Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

Document
Afspraken en Procedures

inzake COVID-19 dataverkeer tussen systemen van de vaccinerende organisaties en het RIVM

Datum:	Mei 2021
Status:	Definitief
Documenteigenaar:	RIVM/DVP/BIS
Versie:	1.0

Inhoudsopgave

1. Inleiding

In Nederland zorgen de GGD's, huisartsen, zorginstellingen en ziekenhuizen voor het vaccineren tegen COVID-19. De gegevens van iedere gevaccineerde persoon worden in de systemen van deze organisaties opgeslagen. Het RIVM verzamelt al deze data in het landelijke registratiesysteem COVID-19 vaccinaties (een centrale database): het COVID-19 Informatie- en MonitoringSysteem (CIMS)[1].

U bent softwareleverancier en treedt op als bewerker namens uw klanten (de zorgverleners). Voor zorgverleners geldt dat de softwareleverancier het eerste contactpunt is voor ICT-meldingen. Zorgverleners moeten bij datalekken en fouten in registraties altijd contact opnemen met de softwareleverancier.[2] De zorgverlener is altijd de contactpartij voor de cliënten. Indien er iets mis gaat met de registratie van de vaccinatiegegevens van een cliënt, neemt de zorgverlener contact op met de betreffende cliënt(en).

De vaccinatiegegevens uit uw systeem worden digitaal doorgestuurd (of opgehaald) naar de landelijke database van het RIVM, voor zover de gevaccineerde persoon hiervoor toestemming heeft gegeven. Indien geen toestemming is verleend wordt het RIVM door middel van een beperkte, geanonimiseerde dataset op de hoogte gebracht van de vaccinatie. De data in de systemen van het RIVM wordt gebruikt ten behoeve van:

- de veiligheidsbewaking van de te vaccineren personen en het vaccinatieprogramma,
- het onderzoek naar de effectiviteit van het vaccin,
- de beleidsinformatie ter indicatie van actuele gevaarzetting[3], bestrijdingsmaatregelen en de mogelijke verlichting daarvan.

Over het dataverkeer, wederzijdse verantwoordelijkheden en de samenwerking hieromtrent zijn met u, mogelijk via uw koepelorganisatie of klant, en andere betrokken partijen contractuele afspraken gemaakt en vastgelegd[4]. Dit Document Afspraken en Procedures (DAP) is een praktisch werkdocument dat betrekking heeft op de beveiligde uitwisseling van de data tussen uw systeem en het RIVM-systeem ('van voordeur tot voordeur'). Dit document bevat de communicatiegegevens en de te nemen stappen in diverse situaties. Hierdoor weet u in verschillende situaties met wie u contact kunt opnemen en welke stappen moeten worden gevolgd. Dit document heeft alleen betrekking op de technische oplossing en niet op de inhoud van de registraties en informatie-uitwisseling.

De informatie in deze DAP is alleen voor de softwareleveranciers van de vaccinerende zorgverleners. Wij vragen u om de inhoud hiervan (inclusief het mailadres van CIMS Beheer) niet te verspreiden of op internet te plaatsen en de contactgegevens niet aan burgers te overhandigen. Dit document wordt aan u gestuurd door het RIVM,

---

[1] Vragen over registratie en persoonsgegevens coronavaccinatie | Rijksoverheid.nl

[2] Let op! Datalekken moeten binnen 72 uur bij Autoriteit Datalekken worden gemeld.

[3] Gevaarzetting = het creëren of laten bestaan van een gevaarlijke situatie.

[4] Bijvoorbeeld: d.m.v. de offerteverzoeken en offertes inzake de data-aanleverende systemen van COVID-19 vaccinaties, het 'Convenant Covid-19-vaccinaties' en/of de overeenkomsten 'inzake Gegevens transfer voor de landelijke campagne COVID-19 vaccinaties'.

eventueel via een koepelorganisatie. Dit document geeft een praktische invulling van de organisatie, communicatie en procedures voor de COVID-19 gegevensuitwisseling. Mist u nog iets in dit document? Neem hierover dan contact op met 5.1.2e @rivm.nl.

2. Contactgegevens RIVM

2.1. Contactgegevens RIVM-Servicedesk inzake het dataverkeer

De servicedesk CIMSBeheer[5] van het RIVM (afdeling DVP), zorgt voor het beheer van de aangeleverde data (inclusief de geanonimiseerde data) en de ontvangende systemen met de databases van de vaccinatiegegevens. Dit is het loket bij het RIVM voor alle meldingen m.b.t. het dataverkeer van de vaccinatiegegevens van COVID-19. Het RIVM monitort 24/7 de beschikbaarheid van de RIVM-systemen. De contactgegevens en beschik-/bereikbaarheidstijden staan in onderstaande tabel. In hoofdstuk 3 staat een uitleg van de prioriteringen.

Signaleert u een storing of een datalek? Kijk dan eerst goed na of de oorzaak te vinden is in uw eigen systeem. Betreft het echt (de koppeling met) het CIMS van het RIVM of een datalek? Neem dan altijd contact op met het RIVM.
Bent u een vaccinerende organisatie? Laat dan uw meldingen eerst via uw eigen softwareleverancier lopen (indien nodig kan uw softwareleverancier dan contact opnemen met het RIVM).

Meldingen Prio 2 t/m 4	
Beschik-/ bereik-baarheidstijden en contactgegevens voor Prio 2 t/m 4 meldingen	Op ma t/m vr: 8.00 - 18.00 uur (kantoortijden) **Alleen per mail** 5.1.2e @rivm.nl
Meldingen Calamiteiten en Prio 1 meldingen	
Beschik-/ bereik-baarheidstijden voor Calamiteiten en Prio 1 meldingen **Tijdens kantoortijden**	Op ma t/m vr: 8.00 - 18.00 uur (kantoortijden) N.B. dit contact moet via 2 kanalen verlopen: **Eerst per mail** 5.1.2e @rivm.nl **én daarna per telefoon** 5.1.2e (alléén voor calamiteiten en Prio 1 meldingen tijdens kantoortijden)
Beschik-/ bereik-baarheidstijden voor Calamiteiten en Prio 1 meldingen **Buiten kantoortijden**	Voor calamiteiten en Prio 1 meldingen worden extra bereikbaarheidstijden gehanteerd, namelijk: Op ma-vr: 7.00 - 8.00 uur 18.00 – 21.00 uur Op za: 8.00 - 18.00 uur N.B. dit contact moet via 2 kanalen verlopen: **Eerst per mail**

[5] Zie Bijlage 1 voor de beschrijving van afkortingen en begrippen.

	5.1.2e @rivm.nl **én daarna per telefoon** 5.1.2e (alléén voor calamiteiten en Prio 1 meldingen buiten kantoortijden)

N.B. Deze contactgegevens zijn voor u, maar niet voor iedereen. A.u.b. deze informatie niet op internet publiceren.

3. Prioritering meldingen

Onder een melding verstaan wij een vraag of informatieverzoek, een wijzigingsverzoek of een incident/storing. In onderstaande tabel zijn de prioriteitcodes beschreven voor alle meldingen van incidenten[6], vragen en verzoeken. Wanneer u contact opneemt met het RIVM, kunt u aangeven welke prioriteit uit deze tabel volgens u het beste bij uw melding past. Het RIVM bepaalt de prioritering bij het indienen van een melding. Een (mogelijke) calamiteit begint bij het RIVM eerst als Prio 1.

Prioriteit	Code	Omschrijving
Calamiteiten	Cal	Incidenten die worden opgeschaald naar de calamiteitstatus, waarbij geldt dat sprake is van: • een datalek en/of een andere vorm waarbij de veiligheid van meerdere personen in het geding is of kan komen, en/of • een risico voor negatieve publiciteit en/of het imago van één van de betrokken organisaties.
Hoog	Prio 1	Incidenten waarbij • de koppeling en/of software van het RIVM niet meer functioneert of bruikbaar is, en/of • er geen work around beschikbaar is op het moment dat het incident zich voordoet of een ingreep noodzakelijk is om het systeem weer naar behoren te laten functioneren.
Normaal	Prio 2	Incidenten waarbij de koppeling en/of software van het RIVM (deels) werkt, echter deze incidenten hebben tot gevolg dat gebruikers minder efficiënt kunnen werken. Work around is mogelijk.
Laag	Prio 3	Incidenten waarbij de koppeling en/of software van het RIVM kan worden gebruikt en die geen of zeer beperkt effect hebben op het gebruik. Work around is mogelijk.
Overig	Prio 4	Dit betreft meldingen over de testomgeving en alle andere meldingen dan incidentmeldingen, dus bijvoorbeeld vragen en verzoeken (bijv. voor wijzigingen). Dit betreft ook het melden van niet functioneren van uw eigen systeem, zodat het RIVM op de hoogte is van uw situatie[7].

N.B. Is er een storing of knelpunt m.b.t. uw eigen systeem? Los dit dan zelf op, eventueel met betrokken partijen! Dit kan het RIVM niet oplossen.

[6] Incidenten m.b.t. het dataverkeer, de koppelingen en koppelvlakken.
[7] Dit kan het RIVM niet voor u oplossen, maar het is wel belangrijk dat het RIVM weet dat en waarom er geen gegevens van u worden ontvangen en wat de prognose voor oplossing van het probleem is.

4. Streeftermijnen

In onderstaande tabel staan de reactie- en oplostermijnen die het RIVM nastreeft. We doen ons best om binnen deze termijnen te reageren en op te lossen. Onderstaande uren zijn uren tijdens de kantoortijden zoals in hoofdstuk 2 vermeld. Wanneer wij meldingen bij u indienen (bijvoorbeeld voor storingen die u dient op te lossen), willen wij u vragen om ook binnen deze streeftermijnen proberen te reageren en op te lossen.

Prioriteit	Reactietermijn	Oplostermijn
Prio 1	0,5 uur	8 uur
Prio 2	2 uur	16 uur
Prio 3	5 uur	40 uur
Prio 4	10 uur	in overleg

De Reactietermijn = de termijn die start op het moment dat een melding bij het RIVM wordt ontvangen en eindigt op het moment waarop het RIVM aan u als melder laat weten dat de melding goed is ontvangen.
De Oplostermijn = de termijn die start op het moment dat een melding wordt ontvangen door het RIVM en eindigt op het moment waarop de situatie volledig is opgelost.

Calamiteiten
Voor calamiteiten is niet aangegeven wat de reactie- en oplostermijnen zijn, omdat in het geval van een calamiteit diverse (ambtelijke) verantwoordelijken en partijen worden betrokken en de aanpak afhangt van de aard van de calamiteit. Zie 5.3.

Overschrijding oplostermijn
Indien de verwachte oplostermijn voor een incident dreigt te worden overschreden, kan het RIVM een schriftelijk voorstel doen voor een mogelijke tussentijdse oplossing. In het geval van niet behalen van de oplostermijn van een Prio 1 kan eventueel worden opgeschaald naar het calamiteitenniveau.

5. Informatie en procedures voor mogelijke situaties

Dit hoofdstuk beschrijft de belangrijkste informatie en stappen voor mogelijke situaties.

5.1. Doorgifte van de gegevens bij vaccinatie

Bij het vaccineren doorloopt de vaccineerder (op hoofdlijnen) de onderstaande stappen v.w.b. de registratie van persoonsgegevens.

Stap	Handeling
1	De vaccineerder vraagt de te vaccineren persoon toestemming voor doorsturen gegevens[8] en registreert dit, door het vastleggen van informed

[8] De vaccineerder is verantwoordelijk voor het verkrijgen en registreren van de instemming van de te vaccineren persoon/cliënt voor het verstrekken van de vaccinatiegegevens aan de landelijke registratie bij het RIVM. Deze toestemming dient geregistreerd te worden. De regelgeving laat toe dat in bijzondere omstandigheden mondelinge toestemming wordt verleend, mits deze zorgvuldig wordt vastgelegd.

	consent. Dit betekent dat dus alleen wanneer in het systeem is vastgelegd dat de cliënt uitdrukkelijk toestemming heeft gegeven dat de vaccineerder de betreffende gegevens beschikbaar mag stellen aan het RIVM.
2	De vaccineerder zorgt voor de vaccinatie en de invoering van de volledige registratiegegevens in het eigen systeem.
3	De gegevens worden langs elektronische weg verstrekt aan het RIVM via een koppeling tussen uw registratiesysteem en het RIVM-systeem. Wanneer dit niet lukt, moet dit direct worden gemeld en opgelost. Het systeem van de vaccineerder dient, conform contractuele afspraken, de gegevens dagelijks aan het RIVM te verstrekken.

5.2.Incidenten (prio 1 t/m 3 meldingen)

Een incident = een niet beoogde of onverwachte gebeurtenis of meerdere gebeurtenissen die binnen een korte tijd leidt/leiden tot verlies of vermindering van de kwaliteit en/of de continuïteit van het systeem, of het niet kunnen doorsturen van de data.

Indien er incidenten optreden zullen de aanmelding en de afhandeling volgens onderstaande route verlopen.

Stap	Handeling
1	U stelt een incident vast en controleert of dit incident uw eigen systeem betreft. Indien het incident niet uw eigen systeem betreft, doorloopt u onderstaande stappen.
2	U mailt de melding naar het mailadres in 2.1 o.v.v. minimaal: • naam aanmelder, organisatie, contactgegevens; • beschrijving incident (indien mogelijk inclusief screenshot); • vermoedelijke prioritering. Wanneer het een vermoedelijke Prio 1 melding is, dient u ook te bellen naar het betreffende telefoonnummer in 2.1. Bij foutmeldingen in het systeem dienen de volgende gegevens te worden gemeld: • de naam van het aangeleverde bestand; • het voorlooprecord van het aangeleverde bestand; • de regel waar de fout is geconstateerd; • eventuele foutcode; • tijdstippen inloggegevens.
3	De servicedesk informeert u dat uw melding goed is ontvangen en hoe het vervolgproces zal verlopen.
4	Het RIVM zal het incident oplossen, indien dit het systeem van het RIVM betreft. N.B. Bij ieder Prio 1 incident wordt, op basis van een impact-analyse, bepaald of het nodig is om het CMT te informeren en op de hoogte te houden.
5	Indien de oplossing niet akkoord is of het oplossen te lang duurt, volgt u de escalatieprocedure in 5.8.

5.3.Calamiteiten

Een calamiteit is een incident dat wordt opgeschaald naar de calamiteitstatus, waarbij geldt dat sprake is van:

- een datalek en/of een andere vorm waarbij de veiligheid van meerdere personen in het geding is of kan komen, en/of
- een risico voor negatieve publiciteit en/of het imago van één van de betrokken organisaties.

Voorbeeldsituaties:

- Situatie waarbij de beschikbaarheid, integriteit en/of vertrouwelijkheid van een groot deel van de geëxploiteerde diensten en/of zorginfrastructuur in het geding is (ook cyberbedreigingen/ -aanvallen).
- Situatie die het verantwoordelijkheidsgebied overstijgt van de individuele organisaties, die samen de keten vormen van COVID-19 vaccinatiegegevens-aanlevering, bijvoorbeeld het uitvallen van een datacenter waar HIS-leveranciers gebruik van maken.
- Situatie buiten de directe invloedsfeer van de keten van geëxploiteerde diensten en/of zorginfrastructuur die direct of indirect invloed heeft op deze keten en/of gerechtelijke implicaties kan hebben. Een voorbeeld hiervan zijn fouten in de koppelingen van BSN, persoonsgegevens en medische gegevens, Ook het uitvallen van een e-zorg- of ASP-omgeving, waardoor berichtuitwisseling met een grote groep zorginstellingen onmogelijk wordt, is hiervan een voorbeeld.

Wanneer sprake is van een calamiteit, wordt geëscaleerd volgens de interne calamiteitenprocedures van betrokken organisaties en, indien nodig, de gemeenschappelijke ketencalamiteitenprocedure.

Stap	Handeling
1	De signalerende organisatie escaleert binnen de eigen organisatie volgens de interne calamiteitenprocedure. U meldt deze als een Prio 1 melding bij 5.1.2e @rivm.nl. Hier wordt bepaald of daadwerkelijk sprake is van een calamiteit en welke calamiteitenprocedure moet worden gevolgd.
2	Indien sprake is van een calamiteit, wordt de betreffende calamiteitenprocedure opgestart. Wanneer meerdere ketenpartijen zijn betrokken, wordt de ketencalamiteitenprocedure gevolgd.
3	Indien nodig wordt een crisismanagementteam (CMT) samengesteld. Het CMT doet onderzoek naar de mogelijke impact, risico's en oplossing(en) en zet de oplossing in gang.
4	Betrokken partijen en personen worden geïnformeerd, indien gewenst/ noodzakelijk.[9]
5	De calamiteitenprocedure van iedere betrokken organisatie c.q. de ketencalamiteitenprocedure (wanneer meerdere partijen zijn betrokken) wordt verder gevolgd.

[9] Voor de keten HIS en RIVM zal VZVZ SC als ketenbeheerpartij in geval van een calamiteit het proces mee-begeleiden.

5.4.Verzoeken voor wijzigingen (changes; Prio 4)

Verzoeken voor wijzigingen door het RIVM aangaande de koppeling doorlopen een eigen procedure.

Stap	Handeling
1	U constateert dat een wijziging/change nodig is.
2	U mailt uw wijzigingsverzoek (request for change; RFC) aan 5.1.2e @rivm.nl o.v.v.: • aanmelder (kennishouder functionele vraag); • omschrijving van uw verzoek; • verwacht resultaat.
4	Het RIVM zal uw verzoek in behandeling nemen en met betrokken partijen bespreken. Hiervoor worden een business case en impact analyse opgesteld en voorgelegd aan de beslissers van betrokken organisaties. Indien het verzoek akkoord wordt bevonden, zal dit worden uitgewerkt aan de hand van de onderstaande aspecten: • technische en functionele complexiteit; • beschrijving en doel van de aanvragen; • risico's en mitigerende maatregelen; • oplossingsvoorstel + evt. financiële onderbouwing/ prijs; • globale werk breakdown; • concept planning.
5	Afhankelijk van de prioriteit zal één van de volgende updates plaatsvinden: • release (planbaar); • patch (planbaar korte termijn); • hotfix (spoed).
6	De RFC wordt afgesloten na akkoord van RIVM.

5.5.Algemene vragen/ informatieverzoeken (Prio 4)

Al uw algemene ICT-gerelateerde vragen m.b.t. de koppelingen voor het dataverkeer i.v.m. de COVID-19 vaccinaties kunt u stellen via 5.1.2e @rivm.nl. Voor algemene niet-ICT-gerelateerde vragen kunt u contact opnemen via de contactgegevens op www.rivm.nl.

5.6.Updates, upgrades, testprocedures

Updates, upgrades en tests die voor u (mogelijk) merkbaar zullen zijn, zullen in onderling overleg worden afgestemd, voorbereid, ingepland en uitgevoerd. Upgrades en andere mogelijke onderbrekingen in uw eigen systeem die effect hebben op het dataverkeer kunt u ter informatie melden aan 5.1.2e @rivm.nl.

5.7.Overige mogelijke situaties

In het geval dat	**Onderneemt wie welke actie?**
Een fout in één of meer registraties wordt geconstateerd.....	.... zal de constaterende partij met de andere betrokken partij(en) contact opnemen; u neemt contact op met het RIVM, het RIVM neemt contact op met u (als u

	betrokken bent). In gezamenlijkheid wordt bepaald hoe de fout kan worden opgelost en of benadeelden moeten worden geïnformeerd, of het een calamiteit betreft en of het CMT moet worden geactiveerd.

5.8. Escalatie

Escalatie vindt plaats doordat u of andere betrokken partijen de verantwoordelijke(n) op een hoger niveau inschakelen. Deze persoon zal vervolgens overeenstemming gaan zoeken met de counterpart van de andere partij op dat niveau. Indien op dit niveau wederom een 'conflict' blijft bestaan zal ook hier naar bovenliggend niveau worden geëscaleerd.

Onverminderd het bepaalde in de afgesloten overeenkomst beschikken partijen over een interne escalatieprocedure of dragen zij zorg voor het opstellen daarvan.

Indien escalatie noodzakelijk is, bijvoorbeeld in geval van het niet behalen van een oplostermijn of een andere dringende situatie, volgt u de escalatieroute binnen uw eigen organisatie. Indien verantwoordelijke personen hierover in gesprek willen komen met verantwoordelijken binnen het RIVM, kan dit worden aangegeven door contact op te nemen met een volgend escalatieniveau en aan te geven dat het een escalatie betreft.

De escalatieroute binnen het RIVM is: CIMSBeheer -> Afdelingshoofd DVP/BIS -> Hoofd DVP en indien nodig verder binnen de organisatie.

Bijlage 1 Begrippen

Begrip	Omschrijving
BIS	Beheer Informatie Systemen
Calamiteit	Een incident dat wordt opgeschaald naar de calamiteitstatus, waarbij geldt dat sprake is van: • een datalek en/of een andere vorm waarbij de veiligheid van meerdere personen in het geding is of kan komen, en/of • een risico voor negatieve publiciteit c.q. voor het imago van één van de betrokken organisaties.
CIMS	COVID-19 Informatie- en MonitoringSysteem
CMT	Crisismanagementteam
Datalek	Het (on)opzettelijk vrijgeven van beveiligde informatie aan een onvertrouwd publiek.
DVP	Dienst Vaccinvoorziening en Preventieprogramma's
Incident	Een niet beoogde of onverwachte gebeurtenis of meerdere gebeurtenissen die binnen een korte tijd leidt/leiden tot verlies of vermindering van de kwaliteit en/of de continuïteit van het systeem, of het doorgeven van de data.
Melding	Een melding van een vraag of informatieverzoek, een wijzigingsverzoek of een incident.
Oplostermijn	De termijn die start op het moment dat een melding wordt ontvangen door het RIVM en eindigt op het moment waarop de situatie volledig is opgelost.
Reactietermijn	De termijn die start op het moment dat een melding bij het RIVM wordt ontvangen en eindigt op het moment waarop het RIVM aan u als melder laat weten dat de melding goed is ontvangen.
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
Vraag of informatieverzoek	Vragen over CIMS, de koppeling of het dataverkeer.
Wijzigingsverzoek	Een verzoek om een wijziging in de koppeling die het dataverkeer mogelijk maakt.