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

Ketencalamiteitenprocedure

inzake het Dataverkeer tussen systemen van de vaccinerende organisaties en de systemen van het RIVM inzake Covid-19

Eigenaar:	5.1.2e, RIVM/DVP
Documentbeheer:	5.1.2e RIVM/DVP/BIS
Datum:	Mei 2021
Status:	Definitief
Versie:	1.0

Inhoudsopgave

1. Inleiding

De vaccinatiegegevens (anoniem en niet-anoniem) uit systemen van diverse vaccinerende organisaties worden digitaal doorgestuurd naar de landelijke database in de systemen van het RIVM. De data 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, bestrijdingsmaatregelen en de mogelijke verlichting daarvan.

Deze calamiteitenprocedure heeft betrekking op de functionaliteiten die bijdragen aan het dataverkeer ten behoeve van de Covid-19-vaccinaties. Het doel van dit document is het vastleggen van de afspraken die van toepassing zijn bij het zich voordoen van calamiteiten in het dataverkeer tussen de systemen van vaccinerende organisaties en de database van het RIVM. Dit document is van toepassing op het moment dat zich een calamiteit voordoet in het dataverkeer tussen voornoemde systemen.

Deze gemeenschappelijke ketencalamiteitenprocedure is overkoepelend voor alle ketenpartners en hierin worden de individuele calamiteitenprocedures in elkaar vervlochten.

Deze ketencalamiteitenprocedure heeft betrekking op alle partijen die betrokken zijn bij de registratie en het beheer van vaccinatiedata t.b.v. Covid-19 (ketenpartners). De calamiteitenprocedures van de ketenpartners dienen op elkaar aan te sluiten.

Over het dataverkeer, wederzijdse verantwoordelijkheden en de samenwerking hieromtrent zijn met deze vaccinerende organisaties en/of hun leveranciers en/of beheerders van de datasystemen contractuele afspraken gemaakt en vastgelegd[1].

Wanneer een calamiteit zich voordoet, wordt eerst geëscaleerd volgens de calamiteitenprocedure van de signalerende organisatie. Indien bij de calamiteit een (of meer) ketenpartij(en) betrokken is (/zijn) dan wordt de gemeenschappelijke ketencalamiteitenprocedure opgestart. Het RIVM heeft de regie op de gemeenschappelijke ketencalamiteitenprocedure en is 5.1.2e van het keten-CMT.

Een calamiteit start als een incident. Het incidentmeldingenproces is beschreven in het Document Afspraken en Procedures (DAP) Dataverkeer Covid-19. Dit is een praktisch document over de reguliere, praktische communicatie over de digitale aansluiting tussen de systemen van de vaccinerende organisaties en het CIMS. Hierin staan onder andere contactgegevens en procedures die betrekking hebben op het melden en oplossen van incidenten. Deze ketencalamiteitenprocedure is een verlengstuk van het DAP. Een calamiteit zal beginnen als een melding die bij CIMSBeheer (RIVM/DVP/BIS)[2] wordt ontvangen. Via de escalatieroute binnen het

[1] Bijvoorbeeld: de overeenkomsten 'inzake gegevens transfer voor de landelijke campagne COVID-19 vaccinaties', of d.m.v. de offerteverzoeken en offertes inzake de data-aanleverende systemen van COVID-19 vaccinaties.

[2] Zie bijlage 1 voor omschrijvingen van afkortingen en begrippen.

RIVM wordt de ketencalamiteitenprocedure opgestart.

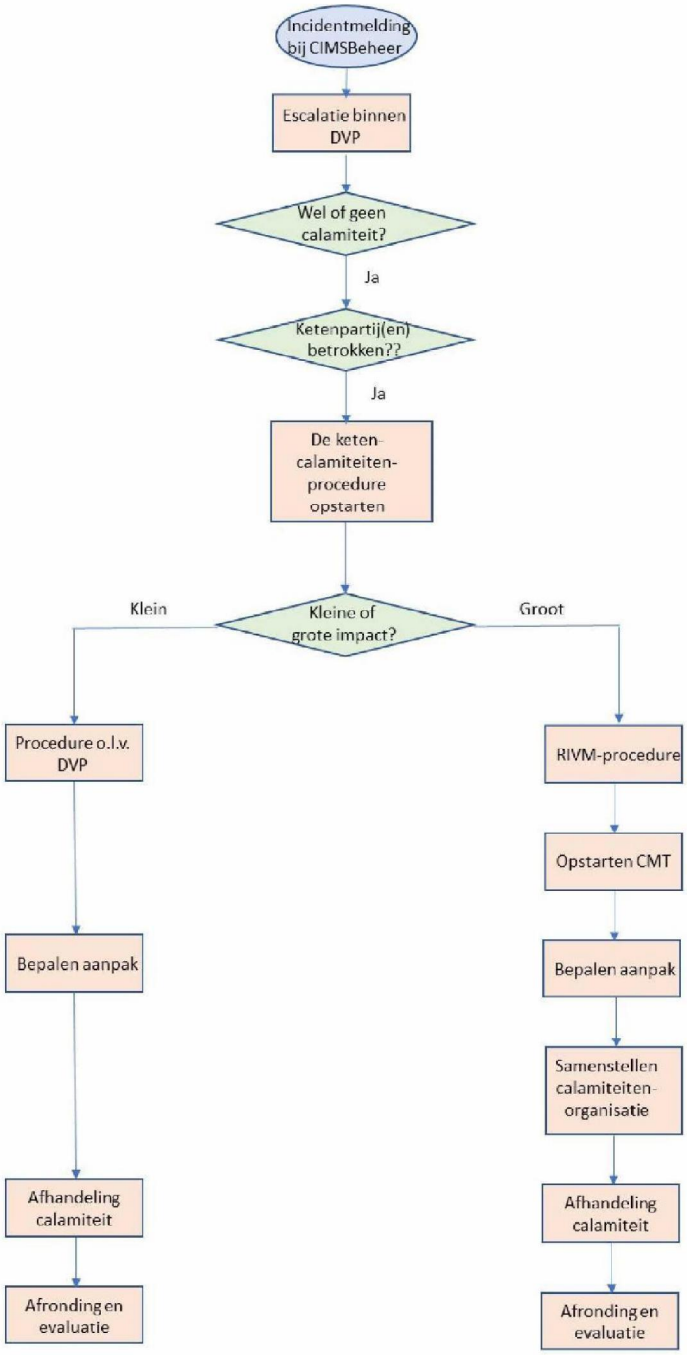
In het geval van een mogelijke calamiteit wordt door CIMSBeheer, via de lijnorganisatie, geëscaleerd naar het 5.1.2e Het 5.1.2e bepaalt of het incident definitief wordt opgeschaald naar een calamiteit en of het een calamiteit met een grote of kleine impact betreft (door middel van een impact analyse). Het onderscheid tussen een calamiteit met een kleine of grote impact wordt door het 5.1.2e per calamiteit bepaald.

Indien het een calamiteit betreft met een kleine impact zal het 5.1.2e de aanpak en samenstelling van de calamiteitenorganisatie bepalen. Het 5.1.2e zorgt in dit geval voor de afstemming met de betrokken ketenpartij(en). In dit geval wordt een 'beknoptere' versie van de procedure in dit document toegepast.

Indien het een calamiteit betreft met een grote impact, wordt geëscaleerd naar de 5.1.2e die vervolgens het keten-CMT activeert. Het bepalen van de specifiek benodigde aanpak en de opvolging van deze calamiteit vindt plaats door het keten-CMT. Indien gewenst of benodigd zal uw organisatie ook worden betrokken bij/ uitgenodigd voor deelname aan het keten-CMT, of geïnformeerd over het verloop en de afhandeling.

Hoofdstuk 2 bevat een visuele weergave van het proces. In hoofdstuk 3 wordt uitgelegd wat een calamiteit is. Hoofdstuk 4 beschrijft de ketencalamiteitenprocedure. Het laatste hoofdstuk geeft gerelateerde documenten aan. Bijlage 1 geeft een beschrijving van alle begrippen en in bijlage 2 zijn de contactpersonen van alle ketenpartijen opgenomen.

2. Proces flow Ketencalamiteitenprocedure



3. Wat is een calamiteit?

Een calamiteit = een gebeurtenis, direct of indirect, die het dataverkeer tussen de systemen van beide partijen c.q. de veiligheid van gegevens in gevaar brengt of kan brengen en/of waarbij er (mogelijk) een risico is voor het imago van één van de betrokken partijen. Dit betreft in ieder geval datalekken. 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.

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 de verantwoordelijkheidsgebieden van de ketenpartners overstijgen, bijvoorbeeld het uitvallen van een datacenter.
- 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 vaccinerende partijen onmogelijk wordt.

Wanneer sprake is van een calamiteit worden diverse betrokken verantwoordelijken en partijen betrokken en de aanpak en doorlooptermijn hangt af van de aard van de calamiteit. Een ketencalamiteit is een calamiteit die betrekking hebben op meerdere ketenpartners. De betreffende ketenpartners zullen daarom ook deel uitmaken van de calamiteitenorganisatie.

4. Ketencalamiteitenprocedure

4.1.Ketencalamiteitenorganisatie

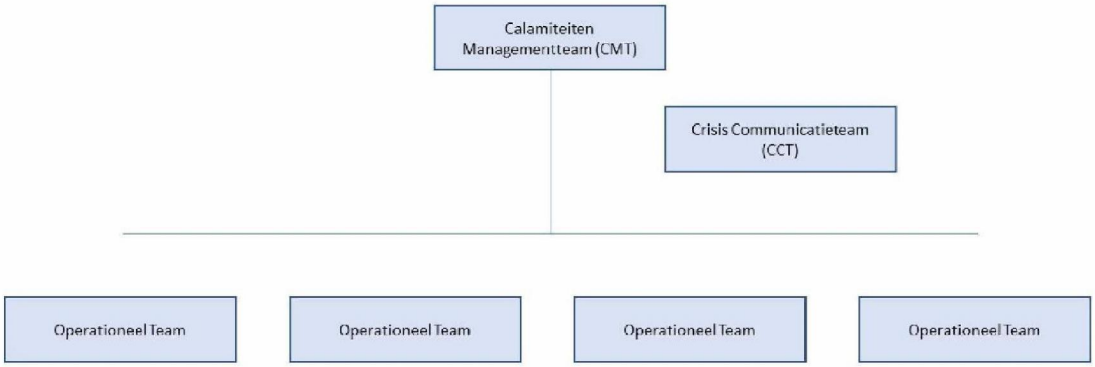
In het geval van een mogelijke calamiteit wordt door CIMSBeheer, via het 5.1.2e geëscaleerd naar het Crisis Managementteam van het RIVM (CMT)[3]. Indien sprake is van een calamiteit met een grote impact (of de kans daarop is erg groot), zal het 5.1.2e contact opnemen met de op dat moment dienstdoende 5.1.2e die vervolgens contact opneemt met de 5.1.2e over het activeren van het CMT. Binnen het RIVM is een groep 5.1.2e aanwezig die werkt met piketdiensten. 5.1.2e die op het moment van een ketencalamiteit 'dienst' heeft zal de rol van 5.1.2e invullen. De regie op het keten-CMT ligt bij het RIVM, namelijk bij 5.1.2e 5.1.2e Safety & Security (S&S) van RIVM/FCC is aanspreekpunt en coördineert het

[3] Hierbij wordt onderscheid gemaakt tussen grote en kleine calamiteiten: kleine calamiteiten worden door DVP met betrokkenen opgepakt en hiervoor wordt het CMT niet geactiveerd. De besluitvorming of een calamiteit 'groot' of 'klein' is, ligt bij het 5.1.2e

ketenCMT.

Het keten-CMT volgt deze ketencalamiteitenprocedure. De ketencalamiteitenorganisatie en ketencalamiteitenprocedure zijn op hoofdlijnen beschreven. Het bepalen van de specifiek benodigde organisatie, aanpak en de opvolging van de betreffende calamiteit is maatwerk op basis van de aard van de calamiteit en vindt plaats door het keten-CMT.

Onderstaand figuur geeft het algemene organigram van de ketencalamiteitenorganisatie weer.



Leden Keten-CMT

De samenstelling van het keten-CMT wordt bepaald aan de hand van de aard van de betreffende calamiteit. De definitieve samenstelling en de onderlinge taakverdeling worden in onderling overleg bepaald. Voor de samenstelling kan worden gedacht aan:

5.1.2e 5.1.2e	Geeft leiding aan het CMT, neemt alle noodzakelijke besluiten, coördineert en onderhoudt de bestuurlijke contacten met overheid (Burgemeester, SG VWS) en coördineert alle activiteiten van het CMT.
5.1.2e 5.1.2e	Adviseert over het te voeren communicatiebeleid, coördineert alle in- en externe communicatieactiviteiten, coördineert en verzorgt de contacten met de media, onderhoudt de contacten met de voorlichters van de bij de crisis betrokken externe organisaties.
5.1.2e	Adviseert over de wijze en mate van betrekken van of het ondernemen van actie richting medewerkers en organisatieonderdelen.
5.1.2e	Adviseert inzake de informatiebeveiliging.

[4] Het voorzitterschap rouleert binnen een groep hiertoe aangewezen personen.

5.1.2e	Adviseert inzake financiële en controlaspecten.
	Organiseert de bijeenkomsten en legt de genomen besluiten en acties vast in een logboek.

Mogelijke extra leden:

5.1.2e	Afhankelijk van de aard van de calamiteit en de betrokkenheid en rol van de ketenpartner.
	Verantwoordelijk voor de aansturing van DVP.
	Verantwoordelijk voor de aansturing van DVP/BIS.
	Adviseert m.b.t. privacy- aspecten en -maatregelen.
	Coördineert de maatregelen in het kader van het bedrijfsnetwerk en (herstel, opschaling van) de informatiesystemen.
	Is verantwoordelijk voor het beantwoorden van telefoon en noteren van berichten gedurende de periode dat het CMT bij elkaar is geroepen. Berichten worden overhandigd aan 5.1.2e 5.1.2e

4.2.Crisis Communicatieteam (CCT)

In het geval van een calamiteit kan ook het Crisis Communicatieteam (CCT) worden geactiveerd door het CMT (dit zal met name gebeuren in het geval van activering van het RIVM-CMT). Als sprake is van negatieve publiciteit en het calamiteitenproces wordt gevolgd, wordt het CCT per definitie geactiveerd. Het CCT wordt aangestuurd door de 5.1.2e , die ook de 5.1.2e is.

Het CCT verzorgt/ ondersteunt de interne en externe communicatie en verricht de volgende activiteiten, in opdracht van het CMT:

- advies aan het CMT;
- coördinatie crisiscommunicatie;
- interne Communicatie;
- persvoorlichting;
- externe Communicatie (incl. RIVM Informatiepunt);
- webcare;
- (web)redactie;
- ondersteuning.

4.3.Operationele teams

Afhankelijk van de calamiteit (soort, omvang en aanpak) kunnen door het CMT diverse operationele teams worden samengesteld en geactiveerd, zoals Informatiebeveiliging, RIVM/SSC Campus, leverancier CIMS, leveranciers/ beheerders systemen ketenpartners, Functioneel Beheer DVP/BIS, enzovoorts.

Het CMT kan besluiten een samengesteld operationeel team te activeren of

besluiten één of meerdere operationele teams te activeren, dan wel stand-by te zetten. De belangrijkste verantwoordelijkheden en bevoegdheden van deze teams tijdens een calamiteit kunnen zijn:

- In overleg met en in opdracht van het CMT uitvoeren van operationele werkzaamheden voor het zo spoedig mogelijk oplossen van de calamiteit, eventueel door middel van een tijdelijke oplossing.
- Het zo veel als mogelijk is hanteren van reguliere (beheer)procedures bij het oplossen van de calamiteit.
- Het registreren van de communicatie, beslissingen en aangegane overeenkomsten in een logboek.
- Het periodiek rapporteren van de status en voortgang aan (de afgevaardigde in) het keten-CMT.
- Het verzorgen van de communicatie/informatievoorziening richting de (operationele teams van) betrokken partijen in de keten.
- Het assisteren van personen die betrokken zijn bij forensisch onderzoek, in geval van het vermoeden van een strafbaar feit.

4.4.Procesbeschrijving

0. Voorafgaand: melding van een incident

- Er wordt een incident geconstateerd door het RIVM of één van de ketenpartners (vaccinerende organisatie of beheerder/ leverancier van het systeem van de vaccinerende organisatie).
- Het incident wordt gemeld bij CIMSBeheer.
- Indien het incident een prio 1 melding betreft, of wanneer gelijk het vermoeden bestaat dat het een calamiteit betreft, wordt deze door CIMSBeheer gemeld aan 5.1.2e

1. Analyse: is sprake van een calamiteit of niet?

- Wanneer het vermoeden bestaat dat het incident een calamiteit is, voert CIMSBeheer een nadere analyse uit.
- Op basis van de uitkomst van de analyse wordt bepaald of sprake is van een ketencalamiteit: als hiervan sprake is, wordt direct de ketencalamiteitenprocedure gestart.

2. Opstarten calamiteitenprocedure

- Het 5.1.2e meldt een (mogelijke) ketencalamiteit bij het 5.1.2e
- Het 5.1.2e en de 5.1.2e nemen contact op met de 5.1.2e om te bepalen of het keten-CMT moet worden geactiveerd. De 5.1.2e activeert het CMT.
- De 5.1.2e zorgt voor het opstarten van het keten-CMT.
- De 5.1.2e bepaalt wie deel moeten uitmaken van het keten-CMT, welke ketenpartners en personen/ partijen verder moeten worden betrokken, welke ketenpartners en andere partijen worden geïnformeerd, welke aanpak (intern calamiteitenplan) en welk communicatieplan worden gevolgd.

- Het keten-CMT doet verder onderzoek naar de mogelijke impact, risico's en oplossing(en).
- Het keten-CMT bepaalt of daadwerkelijk sprake is van een (keten)calamiteit.
- Indien nodig worden Operationele Teams samengesteld en opgestart.
- Het keten-CMT zorgt ervoor dat betrokken partijen en personen worden geïnformeerd, indien gewenst/ noodzakelijk.
- De afdeling Informatiebeveiliging/CHIO/privacy officers van het RIVM zorgt ervoor, indien nodig, dat contact wordt opgenomen met de Autoriteit Persoonsgegevens (AP)[5].

Beoordeling datalek
Om te beoordelen of een datalek aan de AP moet worden gemeld, moeten alle van de volgende drie vragen bevestigend worden beantwoord:

- Is er sprake van een inbreuk op de beveiligingsmaatregelen (een datalek)?
- Zijn de verwerkte persoonsgegevens daardoor blootgesteld aan verlies of onrechtmatige verwerking?
- Heeft deze blootstelling geleid tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of de privacy van de betrokkenen.

Als er geen sprake is van verwerking van persoonsgegevens, dan is de meldplicht datalekken niet van toepassing.

Voorbeeldsituaties:

- Verlies persoonsgegevens.
- Versturen van informatie die niet voor de ander bedoeld is (zoals verkeerd bezorgen uitnodiging vaccinatie).
- Verkeerde batchnummers zijn geregistreerd bij een groep patiënten.
- Patiënten die geen toestemming hebben verleend, maar toch zijn geregistreerd in de persoonlijke database in CIMS.
- Verkeerde koppeling BSN en persoonsgegevens, waardoor verkeerde gegevens worden geregistreerd en uitgewisseld.
- Illegale handel in persoonsgegevens.
- Ransomware op systemen met persoonsgegevens.
- Opmerken van onbevoegde toegang tot persoonsgegevens.
- Collega's die wachtwoorden kwijt raken van systemen met persoonsgegevens
- Een kwijtgeraakte USB-stick.
- Een gestolen laptop.
- Een inbraak door een hacker.
- Verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden.
- Een malware-besmetting.

[5] De meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek constateren. Soms moeten zij het datalek ook melden aan de betrokkenen personen (de mensen van wie de persoonsgegevens zijn gelekt). Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#:~:text=De%20meldplicht%20datalekken%20houdt%20in,zij%20een%20ernstig%20datalek%20hebben

- Een calamiteit zoals een brand in een datacentrum.

3. Afhandeling van de calamiteit

- Afhankelijk van de oorzaak, zorgt de afdeling/ het team dat hiertoe in staat is ervoor dat de calamiteit wordt verholpen. Indien nodig wordt dit in samenwerking tussen ketenpartners uitgevoerd, eventueel via de ketencalamiteitenprocedure.

4. Afronden calamiteitenprocedure en evaluatie

- Het CMT bepaalt of een calamiteit is verholpen en hoe de procedure wordt afgesloten.
- Het CCT (of 5.1.2e informeert, waar nodig, betrokken partijen en/of personen, met onderscheid in:
  - interne communicatie;
  - externe communicatie[6]:
    - welke boodschap naar het publiek?
    - welke boodschap naar de zorgaanbieders?
    - welke boodschap naar de leveranciers?
- Het CMT evalueert met alle betrokken partijen het doorlopen proces en de afhandeling en stelt vast welke (structurele) verbeteracties nodig zijn om een soortgelijke calamiteit in de toekomst zo goed mogelijk te voorkomen. Aan de hand hiervan wordt een plan van aanpak vastgesteld en gemonitord. De 5.1.2e 5.1.2e is ervoor verantwoordelijk dat dit daadwerkelijk plaatsvindt.
- Waar nodig vindt nazorg plaats.
- Het CMT evalueert het doorlopen proces en de afhandeling aan de hand van:
  - zijn er verbeterpunten aan de calamiteitenprocedure nodig (proces)?
  - zijn er verbeterpunten aan de gekozen oplossing/maatregelen (inhoud/kwaliteit)?

[6] De afspraak is dat leveranciers met hun gebruikers/zorgverleners communiceren. Over individuele gevallen kan direct met de zorgaanbieder/zorgverlener gecommuniceerd worden zolang er maar geen actie van de leverancier nodig is.

Bijlage 1 Begrippen

Begrip	Omschrijving
AP	Autoriteit Persoonsgegevens
Beschik-/ bereik-baarheidstijden	De werktijden van het team CIMSBeheer van het RIVM: tijdens deze uren zijn de medewerkers van CIMSBeheer werkzaam en bereikbaar.
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	Corona 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.
Ketenpartner	Alle partijen die betrokken zijn bij de registratie en het beheer van vaccinatiedata t.b.v. Covid-19.
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.
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
Wijzigingsverzoek	Een verzoek om een wijziging in de koppeling die het dataverkeer mogelijk maakt.

Bijlage 2 Contactpersonen en -gegevens voor het Keten-CMT

RIVM

Functie	Naam	Organisatie -onderdeel	Telefoon	e-mail
5.1.2e	CIMS Beheer	RIVM/DVP/ CIMS Beheer	5.1.2e Op ma t/m vr: 8.00 - 18.00 uur 5.1.2e Op ma-vr: 7.00 - 8.00 uur 18.00 – 21.00 uur Op za: 8.00 - 18.00 uur	5.1.2e
	5.1.2e 5.1.2e	RIVM/DVP/ BIS	5.1.2e	
	5.1.2e 5.1.2e	RIVM/DVP	5.1.2e 5.1.2e	

VZVZ (ketenregisseur huisartsen en zorginstellingen)

Functie	Naam	Organisatie	Telefoon	e-mail
5.1.2e	5.1.2e 5.1.2e	VZVZ Servicecentrum	**telefoon zakelijk:** 5.1.2e	**e-mail zakelijk:** 5.1.2e @vzvz.nl
	5.1.2e 5.1.2e	VZVZ Servicecentrum	**telefoon zakelijk:** 5.1.2e	**e-mail zakelijk:** 5.1.2e @vzvz.nl
	5.1.2e	VZVZ Servicecentrum	**telefoon zakelijk:** 5.1.2e	**e-mail zakelijk:** 5.1.2e @vzvz.nl

Het contact met **huisartsen** en **zorginstellingen** verloopt via of in overleg met VZVZ en/of de ICT-leveranciers van de huisartsen. Bij VZVZ zijn de contactgegevens van de huisartsen, zorginstellingen en de ICT-leveranciers bekend.

GGD GHOR (GGD's)

5.1.2e, 5.1.2e @ggdghor.nl, en 5.1.2e 5.1.2e @ggdghor.nl.

ROAZ/ ziekenhuizen
Via 5.1.2e (RIVM), 5.1.2e@rivm.nl

Ministerie van VWS (inzake BRBA)
5.1.2e 5.1.2e

ZKVI
Via 5.1.2e (RIVM), 5.1.2e@rivm.nl

BES/CAS
Via 5.1.2e (RIVM), 5.1.2e@rivm.nl

Overige contactgegevens

NCSC **Nationaal Cyber Security Centrum**	e-mail (7/24): 5.1.2e@ncsc.nl telefoon: 5.1.2e (kantoortijden)
Z-CERT **Computer Emergency Response Team voor de Zorg**	e-mail: 5.1.2e@z-cert.nl