Pseudonimisering van persoonsgegevens

Auditraamwerk conformiteit CBP voorwaarden voor ZorgTTP en Afnemers

Houten, mei 2013

Inhoudsopgave

1 Introductie

1.1. Achtergrond

1.1.1. ZorgTTP en pseudonimisering

De ZorgTTP is een onafhankelijke organisatie die vanaf 1 januari 2007 werkzaam is als 'Trusted Third Party' (TTP) op het gebied van pseudonimisering van persoonsgegevens.

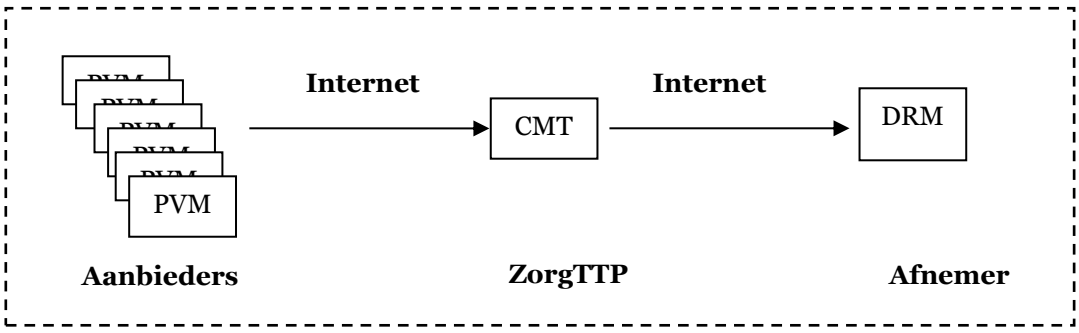
Gepseudonimiseerde persoonsgegevens dienen in voldoende mate onherleidbaar te zijn naar personen. Daarom dienen zij geen direct identificerende gegevens (zoals naam en adres) te bevatten maar ook geen indirect identificeerbare gegevens (zoals de volledige postcode en/of geboortedatum). Bij de pseudonimisering van persoonsgegevens door ZorgTTP worden daarom (in)direct identificerende gegevens ofwel verwijderd of vervangen door pseudoniemen afgeleid van deze gegevens (technisch gezien cryptogrammen). Deze afleiding is herhaalbaar hetgeen een fundamenteel verschil is met anonimisering.

Door deze herhaalbaarheid kunnen ondermeer:

- gepseudonimiseerde gegevens later worden aangevuld met nieuwe gegevens;
- de gegevens van een persoon die voorkomt in persoonsregistraties van verschillende partijen worden geplaatst onder hetzelfde pseudoniem.

Deze eigenschappen maken het mogelijk statistische analyses uit te voeren zonder dat er gebruik hoeft te worden gemaakt van persoonsgegevens.

De pseudonimisering binnen de ZorgTTP vindt plaats binnen schema's. Elk schema kent één of meerdere Aanbieders van persoonsgegevens en één Afnemer van de gepseudonimiseerde resultaten. De ZorgTTP verzorgt daarbij de pseudonimisering van de persoonsgegevens afkomstig van de Aanbieder(s) en levert deze uit aan de Afnemer. Hiertoe levert de ZorgTTP software aan zowel de Aanbieder(s) als aan de Afnemer. Het eerste type software heet Privacy- en Verzend Module (PVM) en het tweede type software heet Doel- en Retour Module (DRM). De PVM software levert gegevens aan de Centrale Module TTP (CMT) die wordt beheerd door de ZorgTTP (zie onderstaand figuur).



Schema

De PVM en DRM software worden niet specifiek ontwikkeld voor Aanbieders en Afnemers, maar zijn XML gebaseerde configuraties van generieke PVM en DRM software.

1.1.2. Regelgeving rond pseudonimisering

In verschillende publicaties[1] heeft het College Bescherming Persoonsgegevens (CBP) beschreven dat bij de toepassing van pseudonimisering geen sprake is van de verwerking van persoonsgegevens, indien aan de volgende voorwaarden is voldaan:

1. *"er wordt (vakkundig) gebruikgemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens;*

2. *er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ("replay back") te voorkomen;*

3. *de verwerkte gegevens zijn niet indirect identificerend;*

4. *in een onafhankelijk deskundig oordeel (audit) wordt voor aanvang van de verwerking en daarna periodiek vastgesteld dat aan de voorwaarden 1, 2 en 3 is voldaan;*

5. *de pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt."*

Voor de afnemers van ZorgTTP betekenen deze voorwaarden concreet dat zij de (positieve) resultaten van de audit moet kunnen overhandigen aan het CBP zoals beschreven onder punt 4 en dat deze verklaring periodiek moet worden geactualiseerd.

1.2. Doel van dit document

Om voor Afnemers en andere belanghebbenden aantoonbaar te maken, dat aan de voorwaarden 1 - 3 en 5 van het CBP is voldaan middels een oordeel genoemd onder voorwaarde 4, is in opdracht van ZorgTTP door PwC een auditraamwerk ontwikkeld. Dit document is een bewerking van het oorspronkelijke door PWC opgeleverde document teneinde gunning van de audit opdracht aan wisselende daarvoor gekwalificeerde partijen te kunnen gunnen.

Het raamwerk geeft een beschrijving van:
1. de door ZorgTTP nagestreefde beheersdoelen;
2. de te volgen werkwijze tijdens het onderzoek en de gewenste mate van zekerheid waarmee de externe deskundige partij (auditor) de gevraagde beoordeling zal uitvoeren.

De uit te voeren werkzaamheden omvatten geen toetsing van conformiteit met voorwaarde 5, wel dient onderzochte te worden of de openbare beschrijving van de pseudonimiseringsoplossing genoemd onder deze voorwaarde niet inconsistent is met de daadwerkelijk geïmplementeerde oplossing.

Het auditraamwerk en de teksten van de Assurance-rapporten zijn in overeenstemming met de COS 3000 standaard 'Assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie'[2].

[1] Zie bijvoorbeeld: http://www.cbpweb.nl/downloads_uit/z2006-1382.pdf; http://www.cbpweb.nl/downloads_med/med_20090616_cvz.pdf; http://www.cbpweb.nl/downloads_uit/z2005-0882.pdf.
[2] Zie http://www.nivra.nl/Sites/nivra_site/COS/HTML/50438.asp.

1.3. Leeswijzer

In hoofdstuk 2 is een beschrijving opgenomen van de soorten onderzoeken die worden uitgevoerd om conformiteit aan de voorwaarden inzake pseudonimisering gesteld door het CBP vast te stellen.

In hoofdstuk 3 is beschreven welke aanpak wordt gehanteerd voor het uitvoeren van elk van de onderzoeken.

In bijlage A is een lijst opgenomen met afkortingen en definities, zoals die worden gehanteerd binnen dit document. Verder zijn in bijlage B de te hanteren normen opgenomen.`

[1] Zie http://www.nivra.nl/Sites/nivra_site/COS/HTML/50438.asp.

2 Soorten onderzoeken

2.1. Inleiding

Om te kunnen beoordelen of door ZorgTTP en de Afnemers aan de voor hen relevante CBP voorwaarden 1, 2 en 3 is voldaan, zijn de volgende twee onderzoeken voorzien. Deze onderzoeken zullen geen oordeel geven of is voldaan aan CBP voorwaarde 5.

I. ***Onderzoek I:*** **ZorgTTP Beheerorganisatie** Een algemeen onderzoek rond de beheerorganisatie van ZorgTTP betreffende de gemaakte afspraken tussen aanbieders en afnemers met ZorgTTP, de gebruikte cryptografische technieken en de geïmplementeerde technische en organisatorische maatregelen.

II. ***Onderzoek II:*** **Afnemer** Een afnemer specifiek onderzoek met betrekking tot de conformiteit tussen de met de Afnemer afgesproken pseudonimisering techniek enerzijds en de generieke pseudonimisering specificatie van ZorgTTP anderzijds. Het onderzoek richt zich ook op de zelfstandig indirecte identificeerbaarheid van de aangeleverde gepseudonimiseerde gegevens. Verder wordt ook onderzocht naar de (contextafhankelijke) indirecte identificeerbaarheid van deze gegevens vanuit mogelijke andere (persoons)gegevens binnen de Afnemer.

Tabel 1: In onderstaande tabel is per deelonderzoek de relatie met de voorwaarden van het CBP aangegeven:

	CBP voorwaarde:	Wordt getoetst in:
1	"Er wordt (vakkundig) gebruikgemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens".	***Onderzoek I: ZorgTTP beheerorganisatie*** Het onderzoek naar de ZorgTTP Beheerorganisatie bestaat uit twee onderdelen: a) een onderzoek naar de cryptografie en implementatie daarvan in de broncode; b) een onderzoek naar de beheerprocessen van ZorgTTP; c) een onderzoek naar de afspraken met de aanbieders en de afnemers. Onderdeel a, b en c adresseren CBP voorwaarde 1.
2	"Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ('replay back') te voorkomen".	***Onderzoek I: ZorgTTP beheerorganisatie*** Herleidbaarheid van de versleuteling kan op twee manieren plaatsvinden: 1. doordat de versleuteling niet adequaat is; 2. doordat het ongeautoriseerd mogelijk is om directe identificerende gegevens om te zetten in pseudoniemen zodat het makkelijk is om bijvoorbeeld een volledige tabel BSN – pseudoniem te krijgen. Het eerste punt wordt afgedekt door CBP voorwaarde 1 en het tweede punt wordt afgedekt door de ISO 27002 eisen.
3	"De verwerkte gegevens zijn niet indirect identificerend".	***Onderzoek I: ZorgTTP beheerorganisatie*** ***Onderzoek II:*** **Afnemer** Onderzoek I geeft aan dat de cryptografie adequaat is (en blijft). Daarnaast zal zijn onderzocht, dat geen onderzoeksinformatie ter beschikking is gekomen van ZorgTTP. Onderzoek II (deel inzake technische conformiteit) geeft aan dat de specificatie wordt gevolgd en (deel inzake functionaliteit conformiteit) dat wat de specificatie aangeeft – zelfstandig of in combinatie met de andere gegevens bij de afnemer – niet indirect identificerend is. Verder zal worden onderzocht of aanbieders en afnemers niet samenspannen.
5	'de pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt."	***Onderzoek I: ZorgTTP beheerorganisatie*** *Onderzoek I geeft aan of de openbare beschrijving van de pseudonimiseringsoplossing genoemd onder deze voorwaarde niet inconsistent is met de daadwerkelijk geïmplementeerde oplossing.*

Deze twee onderzoeken worden hieronder verder toegelicht.

2.2. Onderzoek I: ZorgTTP Beheerorganisatie

2.2.1. Onderzoek I.1 inzake CBP voorwaarde 1 'Gebruik van pseudonimisering'

2.2.1.1 Doelstelling

Doelstelling is vast te stellen dat wordt voldaan aan CBP voorwaarde 1, namelijk "Er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens".

#	Onderdeel
I.1.a	Een onderzoek naar de opzet van de cryptografie en implementatie daarvan in de broncode (dat wil zeggen dat de cryptografie adequaat is, zowel in opzet / op papier als bestaan / in de software).
I.1.b	Een onderzoek naar het opzet en bestaan van beheerprocessen (dat wil zeggen de maatregelen die erop gericht zijn dat het gebruik van cryptografie adequaat blijft).
I.1.c	Een onderzoek naar het bestaan van afspraken met Aanbieders en Afnemers (dat wil zeggen dat de afspraken bestaan en adequaat worden nageleefd).

2.2.1.2 Reikwijdte (objecten, aspecten en normen)

De te onderzoeken reikwijdte bestaat uit:

- **Geschetste pseudonimisering opzet**: Beoordeeld zal worden of de beschreven pseudonimisering opzet voldoet aan de normen beschreven in NPR-ISO/TS 25237 standaard: Medische informatica – Pseudonimisatie. Verder wordt gekeken naar de cryptografische opzet van de pseudoniemgeneratie of deze voldoet aan 'good practice' cryptografische principes om de vertrouwelijkheid van de identificerende persoonsgegevens te beschermen. Hiertoe wordt gebruik gemaakt van erkende open cryptografische standaarden.
- **Broncode / pseudonimisering applicaties**: Beoordeeld zal worden of de code van generieke PVM, CMT en DRM software in lijn is met de beschreven pseudonimisering opzet.
- **Beheerprocessen**: Beoordeeld zal worden of het changemanagement, incidentmanagement, configuration management en problemmanagement proces rond de PVM, CMT en DRM software zodanig is ingericht dat de cryptografie adequaat blijft.
- **Afspraken met Aanbieders en Afnemers:** Beoordeeld zal worden of afspraken zijn gemaakt tussen de aanbieders en afnemers met ZorgTTP. Hierbij zal niet alleen worden gekeken naar het bestaan van deze afspraken, maar ook naar adequaatheid van deze afspraken.

2.2.1.3 Werkzaamheden

Inzake het eerste deel van het onderzoek (inzake de cryptografie) worden de volgende werkzaamheden uitgevoerd:

- Het uitvoeren van een beoordeling op de cryptografische opzet van de pseudonimisering specificatie.
- Consistentie vergelijking van deze opzet met de beschrijving van de pseudonimiseringoplossing genoemd onder de vijfde CBP voorwaarde.
- Bestuderen van de broncode en uitvoeren van een quick scan (aan de hand van een kleine steekproef) op de broncode van de gebruikte PVM-CMT-DRM software waarbij wordt onderzocht of de cryptografische aanroepen in de code in lijn zijn met de cryptografische opzet van de pseudoniem generatie). Voorts wordt middels testbestanden onderzocht of de pseudoniemgeneratie conform is met het ontwerp.

Inzake het tweede deel van het onderzoek (inzake beheerprocessen) worden de volgende werkzaamheden uitgevoerd:

- Uitvoeren van een review op de beheerprocessen rond de PVM-CMT-DRM software.

Inzake het derde deel van het onderzoek (inzake afspraken) worden de volgende werkzaamheden uitgevoerd:

- Uitvoeren van een review van de afspraken tussen aanbieders met ZorgTTP.
- Uitvoeren van een review van de afspraken tussen afnemers met ZorgTTP.

Waar nodig kunnen overige werkzaamheden worden uitgevoerd, voor zover de auditor die gedurende de uitvoering van het onderzoek noodzakelijk acht.

2.2.2. Onderzoek I.2 inzake CBP voorwaarde 2 'Voorkomen replay back'

2.2.2.1 Doelstelling

Doelstelling is vast te stellen dat wordt voldaan aan CBP voorwaarde 2, namelijk "Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ('replay back') te voorkomen".

Toelichting:
Onder een 'replay back' genoemd onder CBP voorwaarde 2) wordt in dit geval verstaan de mogelijkheid om een verzameling identificerende persoonsgegevens (wederom) om te zetten in pseudo-identiteiten, zoals die in gebruik zijn binnen de ZorgTTP.
Replay back, ofwel herleidbaarheid van de versleuteling kan op twee manieren plaatsvinden:

1. *doordat de versleuteling niet adequaat is;*
2. *doordat het ongeautoriseerd mogelijk is om directe identificerende gegevens om te zetten in pseudoniemen zodat het makkelijk is om een bijvoorbeeld een volledige tabel BSN – pseudoniem te krijgen.*

Het eerste punt (dat wil zeggen het risico dat de versleuteling niet adequaat is) wordt afgedekt door CBP voorwaarde 1; het tweede punt (dat wil zeggen het risico dat ongeautoriseerde in staat zijn de versleuteling te herleiden) wordt afgedekt door (een selectie van) de ISO 27002 eisen aangaande informatiebeveiliging.

2.2.2.2 Reikwijdte (objecten, aspect en normen)

De te onderzoeken objecten zijn de geïmplementeerde technische en organisatorische maatregelen. Beoordeeld wordt of ZorgTTP zowel in opzet als bestaan voldoet aan de in bijlage B2 opgenomen selectie van maatregelen uit de norm ISO 27002 getiteld 'Information technology - Security techniques - Code of practice for information security management'.

2.2.2.3 Werkzaamheden

De volgende werkzaamheden zullen worden uitgevoerd:

- Opvragen / bestuderen van documenten, waaronder bijvoorbeeld interne analyses van (onderdelen van) het normenkader in verhouding tot het bij ZorgTTP getroffen stelsel van maatregelen en procedures.
- Consistentie vergelijking van deze opzet met de beschrijving van de pseudonimiseringoplossing genoemd onder de vijfde CBP voorwaarde.
- Onderzoeken van de opzet van de interne beheersmaatregelen en het bestaan van deze maatregelen.
- Uitvoeren van een infrastructurele penetratietest met het NESSUS tool (www.nessus.org). Deze zal zich richten op de publieke IP-adressen van ZorgTTP waaronder het PVM aanlever-IP-adres, de CMT interface en het DRM afleveradres om te toetsen of ongeautoriseerde toegang mogelijk is.

- Waar nodig overige werkzaamheden die de auditor gedurende de uitvoering van het onderzoek noodzakelijk acht.

2.2.3. Onderzoek inzake CBP voorwaarde 3 'De verwerkte gegevens zijn niet indirect identificerend'

2.2.3.1 Doelstelling

Doelstelling is vast te stellen dat wordt voldaan aan CBP voorwaarde 3, namelijk "De verwerkte gegevens zijn niet indirect identificerend". Zoals aangegeven in tabel 1 wordt deze voorwaarde voor wat betreft de Afnemers ook getoetst in onderzoek II.

Dit onderzoek bestaat uit vijf onderdelen.

#	Onderdeel
I.3.a	Een onderzoek naar technische conformiteit om vast te stellen dat de generieke pseudonimisering specificatie wordt gevolgd: opereert ZorgTTP pseudonimisering techniek conform de generieke pseudonimisering specificatie / is de ZorgTTP pseudonimisering techniek in conformiteit met de generieke pseudonimisering specificatie geïmplementeerd? Dit omvat ook onderzoek naar functionele conformiteit om vast te stellen dat wat de specificatie aangeeft niet zelfstandig, i.e. zonder gebruik te maken van additionele gegevens, herleidbaarheid naar persoon mogelijk maakt.
I.3.b	Een onderzoek naar functionele conformiteit om vast te stellen dat wat de specificatie aangeeft niet in combinatie met de andere gegevens herleidbaarheid naar persoon mogelijk maakt.
I.3.c	Een onderzoek naar de opzet van de logische en fysieke beveiliging van de gepseudonimiseerde gegevens.
I.3.d	Een onderzoek naar het bestaan van onderzoeksbestanden en/of andere koppelbare data binnen ZorgTTP.
I.3.e	Een onderzoek naar het bestaan van afspraken tussen aanbieders en afnemers met ZorgTTP gelet op het voorkomen van replay en samenspanning tussen aanbieders en afnemers.

2.2.3.2 Reikwijdte (object, aspect en norm)

Voor het onderzoek met betrekking tot technische conformiteit is het te onderzoeken object de door ZorgTTP gedocumenteerde pseudonimisering specificatie (functionaliteit). (*)

(*) De specificatie dient in detail aan te geven:

- normalisatie van de input;
- de datavelden als input van de DRM;
- de wijze waarop datavelden worden verwijderd of 'uitgedund' (e.g., volledige geboortedatum wordt uitgedund tot geboortejaar);
- welke combinaties van datavelden gaan fungeren als basis voor pseudoniemen;
- wat de uiteindelijke output is zoals geleverd aan de afnemende partij in de DRM.

Voor het onderzoek met betrekking tot functionaliteit conformiteit zijn de te onderzoeken objecten:

- gegevensspecificatie;
- opgave van gegevensbestanden waar Afnemer over beschikt / kan beschikken.

Voor het onderzoek naar de opzet van de logische en fysieke beveiliging van de gepseudonimiseerde gegevens zijn de te onderzoeken objecten:

- opgave van fysieke en logische toegangsbeveiliging tot de productieomgeving waarin de pseudoniemen worden gemaakt.

Voor het onderzoek naar het bestaan van onderzoeksbestanden en/of andere koppelbare data binnen ZorgTTP zijn de te onderzoeken objecten:

- opgave van gegevensbestanden waar ZorgTTP over beschikt / kan beschikken.

Voor het onderzoek naar het bestaan van afspraken tussen aanbieders en afnemers met ZorgTTP gelet op het voorkomen van replay en samenspanning tussen aanbieders en afnemers zijn de te onderzoeken objecten:

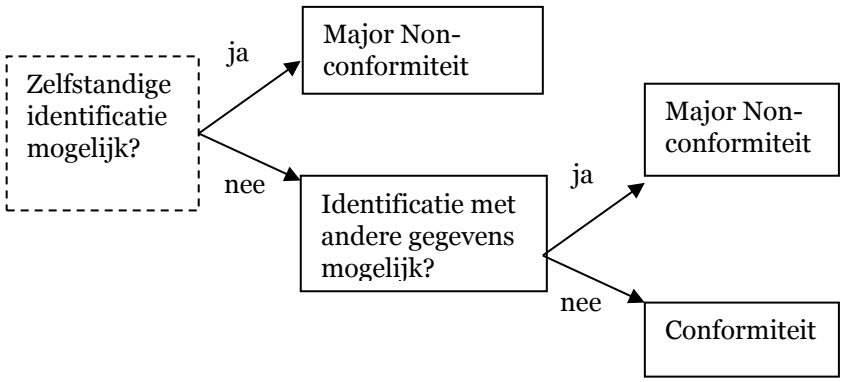
- afspraken tussen aanbieders en afnemer met ZorgTTP.

Allereerst wordt aan de hand van de gegevensspecificatie onderzocht of de aangeleverde gepseudonimiseerde gegevens zelfstandig (op zich zelfstaand) indirect identificerend zijn. Een voorbeeld van een dergelijke situatie is als de specificatie aangeeft dat volledige postcodes of volledige geboortedata zijn opgenomen in de gegevens.

- Indien dit wel het geval is, is sprake van een zogenaamde major non-conformiteit. In een dergelijke situatie moet ZorgTTP de pseudonimisering opzet (en specificatie) aanpassen, voordat de audit met een positief resultaat kan worden afgerond.

- Indien dit niet het geval is, dient de Afnemer aan de auditor opgave te doen van de andere gegevensbestanden waarover zij beschikt en waarin zich gerelateerde (persoon) gegevens bevinden. De auditor voert geen zelfstandig onderzoek uit binnen de Afnemer naar het bestaan van dergelijke gegevensbestanden; dit ligt nadrukkelijk buiten de reikwijdte van het onderzoek van de auditor. Aan de hand van deze opgave zal worden onderzocht of in combinatie met deze registraties de gepseudonimiseerde gegevens niet indirect identificerend zijn. Er wordt een major non-conformiteit gerapporteerd en de Afnemer past in dialoog met ZorgTTP de pseudonimisering aan, voordat de audit met een positief resultaat kan worden afgerond.

Voor het beoordelen van indirecte identificatie zal geen theoretische insteek worden genomen (‘verwijst de data noodzakelijk naar een uniek individu’) maar een praktische insteek (‘is het praktisch voldoende mogelijk voor de medewerkers werkzaam binnen ZorgTTP de identiteit van een individu alsnog te achterhalen’). In onderstaande figuur zijn de stappen van onderzoek I.3 beschreven:



Hoewel dit geen formeel vereiste is vanuit de CBP voorwaarden, dient ZorgTTP ook opgave te doen van de fysieke en logische toegangsbeveiliging tot de productieomgeving van pseudoniemen. Deze zal in opzet worden beoordeeld: is deze beveiliging voldoende om ongeautoriseerde toegang tot deze gegevens te voorkomen?

2.2.3.3 Werkzaamheden

Voor het technische conformiteitonderzoek zullen de volgende werkzaamheden worden uitgevoerd:

- Uitvoeren van testen in de ZorgTTP acceptatieomgeving, gebruik makende van (in samenwerking met ZorgTTP aan te maken) testinputbestanden. Nagegaan zal worden of de ZorgTTP pseudonimisering techniek in conformiteit met de generieke pseudonimisering specificatie is geïmplementeerd. Voorts zal worden nagegaan of datavelden conform de afspraken worden verwijderd of 'uitgedund'.
- Waar nodig overige werkzaamheden die de auditor gedurende de uitvoering van het onderzoek noodzakelijk acht.

Voor het functionele conformiteitonderzoek worden de volgende werkzaamheden uitgevoerd:

- Opvragen / bestuderen van documenten, waaronder de gegevensspecificatie en de opgegeven andere bestanden met daarin persoonsgegevens waarover ZorgTTP beschikt of kan beschikken.
- Consistentie vergelijking van deze opzet met de beschrijving van de pseudonimiseringoplossing genoemd onder de vijfde CBP voorwaarde.
- Waar nodig overige werkzaamheden die de auditor gedurende de uitvoering van het onderzoek noodzakelijk acht.

Voor het onderzoek naar de opzet van de logische en fysieke beveiliging van de gepseudonimiseerde gegevens worden de volgende werkzaamheden uitgevoerd:

- Uitvoeren van een review op de logische en fysieke beveiliging rond de PVM-CMT-DRM software op basis van de ISO 27002 normen.

Voor het onderzoek naar het bestaan van onderzoeksbestanden en/of andere koppelbare data binnen ZorgTTP worden de volgende werkzaamheden uitgevoerd:

- Onderzoek naar de locatie van de onderzoeksbestanden van de PVM-CMT-DRM software.

Voor het onderzoek naar het bestaan van afspraken tussen aanbieders en afnemers met ZorgTTP gelet op het voorkomen van replay en samenspanning tussen aanbieders en afnemers worden de volgende werkzaamheden uitgevoerd:

- Opvragen / bestuderen van de afspraken tussen aanbieders en afnemers met ZorgTTP.

2.2.4. Onderzoek I.4 inzake CBP voorwaarde 5 'openbare beschrijving van de pseudonimiseringsoplossing'

2.2.4.1 Doelstelling

Doelstelling is vast te stellen of de openbare beschrijving van de pseudonimiseringsoplossing niet inconsistent is met de daadwerkelijk geïmplementeerde oplossing.

2.2.4.2 Reikwijdte (objecten, aspect en normen)

De te onderzoeken objecten zijn:

- De openbare beschrijvingen van de pseudonimeringsoplossing.
- De daadwerkelijk geïmplementeerde oplossing.

2.2.4.3 Werkzaamheden

De volgende werkzaamheden zullen worden uitgevoerd:

- Opvragen / bestuderen van de openbare documenten met de beschrijving van de pseudonimiseringsoplossing in verhouding tot de daadwerkelijk geïmplementeerde oplossing.

2.3. Onderzoek II: Afnemer

2.3.1 Onderzoek inzake CBP voorwaarde 3 ‘De verwerkte gegevens zijn niet indirect identificerend’

2.3.1.1 Doelstelling

Onderzoek II betreft een Afnemer specifiek onderzoek. Dit onderzoek heeft betrekking op CBP voorwaarde 3, namelijk “De verwerkte gegevens zijn niet indirect identificerend”. Zoals aangegeven in tabel 1 wordt deze voorwaarde ook gedeeltelijk getoetst in onderzoek I.

Dit onderzoek bestaat uit vijf onderdelen, waarvan één conditioneel.

#	Onderdeel
II.1	Een onderzoek naar technische conformiteit om vast te stellen dat de generieke pseudonimisering specificatie wordt gevolgd: opereert de met de afnemer afgesproken methode pseudonimisering techniek conform de generieke pseudonimisering specificatie / is de met de afnemer afgesproken methode pseudonimisering techniek in conformiteit met de generieke pseudonimisering specificatie geïmplementeerd? Dit omvat ook onderzoek naar functionele conformiteit om vast te stellen dat wat de specificatie aangeeft niet zelfstandig, i.e. zonder gebruik te maken van additionele gegevens, herleidbaarheid naar persoon mogelijk maakt.
II.2	Een onderzoek naar functionele conformiteit om vast te stellen dat wat de specificatie aangeeft niet in combinatie met de andere gegevens bij de afnemer herleidbaarheid naar persoon mogelijk maakt.
II.3	Een onderzoek naar de opzet van de logische en fysieke beveiliging van de gepseudonimiseerde gegevens.
II.4	Een onderzoek naar opzet en bestaan van een ‘Chinese wall’ bij de afnemer tussen de gepseudonimiseerde gegevens en overige gegevens waarmee indirecte identificatie mogelijk is.

2.3.1.2 Reikwijdte (object, aspect en norm)

Voor het onderzoek met betrekking tot technische conformiteit is het te onderzoeken object de met de Afnemer afgesproken gedocumenteerde pseudonimisering specificatie (functionaliteit). (*) Per Afnemer dient er een gedocumenteerde pseudonimisering specificatie te bestaan. NB: Het niet aanwezig zijn van een gedocumenteerde pseudonimisering specificatie zal worden aangemerkt als een major non-conformiteit (zie Sectie 3.2.1.2 en tabel 2).

(*) De specificatie dient in detail aan te geven:

- de datavelden als input van de DRM;
- de wijze waarop datavelden worden verwijderd of ‘uitgedund’ (e.g., volledige geboortedatum wordt uitgedund tot geboortejaar);
- welke combinaties van datavelden gaan fungeren als basis voor pseudoniemen;
- wat de uiteindelijke output is zoals geleverd aan de afnemende partij in de DRM.

Voor het onderzoek met betrekking tot functionaliteit conformiteit zijn de te onderzoeken objecten:

- gegevensspecificatie;
- opgave van gegevensbestanden waar Afnemer over beschikt / kan beschikken.

Voor het onderzoek naar de opzet van de logische en fysieke beveiliging van de gepseudonimiseerde gegevens.:

- opgave van fysieke en logische toegangsbeveiliging rond de gepseudonimiseerde gegevens op basis van de ISO 27002 normen.

Allereerst wordt aan de hand van de gegevensspecificatie onderzocht of de aangeleverde gepseudonimiseerde gegevens zelfstandig (op zich zelfstaand) indirect identificerend zijn. Een voorbeeld van een dergelijke situatie is als de specificatie aangeeft dat volledige postcodes of volledige geboortedata zijn opgenomen in de gegevens.

- Indien dit wel het geval is, is sprake van een zogenaamde major non-conformiteit. In een dergelijke situatie moet de Afnemer in dialoog met de ZorgTTP de pseudonimisering opzet (en specificatie) aanpassen, voordat de audit met een positief resultaat kan worden afgerond.

- Indien dit niet het geval is, dient de Afnemer aan de auditor opgave te doen van de andere gegevensbestanden waarover zij beschikt en waarin zich gerelateerde (persoon) gegevens bevinden. De auditor voert geen zelfstandig onderzoek uit binnen de Afnemer naar het bestaan van dergelijke gegevensbestanden; dit ligt nadrukkelijk buiten de reikwijdte van het onderzoek van de auditor. Aan de hand van deze opgave zal worden onderzocht of in combinatie met deze registraties de gepseudonimiseerde gegevens niet indirect identificerend zijn.

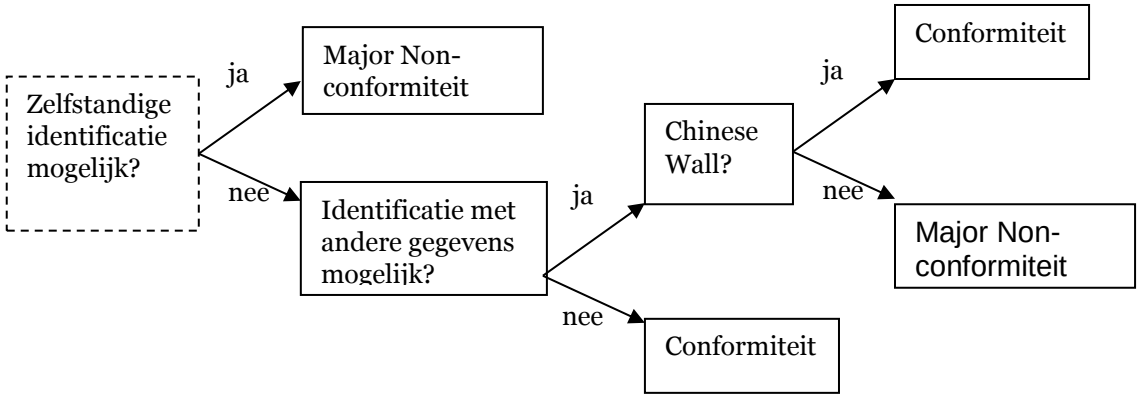
Indien dit laatste niet het geval is, dan is er een tweetal mogelijkheden voor het verdere onderzoek:

1) Er wordt een major non-conformiteit gerapporteerd en de Afnemer past in dialoog met ZorgTTP de pseudonimisering aan, voordat de audit met een positief resultaat kan worden afgerond.

2) Er wordt aanvullend onderzoek gedaan naar opzet en bestaan van de organisatorische scheiding (‘Chinese Wall’) tussen de gepseudonimiseerde gegevens en de overige gegevens waarmee indirecte identificatie mogelijk is. Het uitgangspunt hierbij is dat het niet mogelijk moet zijn dat één persoon binnen de Afnemer zelfstandig in staat is een koppeling uit te voeren tussen de gepseudonimiseerde gegevens en de overige gegevens.

Voor het beoordelen van indirecte identificatie zal geen theoretische insteek worden genomen (‘verwijst de data noodzakelijk naar een uniek individu’) maar een praktische insteek (‘is het praktisch voldoende mogelijk voor de medewerkers werkzaam binnen de afnemende partij de identiteit van een individu alsnog te achterhalen’).

In onderstaande figuur zijn de stappen van onderzoek II beschreven:



Hoewel dit geen formeel vereiste is vanuit de CBP voorwaarden, dient de Afnemer ook opgave te doen van de fysieke en logische toegangsbeveiliging rond de gepseudonimiseerde gegevens. Deze zal in opzet worden beoordeeld: is deze beveiliging voldoende om ongeautoriseerde toegang tot deze gegevens te voorkomen?

2.3.1.3 Werkzaamheden

Voor het technische conformiteitonderzoek zullen de volgende werkzaamheden worden uitgevoerd:

- Uitvoeren van testen in de ZorgTTP acceptatieomgeving, gebruik makende van (in samenwerking met ZorgTTP aan te maken) testinputbestanden. Nagegaan zal worden of de met de afnemer afgesproken methode pseudonimisering techniek in conformiteit met de generieke pseudonimisering specificatie is geïmplementeerd. Voorts zal worden nagegaan of datavelden conform de afspraken worden verwijderd of 'uitgedund'.
- Waar nodig overige werkzaamheden die de auditor gedurende de uitvoering van het onderzoek noodzakelijk acht.

Voor het functionele conformiteitonderzoek worden de volgende werkzaamheden uitgevoerd:

- Opvragen / bestuderen van documenten, waaronder de gegevensspecificatie en de opgegeven andere bestanden met daarin persoonsgegevens waarover de Afnemer beschikt of kan beschikken.
- Consistentie vergelijking van deze opzet met de beschrijving van de pseudonimiseringoplossing genoemd onder de vijfde CBP voorwaarde.
- in verband met onderzoek naar 'Chinese Wall': Uitvoeren van interviews, bestuderen van documentatie en doen van waarnemingen.
- Bestuderen van de door de Afnemer opgegeven beschrijving van de fysieke en logische toegangsbeveiliging rond de gepseudonimiseerde gegevens.
- Waar nodig overige werkzaamheden die de auditor gedurende de uitvoering van het onderzoek noodzakelijk acht.

3 Onderzoeksaanpak

3.1. Inleiding

In dit hoofdstuk wordt uiteengezet hoe het onderzoek dient te verlopen. Er is rekening gehouden met de NV COS 3000 – Assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie.

3.2. Werkwijze

Hieronder volgt in hoofdlijnen de werkwijze wordt gevolgd voor het afgeven van een assurance-rapport.

3.2.1. Initiële beoordeling

3.2.1.1 Opstellen van een auditplan

Voorafgaand aan de onderzoeken zoals beschreven in hoofdstuk 2 zal samen met de betrokken partij (ZorgTTP of Afnemer) een auditplan worden opgesteld. Dit auditplan bevat minimaal het volgende:

- doelstelling;
- criteria of gehanteerde normenkader;
- reikwijdte;
- data en locaties voor onderzoeken op locatie;
- verwachte tijd en duur van onderzoeksactiviteiten;
- rollen en verantwoordelijkheden van het onderzoeksteam;
- contactpersoon waar klachten ingediend kunnen worden.

3.2.1.2 Tweefasen onderzoek

De initiële beoordeling bestaat uit twee fasen. Allereerst wordt de opzet op basis van documentatie beoordeeld. De bevindingen zullen worden vastgelegd in een rapportage. Hierbij zal additionele aandacht besteedt worden aan bevindingen die in de volgende fase mogelijk tot non-conformiteiten kunnen leiden. Vervolgens wordt de implementatie van de normen te beoordeeld. Alleen de gesignaleerde tekortkomingen zullen worden vastgelegd.

Bij het beoordelen van de gesignaleerde tekortkomingen zal de onderzoeker een vergelijking maken tussen de norm en de aangetroffen situatie. Indien geen verschil wordt vastgesteld, functioneert het (deel)object conform de norm. Indien verschillen worden aangetroffen maakt het toetsingskader onderscheid in twee soorten bevindingen:

- **Major non-conformiteit**: een materiële tekortkoming ten opzichte van de van CBP voorwaarden. Indien niet aan de CBP voorwaarden wordt voldaan, dan is sprake van een major non-conformiteit. Indien sprake is van één of meerdere non-conformiteiten, dan dienen deze te worden opgelost dan wel zal de audit niet met een positief resultaat kunnen worden afgerond.
- **Minor non-conformiteit**: een niet-materiële tekortkoming ten opzichte van de CBP voorwaarden.

Bij de toetsing kunnen min of meer ernstige tekortkomingen worden gesignaleerd. Afhankelijk van de ernst van de gesignaleerde tekortkomingen zal de auditor vaststellen of het om een major dan wel om een minor non-conformiteit gaat. Minor non-conformiteiten corresponderen doorgaans met beperkte risico's. Meerdere minor non-conformiteiten rond een zelfde CBP voorwaarde kunnen door de auditor gelijk worden gesteld aan een major non-conformiteit, dit op basis van zijn professional judgement, overwegende de ernst van de afwijking.

Tabel 2 (op de volgende pagina) geeft inzicht in de mogelijk te signaleren tekortkomingen en of deze per definitie een positief resultaat van de audit in de weg staan (major non-conformiteit) dan wel of de auditor de ernst van de afwijking zal moeten bepalen (betreft de afwijking een major dan wel een minor conformiteit?).

3.2.1.3 Opvolgingsonderzoek (eventueel)

Indien non-conformiteiten worden geconstateerd bij een onderzoek dan dient de betrokken partij een correctief actieplan te schrijven om deze weg te nemen. Afhankelijk van de ernst van de non-conformiteiten kan een opvolgingsonderzoek noodzakelijk zijn.

3.2.1.4 Auditrapportage

Van de initiële beoordeling zal een auditrapportage worden gemaakt. Hierin kunnen mogelijkheden tot verbetering worden opgenomen, maar in de rapportage zullen geen specifieke oplossingen worden opgenomen. De rapportage zal een duidelijke en beknopte vastlegging zijn van het uitgevoerde onderzoek. Uit deze vastlegging moet duidelijk zijn of de betreffende audit al dan niet met een positief resultaat is afgerond.

- De rapportage van onderzoek I: ZorgTTP Beheerorganisatie zal worden afgestemd met ZorgTTP en zal in finale vorm slechts worden verstrekt aan ZorgTTP; het is aan ZorgTTP of deze wordt verstrekt aan de Afnemer. Omdat positieve afronding van onderzoek I een noodzakelijke voorwaarde is voor de start van Onderzoek II ligt het evenwel voor de hand dat ZorgTTP deze rapportage aan zijn afnemers (of diens auditors) verstrekt.

- De rapportage van onderzoek II: Afnemer wordt afgestemd met de Afnemer en zal in finale vorm worden verstrekt aan de Afnemer; het is aan de Afnemer of deze wordt verstrekt aan ZorgTTP.

ZorgTTP en Afnemer kunnen het assurance-rapport en de bijbehorende rapportage verstrekken aan elkaar en aan het CBP ter onderbouwing van hun conformiteit. Partijen mogen het assurance-rapport publiceren, bijvoorbeeld op hun website. Dit laatste geldt niet voor de bijbehorende auditrapportage; verstrekking aan andere partijen van de auditrapportage kan slechts geschieden na afstemming met de auditor.

Tabel 2: In onderstaande tabel is per CBP voorwaarde indicatief aangegeven wat de mogelijk te signaleren tekortkomingen kunnen zijn (op hoofdlijnen) alsmede of in een dergelijk geval sprake is van een zogenaamde major non-conformiteit.

CBP Voorwaarden	Mogelijk te signaleren tekortkomingen (op hoofdlijnen):	Major Non-Conformiteit
CBP voorwaarde 1: "Er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens".	**Onderzoek naar de cryptografie en implementatie daarvan in de broncode:**	
	Er wordt geen gebruik gemaakt van pseudonimisering.	ja
	De pseudonimisering opzet is onvoldoende gedetailleerd beschreven.	ja
	Er wordt onvoldoende vakkundig gebruik gemaakt van pseudonimisering, bijvoorbeeld omdat:	
	De pseudonimisering opzet voldoet niet aan 'good practice' cryptografische principes en / of de eerste encryptie vindt niet plaats bij de aanbieder van de gegevens.	ja
	De pseudonimisering opzet voldoet weliswaar aan 'good practice' cryptografische principes, maar deze is niet adequaat geïmplementeerd in de code.	
	De openbare beschrijving van de pseudonimiseringsoplossing genoemd onder de vijfde CBP voorwaarde is wezenlijk inconsistent met de geïmplementeerde oplossing.	ja
	Onderzoek naar beheerprocessen:	
	Er is geen beheerproces ingericht (opzet).	ja
	Het beheerproces vertoont tekortkomingen.	niet noodzakelijk
CBP voorwaarde 2: "Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ('replay back') te voorkomen".	Bij het beoordelen van de maatregelen (zie bijlage B2 voor de gehanteerde normen) getroffen ter beperking van het risico dat bestaat dat ongeautoriseerden in staat zijn de versleuteling te herleiden, zijn tekortkomingen gesignaleerd.	niet noodzakelijk
	De openbare beschrijving van de pseudonimiseringsoplossing genoemd onder de vijfde CBP voorwaarde is wezenlijk inconsistent met de geïmplementeerde oplossing.	ja
	Geen afspraken beschikbaar tussen aanbieders en afnemers met ZorgTTP.	ja
	De penetratietest heeft aangetoond dat er een risico bestaat dat ongeautoriseerden in staat zijn de versleuteling te herleiden en toegang verkrijgen tot data van de pseudonimisatiedienst.	ja
CBP voorwaarde 3: ***"De verwerkte gegevens zijn niet indirect identificerend".***	Het niet aanwezig zijn van een gedocumenteerde pseudonimisering specificatie specifiek voor de betreffende Afnemer/ de met de Afnemer afgesproken specifieke pseudonimisering functionaliteit.	ja
	De gedocumenteerde pseudonimisering specificatie is onvoldoende gedetailleerd dan wel onvolledig.	ja
	De openbare beschrijving van de pseudonimiseringsoplossing genoemd onder de vijfde CBP voorwaarde is wezenlijk inconsistent met de geïmplementeerde oplossing.	ja
	De met de Afnemer afgesproken specifieke gedocumenteerde pseudonimisering functionaliteit is niet in overeenstemming met de gedocumenteerde pseudonimisering specificatie.	niet noodzakelijk
	Geen afspraken beschikbaar tussen aanbieders en afnemers met ZorgTTP.	ja
	De gegevens zijn zelfstandig herleidbaar.	ja
	De gegevens zijn in de context herleidbaar. En eventueel: De gegevens zijn in de context herleidbaar. Hoewel de Afnemer een organisatorische scheiding ('Chinese Wall') heeft aangebracht, zijn de opgegeven maatregelen onvoldoende om het risico af te dekken dat één persoon of meerdere personen binnen de Afnemer zelfstandig in staat is een koppeling uit te voeren tussen de gepseudonimiseerde gegevens en de overige gegevens.	ja
	Additioneel: Bij het beoordelen van de opzet van de opgegeven fysieke en logische toegangsbeveiliging rond de gepseudonimiseerde gegevens gericht op het voorkomen van ongeautoriseerde toegang tot deze gegevens, zijn tekortkomingen gesignaleerd.	niet noodzakelijk

3.2.2. Herhalingsonderzoek (‘Werking’)

Herhalingsonderzoeken zijn jaarlijkse onderzoeken om te beoordelen of een betrokken partij nog steeds aan de normen voldoet. Hierbij wordt met name gekeken naar de werking van de maatregelen die onderzocht zijn tijdens het initiële onderzoek over de afgelopen periode. Dit onderzoek moet binnen twaalf maanden na beëindiging van fase 2 onderzoek worden uitgevoerd. Het omvat ook een selectie van de normen, waarvan de opzet en bestaan opnieuw wordt onderzocht.

Indien non-conformiteiten worden geconstateerd bij een herhalingsonderzoek dan dient de betrokken partij een correctief actieplan te schrijven om deze weg te nemen. Afhankelijk van de ernst van de non-conformiteiten kan een opvolgingsonderzoek noodzakelijk zijn.

De bevindingen van het herhalingsonderzoek en eventueel het opvolgingsonderzoek zullen worden verwerkt in een auditrapportage. Uiteraard zal jaarlijks het assurance-rapport worden geactualiseerd.

3.2.3. Herbeoordeling

In plaats van een herhalingsonderzoek, kan een herbeoordeling noodzakelijk zijn. Een herbeoordeling is nodig als de objecten van onderzoek essentieel wijzigen. In dit geval is een herbeoordeling noodzakelijk. Een herbeoordeling is vergelijkbaar met de initiële beoordeling.

3.3. Het Assurance-rapport

De audit (de initiële beoordeling of de herbeoordeling dan wel het herhalingsonderzoek) kan alleen met een positief resultaat worden afgerond indien er geen major non-conformiteiten bestaan en alle eventuele minor non-conformiteiten zijn afgedekt met een correctief actieplan. In andere gevallen zal doorgaans een negatief oordeel worden gegeven. Het assurance-rapport zal openstaande (minor) non-conformiteiten niet vermelden (deze zijn uiteraard wel opgenomen in de auditrapportage).

De assurance-rapporten zullen minimaal de zogenaamde basiselementen bevatten, zoals beschreven in artikel 49 van de NV COS 3000.

ZorgTTP en Afnemer kunnen het assurance-rapport en de onderliggende detail rapportage verstrekken aan elkaar en aan het CBP ter onderbouwing van hun conformiteit. Partijen dienen het assurance-rapport te publiceren op hun website. Dit laatste geldt niet voor de bijbehorende auditrapportage; verstrekking aan andere partijen van de audit rapportage kan slechts geschieden na afstemming met de auditor.

A.1. Afkortingen en definities

Hieronder volgt een lijst met afkortingen, die worden gebruikt in dit document, en de daarbij behorende betekenis:

Afkorting	Betekenis
CBP	College Bescherming Persoonsgegevens
CMT	Centrale Module TTP
DRM	Doel- en Retour Module
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PVM	Privacy- en Verzend Module
TTP	Trusted Third Party
Wbp	Wet bescherming persoonsgegevens
XML	Extensible Markup Language

Verder volgt hier een lijst met definities met bijbehorende omschrijving:

Begrip	Omschrijving
Aanbieder	Partij, die persoonsgegevens aanlevert aan ZorgTTP.
Afnemer	Partij, die gebruik maakt van de door ZorgTTP gepseudonimiseerde gegevens.
Anonimiseren	Het proces waarmee de relatie tussen de identificerende data en de individu wordt verwijderd.
Audits	Drie typen audits worden in dit document onderscheiden, namelijk: (1) initiële beoordeling (ook wel initiële audit): dit zijn de eerste audits die zich concentreren op opzet en bestaan van maatregelen in conformiteit met de CBP voorwaarden; (2) herhalingsonderzoek: dit zijn de audits, die jaarlijks worden uitgevoerd nadat de initiële audit is uitgevoerd, ook wel herhalingsaudits genoemd die concentreren zich op de werking van de maatregelen onderzocht tijdens de initiële beoordeling over de afgelopen periode, en; (3) opvolgingsonderzoek: audits naar correctieve acties naar aanleiding van geconstateerde non-conformiteiten bij initiële of jaarlijkse audits; (4) herbeoordeling: dit is een audit die wordt uitgevoerd als het object van onderzoek essentieel wijzigt.
CBP Voorwaarden	Voorwaarden opgesteld door het CBP, die voorschrijven wanneer bij toepassing van pseudonimisering geen sprake is van de verwerking van persoonsgegevens.
Chinese Wall	Scheiding tussen de gepseudonimiseerde gegevens en de overige gegevens.
Major non-conformiteit	Een materiële tekortkoming ten opzichte van de van CBP voorwaarden. Indien niet aan de CBP voorwaarden wordt voldaan, dan is sprake van een major non-conformiteit. Indien sprake is van één of meerdere non-conformiteiten, dan dienen deze te worden opgelost dan wel zal de audit niet met een positief resultaat kunnen worden afgerond.
Minor non-conformiteit	Een niet-materiële tekortkoming ten opzichte van de CBP voorwaarden.
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn tot een individu.
Pseudonimiseren	Het proces waarmee de relatie tussen de identificerende data en de individu wordt vervangen door een pseudoniem.
Replay back	De mogelijkheid om een verzameling identificerende persoonsgegevens (wederom) om te zetten in pseudo-identiteiten, zoals die in gebruik zijn binnen de ZorgTTP.
Schema	Elk schema kent één of meerdere Aanbieders van persoonsgegevens en één Afnemer van de gepseudonimiseerde resultaten. De ZorgTTP verzorgt daarbij de pseudonimisering van de persoonsgegevens afkomstig van de Aanbieder(s) en levert deze uit aan de Afnemer.

A.2. Normenkader

In onderstaande tabel is per CBP voorwaarde een verwijzing opgenomen naar de te hanteren normen.

	CBP voorwaarde:	Te hanteren normen
1	“Er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens”.	Het onderzoek naar de ZorgTTP Beheerorganisatie bestaat uit twee onderdelen: (1) een onderzoek naar de cryptografie en implementatie daarvan in de broncode; (2) een onderzoek beheerprocessen. De normen voor onderdeel a worden ontleend aan erkende open cryptografische standaarden, zoals beschreven in ISO standaarden of in publicaties van het National Institute of Standards and Technology (NIST). De normen voor beheerprocessen wordt afgedekt door de ISO 27002 eisen die zijn opgenomen in bijlage B1.
2	“Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling (‘replay back’) te voorkomen”.	Herleidbaarheid van de versleuteling kan op twee manieren plaatsvinden: 1. doordat de versleuteling niet adequaat is; 2. doordat het ongeautoriseerd mogelijk is om directe identificerende gegevens om te zetten in pseudoniemen zodat het makkelijk is om een bijvoorbeeld een volledige tabel BSN – pseudoniem te krijgen. Het eerste punt wordt afgedekt door CBP voorwaarde 1 en het tweede punt wordt afgedekt door de ISO 27002 eisen. Zie voor de geselecteerde maatregelen bijlage B1.
3	“De verwerkte gegevens zijn niet indirect identificerend”.	De normen worden ontleend aan wat wordt verstaan onder indirecte identificeerbaarheid, namelijk dat de gegevens niet zelfstandig (op zich zelf staand) en in combinatie herleidbaar mogen zijn tot individuen, en, dat de gegevens niet alsnog indirect identificeerbaar mogen zijn in de context waarin deze worden verwerkt omdat de gepseudonimiseerde gegevens in combinatie met andere gegevens waarover de afnemer beschikt alsnog indirect identificerend zijn (en additioneel als gevolg van onvoldoende bescherming tegen ongeautoriseerde toegang).

A.3. Normen m.b.t. geïmplementeerde technische en organisatorische maatregelen

#	Hoofdstuk ISO 27002	Toelichting
5.1	**Informatiebeveiligingsbeleid**	
5.1.1	Beleidsdocument voor informatiebeveiliging	Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.
6	**Organisatie van de beveiliging**	
6.1	**Interne organisatie**	
6.1.3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.
6.2	**Externe partijen**	
6.2.3	Beveiliging behandelen in overeenkomsten met een derde partij	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen. Aandachtspunten: - de cruciale cryptografische sleutels van het ZorgTTP systeem mogen niet benaderbaar zijn voor de externe leverancier; - het systeem dat deze cryptografische sleutels herbergt of waarvandaan deze functioneel benaderbaar zijn, mag niet draaien op server hardware die gedeeld wordt met andere klanten van een leverancier.
7	**Beheer van bedrijfsmiddelen**	
7.1	**Verantwoordelijkheid voor bedrijfsmiddelen**	
7.1.1	Inventarisatie van bedrijfsmiddelen	Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.
8	**Beveiliging van personeel**	
8.1	**Voorafgaand aan het dienstverband**	
8.1.2	Screening	Verificatie van de achtergrond van alle kandidaten voor een diensverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.
8.3	**Beëindiging of wijziging van het dienstverband**	
8.3.3	Blokkering van toegangsrechten	De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT- voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.
9	**Fysieke beveiliging en beveiliging van de omgeving**	
9.1	**Beveiligde ruimten**	
9.1.1	Fysieke beveiliging van de omgeving	Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.

9.1.2	Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.
10	**Beheer van communicatie- en bedieningsprocessen**	
10.1	**Bedieningsprocedures en verantwoordelijkheden**	
10.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.
10.1.2	Wijzigingsbeheer	Wijzigingen in IT-voorzieningen en informatiesystemen behoren te worden beheerst.
10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie	Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.
10.2	**Beheer van de dienstverlening door een derde partij**	
10.2.1	Dienstverlening	Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening, door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.
10.2.2	Controle en beoordeling van dienstverlening door een derde partij	De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.
10.4	**Bescherming tegen virussen en ´mobile code´**	
10.4.1	Maatregelen tegen virussen	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten. Aandachtspunt: - dit omvat ook bescherming tegen andere kwaadaardige software.
10.5	**Back-up**	
10.5.1	Reservekopieën maken (back-ups)	Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid. Aandachtspunten: - de back-upmedia moeten dezelfde fysieke beveiliging krijgen als de oorspronkelijke data, dit geldt met name voor de ZorgTTP cryptografische sleutels; - back-ups moeten periodiek worden getest.
10.6	**Beheer van netwerkbeveiliging**	
10.6.1	Maatregelen voor netwerken	Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd. Aandachtspunt: - een beschrijving van de netwerkbeveiliging dient gedocumenteerd te zijn, waaronder een kopie van een firewall rulebase en een nadere duiding daarvan indien deze complex is. Ook het proces van het doorvoeren van veranderingen in de configuratie moet zijn gedocumenteerd, waarbij geldt dat dergelijke veranderingen alleen middels een vier ogen principe mogen worden doorgevoerd.

10.8	**Uitwisseling van informatie**	
10.8.1	Beleid en procedures voor informatie-uitwisseling	Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
10.8.2	Uitwisselingsovereenkomsten	Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
10.8.4	Elektronisch berichtenuitwisseling	Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.
10.10	**Controle**	
10.10.1	Aanmaken audit-logbestanden	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
11	**Toegangsbeveiliging**	
11.1	**Bedrijfseisen ten aanzien van toegangsbeheersing**	
11.1.1	Toegangsbeleid	Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.
11.2	**Beheer van toegangsrechten**	
11.2.1	Registratie van gebruikers	Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
11.2.2	Beheer van speciale bevoegdheden	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst. Aandachtspunt: - dit betekent in het bijzonder dat het gebruik van de PVM (aanbieders) en DRM software (afnemers) onderhevig moet zijn aan authenticatie.
11.2.3	Beheer van gebruikerswachtwoorden	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.
11.2.4	Beoordeling van toegangsrechten	De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces. Aandachtspunt: - dit omvat ook de beoordeling van de rechten van aanbieders (PVM) en afnemers (DRM).
11.3	**Verantwoordelijkheden van gebruikers**	
11.3.1	Gebruik van wachtwoorden	Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden. Aandachtpunten: - gebruikers moeten zelfstandig in staat zijn hun wachtwoord te veranderen; - wachtwoorden mogen niet in klare taal worden opgeslagen in een applicatie of database maar alleen in versleutelde ('gehashde') vorm; - wachtwoorden hebben een minimale lengte van 8 karakers; - na drie mislukte aanlogpogingen wordt het systeem voor de gebruiker geblokkeerd;

		- initiële wachtwoorden moeten random zijn en moeten bij eerste gebruik veranderd worden door de gebruiker.
11.4	**Toegangsbeheersing voor netwerken**	
11.4.4	Bescherming op afstand van poorten voor diagnose en configuratie	De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst. Aandachtpunten: - voor de beveiliging van infrastructuur (switches, routers, besturingsystemen, webservers, databases) dienen gedocumenteerde standaarden te worden gebruikt.
11.5	**Toegangsbeveiliging voor besturingssystemen**	
11.5.1	Beveiligde inlogprocedures	Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.
11.5.2	Gebruikersidentificatie en -authenticatie	Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
11.5.3	Systemen voor wachtwoordbeheer	Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
11.5.5	Time-out van sessies	Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld. Aandachtspunten: - dit omvat het ook gebruik van automatische screensavers.
11.6	**Toegangsbeheersing voor toepassingen en informatie**	
11.6.2	Isoleren van gevoelige systemen	Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.
12	**Verwerving, ontwikkeling en onderhoud van informatiesystemen**	
12.1	**Beveiligingseisen voor informatiesystemen**	
12.1.1	Analyse en specificatie van beveiligingseisen	In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.
12.2	**Correcte verwerking in toepassingen**	
12.2.1	Validatie van invoergegevens	Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.
12.2.2	Beheersing van interne gegevensverwerking	Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.
12.2.3	Integriteit van berichten	Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
12.2.4	Validatie van uitvoergegevens	Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.
12.3	**Cryptografische beveiliging**	

12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.
12.3.2	Sleutelbeheer	Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie. Aandachtspunt: - de generatie van de centrale cryptografische sleutels dient beschreven te zijn waarbij met name onderbouwing moet zijn dat dit leidt tot veilige sleutels, dat wil zeggen van voldoende lengte en voldoende entropie; - de toegangsbeveiliging van de centrale cryptografische sleutels dient beschreven te zijn en te voorkomen dat ongeautoriseerde toegang mogelijk is dan wel ongeautoriseerde kopieën kunnen worden gemaakt; - het 'hardcoded' opnemen van cryptografische sleutels in broncode wordt afgeraden, indien dit toch gebeurt dan moet uitgesloten worden dat ontwikkelaars beschikking krijgen over de productiesleutels; het betreft hier de sleutel zelf in het geval van geheime sleutel (‘symmetrische’) cryptografie en de private sleutel in het geval van publieke sleutel (‘asymmetrische’) cryptografie; - de beveiliging van de centrale cryptografische cryptografische sleutels dient zodanig te zijn dat deze niet onder single control kunnen worden gebruikt of gekopieerd door 1 persoon (beheerder). Wat voorkomen moet worden is dat een beheerder een willekeurig pseudoniem kan terugzetten naar zijn hash waarde op basis waarvan een identiteit kan worden herleid; - indien gebruik wordt gemaakt van digitale certificaten dan dienen de 'standaard' PKI controles te worden uitgevoerd: validatie certificatie keten, controle op revocatie van certificaat.
12.5	**Beveiliging bij ontwikkelings- en ondersteuningsprocessen**	
12.5.1	Procedures voor wijzigingsbeheer	De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer. Aandachtspunten: - voor elke PVM en DRM module moet eenduidig gedocumenteerd zijn wat de input data en output data is en voor elke productieversie moet een testverslag zijn waaruit blijkt dat de opzet klopt met de implementatie. Voorkomen moet worden dat per ongeluk meer data wordt verstuurd naar de afnemer dan bedoeld.
12.5.5	Uitbestede ontwikkeling van programmatuur	Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.
12.6	**Beheer van technische kwetsbaarheden**	
12.6.1	Beheersing van technische kwetsbaarheden	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico’s. Aandachtspunten: - dit omvat het periodiek uitvoeren van security patching op alle systemen en applicaties die intern verbonden zijn met de systemen betrokken bij pseudonimisering.

15	**Naleving**	
15.1	**Naleving van wettelijke voorschriften**	
15.1.1	Identificatie van toepassing wetgeving	Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.
15.2	**Naleving van het beveiligingsbeleid en -normen en technische naleving**	
15.2.1	Naleving van beveiligingsbeleid en -normen	Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.
15.2.2	Controle op technische naleven	Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.