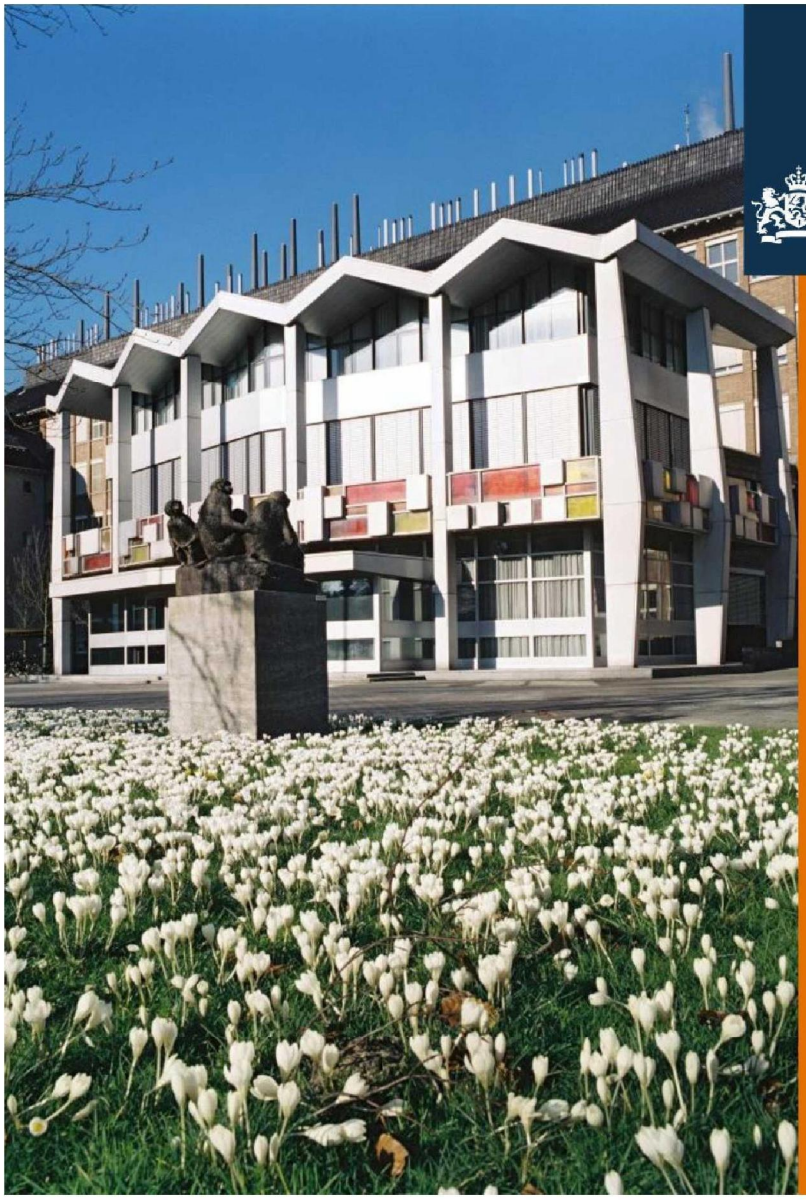
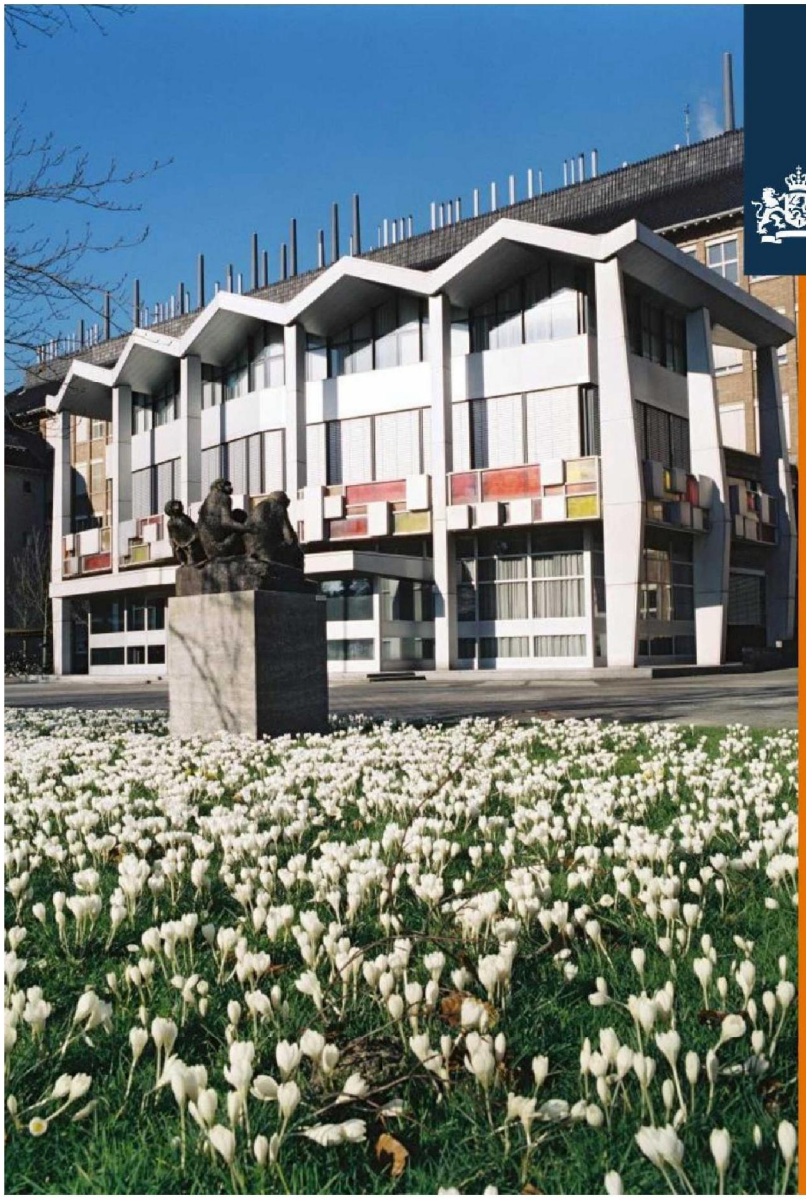


Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

RIVM
Systeem voor centrale verwerking Covid vaccinatie gegevens



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

Inhoud

1. Inleiding
2. Extra onderzoek nodig
3. Bevindingen uit de scans
4. Conclusies en acties voor vervolg
5. Scenario's voor centrale verwerking na 7 januari
6. Risico's (1,2,3)
7. Communicatie

Inleiding

- Afgelopen maanden/weken is hard gewerkt aan het op orde brengen van het systeem voor verwerking van Covid vaccinatie gegevens inclusief persoonsgegevens.
- Basis is een bestaand systeem dat voor andere vaccinatieprogramma's gebruikt wordt.
- Er zijn uitgebreide en extra risicoanalyses op IB en Privacy gedaan, t.b.v. de verwerking van persoonsgegevens.
- Veel bevindingen zijn inmiddels opgelost; nog een aantal over.
- In samenwerking met:

  5.1.2e : aanvulling risicolijst.

  NCSC: Check op de mitigerende maatregelen.

  ADR: Check en pentest sFTP omgeving.

  AIVD: advisering over digitale dreigingsniveau RIVM

Extra onderzoek nodig

- Er zijn recent twee extra scans uitgevoerd door resp. Secura en Noordbeek vanwege evident belang beschermen persoonsgegevens van in potentie 17 M Nederlanders, en aanvullend omdat:
  - RIVM al langer onder 'digitaal vuur' ligt, met vanwege de huidige situatie extra risico's.
  - Uit dreigingscans van o.a. de AIVD blijkt dat er recent ook meer statelijke actoren een bijzonder interesse hebben in het RIVM.
  - Recente (buitenlandse) aanvallen op RIVM.nl en de hack bij de EMA.

Bevindingen uit de scans

- Rapport Noordbeek *"Tijdens de scan zijn geen materiele afwijkingen geconstateerd die een inproductiename van CIMS release 1 in de weg staan"*
- Rapport Secura *"De infrastructuur is nog niet klaar voor inproductiename ondanks dat er al veel verbeterd is".*

Conclusies en acties voor vervolg

- Op 8-1 is er centrale gegevensverwerking bij RIVM, in ieder geval op geaggregeerd niveau en hoogstwaarschijnlijk inclusief persoonsgegevens.
- Livegang per 30 december 2020 met persoonsgegevens niet mogelijk, want nog aantal hoge risico's die gemitigeerd moeten worden. Belangrijkste bottle-neck is realisatie van een offsite backup.
- RIVM denkt met aan zekerheid grenzende waarschijnlijkheid dat al deze hoge risico's inclusief bottle-neck te mitigeren zijn per uiterlijk 7 januari 2021.
- Go-NoGo besluit uiterlijk 7 januari 2021.
- dPia wordt aangepast op laatste maatregelen en aangeboden aan de FG (en AP?)
- Extra externe check op realisatie resterende mitigerende maatregelen.

Scenario's bij uitstel na 7 januari

Live gang per 8-1-2021 met verwerking persoonsgegevens zeer waarschijnlijk, maar nu nog geen absolute zekerheid. Wat als niet alle hoog risico's voldoende gemitigeerd kunnen worden voor 8-1?

- Scenario 1: we hebben na 8-1 nog maximaal 3 weken nodig voor wegnemen hoog risico's:
  - *Plan B RIVM wordt actief: verwerking gegevens op persoonsniveau bij de GGD. Centrale verwerking van geaggregeerde gegevens bij RIVM. Achteraf met terugwerkende kracht gegevens inclusief persoonsgegevens naar het RIVM voor centrale verwerking op persoonsgegevensniveau.*
- Scenario 2: hoog risico's zijn niet op korte termijn mitigeerbaar:
  - *Plan B RIVM wordt voortgezet. Oorspronkelijke doelen van de centrale registratie worden niet bereikt.*
  - *Plan C VWS. Nieuw systeem inzetten voor verwerking vaccinatiegegevens met persoonsgegevens.*

Risico's (1)

- Ontbreken offsite backup:

  Bij een gijzeling van de data (bijvoorbeeld door ransomware) moeten we beschikken over een backup die buiten het eigen rekencentrum wordt opgeslagen.

  Maatregel is dat deze offsite backup wordt georganiseerd met een externe partij.

- Niet alle patches van onderliggende software staan op de laatste versie.

  Zonder de laatste updates kan je kwetsbaar zijn voor beveiligingslekken.

  Maatregel: alsnog de benodigde patches uitvoeren.

Risico's (2)

- Handelingen van gebruikers en beheerders worden onvoldoende volledig vastgelegd.

  Om de sporen te kunnen volgen van afwijkende handelingen moeten alle handelingen van betrokkenen vastgelegd worden.

  Maatregel is het volledig activeren van de logging mogelijkheden en het inrichten van een zgn SOC om al het afwijkende gedrag te monitoren en signaleren.

Risico's (3)

- Meer adminstrators dan noodzakelijke hebben nog ruime toegangsrechten.

  Maatregel is een opschoning van de benodigde rechten en het verscherpen van de procedures voor het toekennen van deze rechten.

Voor alle hoge risico's zijn inmiddels de afgesproken maatregelen doorgevoerd of wordt dat in de komende dagen nog gedaan. Ook na live gang zullen we door middel van (externe) scans volgen of er aanleiding ontstaat om verdere maatregelen te nemen.

Tevens zijn er afspraken om NCSC ook in de toekomst te betrekken bij eventueel aanvullende maatregelen.

Communicatie

- Informeren stakeholders (VWS en RIVM).
- Woordvoeringslijn (reactief) en Q&A voorbereiden (VWS).

- Kernboodschap. Voor centrale verwerking van naar persoon herleidbare gegevens is in de actualiteit bescherming van persoonsgegevens van 17 miljoen Nederlanders van evident en vanzelfsprekend groot belang. Deze naar de persoon herleidbare gegevens zijn noodzakelijk om alle doelen van de centrale gegevens verwerking bij het RIVM te kunnen realiseren. Extra aandacht voor en inzet op informatie beveiliging en privacy is daarom nu noodzakelijk.