Dienstverlening ZorgTTP
Voor Rijksvaccinatieprogramma COVID RIVM

Aan:
5.1.2e 5.1.2e 5.1.2e, Enterprise Architect VZVZ
5.1.2e 5.1.2e, Productmanager Infrastructuur VZVZ

Van:
5.1.2e
5.1.2e
5.1.2e @zorgttp.nl
06 5.1.2e

Onderwerp:
Aanvullende informatie over de dienstverlening van ZorgTTP naar aanleiding van onze telefoongesprekken d.d. 16 en 17 december 2020

Datum:
17 december 2020

Versie:
1.0

Beste 5.1.2e

Veel dank voor de prettige gesprekken van gisteren en vandaag. Zoals vanochtend beloofd aan 5.1.2e stuur ik jullie hierbij wat meer informatie over onze dienstverlening en beveiligingsmaatregelen. Op de volgende pagina's ontvangen jullie meer informatie over de volgende onderwerpen:

1) Pseudonimisatie; inleiding (pagina 2);
2) Pseudonimisatieketen; applicaties en functies (pagina 3);
3) Pseudonimisatiemethode; methode van versleuteling (pagina 4);
4) Transportbeveiliging (pagina 5);
5) Domeinen (pagina 6);
6) Opdrachtgevers; enkele voorbeelden met overeenkomstige projectkenmerken (pagina 6);
7) Certificering; ISO27001, NEN7510, NEN7524 (pagina 7).

Hopelijk geeft deze memo meer informatie over onze dienstverlening. Uiteraard zijn wij graag bereid op korte termijn in meer detail de voorgenomen gegevensverwerking en requirements met jullie af te stemmen.

Met vriendelijke groet,

5.1.2e

5.1.2e

ZorgTTP
Privacy & vertrouwen

1. Inleiding

Pseudonimisatie is een maatregel die kan worden ingezet bij gegevensverwerkingen om de privacy van betrokkenen te beschermen. Stichting ZorgTTP is sinds 2007 actief als Trusted Third Party (TTP) en is gespecialiseerd in het ondersteunen van organisaties bij het op passende wijze beschermen van privacygevoelige informatie ten behoeve van beleids- en onderzoeksdoeleinden. In deze memo wordt beknopt de door ZorgTTP ontwikkelde systematiek voor het pseudonimiseren van persoonsgegevens beschreven.

1.1 Pseudonimisatie

Pseudonimisatie kan omkeerbaar en onomkeerbaar worden opgezet. De dienstverlening van ZorgTTP bestond aanvankelijk alleen uit onomkeerbare pseudonimisatie, waarbij persoonsgegevens naar een niet tot de oorspronkelijke persoon terug te herleiden unieke code worden versleuteld. Sinds de komst van de Algemene Verordening Gegevensbescherming (AVG) gaat het niet meer om pseudonimisatie in absolute zin maar worden omkeerbaar versleutelde persoonsgegevens ook onder pseudoniemen verstaan. Binnen de huidige dienstverlening van ZorgTTP kan daarom gekozen worden voor zowel onomkeerbare als omkeerbare pseudonimisatie. In deze memo wordt de onomkeerbare pseudonimisatie dienstverlening van ZorgTTP verder toegelicht.

De omzetting van persoonsgegevens naar onomkeerbare pseudoniemen verloopt in een aantal stappen waarbij het cruciaal is dat één van deze stappen bij een zogenaamde Trusted Third Party (TTP) wordt uitgevoerd. De bij de TTP uitgevoerde stap is geheim voor zowel de aanbieder van de gegevens als de ontvangende partij in de pseudonimisatieketen. Op deze wijze kan de relatie tussen pseudoniem en persoonsgegeven worden verbroken en is het niet langer mogelijk om via het aangemaakte pseudoniem terug te gaan naar de direct identificerende gegevens behorende bij de natuurlijke persoon waarop het pseudoniem betrekking heeft.

Persoons-identificerende kenmerken (bijvoorbeeld een BSN, geboortedatum geslacht, postcode) worden bij pseudonimisatie vervangen door een pseudoniem, zodanig dat voor ieder persoonsgegeven steeds hetzelfde pseudoniem wordt gegenereerd. Individuen worden op deze wijze koppelbaar in tijd en over verschillende bronnen heen zonder dat daartoe de oorspronkelijke persoonsgegevens verstrekt hoeven te worden. Door tussenkomst van de TTP zijn bron en doel niet in staat om persoonsgegeven en het daar uit resulterende pseudoniem aan elkaar te relateren. De inzet van pseudonimisatie via ZorgTTP werkt via een gelaagd model. Hierin worden een aantal vormen van beveiliging gehanteerd. Het gaat om maatregelen op de volgende niveaus:

1) Pseudonimisatie op recordniveau
2) Versleuteling op bestandsniveau
3) Transportbeveiliging
4) Controle afzender middels certificaat

In de volgende hoofdstukken wordt de werking van de pseudonimisatiesoftware en de getroffen beveiligingsmaatregelen toegelicht.

ZorgTTP
Privacy & vertrouwen

2. Pseudonimisatieketen

De pseudonimisatieketen van ZorgTTP bestaat uit drie onderdelen:

1) **Privacy- en Verzend Module** (PVM); deze module wordt door de afzender gebruikt om bestanden een eerste keer te pseudonimiseren en te verzenden;
2) **Centrale Module TTP** (CMT) de centrale omgeving wordt door ZorgTTP gebruikt om bestanden voor een tweede maal te pseudonimiseren;
3) **Doel- en Receive Module** (DRM) wordt door de eindontvanger gebruikt om de bestanden vanaf CMT te downloaden.

2.1 Privacy- en Verzend Module (PVM)

De PVM maakt gebruik van Java en wordt via het internet beschikbaar gesteld. Deze lokale module wordt gebruikt door de databron en kent een aantal functies:

- Splitsen van gegevens in een pseudoniemendeel en een datadeel;
- Pre-pseudonimisatie van de identificerende persoonsgegevens;
- Ondertekening van de te verzenden gegevens met een afzendercertificaat;
- Transportbeveiliging van de pre-pseudoniemen (sleuteldeel) en de bijbehorende data (datadeel).

Volgens de door ZorgTTP gehanteerde pseudonimisatiemethode vindt de eerste onomkeerbare pseudonimisatie plaats bij de afzender van de gegevens. De PVM genereert de eerste-orde pseudoniemen waarna het pseudoniemendeel en datadeel op beveiligde wijze naar ZorgTTP worden verstuurd. Daarbij zijn de gegevens door middel van PKI (Public Key Infrastructure) zodanig beveiligd dat alleen het pseudoniemendeel toegankelijk is voor ZorgTTP om de tweede pseudonimisatie uit te voeren.

2.2 Centrale Module TTP (CMT)

Na verwerking van de gegevens met de PVM worden de versleutelde bestanden automatisch verzonden naar de Centrale Module TTP (CMT), de centrale verwerkingsomgeving die onder beheer van ZorgTTP valt en verantwoordelijk is voor het produceren van de definitieve pseudoniemen. In de centrale omgeving worden de volgende handelingen uitgevoerd:

1) CMT opent het deel met pre-pseudoniemen met de private sleutel van ZorgTTP;
2) De pre-pseudoniemen worden voor de tweede maal versleuteld. Onderdeel van de tweede versleuteling is een domein specifieke versleuteling (AES) op het pseudoniemen deel. Deze versleuteling is enkel door ZorgTTP om te keren ten behoeve van een eventuele domeinconversie;
3) Het bestand met pseudoniemen wordt versleuteld met de publieke sleutel van het de ontvanger.

ZorgTTP heeft geen toegang tot het datadeel. Dit is beveiligd en kan enkel door het informatiedoel worden ontsleuteld.

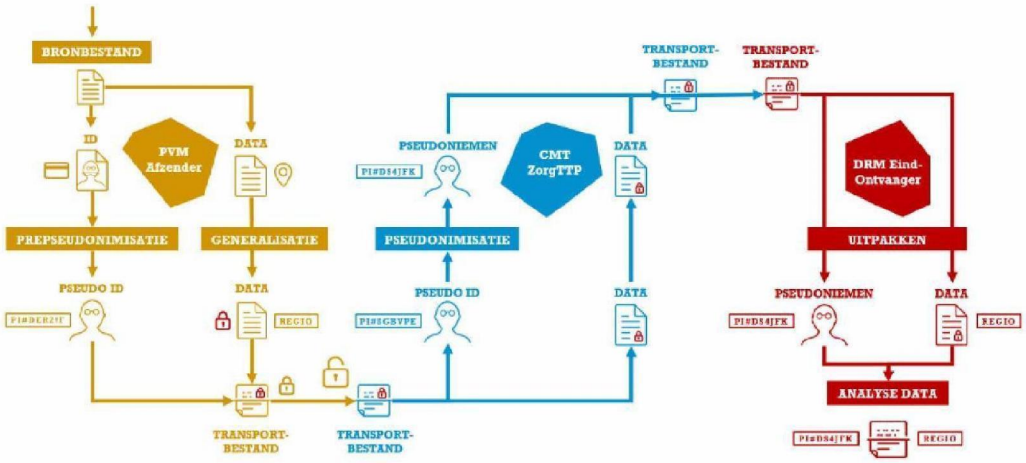
2.3 Doel- en Retour Module (DRM)

De lokale ontvangstmodule wordt gebruikt door de ontvanger van de gepseudonimiseerde data en ontvangt berichten afkomstig van de centrale applicatie CMT. De module ontsleutelt het transportbestand en voegt het sleutel- en het datadeel vervolgens weer samen. De volgende stappen zijn daarbij van belang:

1) De DRM legt contact met de server van ZorgTTP;
2) Als er bestanden beschikbaar zijn, worden deze gedownload;
3) De bestanden worden ontsleuteld met de private sleutel van het informatiedoel;
4) De bestandsdelen – deel met pseudoniemen én deel met inhoudelijke gegevens – worden samengevoegd;
5) Het bestand wordt omgezet naar het gewenste opleverformaat.

3. Pseudonimisatiemethode; versleuteling

ZorgTTP stelt de databron software ter beschikking voor de eerste bewerking. Daarbij worden persoonsgegevens omgezet naar pseudoniemen en er vinden, indien gewenst, aggregaties plaats. Bijvoorbeeld door het omzetten van een geboortedatum naar een leeftijdscategorie. De inhoudelijke informatie wordt vervolgens versleuteld, deze informatie is voor ZorgTTP gedurende het transport ontoegankelijk. Vanwege logistieke voordelen worden de pseudoniemen én inhoudelijke data in de huidige opzet in één levering via ZorgTTP aan de ontvanger aangeboden. Uitwisseling van gegevens tussen de diverse partijen vindt plaats over beveiligde internetverbindingen (TLS). De identiteit van partijen wordt gevalideerd middels digitale certificaten (Public Key Infrastructure (PKI).



3.1 Versleuteling bij de aanbieder van de gegevens

Een lokale pseudonimiseringsmodule van ZorgTTP geïnstalleerd bij een aanbieder van gegevens leest een bronbestand in en voert een eerste onomkeerbare versleuteling uit op direct identificerende persoonsgegevens. In alle gevallen wordt een combinatie gemaakt van enkele (genormaliseerde) persoons-identificerende gegevens. Deze combinatie plus een sector-afhankelijke salt worden aangeboden aan de huidige hashfuncties MD5, SHA 2 of SHA 3. Het resulterende pseudo-ID worden eerste-orde pseudoniemen genoemd. De eerste orde pseudoniemen worden voor verdere verwerking aangeboden aan ZorgTTP.

3.2 Versleuteling bij ZorgTTP

De berekening van de definitieve tweede-orde pseudoniemen vindt plaats bij ZorgTTP. De berekening bij ZorgTTP vindt plaats in twee stappen.

De eerste stap is een onomkeerbare versleuteling van de eerste-orde pseudoniemen door middel van een MD5, SHA 2 of SHA 3 hashfunctie. De tweede stap is een versleuteling met AES, waarbij een voor de gegevensverzameling specifieke geheime sleutel wordt gebruikt die alleen bij ZorgTTP bekend is. De AES-sleutel is zogenaamd domeinspecifiek en blijft na het genereren altijd hetzelfde. De sleutels worden in CMT (RSA)versleuteld middels de public key van ZorgTTP opgeslagen en zijn niet toegankelijk.

Na definitieve pseudonimisering worden de bestanden beschikbaar gesteld aan de eindontvanger. De eindontvanger kan alleen met een lokaal geïnstalleerde ontvangstmodule van ZorgTTP de gepseudonimiseerde gegevens ontvangen. Het resultaat van deze operatie is een effectieve doorbreking van de relatie tussen brongegeven en gepseudonimiseerd afgeleide. Geen van de partijen kan zonder samen te spannen met een van de andere partijen de keten doorbreken.

ZorgTTP
Privacy & vertrouwen

4. Transportbeveiliging

4.1 Transportbeveiliging

Bij de inzet van de pseudonimisatieketen worden gegevens verzonden vanaf één of meerdere afzenders, welke via ZorgTTP afgeleverd worden aan de eindontvanger. Om de gegevens te beschermen tegen ongeautoriseerde inzage, wijziging of verwijdering worden verschillende methodes van transportbeveiliging ingezet.

4.2 Beveiligde verbinding

Bij het opbouwen van beveiligde verbindingen tussen de verschillende modules van de pseudonimisatieketen maakt ZorgTTP gebruik van het Transport Layer Security (TLS) protocol. Vanaf 7 januari 2019 ondersteunt ZorgTTP enkel TLS versie 1.2 en hoger. Bovendien worden enkel verbindingen toegestaan op basis van sterke "ciphers".

4.3 Bestandsversleuteling

Het verwerkte bestand wordt bij de afzender versleuteld door middel van symmetrische encryptie op basis van AES met een sleutel (AES-128-CBC). De (publieke en private) AES-sleutel wordt op basis van asymmetrische encryptie versleuteld met een sleutel van 2048 bit. Omdat het verwerkte bestand voor verzending in twee delen is gesplitst, het pseudoniemendeel en het datadeel, kunnen beide delen met verschillende publieke sleutels worden versleuteld.

4.3.1 Datadeel

Voor ZorgTTP is het niet noodzakelijk om inzage te krijgen in het datadeel. De AES-sleutel van het datadeel wordt daarom versleuteld met de publieke sleutel van de eindontvanger. Alleen de eindontvanger is zo in staat om met de private sleutel, het zogenaamde routecertificaat dat alleen bekend is bij eindontvanger, te ontsleutelen.

4.3.2 Pseudoniemendeel

Binnen de pseudonimisatiemethode van ZorgTTP is het noodzakelijk om toegang te krijgen tot het pseudoniemendeel, zodat de pre-pseudoniemen door ZorgTTP met een tweede pseudonimisatie omgezet kunnen worden naar de definitieve pseudoniemen voor de eindontvanger. De AES-sleutel van het datadeel wordt daarom bij de afzender versleuteld met de publieke sleutel van ZorgTTP. Alleen ZorgTTP is zo in staat om met haar private sleutel het pseudoniemendeel te ontsleutelen. Nadat ZorgTTP op haar centrale platform de pre-pseudoniemen heeft omgezet in definitieve pseudoniemen, wordt ook de AES-sleutel van het pseudoniemendeel versleuteld met de publieke sleutel van de eindontvanger. Vanaf verzending van ZorgTTP naar de eindontvanger is dus alleen de eindontvanger in staat om met de private sleutel ook het pseudoniemendeel met de definitieve pseudoniemen te ontsleutelen.

4.4 Integriteitscontrole

De integriteit van de verzonden bestanden wordt bewaakt op basis van HMAC-SHA256 en ondertekening van de data. Bij verzenden van een bestand wordt een message digest berekend en deze digest waarde wordt versleuteld met de private sleutel van de afzender. Bij het verzenden van de data worden de versleutelde digest waarde en de publieke sleutel van de afzender meegestuurd.

Bij het ontvangen van een bestand bij de eindontvanger wordt ook een message digest berekend. Daarnaast wordt de versleutelde digest waarde ontsleuteld met de meegestuurde publieke sleutel van de afzender. De bij de eindontvanger berekende digest waarde wordt vergeleken met de ontsleutelde digestwaarde die berekend is bij de afzender. Beide waarden worden vergeleken, wanneer deze overeenkomen is aangetoond dat het ontvangen bestand niet is gewijzigd tijdens transport.

ZorgTTP
Privacy & vertrouwen

5. Domeinen; voorkomen van ongeautoriseerde verrijking

Voor elke gegevensverzameling richt ZorgTTP een eigen pseudonimisatiedomein in. Dat wil zeggen dat iedere gegevensverwerking een eigen set pseudoniemen krijgt. Voor elk pseudonimisatiedomein wordt een specifieke geheime sleutel gebruikt waarmee de definitieve pseudoniemen worden gegenereerd. Hierdoor zullen de definitieve pseudoniemen bij de eindontvanger niet gelijk zijn aan de definitieve pseudoniemen bij een eindontvanger van een andere gegevensverzameling. Op deze manier is het onmogelijk voor eindontvangers van verschillende domeinen om zelfstandig gepseudonimiseerde gegevens aan elkaar te koppelen. Met deze maatregel voorkomen we ongeautoriseerde (indirecte) herleiding door verrijking van gepseudonimiseerde gegevens met andere gepseudonimiseerde gegevens. Alleen met behulp van ZorgTTP en de gehanteerde procedure voor domeinconversie kan geautoriseerde koppeling van gepseudonimiseerde gegevens van verschillende gegevensverzamelingen worden aangevraagd. Naast deze maatregel zijn er ook procedures voor authentiseren en autoriseren van transacties en het op betrouwbare wijze aan- en afsluiten van databronnen en afnemers.

6. Opdrachtgevers

Naar aanleiding van de gevoerde gesprekken op 16 en 17 december j.l. zijn in deze memo ook enkele opdrachtgevers van ZorgTTP beschreven die vanwege de aard of omvang relevant zijn voor het RIVM.

6.1 Nivel

Het doel van Nivel Zorgregistraties eerste lijn is onderzoek doen naar de zorgpaden van patiënten in de gehele eerste lijn. In dit kader beheert het Nivel een landelijk representatief netwerk van huisartsen, huisartsenposten, fysiotherapeuten, oefentherapeuten, diëtisten en logopedisten. In dat kader leveren meer dan 800 zorgverleners individueel of via softwareleveranciers aan (ongeveer 30 leveranciers waaronder Promedico, Pharmapartners, Monitored Rehab systems, Callmanager/CGM, etc.). In 2020 zijn voor Nivel ongeveer 60.000 bestanden verwerkt en meer dan 1,5 miljard pseudoniemen aangemaakt. Daarnaast leveren verpleeghuisorganisaties sinds dit jaar covid-gerelateerde informatie aan het Nivel aan in opdracht van het RIVM.

6.2 De Nederlandse Zorgautoriteit; DBC-informatiesysteem

In opdracht van de Nederlandse Zorgautoriteit (NZa) voert ZorgTTP sinds 2007 de pseudonimisatie uit voor het DBC Informatie Systeem (DIS). In het DIS systeem ontvangt de NZa alle informatie over DBC's: een DBC is het totale behandelingstraject van een patiënt vanaf de diagnose van de specialist tot en met de behandeling die hieruit volgt. De registratie bevat de DBC-gegevens van zorgaanbieders in onder andere de ziekenhuiszorg, de geestelijke gezondheidszorg en de forensische zorg. Zorgaanbieders zoals ziekenhuizen en huisartsen leveren de gegevens maandelijks aan vanuit hun basisregistratie.

Door het verzamelen en analyseren van deze gegevens wil de NZa bijdragen aan betere, betaalbare en toetsbare gezondheidszorg in Nederland. Daarnaast verzorgt de NZa wettelijk vastgelegde data-uitleveringen aan onder andere het Centraal Bureau Statistiek, het ministerie van Volksgezondheid, Welzijn en Sport en het Zorginstituut Nederland. Ongeveer 2.500 zorgaanbieders leveren hiervoor via het pseudonimisatieplatform van ZorgTTP de maandelijkse gegevens aan. De NZa kan door de gepseudonimiseerde bestanden de data aan elkaar koppelen en zo ontwikkelingen in de zorg volgen en tarieven en prestaties vaststellen. Jaarlijks worden, inclusief data vanuit verzekeraars, ongeveer 20.000.000.000 records door ZorgTTP voor de NZa verwerkt.

6.3 Het Ministerie van Volksgezondheid, Welzijn en Sport; onderzoek rekenmodel risicoverevening

In Nederland hebben zorgverzekeraars een acceptatieplicht en is er een verbod op premiedifferentiatie in het basispakket. Dat betekent dat alle Nederlanders – ongeacht hun gezondheid – zich kunnen verzekeren en dezelfde zorgpremie betalen. Om een gelijk speelveld te creëren, worden zorgverzekeraars gecompenseerd voor voorspelbare gezondheidsverschillen van verzekerden in hun portefeuille. De informatie die noodzakelijk is voor de risicoverevening is afkomstig van de verzekeraars, de belastingdienst en het UWV.

Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) – opdrachtgever Risicoverevening – wil dat de informatie op aantoonbaar betrouwbare en veilige wijze wordt aangeleverd. ZorgTTP voorziet daarbij sinds 2006 in de pseudonimisering van de persoonsgegevens conform de door het ministerie van VWS opgestelde specificatie en

ZorgTTP maakt daarmee veilige verzameling van de informatie mogelijk. De beveiligde informatie wordt door diverse onderzoeksbureaus gebruikt voor analyse en verdere doorontwikkeling van het rekenmodel voor de Risicoverevening.

6.4 Het Zorginstituut Nederland; uitvoering risicoverevening

Het Zorginstituut heeft de wettelijke taak om het risicovereveningsmodel uit te voeren. De daarvoor benodigde informatie wordt op beveiligde wijze verzonden aan het Zorginstituut Nederland. ZorgTTP is hierbij verantwoordelijk voor de pseudonimisatie en het transport van de gegevens afkomstig van zorgverzekeraars, UWV, DUO en de Nederlandse zorgautoriteit. Ook het Centraal Bureau voor de Statistiek wordt in dit kader voorzien van gepseudonimiseerde resultaten door het Zorginstituut.

7. Certificering

ZorgTTP is gecertificeerd voor ISO 27001. ISO 27001 is een ISO standaard voor informatiebeveiliging. Deze internationale norm is van toepassing op alle typen organisaties (bijvoorbeeld commerciële ondernemingen, overheidsinstanties, non-profitorganisaties). De norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. ZorgTTP is eveneens gecertificeerd voor NEN7510, de norm voor informatiebeveiliging in de zorgsector. In 2019 is de NEN7524 voor pseudonimisatiedienstverlening gepubliceerd. ZorgTTP is als schrijver betrokken geweest bij de totstandkoming van deze norm. Momenteel wordt de implementatie van de norm en het daarbij vereiste kwaliteitsmanagementsysteem voorbereid. Zodra het mogelijk is om te certificeren voor deze norm zal ZorgTTP dat doen.