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

Aan: 5.1.2e 5.1.2e

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

T 5.1.2e
info@rivm.nl

Datum
14 februari 2021

Ons kenmerk

Uw kenmerk

Behandeld door
5.1.2e

5.1.2e @rivm.nl

Kopie aan
5.1.2e 5.1.2e, 5.1.2e 5.1.2e,
5.1.2e 5.1.2e 5.1.2e

Bijlage(n)
Risicoacceptatieformulier
xxxxxx

memo

Risicoanalyse informatiebeveiliging CIMS 2.0

1. Inleiding

Begin januari 2021 is CIMS versie 1.0 live gegaan. Er wordt door middel van het aansluiten van diverse bronsystemen (HIS leveranciers (huisartsen), EVS leveranciers (instellingen), BRBA (VWS) en GGD GOHR) geregistreerd wie gevaccineerd is en met welk vaccin. Deze bronsystemen leveren op dagelijkse basis data.

Vanaf begin januari is vanuit het project gewerkt aan overdracht aan beheer (regiomedewerkers) en de bouw van release 2.0.

Functionaliteit CIMS 2.0
De belangrijkste functionaliteit in CIMS 2.0 heeft betrekking op het selecteren en oproepen van doelgroepen op leeftijd.
Bij selecteren en oproepen kan een selecte groep medewerkers van RIVM middels de applicatie een groep selecteren en vastleggen voor oproep voor vaccinatie. Vervolgens kan de betreffende medewerker het door CIMS gegenereerde bestand met behulp van Filesender naar de drukker sturen.

Naast deze nieuwe functionaliteit worden ook twee nieuwe persoonsregisters toegevoegd: COA (Centraal Orgaan opvang Asielzoekers) en PROBAS (Protocollaire Basisadministratie).

Dit document beschrijft de resultaten van de risicoanalyse op het vlak van informatiebeveiliging voor deze CIMS 2.0 release.

2. Scope

Voor de informatiebeveiligingsanalyse van CIMS 2.0 is de basisinfrastructuur van de applicatie CIMS 1.0 als een gegeven beschouwd, aangezien hier al een zeer uitgebreide risicoanalyse op is uitgevoerd en afgerond.
Voor CIMS 2.0 zijn de volgende twee aanvullingen op CIMS 1.0 beoordeeld:

1. Het laden van de COA- en PROBAS-persoonsregisters;
2. De nieuwe functionaliteit 'Selecteren en oproepen op leeftijdsgroep'.

3. Samenvatting

Voor CIMS 2.0 zijn er op het vlak van informatiebeveiliging **geen restrisico's** waar aanvullende mitigerende maatregelen voor getroffen moeten worden.

Voor het laden van de COA- en PROBAS-persoonsregisters wordt gebruik gemaakt van functionaliteit die in de risicoanalyse van CIMS 1.0 al is beoordeeld en geaccepteerd; importeren van de gegevens in de CIMS-database zal lopen via de SFTP-server van CIMS.

Voor de functionaliteit 'selecteren en oproepen' is het deelproces beoordeeld vanaf 'opdracht tot selecteren' tot en met verwerking bij de drukker. Voor dit proces zijn diverse aanvullende maatregelen voorgesteld om de informatiebeveiliging naar een hoger niveau te tillen. Alle gevraagde maatregelen zijn meegenomen in het definitieve proces.

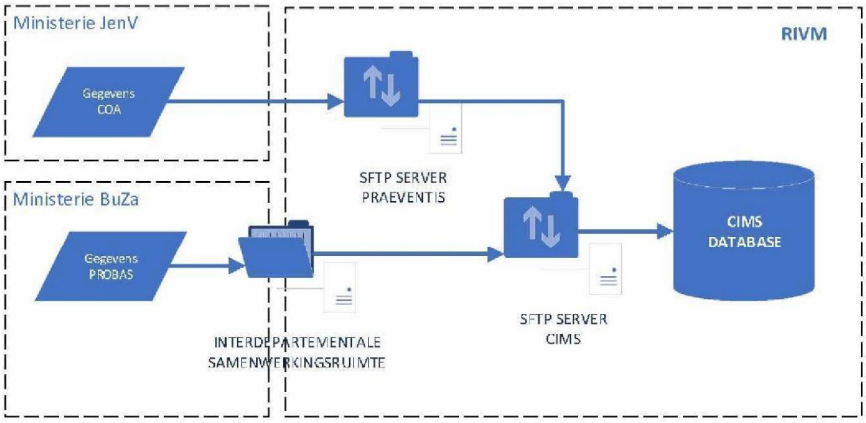
ADVIES: Geen bezwaren vanuit het perspectief van informatiebeveiliging voor het in productie nemen van CIMS 2.0.

4. IB Analyse CIMS 2.0

Voor CIMS 2.0 zullen voor de nieuwe functionaliteit en toevoeging van persoonsgegevens ook separate DPIA's worden uitgevoerd door de privacy coördinator. Om de verwerkingen in CIMS 2.0 te kunnen relateren aan de fases die onderkend zijn in de oorspronkelijke DPIA van CIMS 1.0 kan onderstaande tabel gebruikt worden. Dit document kan als input gebruikt worden voor de uit te voeren DPIA's.

Onderdeel CIMS 2.0	Relevante fase voor DPIA
Laden COA en PROBAS	fase i - het inladen van gegevens cliëntregister
Selecteren en oproepen	fase ii - het selecteren en oproepen van personen uit een doelgroep

4.1 Laden van COA- en PROBAS-gegevens



COA-bestand
Het persoonsregister van COA werd al ontvangen voor het vastleggen van vaccinaties in het rijksvaccinatieprogramma (RVP). Dit bestand wordt aangeboden op de SFTP-server van Praeventis en vervolgens automatisch verwerkt in de Praeventis database.

Voor import in de CIMS-database zal het aangeboden bestand via een script ook worden geplaatst op de SFTP-server van CIMS, waarna het via het reguliere importproces zal worden verwerkt in de CIMS-database. Het bestand hoeft op deze manier maar één keer aangeboden te worden door COA en zal verder intern verwerkt worden op de infrastructuur van RIVM.

PROBAS-bestand
Voor uitwisseling van het PROBAS-bestand zijn twee openstaande vragen behandeld en opgelost:

1. Wat is de rubricering van de gegevens in het PROBAS-bestand?
2. Hoe kan het bestand op een veilige manier worden aangeleverd die werkt voor beide partijen?

Rubricering
In overleg met het Ministerie van Buitenlandse Zaken (BuZa) is vastgesteld dat het PROBAS-bestand geen gerubriceerde informatie bevat; de VIR-BI is hier niet op van toepassing. De classificatie van het bestand volgens BIO kunnen we beschouwen als BBN3. Deze informatie mag geïmporteerd worden in de CIMS-database.

Aanlevering
BuZa heeft niet de mogelijkheid om het PROBAS-bestand zelf aan te bieden op de SFTP-server van CIMS. Als tijdelijke oplossing zal het bestand worden versleuteld en geplaatst in een beveiligde folder op de 'interdepartementale samenwerkingsruimte'. Deze ruimte is beschikbaar gesteld om informatie op een veilige manier te kunnen delen tussen verschillende departementen en overheidsinstellingen. Deze omgeving is geschikt om

informatie te delen tot en met de rubricering 'departementaal vertrouwelijk' (TBB 4, VIR-BI). Het aangeleverde bestand zal vervolgens door een medewerker van RIVM worden ontsleuteld en volgens de reguliere procedure via de SFTP-server worden geïmporteerd in de CIMS-database. Er zullen 3 personen bij BuZa en 3 personen van RIVM toegang krijgen tot het (versleutelde) bestand.

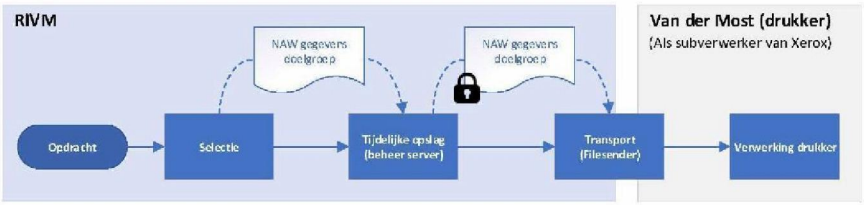
In een volgend traject zal worden onderzocht of er een ODBC-koppeling vanuit BuZa met CIMS kan worden gerealiseerd (vergelijkbaar met de koppeling met GGD GHOR), zodat de data geautomatiseerd opgehaald kan worden door het RIVM. Planning hiervan is nog niet bekend.

Contactpersoon bij het Ministerie van Buitenlandse Zaken:

5.1.2e

Ministerie van Buitenlandse Zaken
Directie Protocol en Gastlandzaken

4.2 Selecteren en oproepen



Het doel van dit proces is om via CIMS een selectie te maken van te vaccineren personen op basis van leeftijd en deze personen vervolgens uit te nodigen voor vaccinatie.

Voor dit proces is een versnelde analyse uitgevoerd van de stappen in het proces en de informatiebeveiligingsrichtlijnen die bij deze stappen genomen moeten worden. Dit was een analyse voor de tijdelijke oplossing (handmatig selecteren en oproepen), waarvoor ook een risicoacceptatie-traject is doorlopen.

Voor de permanente oplossing (in CIMS 2.0) zijn de beoordeelde stappen vergelijkbaar, maar de details van de uitvoering zijn verschillend. Deze worden hieronder kort toegelicht.

De opdracht tot selectie zal worden geregistreerd in Topdesk, waarbij het akkoord wordt vastgelegd en de opdracht wordt doorgezet naar de RIVM-medewerker die de selectie moet uitvoeren in CIMS (waarvoor in CIMS 2.0 de juiste schermen beschikbaar worden gesteld).

Transport via Filesender blijft ook in de definitieve versie ongewijzigd. De ontvangende partij is echter niet Xerox, maar de drukker Van der Most (de Nederlandse subverwerker van Xerox). Met opdrachtnemer Xerox is afgesproken dat de volgende richtlijnen met betrekking tot informatiebeveiliging (en privacy) worden nageleefd:

1. alleen bevoegd personeel heeft toegang tot de te verwerken gegevens;
2. de te verwerken gegevens worden alleen via een versleuteld communicatiekanaal aangeleverd/opgehaald;
3. het aangeleverde versleutelde bestand wordt pas ontsleuteld bij start van de daadwerkelijke verwerking;
4. er wordt vóór verwerking vastgesteld of de aangeleverde informatie niet onrechtmatig is aangepast door controleren van de hash-waarde(n) die worden meegeleverd;
5. het resultaat van de controle in punt 4 wordt vastgelegd en kan op verzoek worden aangeleverd bij Opdrachtgever;
6. het versleutelde bestand mag nog maximaal twee weken na verzending van de oproepen worden bewaard en worden gebruikt voor opsporing van eventuele fouten;
7. de dataset dient na maximaal twee weken na verzending van de oproepen te worden vernietigd;
8. alle verwerkingen (inclusief de vernietiging) worden vastgelegd in een logbestand (conform BIO & AVG-richtlijnen);
9. er wordt zeker gesteld dat de te verwerken gegevens geen onderdeel worden van een dataset die zich buiten de Europese Economische Ruimte (EER) zou kunnen bevinden (geen doorgifte hoofdstuk 5 AVG). Deze maatregel heeft ook betrekking op de dataset in een back-up bestand of tijdens fail-over situatie.

Naleving van deze richtlijnen is door Xerox schriftelijk bevestigd.

De nog openstaande IB risico's waarvoor een risicoacceptatie actief is kunnen worden afgesloten.

5. Conclusie

Vanuit het perspectief van informatiebeveiliging is er geen bezwaar tegen het in productie nemen van de in dit document beschreven CIMS 2.0 functionaliteit. Er zijn ook geen aanvullende maatregelen nodig.

De IB risico's voor het proces 'selecteren en oproepen' waarvoor nog een risicoacceptatie geldt zijn opgelost en kunnen worden afgesloten.

LET OP: dit memo betreft alleen de analyse van de risico's op het gebied van informatiebeveiliging. Voor de analyse van eventuele privacy-risico's zullen separate DPIA's uitgevoerd en beoordeeld worden.