Data Protection Impact Assessment CIMS release 1.0
Aanvulling risicoparagraaf 31 december 2020

Bij de vaststelling van privacy risico's door het gebruik van CIMS is behalve aan de rechten en vrijheden van degenen wiens persoonsgegevens worden verwerkt ook aandacht geschonken aan de bestuurlijke en politieke risico's. Voor wat betreft de impact op de persoonlijke levenssfeer van de betrokkenen is een accent gelegd op de risico's verband houdend met het verlies van controle over hun persoonsgegevens of de onmogelijkheid hun rechten en vrijheden uit te oefenen; risico's verband houdend met discriminatie, stigmatisering en uitsluiting; de mogelijkheden van blootstelling aan identiteitsdiefstal of –fraude; gezondheidsschade; verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens; reputatie- of anderszins relationele schade; ongeoorloofde ongedaan making van pseudonimisatie. [1]

Er wordt gekeken naar de impact van een risico als dat zou materialiseren en de kans dat dit daadwerkelijk gebeurt. Daarbij wordt een score gemaakt op basis van Laag, Medium, Hoog. De normering is dan als volgt:

Impact

Hoog De gevolgen voor de betrokkene hebben bij het materialen van het risico forse invloed op het leven van de betrokkene

Medium De gevolgen voor de betrokkene hebben bij materialiseren van het risico geen beperkte impact op het leven van de betrokkene

Laag De gevolgen voor de betrokkene hebben materialiseren van het risico weinig of verwaarloosbare invloed op het leven van de betrokkene

Kans

Hoog Het is zeer waarschijnlijk of zeker dat het risico zal materialiseren

Medium Het is denkbaar dat dit risico zal materialiseren

Laag Het is onwaarschijnlijk dat dit risico zal materialiseren

Risico

Het risico wordt dan als volgt vastgesteld:

impact	kans	risico
laag	laag	laag-laag
laag	medium	laag
laag	hoog	medium
medium	laag	laag
medium	medium	medium
medium	hoog	hoog
hoog	laag	medium
hoog	medium	hoog
hoog	hoog	hoog-hoog

[1] Z'e overw. 75 uit de Preambule bij de AVG

1.1 Risico's en maatregelen

1. *Betrokkene onvoldoende geïnformeerd over opneming van persoonsgegevens, niet zijnde vaccinnatiegegevens, in CIMS*

fase(n): i, ii en iv.

categorie: controle van betrokkene over persoonsgegevens, geïnformeerde vrije keuze

incident: te weinig specifieke informatie

Impact: Laag. In fase i worden persoonsgegevens in het cliëntregister ingeladen uit BRP en RNI en verkregen van COA. Een en ander gebeurt op basis van wettelijke regelingen (zie nrs. 3.1.1 e.v. van de DPIA). Een betrokkene die hierover niet specifiek is geïnformeerd, wordt mogelijk verrast wanneer hij in fase ii. via RIVM wordt opgeroepen (restgroep) of als hem in fase iii. wordt gevraagd om toestemming voor opneming van zijn vaccinatiegegevens in CIMS.

Kans: Laag. Er wordt in landelijke media uitvoerig aandacht gegeven aan het vaccinatieprogramma en gedetailleerde informatie daarover is te vinden via de gebruikelijke kanalen van de rijksoverheid.

Risico: Laag-Laag

Maatregelen: Duidelijke informatievoorziening via de gebruikelijke kanalen, op een voor alle betrokkenen begrijpelijke wijze, in een taal die de meeste betrokkenen in Nederland verstaan.

Impact na maatregelen: Laag-Laag

2. *Betrokkene onvoldoende specifiek geïnformeerd over opneming van vaccinnatiegegevens in CIMS*

fase(n): iii.

categorie: controle van betrokkene over persoonsgegevens, geïnformeerde vrije keuze

incident: te weinig specifieke informatie

Impact: Medium. In fase iii wordt betrokkenen die zijn gevaccineerd gevraagd om toestemming voor verstrekking van hun vaccinatiegegevens aan RIVM en opneming van die gegevens in CIMS. Onvoldoende specifieke informatie hierover kan betekenen dat ten onrechte vaccinatiegegevens in CIMS worden opgenomen.

Kans: Laag. Aan de betrokkene wordt, zowel via de gebruikelijke kanalen als in de oproepingsbrief, specifieke informatie verstrekt, waarbij op basis van gegevens over het geboorteland zo nodig ook rekening kan worden gehouden met de taal die de betrokkene verstaat.

Risico: Laag

Maatregelen: RIVM draagt zorg voor procedures waarmee de betrokkene snel en gemakkelijk inzage kan verkrijgen in de verwerkte gegevens en deze desgewenst kan verwijderen uit CIMS, ook als de RIVM op basis van de AVG en UAVG daartoe mogelijk niet is gehouden.

Impact na maatregelen: Laag

3. *Betrokkene onvoldoende specifiek geïnformeerd over verwerking van persoonsgegevens, met inbegrip van vaccinnatiegegevens voor evaluatiedoelen en epidemiologisch onderzoek*

fase(n): v. en vii.

categorie: controle van betrokkene over persoonsgegevens, geïnformeerde vrije keuze

incident: te weinig specifieke informatie

Impact: Laag. In fase v. wordt het vaccinatieprogramma geëvalueerd en in fase vii wordt op basis van gepseudonimiseerde gegevens epidemiologisch onderzoek gedaan. Als de betrokkene hierover niet specifiek worden geïnformeerd heeft dat geen of een verwaarloosbare invloed op het leven van de betrokkene.

Kans: Laag. Aan de betrokkene wordt, zowel via de gebruikelijke kanalen als in de oproepingsbrief, specifieke informatie verstrekt, waarbij op basis van gegevens over het geboorteland zo nodig ook rekening kan worden gehouden met de taal die de betrokkene verstaat.

Risico: Laag-Laag

Maatregelen: RIVM draagt zorg voor procedures waarmee de betrokkene snel en gemakkelijk inzage kan verkrijgen in de verwerkte gegevens en deze desgewenst kan verwijderen uit CIMS, ook als de RIVM op basis van de AVG en UAVG daartoe mogelijk niet is gehouden.

Impact na maatregelen: Laag-Laag

4. ***Betrokkene geeft ten onrechte en onbedoeld toestemming voor opneming van vaccinatiegegevens in CIMS***

fase(n): iii.

categorie: controle van betrokkene over persoonsgegevens, geïnformeerde vrije keuze

incident: geen geldige toestemming

Impact: Medium. In fase iii wordt de betrokkene gevraagd om toestemming voor de verstrekking van zijn vaccinatiegegevens aan RIVM en de opneming daarvan in CIMS. Als er ten onrechte van wordt uitgegaan dat de betrokkene deze toestemming heeft gegeven, worden zijn vaccinatiegegevens opgenomen in CIMS.

Kans: Laag. Als de betrokkene om deze toestemming wordt gevraagd wordt hij erop gewezen dat het weigeren daarvan niet in de weg staat aan het verkrijgen van de vaccinatie. Ook via de gebruikelijke kanalen en in de oproepingsbrief wordt dit duidelijk gemaakt.

Risico: Laag

Maatregelen: De zorgverlener of GGD-medewerker die om toestemming vraagt wordt goed en duidelijk geïnstrueerd en legt de gegeven toestemming vast en bevestigt dat aan de betrokkene. RIVM draagt zorg voor procedures waarmee de betrokkene snel en gemakkelijk inzage kan verkrijgen in de verwerkte gegevens en deze desgewenst kan verwijderen uit CIMS, ook als de RIVM op basis van de AVG en UAVG daartoe mogelijk niet is gehouden. De betrokkene kan daarmee, als hij meent zijn toestemming niet te hebben gegeven of als hij deze wenst in te trekken, de vaccinatiegegevens verwijderen uit CIMS.

Impact na maatregelen: Laag

5. Inbreuk in verband met persoonsgegevens bij verstrekking gegevens door zorgverleners, niet zijnde GGD, aan RIVM

fase(n): iii.

categorie: middelen, gegevens

incident: zoekraken van vaccinatiegegevens

Impact: Medium. De zorgverlener (huisarts) legt in het eigen informatiesysteem vast dat de betrokkene is gevaccineerd met welk vaccin (type, batch). Als de betrokkene daarvoor toestemming heeft gegeven verstrekt de zorgverlener de vaccinatiegegevens aan RIVM. Daarvoor maakt hij gebruik van een door RIVM beschikbaar gesteld standaard Excel-bestand. Als daarbij wat misgaat kan dit betekenen dat vaccinatiegegevens zoekraken en/of bekend worden bij onbevoegden.

Kans: Laag. De zorgverlener beroepsgeheim en degenen die hem bij de vaccinatie ondersteunen een afgeleid beroepsgeheim. Er kan vanuit worden gegaan dat zij bekend zijn met de risico's en daarnaar handelen. De zorgverlener maakt voor de verstrekking van het Excelbestand gebruik van de beveiligde emailapplicatie Zorgmail, waardoor alleen kennis kan worden genomen van de vaccinatiegegevens door de beoogde ontvanger, RIVM.

Risico: Laag

Maatregelen: De zorgverlener ontvangt via Zorgmail bevestiging van de goede ontvangst van de door hem verstuurde Excel-bestanden. Op termijn kunnen koppelingen met de door huisartsen gebruikte informatiesystemen worden gerealiseerd. De door RIVM ontvangen Excelbestanden worden niet langer dan twee weken bewaard voor kwaliteitsdoeleinden.

Impact na maatregelen: Laag

7. Inbreuk in verband met persoonsgegevens bij verstrekking gegevens door GGD aan RIVM

fase(n): iii.

categorie: middelen, gegevens

incident: zoekraken van vaccinatiegegevens

Impact: Medium. De GGD-medewerker legt in het door GGD voor vaccinaties gebruikte informatiesysteem vast dat de betrokkene is gevaccineerd met welk vaccin (type, batch). Als de betrokkene daarvoor toestemming heeft gegeven verstrekt de GGD de vaccinatiegegevens aan RIVM. Als daarbij wat misgaat kan dit betekenen dat vaccinatiegegevens zoekraken en/of bekend worden bij onbevoegden.

Kans: Laag. De GGD-medewerkers hebben een beroepsgeheim en er kan vanuit worden gegaan dat zij bekend zijn met de risico's en daarnaar handelen. Voor de verstrekking van de vaccinatiegegevens wordt gebruik gemaakt van een beveiligde verbinding van e-Zorg, waarmee de gegevens op de SFTP-server van RIVM worden geplaatst. De gegevens worden vervolgens automatisch in CIMS opgenomen verwerkt.

Risico: Laag

Maatregelen:

Impact na maatregelen: Laag

8. Inbreuk in verband met persoonsgegevens na ontvangst van vaccinatiegegevens op SFTP-server van RIVM

fase(n): iii

categorie: middelen, gegevens

incident: onbevoegde toegang tot SFTP-server

Impact: Medium. De door zorgverleners [?] en GGD [?] verstrekte vaccinatiegegevens komen binnen op de SFTP-server van RIVM en worden vandaar ingelezen in CIMS. Vervolgens worden deze bestanden enige tijd bewaard in een interne opslagomgeving (de zgn. NAS). Een beheerder heeft toegang tot de SFTP-server. Een beheerder, of iemand met beheerdersrechten, kan aldus kennisnemen van de vaccinatiegegevens op de SFTP-server en/of de NAS.

Kans: Laag. Er heeft maar een beperkt aantal personen beheerdersrechten.

Risico: Laag

Maatregelen: de tijd waarbinnen de gegevens van de SFTP-server naar CIMS worden overgezet kan tot een minimum worden beperkt, door de gegevens direct na ontvangst over te zetten naar CIMS. Het aantal personen dat toegang heeft tot de SFTP-server en de NAS kan worden beperkt en deze toegang kan verder worden beperkt tot situaties waarin er sprake is van calamiteiten. Op de NAS wordt verder een standaard toegangscontrole ingericht die voldoet aan NEN7513.

Impact na maatregelen: Laag.

9. Verstrekking aan RIVM van persoonsgegevens betreffende niet gevaccineerde personen of betreffende gevaccineerde personen die geen toestemming hebben gegeven voor de verstrekking van hun vaccinatiegegevens

fase(n): iii

categorie: gegevens

incident: ontoereikende anonimisering

Impact: Hoog. Om RIVM in staat te stellen de vaccinatiegraad te bepalen en inzicht te verkrijgen in de effectiviteit van het vaccinatieprogramma verstrekken zorgverleners en GGD aan RIVM ook informatie over het aantal personen dat is opgeroepen en het aantal personen dat daadwerkelijk aan de oproep gehoor heeft gegeven, alsmede over het aantal personen dat wel is gevaccineerd maar geen toestemming heeft gegeven voor de verstrekking van vaccinatiegegevens aan RIVM en opneming daarvan in CIMS. In de gevallen waarin er betrekkelijk weinig personen zijn opgeroepen is het in theorie niet uit te sluiten dat met aanvullende informatie over de periode waarin de oproep is verstuurd of de vaccinatie is gegeven de identiteit van de desbetreffende persoon kan worden achterhaald. Bijvoorbeeld als er in een bepaalde periode één of twee werknemers uit een verpleeghuis is opgeroepen maar zich vervolgens niet heeft laten vaccineren. Als aldus bekend wordt wie ervoor heeft gekozen zich niet te laten vaccineren, kan dat voor de desbetreffende persoon substantiële gevolgen hebben.

Kans: Laag. De aantallen van personen die worden opgeroepen zijn niet zo klein dat op basis daarvan het redelijkerwijs mogelijk is de identiteit van dergelijke personen te achterhalen.

Risico. Medium.

Maatregelen. Als er sprake blijkt te zijn van dergelijke situatie kan ervoor worden gekozen om geen exacte aantallen door te geven maar bandbreedtes, waarmee het risico op identificatie wordt beperkt. In aanvulling daarop kan ook door middel van technische en organisatorische maatregelen binnen RIVM worden geborgd dat het risico op identificatie wordt verkleind. Bijvoorbeeld door de gegevens na ontvangst verder te aggregeren.

Impact na maatregelen: Laag

10. Inbreuk in verband met persoonsgegevens opgenomen in CIMS

fase(n): iii t/vii

categorie: middelen, gegevens

incident: zoekraken van vaccinatiegegevens

Impact: Hoog. In CIMS worden persoonsgegevens, waaronder vaccinatiegegevens vastgelegd van miljoenen betrokkenen. Een inbreuk in verband met persoonsgegevens kan betekenen dat deze gegevens zoekraken of bekend worden bij onbevoegden, wat gelet op het gevoelige karakter van de gegevens een niet verwaarloosbare impact kan hebben op het leven van de betrokkenen.

Kans: Laag.

Risico: Medium

Maatregelen: Versleuteling van de persoonsgegevens in CIMS en implementatie zgn. IB+P-controls ter voorkoming van ongeautoriseerde toegang. Logging van gebruik van CIMS op persoonsniveau en actieve monitoring daarvan overeenkomstig BIO. Versleutelde back-ups op externe locaties. Audits.

Impact na maatregelen: Laag

11. Onbeschikbaarheid of verminderde beschikbaarheid van CIMS

fase(n): iii t/m vii

categorie: middelen, gegevens

incident: ontoegankelijkheid van vaccinatiegegevens

Impact: Medium. Een verminderde beschikbaarheid van CIMS en ontoegankelijkheid van vaccinatiegegevens kan ertoe leiden dat bij RIVM onduidelijk is wie nog niet zijn opgeroepen voor eerste, tweede of derde vaccinatie. Ook kunnen opvolgende zorgverleners niet via RIVM worden geïnformeerd over eventuele eerdere vaccinaties. De desbetreffende gegevens zijn ook vastgelegd bij de zorgverlener of GGD. In zoverre is de impact voor de betrokkene beperkt.

Kans: Laag

Risico: Laag

Maatregelen: maatregelen gericht op waarborging redundantie

Impact na maatregelen: Laag

12. Vaccinatiegegevens gerelateerd aan verkeerde personen in CIMS

fase(n): iii

categorie: **middelen, gegevens**

incident: **vaccinatiegegevens gerelateerd aan verkeerde personen**

Impact: Hoog. De vaccinatiegegevens die door zorgverlener en GGD worden verstrekt moeten in CIMS worden gerelateerd aan de juiste personen. Als vaccinatiegegevens worden gerelateerd aan iemand anders dan de persoon op wie deze gegevens betrekking hebben kan dat serieuze gezondheidsgevolgen hebben voor zowel voor de gevaccineerde persoon als degene aan wie deze gegevens ten onrechte worden gerelateerd.

Kans: Laag. In CIMS is voorzien in een automatische koppeling aan de hand van BSN en geboortedatum – met daarbij voor BSN ook de 11-proef zodat incorrecte BSNs worden opgemerkt. Als er om wat voor reden dan ook meer dan één koppeling mogelijk blijkt worden de desbetreffende gegevens door een RIVM medewerker handmatig verwerkt, aan de hand van nog uit te werken kuezecriteria.

Risico: Medium

Maatregelen: De keuzecriteria en methode voor validatie van gegevens worden verder uitgewerkt.

Impact na maatregelen: Laag

13. Ongedaan making pseudonimisering

fase(n): **vii**

categorie: **middelen, gegevens**

incident: **vaccinatiegegevens**

Impact: Medium. In fase vii doet RIVM op basis van de in CIMS vastgelegde vaccinatiegegevens epidemiologisch onderzoek teneinde inzicht te verkrijgen in de vaccinatiegraad en de effectiviteit, impact en veiligheid van de vaccinatie (zie art. 6c Wpg). Daartoe worden de gegevens op de voor dergelijk door RIVM te verrichten onderzoek gebruikelijke wijze gepseudonimiseerd. Ongedaan making van deze pseudonimisering kan ertoe leiden dat de desbetreffende onderzoekers de identiteit kunnen achterhalen van gevaccineerde personen

Kans: Laag

Risico: Laag

Maatregelen: Aan onderzoekers is een geheimhoudingsverplichting opgelegd. Audits.

Impact na maatregelen: Laag

14 Aanvullende analyses en maatregelen

In aanvulling op de in deze paragraaf beschreven risico's en de beoordeling daarvan is er door verschillende andere experts een analyse gedaan van onder andere de beveiligingsaspecten van CIMS. Dit betreft (a) de beoordeling door de Chief Security &Privacy Operations van het Programma Realisatie Digitale Ondersteuninng, (b) een analyse van Bureau Noordbeek, (c) een analyse van Secura, en (d) een audit door de Audit Dienst Rijk (ADR). De risico inschatting naar aanleiding van deze analyses is reeds beschreven in de Data Protection Impact Assessment CIMS release 1.0, zoals toegestuurd op 31 december 2020 om 16.21.