico's in als kritiek, hoog, middel of laag, perkt ze in en herstelt ze binnen de behandeltermijnen uit Bijlage 2 van de Verwerkersovereenkomst, en registreert risico, besluit, maatregel en responstijd. Een onafhankelijke beveiligingstest volgt vóór de vooraf schriftelijk vastgelegde datum voor de betrokken functie en daarna ten minste jaarlijks en na een wezenlijke wijziging	Indeling, behandeltermijnen en registratie: Toezegging vanaf de ingangsdatum van deze versie. Onafhankelijke beveiligingstest: Toezegging vóór de vooraf schriftelijk vastgelegde datum voor de betrokken functie	De behandeltermijnen en, zodra beschikbaar, een samenvatting van de laatste onafhankelijke test
HM23	Invoer wordt gecontroleerd op bestandstype, omvang, schadelijke inhoud en misbruik, met afzonderlijke grenzen voor audio, documenten en tekst	Toezegging vanaf de vooraf schriftelijk vastgelegde datum voor de betrokken functie	Welke grenzen en controles voor de door jou gebruikte invoerroutes gelden
HM24	Hysio evalueert de maatregelen ten minste jaarlijks en bij een relevante wijziging, een incident of een nieuwe beroepscontext, en legt restrisico, compensatie en herstel termijn vast	Toezegging vanaf de vooraf schriftelijk vastgelegde datum voor de betrokken functie	Zodra beschikbaar, het laatste evaluatieverslag met de vastgestelde restrisico's

Hysio werkt conform de AVG en volgens de werkwijze van ISO 27001 en NEN 7510; de certificeringstrajecten zijn in aanloop. Hysio betrekt NEN 7510-1:2024, NEN 7510-2:2024+A1:2026 en ISO/IEC 27001:2022 bij haar risicoanalyse; de twee NEN 7510-delen zijn per 1 juni 2026 aangewezen. Waar zorgwetgeving bepaalde beveiligings- of loggingnormen voorschrijft, rust die plicht op de zorgaanbieder; stel de toepasselijkheid en de aangewezen editie vast. Voldoen aan een wettelijke norm, een onafhankelijke beoordeling en certificering zijn verschillende zaken. Een eventuele toekomstige certificering is nooit een reden om noodzakelijke maatregelen uit te stellen.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

3.3.1 Controleblad Hysio-maatregelen

Leg per gebruikte HM-maatregel vast: document en versie, omgeving, datum, bewijssoort, wat is getest, wat niet is getest, bevinding, herstelactie en oordeel over toepasbaarheid. Een onbekende maatregel blijft onbekend totdat passend bewijs beschikbaar is. Zie je een tegenstrijdigheid, vraag Hysio dan de betreffende route opnieuw te beoordelen.

3.3.2 Nog in te voeren maatregelen

Een nieuwe of aangescherpte maatregel wordt als apart actiepunt opgenomen. Vermeld gewenste werking, reikwijdte, eigenaar en toetsbaar resultaat. Neem maatregelen met de stand Toezegging op als voorwaarde of actiepunt, met de mijlpaal als controlemoment.

3.4 Maatregelen van je organisatie

Onderwerp	Minimaal te organiseren	Eigen bewijs
Rollen en toegang	Persoonlijke accounts, minimale taakrechten, periodieke controle en intrekking bij vertrek. Vraag Hysio welke toegangsmethode en welke aanvullende maatregelen, zoals een extra authenticatiefactor, voor jouw accounts gelden (Bijlage 2, onderdeel B, van de Verwerkersovereenkomst); weeg de uitkomst mee bij R1	[organisatie vult in]
Apparaten	Vergrendeling, updates, opslagbeveiliging, zorgvuldig gedeeld gebruik en wissen bij verlies of afstoten	[organisatie vult in]
Invoer en audio	Doelgerichte selectie, informatie, toepasselijke instemming, controle van derden en achtergrondgesprekken	[organisatie vult in]
Professionele beoordeling	Tijd, deskundigheid, toegang tot bron, correctie en werkelijke mogelijkheid tot afwijzen	[organisatie vult in]
Ontvangers	Voorafgaande bevoegdheid, minimale inhoud, passende beveiliging en geteste ontvangststatus	[organisatie vult in]
Dossier en bewaring	Tijdige vaststelling in het eigen dossier, passende termijn, verzoeken- en vernietigingsprocedure; Sessie laten verwijderen na overname in het eigen dossier	[organisatie vult in]
Incidenten	Bereikbaar contact, interne beoordeling, meldroutes, terugval zonder Hysio en oefening	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Onderwerp	Minimaal te organiseren	Eigen bewijs
Leveranciers	Actuele documenten, controle van wezenlijke maatregelen, bezwaarmeldingen en wijzigingsbeoordeling; aantoonbare controle op informatiebeveiliging, intensiever bij hoog risico; bij de Cyberbeveiligingswet afspraken over incidenten, controle op nakoming en informatie voor het eindverslag; gebruik waar nodig je auditrecht uit artikel 14 van de Verwerkersovereenkomst (AVG artikel 28 lid 3 onder h)	[organisatie vult in]
Opleiding	Functiegrenzen, fouten herkennen, omgaan met hypotheses en geen routinematig overnemen; AI-geletterdheid volgens artikel 4 van de AI-verordening	[organisatie vult in]
Betrokkenen	Begrijpelijke informatie, toegankelijke rechtenroute en passende participatie	[organisatie vult in]
AI-hulpmiddelen	Geen cliëntgegevens invoeren in andere AI-hulpmiddelen dan het overeengekomen platform, vastgelegd in eigen beleid	[organisatie vult in]
Logging	Zorgtoegangslogging en de bewaartermijn daarvan, in je eigen dossiersysteem of via een schriftelijke afspraak met Hysio; een vastgelegde keuze voor de verantwoording van de toegang tot Sessies in Hysio	[organisatie vult in]

3.5 Restrisico en besluitregels

Een hoog restrisico wordt niet gesloten met alleen een handtekening van de leiding. Onderzoek extra maatregelen, een minder ingrijpende inrichting of afzien van de betreffende verwerking. Wanneer het hoge risico niet voldoende kan worden beperkt en je de verwerking toch voorneemt, volg je de voorafgaande raadpleging van artikel 36.

Een lage rekenscore ontslaat je niet van de afzonderlijke toets van rechtmatigheid, noodzaak, zeer ernstige mogelijke schade en rechten. Een onbekende essentiële route via een dienstverlener, onbevoegde verstrekking of strijd met toepasselijke dienstvoorwaarden wordt niet opgelost door een risicogetal te verlagen.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Risico of voorwaarde	Huidige conclusie	Vereiste actie en bewijs	Eigenaar en datum	Startstatus
[organisatie vult in]	[invullen]	[invullen]	[invullen]	[ ] niet starten [ ] na voorwaarden [ ] toegestaan binnen vastgelegde scope

Samenvattend oordeel over noodzaak, evenredigheid, huidig restrisico en resterende voorwaarden: [organisatie vult in].

Sectie 4: raadpleging, advies en formele vaststelling

4.1 Voorafgaande raadpleging van de Autoriteit Persoonsgegevens

Als na de beoordeling geen voldoende maatregelen beschikbaar zijn om het hoge risico te beperken, raadpleegt de verantwoordelijke de AP vóór de betrokken verwerking. Start die verwerking niet tijdens de raadpleging. Onderzoek ook een eventuele bijzondere nationale plicht tot raadpleging of toestemming.

De aanvraag bevat de DPIA, doeleinden en middelen, verantwoordelijkheden van betrokken partijen, maatregelen en waarborgen, FG-contact indien toepasselijk en gevraagde aanvullende informatie. De aanvraag dien je in via het elektronische kanaal dat de AP daarvoor aanwijst. Hysio levert de benodigde informatie binnen haar rol en beschikbare kennis. Je organisatie is verantwoordelijk voor indiening en besluitvorming.

Artikel 36 lid 2 noemt voor het daar bedoelde schriftelijke advies maximaal acht weken, met een mogelijke verlenging van zes weken wegens complexiteit. De termijn kan worden opgeschort in afwachting van gevraagde informatie. Een verlopen termijn, ontvangstbevestiging of gewone reactie is geen automatische goedkeuring. Verwerk het inhoudelijke advies en eventuele maatregelen of bevoegdheidsuitoefening van de AP en beoordeel de verwerking opnieuw.

Vastlegging	Waarde
Hoge risico's en onderzochte alternatieven	[organisatie vult in]
Reden waarom aanvullende beperking niet volstaat	[organisatie vult in]
DPIA-versie en bijlagen bij de aanvraag	[organisatie vult in]
Verantwoordelijkheden, doeleinden, middelen en FG-contact	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Vastlegging	Waarde
Datum, referentie, vragen en antwoorden	[organisatie vult in]
Niet-starten van de betrokken route tijdens raadpleging	[organisatie vult in]
Ontvangen uitkomst, maatregelen, nieuwe beoordeling en besluit	[organisatie vult in]

4.2 Standpunt van betrokkenen

Vraag waar passend betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking. Leg methode, groep, privacywaarborgen, uitkomst en de gevolgen voor je keuzes vast. Houd rekening met commerciële of algemene belangen en beveiliging. Als je geen standpunt vraagt, motiveer concreet waarom dat niet passend of mogelijk is.

Het verstrekken van een informatieblad of het verkrijgen van toestemming is op zichzelf geen raadpleging over de effecten van de verwerking. Als je van ontvangen opvattingen afwijkt, leg je de reden vast.

Passendheidsafweging, methode, bevindingen en verwerking: [organisatie vult in].

4.3 Advies van de FG

Als een FG is aangewezen, wordt diens advies ingewonnen. De FG adviseert onafhankelijk en houdt toezicht op de uitvoering; de verantwoordelijke blijft de besluitvormer. Leg advies, gevolgde maatregelen en gemotiveerde afwijkingen vast.

Beoordeel afzonderlijk of een FG verplicht is, onder meer bij een overheidsorgaan of bepaalde grootschalige kernactiviteiten. Een kleine organisatie of het ontbreken van een interne functietitel beantwoordt die vraag niet. Een verplichte aanstelling kan niet worden vervangen door een roadmap. Vermijd belangenconflicten bij de persoon die onafhankelijk toezicht moet houden.

Aanstellingsbeoordeling, contact, advies en verwerking: [organisatie vult in].

4.4 Externe juridische en professionele toets

Vraag gericht advies waar de concrete toepassing of risico's dat nodig maken. Benoem de precieze vraag, functie, gegevensstroom, documentversie, aannames en gewenste uitkomst. Een externe beoordeling van een oude set of beperkte productscope geldt niet automatisch voor nieuwe functies.

Een juridische lezing door AI en een technische test zijn geen onafhankelijke externe audit, medische validatie of certificering. Leg de daadwerkelijk ontvangen beoordeling en haar scope vast. Los zelfstandig te beantwoorden bronvragen op; gebruik een algemene verwijzing naar een adviseur niet als vervanging voor de eigen analyse.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Externe opdracht, ontvangen oordeel, beperkingen en opvolging indien van toepassing:
[organisatie vult in].

4.5 Formele goedkeuring

Beslispunt	Vastlegging
Verwerking en exact toegelaten scope	[organisatie vult in]
Doelen, grondslagen, noodzakelijkheid en evenredigheid vastgesteld	[organisatie vult in]
Leveranciersinformatie en essentiële maatregelen voldoende onderbouwd	[organisatie vult in]
Eigen maatregelen ingevoerd en gecontroleerd	[organisatie vult in]
Huidig restrisico, ernstige gevolgen en samenloop beoordeeld	[organisatie vult in]
FG-advies en betrokkenenstandpunt verwerkt waar toepasselijk	[organisatie vult in]
Artikel 36: niet nodig, afgerond of nog nodig	[organisatie vult in]
Besluit	[ ] niet uitvoeren [ ] anders inrichten [ ] eerst raadplegen [ ] voorwaardelijk toestaan [ ] toestaan binnen de omschreven scope
Voorwaarden, bewijs, eigenaar en uiterste datum	[organisatie vult in]
Bevoegde besluitvormer, functie en datum	[organisatie vult in]
Feitelijke start pas na vervulde voorwaarden	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Een voorwaardelijk besluit geeft geen toestemming om de afhankelijke verwerking alvast met echte persoonsgegevens te starten. Onafhankelijke, reeds voldoende beoordeelde routes kunnen een eigen besluit krijgen. Een onopgelost kerngebrek in een gedeelde voorziening kan meerdere routes raken.

Sectie 5: herbeoordeling en wijzigingsbeheer

Controleer de beoordeling ten minste wanneer het risico verandert. Als werkbeleid wordt een jaarlijkse actualiteitscontrole geadviseerd, naast beoordeling vóór wezenlijke wijzigingen. De jaarlijkse frequentie is geen algemene wettelijke termijn uit artikel 35.

Heropen de relevante onderdelen bij wijziging van:

- doel, omvang, beroepscontext, betrokkenen of gegevenscategorie;
- Werkstroom, prompt, model, cliëntcontext of inhoudelijke invloed;
- dienstverlener, voorwaarden, verwerkingslocatie, retentie, toegang of doorgiftewaarborg;
- accountrollen, technische integratie, postback of ontvangend systeem;
- lokale opslag, browsergedrag, apparaat of mobiele toegang;
- verwijdering, export, primaire dossiervoering of continuïteit;
- feitelijke menselijke controle of de mate waarin output een besluit bepaalt;
- incident, klacht, auditbevinding of relevante wet- en regelgeving;
- de AVG-regels of lijsten van verwerkingen met of zonder DPIA-plicht;
- een doorgiftewaarborg in de keten, bijvoorbeeld door een uitspraak, of het recht of de praktijk van een derde land;
- Europese richtsnoeren over pseudonimiseren en anonimiseren, zodra daarvan een eindversie verschijnt.

Kondigt Hysio een nieuwe of vervangende Subverwerker aan, gebruik dan de aankondigingstermijn van dertig kalenderdagen om 1.9 en de risico's R3, R12 en R36 opnieuw te beoordelen, zodat je zo nodig nog bezwaar kunt maken.

Een nieuw beleidsdocument bewijst niet dat de bijbehorende maatregel is ingevoerd. Een gewijzigde juridische tijdlijn is aanleiding om de gevolgen voor de concrete verwerking te onderzoeken. De Data Act en EHDS worden meegenomen voor zover zij de gebruikte gegevensstromen, rechten, exit of risico's raken; hun bestaan is geen zelfstandig DPIA-criterium. Onder de EHDS moeten zorgaanbieders vanaf 2029 en 2031 gegevens uit de prioritaire categorieën in een EPD-systeem registreren; de uitvoer van Hysio hoort in je eigen dossier. De Wet DIAZ en de verdere uitwerking van de Wegiz zijn ontwikkelingen zonder vaste datum.

Beheeronderdeel	Waarde
Eigenaar en vervanger	[organisatie vult in]
Volgende geplande controle	[organisatie vult in]

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Beheeronderdeel	Waarde
Ontvanger van Hysio- en leverancierswijzigingen	[organisatie vult in]
Wie beoordeelt juridische, technische en professionele impact?	[organisatie vult in]
Wijziging, getroffen risico-ID's en documenten	[organisatie vult in]
Nieuwe versie, besluit en maatregelen	[organisatie vult in]

Sectie 6: afrondingschecklist en bronnen

6.1 Volledigheidscheck

- [ ] Scope, rollen, team, peildatum en gebruikte versies zijn vastgelegd.
- [ ] Eventuele naleving van een goedgekeurde artikel 40-gedragscode is overeenkomstig artikel 35 lid 8 meegewogen; goedkeuring, scope en naleving zijn onderbouwd.
- [ ] Iedere gebruikte Werkstroom en uitvoerroute is afzonderlijk gekoppeld aan de beoordeling.
- [ ] Gegevens, doelen, ontvangers, landen en de volledige levensloop zijn beschreven.
- [ ] Artikel 6, artikel 9 of 10 waar relevant, beroepsgeheim en bijzondere bevoegdheden zijn beoordeeld.
- [ ] Noodzaak, werkbare alternatieven en evenredigheid zijn onderbouwd.
- [ ] Gevolgen van de ontworpen verwerking en gevolgen van fouten of misbruik zijn beide onderzocht.
- [ ] Menselijke controle, conceptlevering en definitieve vaststelling zijn concreet ingericht.
- [ ] Retentie, lokale opslag, kopieën bij dienstverleners, exit en back-upherstel zijn niet uitsluitend op beleidsbeloften gebaseerd.
- [ ] Het informeren van betrokkenen en de toepasselijke beroepsnorm zijn beoordeeld.
- [ ] Beoordeeld is of je inrichting via Hysio dossiers raadpleegbaar maakt voor een andere zorgaanbieder.
- [ ] Vastgelegd is wie zorgtoegangslogging verzorgt en hoe lang.
- [ ] Vastgelegd is waar het enige primaire dossier staat en wanneer Sessies na overname worden verwijderd.
- [ ] De meldroutes zijn bekend: datalekken aan de Autoriteit Persoonsgegevens (AVG artikel 33 en 34), calamiteiten volgens de Wkkgz, de Jeugdwet of de Wmo 2015, en waar van toepassing significante incidenten onder de Cyberbeveiligingswet.
- [ ] De vragen over de AI-verordening zijn beantwoord.
- [ ] Beoordeeld is of je organisatie onder de Cyberbeveiligingswet valt.
- [ ] Risico's hebben onderbouwde scores, een ernstige-gevolgentoets en een afzonderlijke huidige en verwachte toestand.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

- [ ] Essentiële maatregelen zijn bewezen ingevoerd of vormen een expliciete voorwaarde vóór gebruik.
- [ ] Betrokkenen, FG en eventuele externe beoordelaar zijn passend betrokken en hun inbreng is verwerkt.
- [ ] Artikel 36 en bijzondere raadplegingsplichten zijn beoordeeld.
- [ ] Besluit, beperkingen, voorwaarden, eigenaars en herbeoordeling zijn vastgelegd.
- [ ] Publiek gedeelde informatie bevat geen onnodige persoonsgegevens of beveiligingsgevoelige details.

6.2 Primaire bronnen

De toepasselijke versie en onderdelen worden bij vaststelling van je eigen DPIA opnieuw gecontroleerd. Dit overzicht maakt wetgeving en aanvullende uitleg herkenbaar:

- AVG, onder meer artikelen 4 tot en met 6, 9, 10, 12 tot en met 22, 25, 26, 28, 30, 32 tot en met 40 en hoofdstuk V.
- UAVG, waaronder de actuele regels voor vertegenwoordiging, gezondheidsgegevens en identificatienummers.
- WGBO in Boek 7 BW, artikelen 7:446 tot en met 7:468 voor zover toepasselijk; daarnaast de relevante bijzondere sectorwet.
- AP-besluit verplichte DPIA's, Staatscourant 2019, 64418.
- AP-uitleg van 11 december 2018 over grootschaligheid voor alle zorgaanbieders, inclusief de uitbreiding naar overige zorgaanbieders en de nuancering voor apotheken.
- WP248 rev.01, herpublicatie door de CNIL, aanvullende uitleg over de DPIA, geen afzonderlijke wet.
- EDPB-sjabloon voor een DPIA en de bijbehorende uitleg: versie 1, consultatieversie, geen eindversie per oktober 2026; gebruikt als niet-verplichte structuurcontrole.
- EDPB-advies 22/2024 over verwerkers en subverwerkers, over de beschikbaarheid van de volledige keten.
- EDPB-advies 28/2024 over AI-modellen, onder meer over de rechtmatige ontwikkeling van een ingezet model.
- EDPB-aanbevelingen 01/2020 over aanvullende maatregelen bij doorgifte.
- EDPB-richtsnoeren 9/2022 over de melding van datalekken.
- EDPB-richtsnoeren 01/2025 over pseudonimiseren en 02/2026 over anonimiseren, beide consultatieversies.
- AP-praktijkgids Gezondheidsgegevens in de cloud (maart 2026), over verwerkers, subverwerkers, audits en doorgifte.
- AP-besluit aanwijzing elektronische kanalen, Staatscourant 2025, 43523.
- Bijzondere bewaartermijn voor zorgloggegevens, Staatscourant 2019, 38007, uitsluitend binnen het daarin bedoelde wettelijke bereik.
- Besluit elektronische gegevensverwerking door zorgaanbieders en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

- Aanwijzing van NEN 7510-1:2024 en NEN 7510-2:2024+A1:2026, Staatscourant 2026, 17743, per 1 juni 2026.
- Jeugdwet, Wmo 2015 en Wkkgz, voor dossier, bewaring en meldroutes buiten de WGBO.
- Cyberbeveiligingswet en de Cyberbeveiligingsregeling voor de zorg, Staatscourant 2026, 28763, sinds 15 augustus 2026.
- IGJ, Toetsingskader Digitale Zorg (update juli 2026) en de IGJ-oproep over de invoering van generatieve AI.
- AZWA-doorbraakmiddelen, waaronder het modelplan Spraakgestuurd rapporteren, een veldkader en geen beroepsnorm.
- KNMG-richtlijn Omgaan met medische gegevens (2024) en het KNMG-praktijkadvies van 9 april 2026 over AI-verslaglegging.
- AI-verordening (AI Act), zoals gewijzigd bij Verordening (EU) 2026/1744, MDR, Data Act en EHDS, voor de concrete samenhang met functies, gegevensstromen en toepassingsdata.

6.3 Hysio-bronnen

Gebruik de voor jouw dienstverlening geldende versies van de Algemene Voorwaarden, Privacyverklaring, Verwerkersovereenkomst met alle bijlagen, MDR-positiedocument, AI Act-transparantieverklaring, Disclaimer en Regeling Datatoegang. Hysio biedt op dit moment geen Familiemodules aan. Gebruik daarnaast de openbare samenvatting van de eigen DPIA van Hysio. Vraag waar relevant de ketenopgave per overeenkomst, de doorgiftebeoordeling en de samenvatting van het beveiligingsbeleid op, en gebruik het cliëntinformatieblad voor je patiënten of cliënten.

Noteer welke versie op de datum van je beoordeling geldt en welke aangekondigde wijziging je beoordeelt.

6.4 Ondersteuning vanuit Hysio

Hysio verleent, rekening houdend met de aard van de verwerking en beschikbare informatie, bijstand bij de DPIA en eventuele voorafgaande raadpleging volgens AVG artikel 28 lid 3 onder f en artikel 16 van de Verwerkersovereenkomst. Zij kan feitelijke informatie aanvullen, onjuistheden over haar dienstverlening corrigeren, bewijs toelichten en relevante documenten onder passende geheimhouding beschikbaar stellen.

Hysio neemt de grondslagen, lokale feiten, risicowaardering of goedkeuring van je organisatie niet stilzwijgend over. De verantwoordelijkheid van Hysio voor haar eigen informatie en verplichtingen blijft bestaan. Hysio behandelt bijstand die zij verplicht of volgens afspraak geeft niet als optioneel maatwerk en vertraagt die niet door een discussie over kosten. Voor werkelijk aanvullende werkzaamheden is vooraf een concrete schriftelijke afspraak nodig binnen de kostenregels van de Verwerkersovereenkomst en de Regeling Datatoegang.

Onderwerp	Contact
Feiten, verwerking, retentie, rechten en DPIA-bijstand	privacy@hysio.nl

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

Onderwerp	Contact
Melding van een vermoeden van een datalek of beveiligingsincident bij Hysio	privacy@hysio.nl
Vertrouwelijke documenten en juridische onderbouwing	legal@hysio.nl
Subverwerkerwijziging en bezwaar	compliance@hysio.nl

Versie en wijzigingsoverzicht

Wijzigingen tegenover 4.1.5. De opnametoets geldt voor alle beroepen. De template onderscheidt de keuze over opnemen, de grondslag en de bewaarinstructie.

Versie 4.1.6 (4 november 2026). Versie 4.1.6 volgt versie 4.0 op, die op 16 september 2026 is gepubliceerd. Alle juridische documenten van Hysio gaan tegelijk naar versie 4.1.6. Tegenover versie 4.0 is het volgende veranderd:

- Een korte leeswijzer (Zo gebruik je deze template) en een uitleg van de AI-ondersteuning (1.4.2) zijn toegevoegd. De template verwijst ook naar de openbare samenvatting van de eigen DPIA van Hysio.
- De maatregelentabel geeft nu per maatregel aan of die bij de ingangsdatum van deze versie is ingericht of een toezegging is die vanaf of vóór een genoemde mijlpaal geldt, gelijk aan Bijlage 2 van de Verwerkersovereenkomst, zodat je de stand van iedere maatregel zelf kunt beoordelen. Vier maatregelen zijn toegevoegd: gescheiden omgevingen met testgegevens zonder echte cliëntgegevens, de behandeling van kwetsbaarheden, de controle van invoer en de jaarlijkse evaluatie van de maatregelen.
- De bewaartermijnen staan niet meer als eigen tabel in deze template, maar alleen in Bijlage 1 van de Verwerkersovereenkomst, zodat er één plek is met de termijnen. De termijnen zijn gelijk aan of korter dan in versie 4.0.
- Dienstverleners worden per soort dienst beschreven, met een verwijzing naar Bijlage 3 van de Verwerkersovereenkomst. De volledige keten van verdere subverwerkers ontvang je per overeenkomst. Supportberichten per e-mail hebben een eigen plek gekregen. De template noemt nu ook waar een dienst buiten de EER kan verwerken en de aankondigingstermijn van dertig kalenderdagen voor een nieuwe Subverwerker.
- Privacyvragen over Hysio stel je via privacy@hysio.nl (1.2 en 6.4).
- De opnametoets volgt de eigen beroepsnorm (2.4).
- Nieuwe vragen gaan over het delen van dossiers met andere zorgaanbieders, zorgtoegangslogging, de plek van je primaire dossier, de meldroute, de beroepsnorm voor AI en opname, en de Cyberbeveiligingswet.
- Een nieuw onderdeel over de AI-verordening (2.13) behandelt je rol, AI-geletterdheid, het publiceren van met AI gemaakte tekst en de informatie die je bij Hysio kunt opvragen.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.

- De template sluit aan op het IGJ-toetsingskader Digitale Zorg en het landelijke modelplan voor spraakgestuurd rapporteren (0.9), met de leveranciersinformatie die Hysio daarvoor levert (0.3).
- Vier risico's zijn toegevoegd (R33 tot en met R36): een schaduwdossier naast je eigen dossier, cliëntgegevens in een ander AI-hulpmiddel, een AI-model dat met onrechtmatig verwerkte gegevens is ontwikkeld, en het wegvallen van een doorgiftewaarborg.
- De bewaar- en vernietigingsregels per regime zijn aangevuld met de Jeugdwet, de Wmo 2015 en beroepsrichtlijnen. Een Sessie in Hysio is een werkkopie naast je eigen dossier.
- Hysio verzorgt geen zorgtoegangslogging, tenzij je dat vóór de eerste verwerking schriftelijk met Hysio afspreekt; anders regel je die in je eigen dossiersysteem.
- Hysio werkt conform de AVG en volgens de werkwijze van ISO 27001 en NEN 7510; de certificeringstrajecten zijn in aanloop. De aangewezen edities van NEN 7510 staan in de tekst.
- De Word-versie heeft dezelfde tekst en indeling als deze pagina.
- Bronnen en wetsverwijzingen zijn bijgewerkt naar de stand van oktober 2026.
- Nieuw sinds versie 4.0: 1.9 onderscheidt de voorwaarden per tekstroute en de daadwerkelijk gebruikte route. De vaste zin over certificering is bijgewerkt.

Versie 4.0. Versie 4.0, opgesteld op 8 september 2026, tekstrevisie 15 september 2026, gepubliceerd op 16 september 2026. Deze versie bouwt voort op de daadwerkelijk verstuurde mei-template v1.1, de v3.7-cyclus en de zorgbrede v3.9.9-template. De opbouw en bruikbare analyses blijven behouden; wijzigingen betreffen met name de werkelijke functieruimte, rollen, leveranciers, retentie, bewijsstatus, vertegenwoordiging, uitvoerketen en risico- en besluitmethodiek. Deze versie verwerkt de latere AP-schaaluitleg, goedgekeurde gedragscodes en het KNMG-advies over opnames.

Een ingevulde klant-DPIA krijgt daarnaast een eigen versie, besluitvormer en herbeoordelingsdatum.

© Hysio B.V. Alle rechten voorbehouden. Overnemen, hergebruiken of analyseren met AI-systemen is zonder toestemming niet toegestaan; voorbehoud tekst- en datamining op grond van art. 15o Auteurswet.