Besproken met: 5.1.2e 5.1.2e (RIVM), 5.1.2e 5.1.2e 5.1.2e (RIVM), 5.1.2e 5.1.2e 5.1.2e (VWS)

Datum: 28-1-2021

Nav de issues bij GGD heeft VWS aan RIVM gevraagd om voor zichzelf aan te geven in hoeverre datgene bij GGD is misgegaan ook bij CIMS zou kunnen misgaan. Na vragen van VWS heeft RIVM antwoord gegeven (DVP 216 - Centraal vaccinatieregister CIMS: het voorkomen van illegale handel in data, d.d. 27 januari 2021), waarna 5.1.2e in een plenaire sessie nog wat verduidelijkende vragen / antwoorden hebben doorgenomen.

Allereerst de conclusie – het RIVM heeft de verantwoordelijkheid voor een grote hoeveelheid bijzondere persoonsgegevens van buitengewoon veel Nederlanders. De gevolgen van eventuele gebreken in de bescherming zouden groot zijn, net als bij de GGD.

De kans dat een inbreuk zoals bij de GGD zich ook bij het RIVM voordoet is echter veel geringer. Voornamelijk doordat veel minder mensen bij de gegevens kunnen en dit vrijwel altijd vanuit een gecontroleerde omgeving gebeurt. De komende periode (tot einde Q1) worden de bestaande detectie- en monitoringcapaciteiten verbeterd om eventuele inbreuken sneller en beter te kunnen detecteren.

Nadere toelichting op DVP 216 - Centraal vaccinatieregister CIMS: het voorkomen van illegale handel in data, d.d. 27 januari 2021

In CIMS wordt een selecte set aan BRP gegevens geladen van alle Nederlanders. Er is op verschillende manieren een analyse gedaan om te kijken of een selectievere keuze kan worden gemaakt. Het reduceren van deze set zou als voordeel hebben dat áls er sprake zou zijn van onterechte toegang, in ieder geval geen gegevens worden prijsgegeven waar RIVM eigenlijk niets mee deed. RIVM geeft aan dat zij op dit moment geen verdere mogelijkheden ziet om te werken met selecties van de gegevensset die zij uit BRP ontvangt.

Bij RIVM hebben veel minder mensen toegang tot de persoonsgegevens dan bij GGD. Zo'n 85 medewerkers (voornamelijk RIVM medewerkers) oplopend tot 135 hebben toegang. Dit zijn andere hoeveelheden dan bij GGD (duizenden). De meeste medewerkers met toegang zijn in dienst van RIVM zelf, een deel wordt via strenge selectie geworven via uitzendbureau's. Medewerkers van call center (Infopunt) hebben géén toegang tot persoonsgegevens. Zij beantwoorden primair vragen van zorgprofessionals over vaccinaties. Zij beantwoorden ook wel vragen van burgers, maar deze hebben nooit betrekking op individuele vaccinaties. Deze zullen gaan verlopen via een (nog te realiseren) cliëntportaal. Burger vragen rondom AVG rechten (inzage, correctie, verwijdering) lopen niet via het call center.

Externe beheerders (van Ordina) kunnen zelfstandig inloggen, als zij hiertoe een trigger krijgen vanuit de systemen. Zij loggen dan op een veilige manier in, wat op zichzelf weer leidt tot een logging en signalering bij RIVM beheerders die de dag erna de legitimiteit ervan kunnen vaststellen.

Binnen CIMS wordt uitgebreid gelogd op persoonsniveau. Gelogd wordt: raadplegen, muteren en verwijderen. De logging is ingericht voor alle gebruikersgroepen. De SOC/SIEM is in gebruik en wordt versneld uitgebreid met use cases die een indicatie zijn voor misbruik. RIVM werkt hierin samen met NCSC.

Het nieuws van de issues bij GGD zijn ook bij RIVM hard aangekomen. Dit wordt ook vertaald naar extra maatregelen (onboarding, awareness) en versnelling in de roadmap activiteiten. De meeste van de maatregelen die in de roadmap staan, zullen dan ook in Q1 actief zijn.

We hebben nog gesproken over de generieke baseline die RIVM hanteert. Deze ligt op BBN3 niveau, waarbij ook de standaarden NEN 7510, NEN 7512 en NEN 7513 leidend zijn.

Ook is nog kort gesproken over de dataset die wordt gebruikt in de acceptatieomgeving. Deze heeft niets te maken met de GGD case, maar werd door RIVM wel meegenomen in de beantwoording. Deze dataset is speciaal voor de acceptatieomgeving ontwikkeld, op basis van een dataset uit een andere RIVM voorziening. Deze dataset is door een combinatie van verwijderen en husselen van gegevens niet meer herleidbaar tot feitelijke gegevens, maar nog wel bruikbaar als dataset. De exacte methode waarop dit is gedaan is in ons gesprek niet verder onderzocht.