Datum: 9-7-2020
Betreft: Brief van (10)(2e), (10)(2e), (10)(2e) en (10)(2e) (10)(2e)

Beste (10)(2e) en (10)(2e)

Dank voor het doorsturen van de brief van (10)(2e) (10)(2e) (10)(2e) en (10)(2e) jullie brief waarin zij zorgen uiten over de toegang tot de data in CoronIT. Door gezamenlijk kritisch te blijven kijken naar het proces, kunnen we zorgen dat data adequaat beschermd blijft en dat de bestrijding van COVID-19 goed blijft verlopen.

Voor CoronIT ligt de grondslag in de Algemene Verordening Gegevensbescherming en de Wet publieke gezondheid en zijn we gebonden aan de verplichtingen die in deze wetten uiteen wordt gezet. Dit geldt natuurlijk ook voor de toegang tot de gegevens.
Ten behoeve van een adequate inrichting hebben we onderzocht wat de werkwijze in de praktijk is en wie toegang zouden moeten hebben tot de gegevens. Daarvoor hebben we een autorisatiematrix opgesteld. GGD'en kunnen toegang vragen voor medewerkers, waarbij de GGD zelf afweegt welke rol de medewerker krijgt in CoronIT. GGD'en zijn daar zelf verantwoordelijk wie welke toegang krijgt tot CoronIT, omdat zij de afweging tot wie toegang moet krijgen en aanvraag van het toekennen van die rol voor een medewerker indienen bij GGD GHOR Nederland.

De personen die toegang hebben gekregen tot CoronIT, kunnen, als ze deze rol hebben gekregen, vervolgens inderdaad in heel Nederland op naam zoeken. Deze afweging is gemaakt door de aard van de virusbestrijding, namelijk het opzetten van een landelijk testsysteem waarin snelheid en efficiëntie centraal staan. Mensen kunnen zich overal laten testen, waardoor mensen op de testlocatie moeten kunnen worden gevonden. Daarnaast zal de GGD in de regio waar de betrokkene woont ook de gegevens in moeten zien voor bijvoorbeeld het BCO of om later te kunnen kijken wat eerdere resultaten van de test waren. Indien niet door heel Nederland kan worden gezocht, moet telkens een extra stap in het proces worden genomen om deze inzage wel te hebben, wat de efficiëntie en werkbaarheid van het proces vermindert. Om deze reden is de afweging gemaakt om het zoeken voor heel Nederland mogelijk te maken.

Tussen de GGD'en en GGD GHOR Nederland is een convenant opgesteld, waarin is opgenomen wat het doel van CoronIT is en welke gegevens mogen worden verwerkt. Daarin is bepaald welke persoonsgegevens mogen worden gebruikt en welke maatregelen moeten worden genomen om te zorgen dat de verwerking van persoonsgegevens op een veilige wijze gebeurt. Hierin wordt ook gesteld dat wordt gehandeld volgens de geldende normen, waar ook autorisaties een onderdeel van vormen.

Om te zorgen dat geen misbruik wordt gemaakt van deze toegang tot gegevens, zijn een aantal maatregelen genomen. Deze maatregelen zijn de volgende:

- Het aantal zoekresultaten is beperkt, zodat niet vrij door een lijst kan worden gezocht;
- Op toegang tot en gebruik van CoronIT wordt uitgebreid gelogd. Op deze logging worden controles uitgevoerd. Zo kunnen we zien wie in welke dossier heeft gekeken. Als uit de controles onregelmatigheden komen, zullen daar maatregelen voor worden genomen. Deze maatregelen zullen onder meer bestaan uit het informeren van de betrokkenen GGD zodat zij verdere maatregelen kunnen nemen naar de betrokken medewerkers en het starten van een procedure voor de afhandeling van datalekken.

Naast de medewerkers van de GGD zijn er nog een aantal mensen die toegang krijgen tot CoronIT. Dit zijn:

- De medewerkers van het callcenter die de gegevens registreren om te zorgen dat testen snel kunnen worden afgenomen. Met het callcenter is een verwerkersovereenkomst afgesloten.
- Externe aanvragers, om een cliënt aan te melden en een afspraak te plannen.
- Servicedesk medewerkers, die toegang hebben tot CoronIT en deze enkel gebruiken als het nodig is in het kader van de dienstverlening.
- Toegang tot de uitslagen is beperkt tot een aantal rollen:
- GGD-medewerkers die een dergelijke rol hebben gekregen, kunnen uitslagen individueel inzien en het filter gebruiker.
- Callcenter-medewerkers kunnen uitslagen individueel inzien omdat zij de resultaten terugmelden en daarom altijd moeten controleren of ze de goede persoon hebben gekozen. Dit gebeurt op basis van bellijsten.
- Een zeer geringe groep van 7 personen heeft ook toegang tot het uitslagenfilter in het afsprakenoverzicht. Dat gebruiken zij om op dag 3 alle nog niet bereikte mensen na te lopen.
- Externe aanvragers kunnen uitslagen op individueel niveau zien en kunnen in het uitslagenfilter alleen de uitslagen zien van de personen voor wie ze persoonlijk de afspraak hebben gemaakt.

Voor deze medewerkers zijn ook strikte maatregelen genomen. Toegang voor zowel de callcenter medewerkers als de medewerkers die de rapportages opstellen wordt gelogd. Voor callcenter medewerkers wordt de logging gelegd naast het aantal telefoontjes en het dossiernummer dat ze moeten opgeven na een gesprek. Op deze wijze kan worden achterhaald of er dossier zijn geopend die niet geopend hadden moeten worden. Met het callcenter is daarnaast een verwerkersovereenkomst gesloten, waarin is opgenomen hoe zij om moeten gaan met de persoonsgegevens en welke maatregelen ze moeten nemen om deze persoonsgegevens te beschermen.

Ook de toegang tot CoronIT en de handelingen in het systeem van de Externe aanvragers, callcenter medewerkers met een grote rol en de externe aanvragers worden gelogd. Medewerkers die de rapportages opstellen zijn projectmedewerkers die zijn aangesteld door GGD GHOR Nederland. Deze medewerkers zijn door middel van een verwerkersovereenkomst en/of een geheimhoudingsverklaring gebonden om de persoonsgegevens geheim te houden. Vanuit de overeenkomsten opgesteld met deze medewerkers en de geheimhouding, wordt van medewerkers een integere werkhouding verwacht, die geheimhouding inhoud, maar ook een correcte omgang met de gegevens.

Andere partijen krijgen enkel toegang tot de rapportages. Nu zijn dat het RIVM en het LCDK. Voordat gegevens worden uitgewisseld, wordt bepaald welke grondslag er is voor de uitwisseling van de gegevens en wat deze partijen in moeten zien. De volgende partijen krijgen nu gegevens:

- Het RIVM, in het kader van de uitvoering van de Wet publieke gezondheid. Afspraken over de manier van uitwisseling worden vastgelegd in een overeenkomst om te zorgen dat persoonsgegevens op een verantwoorde wijze worden overgedragen.
- Het LCDK, die een algemene rapportage krijgt waar geen persoonsgegevens in zijn opgenomen. Deze gegevens worden beschikbaar gesteld om de laboratoriumketen te sturen.
- Indien andere partijen gegevens vragen, wordt eerst gezocht naar de grondslag. Vervolgens zal worden onderzocht welke gegevens worden gedeeld en in welke vorm, waarbij pseudonimisering en anonimisering in veel gevallen de standaard zal zijn. Zo zijn de gegevens voor de ontvangende partij niet herleidbaar.

GGD'en worden via verschillende kanalen op de hoogte gehouden van de werking van het systeem. De afwegingen met betrekking tot de verwerking van persoonsgegevens en de maatregelen worden bijgehouden in een Data Protection Impact Assessment (DPIA). Deze DPIA wordt aangepast als er aanpassingen zijn in het proces. De Functionarissen Gegevensbescherming van de GGD'en hebben toegang tot de meest recente en eerdere versies van deze DPIA.

We gaan natuurlijk graag in op jullie aanbod in om in gesprek te gaan over de huidige autorisaties en de maatregelen die voor deze autorisaties zijn getroffen als jullie dit wensen. Wij hopen jullie met deze brief voldoende informatie te hebben gegeven over de autorisaties. Als dat niet zo is, vernemen we dat graag van jullie, zodat we dit verder kunnen toelichten.

Met vriendelijke groet,

(10)(2e), (10)(2e)
(10)(2e), (10)(2e)