GGD Amsterdam

iMPeX advies over deelname

Verantwoordelijk stuurgroep-lid: 5.1,2,e

Naam opsteller: 5.1,2,e

5.1,2,e 5.1,2,e en 5.1,2,e

Stuurgroep 4 augustus 2022

Stuurgroep wordt gevraagd:

Gevraagde beslissing:

1. Deelname GGD Amsterdam aan het registratiesysteem iMPeX voor de PrEP monkeypox vaccinaties, op termijn is het wenselijk de PEP vaccinaties daaraan toe te voegen.
2. In ieder geval een aanvang te gaan maken met het invoeren van het inmiddels grote aantal dossiers.
3. Begin volgende week (32) het systeem ook in gebruik te nemen voor de dagelijkse invoer van gevaccineerden op de rai.
4. Het systeem eind week 32 te hebben ingericht voor planning van afspraken door een landelijk belteam.
5. Daarbij belangrijke voorwaarden te stellen en veiligheidsmaatregelen te treffen rondom IV, privacy en security aan GGD GHOR NL / LCCB.

Projectteam mpx vaccinaties stand van zaken

- Bij de GGD GHOR/LCCB is door alle GGD'en aangedrongen op een landelijk registratie- en afsprakensysteem voor mpx vaccinaties.
  GGD Amsterdam: voorkeur uitgesproken voor een landelijk belteam dat mensen kunnen bellen om een afspraak te maken.

- De druk om snel te starten met vaccineren was groot. Haaglanden en Amsterdam zijn op nadrukkelijk verzoek op 25 juli jl. gestart, met kleine aantallen. Bij gebrek aan een systeem worden noodformulieren gebruikt.
- Na anderhalve week zijn er bijna 1.000 prikken gezet.

- We zijn gestart met de doelgroep prep-gebruikers via CSG.
  → CSG nodigt cliënten uit op alfabet, verstuurt via de mail een brief waarin een bepaald tijdsslot staat vermeld.
  Mensen kunnen mailen naar *mpxvaccinatie@ggd.amsterdam.nl* om aan te geven dat ze een ander tijdsslot willen of helemaal niet in aanmerking willen komen voor een prik.
- I.v.m. de korte termijn en het feit dat veel mensen op vakantie zijn hebben we met de huidige werkwijze te maken met een hoog no show percentage en blijkt het beheer van de mailbox door de vele verzoeken tot herplannen erg arbeidsintensief en foutgevoelig.
- Het niet digitaal kunnen inplannen van afspraken (we sturen groter aantal uitnodigingen per tijdsblok en houden bij wie wel en niet komt) leidt tot minder doelmatig gebruik van de vaccinatiecapaciteit en tot een grote belasting van het emailadres voor het herplannen van cliënten. Daarnaast krijgen we ook klachten van cliënten hierover.

- Doelgroep 1b en 2:
  Voor de patiënten die prep krijgen via de huisarts en de personen die bekend zijn bij de hiv behandelcentra geldt dat de uitnodiging via de behandelaar moet worden verzonden, aangezien de GGD niet over de patiëntgegevens beschikt.
  → Bedacht is dat deze personen een uitnodiging krijgen met een unieke code waarmee zij een afspraak kunnen maken. Om dit in goede banen te leiden is een digitaal afsprakensysteem en een belteam essentieel.

- We hebben te maken met enorme grote druk om het tempo van de vaccinaties op te voeren. Het tempo opvoeren betekent een enorme versterking van de nadelen van het werken op papier en het niet digitaal kunnen inplannen van afspraken (zie punten hierboven).

Stand van zaken iMPeX volgens LCCB

Implementatie:

- Aanvullende maatregelen naar vergelijkbaar met CoronIT -> SOC / CISO akkoord
- Vervolg:
  - Inregelen monitoring
  - API t.b.v. monitoring 2,5 week
  - DPIA en verwerkersovereenkomsten met hoogste prio opgepakt.

Proces en inrichting (wordt geregeld):

- Regioscheiding
- Uitnodigingsmail
- Werkinstructies

iMPeX en Privacy:

- Verwerkersovereenkomst SOS International: Akkoord
- Privacy verklaringen: klaar, worden gedeeld
- RIVM datauitwisseling: akkoord op dataniveau, GGD'en moeten hier zelf nog over besluiten
- Verwerkersovereenkomst Topicus: valt onder huidige overeenkomst, aanvullende wordt opgesteld
- Verwerkersovereenkomst GGD/LCCB: Loopt

Privacy en Security (1/3)

Privacy

- De AVG vereist dat GGD Amsterdam rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.
- In de huidige beleidsregels 'Beveiliging van persoonsgegevens' van de Autoriteit Persoonsgegevens (AP) staat dat verantwoordelijken de beveiligingsstandaarden moeten volgen. Als voorbeeld van zo'n standaard noemt de AP de NEN 7510.

Security normen

- In de zorg komt het er op neer dat men zich houdt aan de beveiligingsnorm NEN7510. De NEN 7510 wordt aangevuld o.a. NEN 7512, NEN 7513, NEN 7521, etc. En dat is zeker het geval bij de verwerking van persoonsgegevens van deze specifieke populatie.

Ontbrekende essentiële zaken in relatie tot de AVG (Privacy) en Security

- Privacy
  - Data Protection Impact Assessement;
  - Er is geen dienstverleningsovereenkomst waarin de rollen en verantwoordelijkheden tussen partijen zijn vastgelegd;
  - Verwerkersovereenkomst;
  - Onvoldoende inzicht in de technische en organisatorische maatregelen.
- Security
  - Een audit en/of analyse of iMpeX die voldoet aan de beveiligingsnorm NEN 7510;
    - Een van de onderdelen is logging en monitoring, dit is nog niet geheel ingeregeld – ***zowel logging in CoronIT als iMPEX is niet helemaal compleet!***
    - De rest van de andere onderdelen is voor ons, GGD Amsterdam, onbekend
  - Er is nog geen pentest uitgevoerd. Bij een pentest wordt er onderzocht naar kwetsbaarheden in het (informatie)systeem;
  - Het dreigingsbeeld is nog niet in kaart gebracht. N.a.v. het dreigingsbeeld wordt er (aanvullende) maatregelen getroffen;
  - Controle op de Verklaring van Toepasselijkheid van de NEN 7510 certificering van de leverancier is nog niet gecontroleerd.

Privacy en Security (2/3)

DPIA & Verwerkersovereenkomst

- In 2019 heeft de Autoriteit Persoonsgegevens een lijst van 17 verwerkingen gepubliceerd waarvoor het uitvoeren van een **DPIA verplicht** is. Één van de 17 verwerkingen is het grootschalig verwerken van gegevens over gezondheid. De DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen.

- De verwerkingsverantwoordelijke (GGD) en de verwerker (GGD GHOR) moeten samen een **Verwerkersovereenkomst** afsluiten. Doen zij dat niet? Dan zijn beide partijen in overtreding.

DPIA	Verwerkersovereenkomst (afspraken met GGD GHOR/LCCB)
Een DPIA geeft inzicht in de risico's die de verwerking oplevert voor de betrokkenen en de te nemen maatregelen om de risico's af te dekken. Het is aan de GGD om die maatregelen ook daadwerkelijk te treffen. Bij het beoordelen van restrisico's in de DPIA is er in elk geval aandacht voor de volgende punten: • Aangeven welke hoge privacyrisico's uit de DPIA niet volledig kunnen worden voorkomen. • Specifiek vermelden in welke situatie(s), of met betrekking tot welke onderdelen, er sprake is van een hoog restrisico. • Aangeven hoe waarschijnlijk het lijkt dat de omschreven situatie zich ondanks de maatregelen die zijn getroffen toch voordoet. • Omschrijven welke schade er dan ontstaat of kan ontstaan voor de personen van wie GGD de persoonsgegevens verwerkt.	- Algemene beschrijving (rollen en verantwoordelijkheden) - Instructies verwerking - Geheimhoudingsplicht - Beveiliging De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Bijvoorbeeld pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot gegevens bij incidenten, regelmatige beveiligingstesten. - Subverwerkers - Privacyrechten burgers - Gegevens verwijderen - Audits

Privacy en Security (3/3)

Opvolging van ontbrekende essentiële zaken in relatie tot de AVG (Privacy) en Security

- GGD GHOR Nederland, met name LCCB, heeft aangegeven de ontbrekende essentiële zaken op te pakken.
- Nog niet voor alle onderwerpen is er een deadline voor afgegeven; dit omdat GGD GHOR Nederland intern nog moeten bespreken en inplannen. Vervolggesprekken tussen GGD GHOR Nederland en GGD Amsterdam wordt nog ingepland.

Gegevensuitwisseling RIVM

- In het kader van de kwaliteit, effectiviteit en monitoring wil het RIVM gegevens ontvangen. Zij willen herleidbare persoonsgegevens ontvangen waar uitdrukkelijke toestemming voor wordt gevraagd. Hiervoor moet in het systeem een 'vinkje' kunnen worden gezet. Dit is nog niet geregeld.
- Daarnaast wil het RIVM gegevens ontvangen op anonieme basis. Hiervoor is een lijst opgesteld die goedgekeurd moet worden door de GGD en het anonimiseren van de gegevens (verwerking) zal plaatsvinden door GHOR.

Samenvatting Privacy en Security

- Onvoldoende waarborgen van de technische en organisatorische maatregelen (NEN 7510);
- Risico's op datalekken met als gevolg imagoschade voor de GGD;
- Door het ontbreken van een DPIA, verwerkersovereenkomst en controle van beveiligingsmaatregelen voldoen we niet aan de wet- en regelgeving.

IV algemeen

IV algemeen – aanvulling op de bevindingen van Privacy en Security

- Uitgangspunt is een landelijk systeem voor MPX vaccinatie dat veilig betrouwbaar en efficiënt is

  T.a.v. veilig en betrouwbaar: zie vorige sheets

  T.a.v. veilig, betrouwbaar en efficiënt: GGD Amsterdam heeft niet kunnen testen en heeft onvoldoende zicht op het landelijk testtraject

Advies Privacy, Security en IV

- **Op basis van de beschikbare informatie op dit moment adviseren wij een no-go**

  Andere, digitale alternatieven zijn nu slechts globaal verkend ; uitwerken en realiseren kosten globaal ook 2 tot 4 weken afhankelijk van het alternatief; belangrijkste informatiebeveiligingsmaatregelen (m.b.t. volledige logging) over 3 weken volgens landelijk planning.

Indien evengoed het besluit genomen wordt om nu live te gaan - gezien de andere gesignaleerde risico's - dan luidt het advies als volgt

- Voer gebruik van het systeem beperkt in (aantal gebruikers, taken);
- Breng de eventuele privacy en beveiligingsrisico's voor dit beperkt gebruik in kaart door team bestaande FB, PC, PO, ISO en beleidsmedewerker en zorg waar mogelijk voor mitigerende maatregelen. Hiervoor is tevens een IV Projectleider beschikbaar;
- Laat GGD GHOR/LCCB een duidelijke planning afgeven voor de realisatie van de privacy- en beveiligingsmaatregelen als ook de gegevensuitwisseling met RIVM;
- Toezicht op planning en werkzaamheden door het wekelijkse, landelijke FG en CISO overleg;
- De PO en ISO GGD (nemen deel aan de wekelijkse landelijke overleggen) rapporteren aan de projectleider vaccinatie (DPG) bij afwijkingen hierop;
- Mocht er een landelijk belteam worden ingezet, borg dat de lessons learned van het datalek begin februari 2021 geïntegreerd worden in de werkprocessen van het landelijk belteam;
- **Leg alle verbeterpunten vast in de verwerkersovereenkomst en stel de verwerker aansprakelijk voor omissies.**

Gezamenlijk advies projectteam mpx vaccinatie en privacy team

- **Vanuit de operatie is het van belang zo snel mogelijk te kunnen beschikken over een digitaal registratie- en afsprakensysteem**
- De huidige werkwijze op papier kent een groot aantal nadelen en is bovendien arbeidsintensief.
- De enorme druk om te versnellen versterkt de nadelen van het werken op papier; en het niet kunnen beschikken over een digitaal systeem staat een verantwoorde opschaling in de weg.
- Tegelijkertijd is van belang dat privacy en informatieveiligheid goed geborgd zijn. We moeten constateren dat aan een aantal voorwaarden nog niet is voldaan; tegelijkertijd zien we dat LCCB daar hard aan werkt. Het van belang de manco's te benoemen en duidelijke afspraken te maken over wanneer die zijn opgelost. Ook de kwestie aansprakelijkheid is een issue.

- Advies is om onder strikte voorwaarden akkoord te gaan met getrapte in gebruik name van het systeem.
  Drietrapsinvoering iMPeX in de operatie:
  1. Noodformulieren van afgelopen weken invoeren in het systeem
  2. Registratie van cliënten op locatie
  3. Afsprakensysteem starten met landelijk belteam

- Vanuit privacy en security oogpunt moeten er duidelijke afspraken gemaakt worden met GGD GHOR NL / LCCB.
  GGD Amsterdam voert iMPeX in met de volgende randvoorwaarden:
  - Oplossen van de volgende knelpunten binnen af te spreken termijn.
  - Wekelijkse rapportage over de voortgang.
  - Aan de voorkant duidelijkheid over wie verantwoordelijk is als lacunes niet of niet tijdig zijn opgelost.