

Uitnodiging slimme digitale oplossingen Corona

IBM Nederland

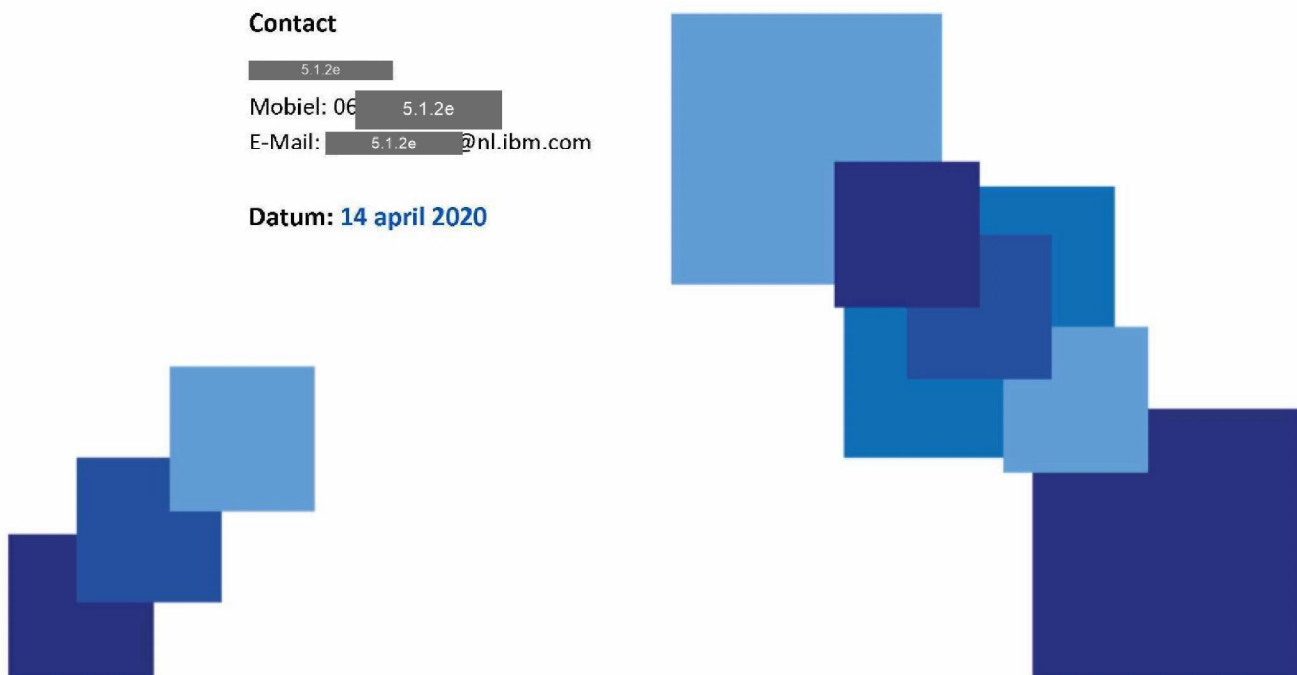
Contact

5.1.2e

Mobiel: 06 5.1.2e

E-Mail: 5.1.2e@nl.ibm.com

Datum: 14 april 2020



Beantwoording slimme digitale oplossingen Corona

Geachte heer/mevrouw,

Hierbij bieden wij u onze reactie aan op de 'Uitnodiging slimme digitale oplossingen Corona', geplaatst op TenderNed op 11 april 2020. De beantwoording beslaat een viertal domeinen waarmee IBM het Ministerie van Volksgezondheid, Welzijn en Sport kan ondersteunen met de transitie naar de volgende fase binnen de intelligente lockdown.

Directe ondersteuning bij de uitrol van apps

IBM is geen aanbieder van de door VWS voorgenomen mobiele apps, echter biedt enerzijds directe ondersteuning aan voor een maximale adoptie van de apps. Anderzijds helpt IBM ervoor te zorgen dat bij uitrol van de apps deze voldoen aan de beveiliging en privacy conform de AVG. Om die reden voldoen niet alle geboden oplossingen aan de uitgangspunten en voorwaarden gesteld in uw uitvraag.

- Een **chatbot** om burgers en bedrijven te ondersteunen bij vragen over de uitrol en het gebruik van de apps. Doel is het ondersteunen van de uitrol van apps in een kort tijdbestek. Kwalitatieve goede communicatie en altijd beschikbare (24/7) gelegenheid tot het stellen van vragen vergroten onzes inziens de acceptatiegraad van burgers. IBM heeft al een groot aantal van deze chatbots geïmplementeerd in Europa en daarbuiten en heeft ondertussen een wereldwijde community voor het doorontwikkelen en implementeren.
- **Waarborgen beveiliging en privacy (AVG compliance) van de apps.** Beveiliging en privacy zijn zeer belangrijke thema's bij de uitrol van de apps, voor de bescherming en afscherming van data om daarmee ook de acceptatiegraad onder de burgers maximaal te laten zijn. Ook al voldoen de apps aan de in deze uitnodiging gestelde eisen, is een integrale aanpak op het gebied van beveiliging en privacy een vereiste. En daar waar de apps, in welke vorm dan ook, gegevens uitwisselen met (landelijke) back-end applicaties is deze integrale aanpak een complexe uitdaging. IBM biedt daarom ondersteuning aan bij het programma management en/of testen van oplossing. Deze ondersteuning is onafhankelijk van de gekozen oplossing, leverancier en technische oplossing en put uit onze internationale ervaring op het gebied van (cyber)security.

Aanvullend op uitrol van de apps: operationele ondersteuning voor pandemie management

Voor het op (middel)lange termijn bestendigen van de afbouw van de lockdown stellen we een tweetal oplossingen voor:

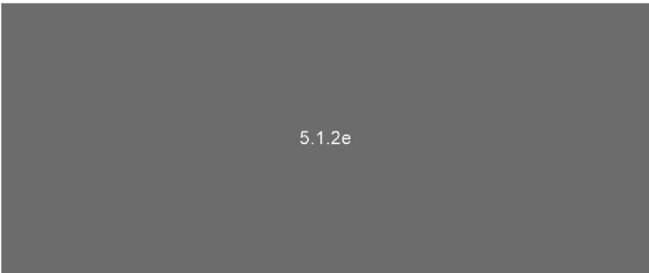
- **Panorama - Pandemie Management Systeem** Dit systeem is reeds jaren in gebruik in Canada en het Midden-Oosten en is geschikt voor de ondersteuning van GGD's bij de uitvoering van het 'Generiek draaiboek (beheersing van infectieziektecrises)'. De oplossing verhoogt de efficiëntie bij het uitvoeren van hun lokale verantwoordelijkheden, en vereenvoudigt het verkrijgen van landelijke informatie.

- **ImmunoProof** – een op blockchain-gebaseerde oplossing voor het aantonen van de immuniteitsstatus van personen. De basisversie is ontwikkeld door IBM en kan op zeer korte termijn beschikbaar zijn voor Nederland. Voor een veilige en efficiënte deelname aan de maatschappij is het van belang dat een individu zijn/haar immuniteit onomstotelijk en veilig kan aantonen. Vooral voor vitale beroepen als zorgmedewerkers, leraren, medewerkers in de openbare orde en veiligheid is dat essentieel. Ook voor een zo snel als mogelijke hervatting van economische activiteiten zoals bedrijfsleven, horeca, cultuursector, etc. is dat van groot belang.

IBM stelt haar lokale en internationale ervaring, research en oplossingen ter beschikking voor de ondersteuning van het Ministerie van Volksgezondheid, Welzijn en Sport, de Ministeriële Commissie Crisisbeheersing en het Outbreak Management Team. Onze brede Europese aanwezigheid zetten we daarbij maximaal in voor zowel de Nederlandse als de Europese gezondheid ten tijde van deze COVID-19 crisis.

Wij wensen u succes met het beoordelen van de respons op uw aanvraag en zijn uiteraard gaarne bereid nadere toelichting te geven op onze voorstellen.

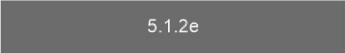
Met vriendelijke groet,



5.1.2e



5.1.2e



5.1.2e

IBM Nederland B.V.

Bijlagen

Bijlage 1 Vraag- en antwoordformulier

Oplossing 1 - Chatbot

Oplossing 2 - Privacy & Security

Oplossing 3 - Panorama

Oplossing 4 – ImmunoProof



Ministerie van Volksgezondheid,
Welzijn en Sport

Bijlage 1 Vraag- en antwoordformulier

Gegevens Uitnodiging	
Titel	Uitnodiging slimme digitale oplossingen Corona
Opdrachtgever	De Staat der Nederlanden (Ministerie van Volksgezondheid, Welzijn en Sport)

Gegevens Ondernemer	
Naam Ondernemer	IBM Nederland B V
Adresgegevens Ondernemer	Johan Huizingalaan 765, 1066VH Amsterdam
Contactpersoon Ondernemer	5.1.2e
Functie contactpersoon	5.1.2e
E-mailadres Ondernemer	5.1.2e @nl.ibm.com
Telefoonnummer Ondernemer	06- 5.1.2e
Website Ondernemer	https://www.ibm.com/nl-en

Verklaring	
Ondernemer verklaart dat:	<i>Doorstrepen wat niet van toepassing is</i>
De aangeboden oplossing voldoet aan de in de uitnodiging geschetste uitgangspunten en is per 28 april 2020 productierijp	Ja / Nee , (zie management samenvatting)
De aangeboden oplossing is per 18 april 2020 beschikbaar voor een publieke proef.	Ja / Nee (zie management samenvatting)

Omwillen van een efficiënte werkwijze vragen we u om een compacte beantwoording en/of beschrijving van uw mogelijkheden ten aanzien van de beoogde oplossing. We verzoeken u dringend om informatie die niet direct de kern van de oplossing raakt, niet in het hoofddocument te verwerken maar als bijlage op te nemen.

1	
Doelstelling	Het verkrijgen van een voorstel voor slimme digitale oplossingen zoals bijvoorbeeld apps die kunnen bijdragen aan bron- en contactopsporing , waarbij stringente eisen gelden voor onder meer snelle beschikbaarheid, privacy en informatiebeveiliging
Vraag	Welke slimme digitale oplossing kunt u leveren die bij kunnen dragen aan bron- en contactopsporing?
Antwoord	Panorama Dit betreft een reeds jaren bestaande en in Canada en een aantal andere landen cloud gebaseerde oplossing voor 'Pandemic Management'. Nu specifiek aangepast en in gebruik voor Contact Tracing, conform het proces van de GGD zoals beschreven in paragraaf 6, ter vervanging van de huidige (handmatige) formulieren. Zie de beschrijving in document: Oplossing 3 - Panorama.

2	
Doelstelling	Het verkrijgen van een voorstel voor slimme digitale oplossingen zoals bijvoorbeeld apps die kunnen bijdragen aan zelfmonitoring en begeleiding op afstand , waarbij stringente eisen gelden voor onder meer snelle beschikbaarheid, privacy en informatiebeveiliging
Vraag	Welke slimme digitale oplossing kunt u leveren die bij kunnen dragen aan zelfmonitoring en begeleiding op afstand?
Antwoord	Geen

3	
Doelstelling	Het verkrijgen van voorstellen voor overige digitale oplossingen, zoals bijvoorbeeld apps, die kunnen bijdragen aan de transitiestrategie en het bestrijdingsbeleid .
Vraag	Welke slimme digitale oplossingen kunt u leveren die bij kunnen dragen aan de afschappingsstrategie en begeleiding op afstand?
Antwoord	ImmunoProof Op het moment dat in Nederland getest gaat worden op antilichamen en bij gebleken juiste test immuniteit kan worden vastgesteld, zal op een eenduidige, veilige en zekere manier door personen hun immuniteit moeten kunnen worden aangetoond. Voor de NHS bouwen wij op dit moment, in ons centrum in Groningen, voor de COVID-19 exit strategie van het Verenigd Koninkrijk een blockchain oplossing, die op de mobiele telefoon de immuniteit en einddatum van deze immuniteit kan bewijzen. Zo kunnen artsen, leraren en mensen in andere vitale beroepen weer ruim aan de slag en kan het openbare leven weer opgestart worden. Zie de beschrijving in document Oplossing 4 - ImmunoProof.

4	
Doelstelling	Het verkrijgen van voorstellen voor voorwaarden waaronder digitale oplossingen kunnen worden ingezet (met betrekking tot techniek, inhoud, werking, implementatie, de privacy en informatieveiligheid)
Vraag	Welke voorstellen voor het op technische en organisatorische wijze borgen van privacy en informatieveiligheid kunt u doen?
Antwoord	Chatbot. Om een snelle adoptie van COVID-19 apps te ondersteunen bieden we een chatbot aan. IBM heeft reeds meerdere COVID-19 gerelateerde chatbots geïmplementeerd zodat zeer snel tot uitrol overgegaan kan worden. Zie de beschrijving in document Oplossing 1 – Chatbot. Privacy & Security ondersteuning in de vorm van veilige applicatieontwikkeling en het testen op kwetsbaarheden. IBM biedt haar rijke wereldwijde ervaring aan om de uitrol van de COVID-19 apps te ondersteunen. Zie de beschrijving in document Oplossing 2 – Privacy en Security.

Belangrijk

Alle informatie verschaft door IBM Nederland B.V. ("IBM") in dit document is vertrouwelijk. De intellectuele eigendomsrechten op de inhoud van dit document berusten bij IBM. Degenen, die dit document van IBM Nederland B.V. ontvangen, zijn geautoriseerd om het document of delen ervan te kopiëren of te dupliceren voor eigen gebruik. Het is niet toegestaan:

- het document of delen ervan te overhandigen aan derden
- derden te informeren over de inhoud van het document
- of het document voor enig ander doel te gebruiken zonder voorafgaande schriftelijke toestemming van IBM Nederland B.V.

Op deze aanbieding is de IBM Klantrelatieovereenkomst van toepassing (via: <http://ibm.com/terms/cra?cc=nl&lc=nl>).

De beschreven oplossingen in dit document geven het Ministerie van VWS ons inziens een goed beeld van mogelijke digitale oplossingen die IBM Nederland B.V., op basis van onze huidige kennis, kan bieden voor een transitie naar de volgende fase van de lockdown. De beschreven oplossingen zijn geen finaal en bindend bod en mogen niet als contractueel bindend worden beschouwd. Een finaal en bindend aanbod kan pas gedaan door IBM Nederland B.V. gedurende de door u aangegeven onderhandelingsprocedure en is afhankelijk van uiteindelijke overeenstemming over voorwaarden en bepalingen.

Oplossing 1 - COVID-19 chatbot

De COVID-19 chatbot: om snel en efficiënt de juiste informatie bij de burger te krijgen rond het gebruik van de COVID-19 apps.

Bijdrage digitale oplossing

Wanneer de twee apps geïntroduceerd worden, zullen er veel vragen uit de samenleving komen over het gebruik hiervan. Wij stellen voor dat het Ministerie de huidige communicatiemiddelen (telefoon en website) aanvult c.q. ontlast met een chatbot die persoonlijk de vragen kan beantwoorden.

Deze chatbot maakt het dus mogelijk dat de juiste informatie, snel en efficiënt de burger bereikt en tegelijkertijd andere cruciale communicatiekanalen, zoals b.v. het 112 noodnummer, beschikbaar blijven voor waar ze voor bedoeld zijn.

Het proactief inzetten van een COVID-19 chatbot zal een gunstig effect hebben op de afhandeling van de informatiebehoefte van de burger:

- Chatbots zijn 24/7 beschikbaar en hebben een grote capaciteit om vragen parallel af te handelen;
- Chatbots kunnen eenvoudige Vraag & Antwoord (V&A) effectief afhandelen (in Nederlands, Engels of andere taal), waardoor de menselijke capaciteit ingezet kan worden op de 'moeilijkere' vragen ofwel vragen waarbij persoonlijke informatie uitgewisseld moet worden. Naast V&A kan de chatbot een cruciale rol spelen in de uitrol, ondersteuning en gebruik van eventuele apps die door overheid als beleidsmaatregel worden ingezet;
- Chatbots spreken de taal van de moderne burger of van de ouderen onder ons (flexibiliteit in gebruik van de door de overheid gehanteerde taalniveaus);
- IBM Watson Assistant, de technologie onderliggend aan de COVID-19 chatbot, wordt door de markt als leidend gezien in het herkennen van vragen van gebruikers en is zelfs al zeer accuraat bij beperkte training. Dit maakt snelle inzetbaarheid mogelijk;
- IBM Watson Assistant is de afgelopen weken al meerdere keren binnen Europa ingezet om COVID-19 gerelateerde vragen te beantwoorden voor (semi-)overheidsinstellingen;
- De IBM oplossing die hier wordt voorgesteld, is de afgelopen twee weken reeds succesvol ingezet in Nederland bij een grote overheidsorganisatie in het veiligheidsdomein om COVID-19 gerelateerde vragen efficiënt richting de burger beantwoord te krijgen.

Werkwijze/Technisch

We stellen samen met experts een lijst met vragen en antwoorden op. Op basis van deze informatie trainen wij de chatbot om de vragen van echte gebruikers te herkennen en het juiste antwoord te geven. Zodra de chatbot live gaat, houden wij de vragen, samen met uw experts, in de gaten en hertrainen wij de chatbot zodat deze zoveel mogelijk vragen correct beantwoordt en de interactie voor de gebruiker als natuurlijk wordt beschouwd.

Bij deze werkwijze maken we gebruik van onze ervaringen bij andere overheden (zoals de politie en DUO) om binnen een korte periode een succesvolle chatbot te realiseren.

Toegang tot de chatbot wordt gecreëerd door het implementeren van een 'widget' op web/mobiele site of via een koppeling in een app op mobiele telefoons. Afhankelijk van het communicatiebeleid kan dit natuurlijk op een algemene (voor)pagina of op een heel specifieke pagina worden ingezet.

Intern zal er vanuit de chatbot beroep worden gedaan op een Natural Language Processing of te wel NLP-module die door IBM zelf wordt geleverd en worden onderhouden (IBM Watson Assistant). Deze NLP-module is beschikbaar in een open ecosysteem en benaderbaar voor de IBM chatbot alsook andere NLP gebruikers.

Alvorens een chatbot live te brengen kan deze in een selecte groep of door testers worden uitgetest. Resultaten van deze tests kunnen weer worden meegenomen in de verbetering van de chatbots.

Indien ervoor wordt gekozen om een chatbot uit te schakelen is dit door zeer kleine wijzigingen op de website of portaal makkelijk en snel uit te voeren.

Toepassingsgebied

IBM ziet voor de COVID-19 chatbot-technologie een belangrijke rol weggelegd:

- In het ondersteunen (eerstelijns ondersteuning) van een gebruiker die voor de bron- en contactopsporing, zelfmonitoring en het bestrijdingsbeleid een app op zijn of haar mobiele telefoon downloadt en gebruikt;
- In het draagvlak creëren bij de burger voor het gebruiken van deze apps;
- In het specifiek aanbieden van informatie aan de gebruikers over COVID-19 maatregelen of begeleiding op afstand en
- In het helpen opschalen van de "OLVG corona check" app – c.q. de mensen in het fysieke call center achter de app te ontlasten door een deel van de vragen reeds van te voren te beantwoorden.

Privacy & Security

Voor het gebruik van de chatbot is geen PII (Persoonlijk Identificeerbare Informatie) noodzakelijk en wordt er ook geen PII verwerkt. Bij implementatie is en wordt data-minimalisatie als uitgangspunt genomen. De voor het operationeel draaien van de chatbot vereiste loggings (letterlijke opslag van de dialogen tussen gebruiker en de chatbot) worden NIET bewaard nadat de chat is afgelopen. Indien de gebruiker (per ongeluk) PII invoert zal deze dus noch gebruikt noch worden bewaard. In de chatbot worden geen gegevens rondom verplaatsingsgedrag, locatie of sociale media koppelingen gebruikt of opgeslagen.

Toegang tot de chatbot, de cloud alsook de logging is afgeschermd door individuele wachtwoorden, die afhankelijk van rollen en verantwoordelijkheden aan verschillende aangewezen partijen kunnen worden verstrekt.

Gegevensstromen in de chatbot zijn volledig inzichtelijk en kunnen geraadpleegd worden.

Doorlooptijden

De COVID-19 chatbot is als basismodule reeds beschikbaar. Aanpassen en uitbreiden van de vragen aan de laatste stand kan plaatsvinden in 1 week, waarna de chatbot live of beschikbaar is voor breedscalige tests. De chatbot is dan beschikbaar voor burgers/ gebruikers met internet-toegang. Om de chatbot beschikbaar te maken via de website van VWS (of andere organisatie), zijn wel kleine aanpassingen aan de betreffende website nodig.

Een bredere chatbot met additionele aandachtsgebieden (zoals begeleiding op afstand, app ondersteuning/ eerstelijns ondersteuning van app gebruikers) zal *agile* (in z.g. *sprints* van 2 weken elk) worden opgebouwd. Afhankelijk van de scope kan een basisversie in 1 tot 3 sprints worden neergezet.

In lijn met de dynamiek van de informatie/ maatregelen kan meerdere malen in een sprint de chatbot worden vernieuwd en worden voorzien van de laatste stand van maatregelen. Tevens worden in deze sprints ook gebruikerservaringen meegenomen indien verzameld.

IBM Services kan op zeer korte termijn de chatbot leveren die een integraal onderdeel uitmaakt van de transitie en ondersteunen van de volgende fase in de intelligente lockdown.

Oplossing 2 - Privacy en Security

Belang van privacy en security

Privacy en security van de COVID-19 apps, en de daarbij behorende informatievoorziening is van groot belang. Ook als applicaties onder hoge tijdsdruk worden ontwikkeld, mag dat niet ten koste gaan van de veiligheid. Wanneer u kiest voor apps waarbij informatie centraal wordt uitgewisseld, zullen strikte beveiligings-, privacy en audit maatregelen getroffen moeten worden. Wij hebben hier jarenlange ervaring mee en stellen onze expertise graag ter beschikking. Dit kunnen wij doen in de rol van System Integrator Privacy & Security.

IBM hanteert een aantal methoden om ervoor te zorgen dat de applicaties veilig zijn en niet langer kwetsbaarheden vertonen, welke door aanvallers kunnen worden uitgebuit. Deze methoden zijn overigens van toepassing op de applicatieontwikkeling door IBM in het algemeen, als voor de applicatieontwikkeling door derde partijen. Twee voorbeelden van methoden die door IBM Security worden gebruikt zijn (1) veilige applicatieontwikkeling/ DevSecOps en (2) Dynamic Application Security Testing (DAST).

Veilige applicatieontwikkeling (DevSecOps)

IBM gebruikt de DevSecOps methode bij applicatieontwikkeling. Dat voegt beveiliging toe aan de softwareontwikkeling en – na de inproductienamen – aan het gebruik van de applicaties. Het doel van de methode is om een balans aan te brengen tussen de ontwikkelsnelheid en beveiligingsvereisten. Door het toepassen van een Agile Framework wordt een continue samenwerking tussen betrokken afdelingen mogelijk gemaakt. De DevSecOps-benadering creëert een cultuur van "Security as Code" die de samenwerking bevordert tussen de software engineers en het beveiligingsteam. Dit model lost het dilemma op tussen het snel schrijven van code en het schrijven van *veilige* code. Silo-denken wordt vervangen door constante communicatie en gedeelde verantwoordelijkheid voor beveiliging door alle betrokkenen, zulks gedurende de gehele ontwikkelingscyclus. Met behulp van deze methode worden organisaties in staat gesteld hun applicaties te beschermen tegen aanvallen, vanaf ontwerp tot release. Enerzijds garandeert dit dus veiligheid van (privacy)gevoelige gegevens, terwijl anderzijds een efficiënt ontwikkelingsproces wordt ondersteund.

Kwetsbaarheden testen

Wij stellen voor mogelijk kwetsbaarheden proactief op te sporen en te verhelpen d.m.v. van wat IBM noemt *Application Security Testing* (DAST). Daarmee wordt de aanpak van een echte aanval nagebootst. Hierbij wordt tevens gebruik gemaakt van geautomatiseerde (DAST-)scanners op live webapplicaties en webservices – liefst in een testomgeving. Er worden real-time aanvallen op applicaties uitgevoerd om de kwetsbaarheden in de applicatie te identificeren. Een DAST-scan vindt kwetsbaarheden zoals: invoervalidatie, authenticatie en autorisatie, configuratie en implementatie, sessiebeheer, foutafhandeling en cryptografie. Bij DAST wordt gebruik gemaakt van IBM X-Force¹ en OWASP (Open Web Application Security Project) om inzicht te krijgen in veelvoorkomende beveiligingslekken en kwetsbaarheden. Belangrijk is een goede kennis van de applicatie (zoals de belangrijkste use cases) en een goed begrip is vereist van de webserver, applicatieserver, databases, businesslogic, applicatiestroom en gebruikersrechten.

¹ <https://www.ibm.com/security/xforce>

Het is aan te bevelen dat een IBM-er onderdeel uitmaakt van het realisatieteam om zo, samen met de partners, te bepalen welke privacy en securitymaatregelen moeten worden genomen.

System Integrator Security & privacy

Wanneer ervoor wordt gekozen om - naast het gebruik van individuele apps - ook centraal informatie uit te wisselen, zullen strikte beveiligings-, privacy en audit maatregelen nodig zijn. Wanneer bijvoorbeeld voor het gebruik van bepaalde applicaties (gevoelige) informatie uit achterliggende systemen / databases nodig is, zal deze beveiligd moeten worden opgeslagen en verzonden. Methoden zoals encryptie en het anonimiseren, van data "at rest" in de database of "in transit" over het netwerk, zijn dan aan te raden. IBM staat klaar om de overheid te ondersteunen als System Integrator Security & Privacy om dit op een veilige en verantwoorde manier te kunnen doen.

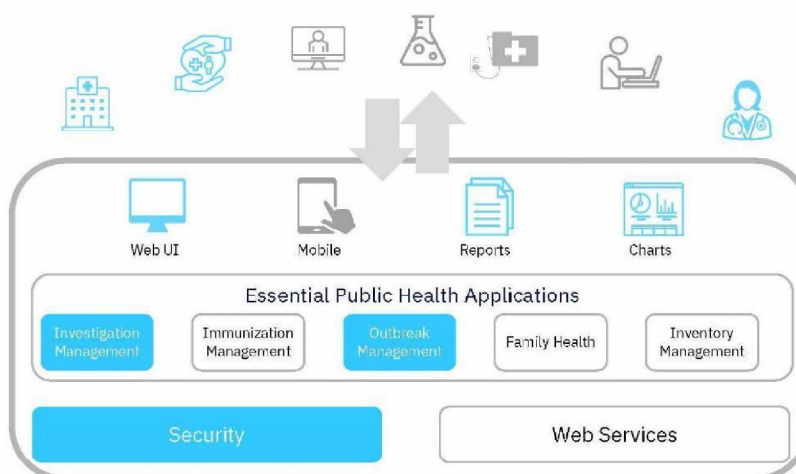
Oplossing 3 - Panorama

Bijdrage digitale oplossing

Panorama is een pandemie management systeem. Zoals in de uitnodiging tot deze RfI wordt aangegeven, wordt in Nederland op dit moment gewerkt op basis van het Draaiboek Beheersing Infectieziekten van het Landelijk Centrum Infectieziekte bestrijding. Panorama is een cloud gebaseerde softwareoplossing die dit gehele proces kan afdekken, maar is voor COVID-19 vooral gericht op het registreren van (verdacht) geïnfecteerden en het opvolgen van de personen waar zij mogelijk mee in contact zijn geweest. De start van de ontwikkeling van Panorama begon in 2005, na de uitbraak van SARS, en wordt op grote schaal gebruikt, o.a. in geheel Canada vanaf 2012 n.a.v. MERS. Panorama bestaat in zijn volledigheid uit meer dan 100 schermen aan functionaliteit. **Speciaal voor COVID-19 en omdat voor de implementatie van de volledige functionaliteit nu aandacht en tijd ontbreekt, heeft IBM een toegesneden COVID-19 versie gemaakt.**

Panorama Pandemic Management

BLAUW is toegesneden COVID-19 functionaliteit



© 2020 IBM Corporation 12 April 2020 IBM Services

Deze speciale COVID-19 versie bevat de volgende drie functionaliteiten:

Besmettingsonderzoek (investigation management): door ziekenhuis of huisarts

- Registreren van verdachte personen.
- Opvolgen besmettingstesten en uitslagen, evt. via gelinkte informatie uit OLVG of andere app.

Contact tracing: door GGD

- Registreren van contacten van geïnfecteerden.
- Opvolgen, waarschuwen contacten van geïnfecteerden (contact tracing), ter vervanging/aanvulling van o.a. het Document "Contactinventarisatie en registratieformulier" uit paragraaf 6.2, Contactonderzoek.
- Groeperen geïnfecteerden en contacten naar geografie, ter ontdekking van (nieuwe) haarden.

Uitbraak management: door RIVM e.a.

- Standard rapportages over verdachten, geïnfecteerden en haarden.
- Meermaalige prognoses van geïnfecteerden.

Wat draagt het bij aan oplossen van het probleem?

Wanneer maatregelen voor de intelligente lockdown langzaam gaan worden losgelaten, kunnen er zich weer nieuwe (grotere) situaties (super spreaders) van infecties gaan voordoen. Het is zaak dat deze dan snel worden geïdentificeerd en dat personen die in contact zijn gekomen met de besmette persoon, worden opgespoord en verwittigd, om verder verspreiding te voorkomen. De wijze waarop de GGD dat tot voor kort heeft kunnen uitvoeren, grensde aan hun maximale capaciteit. Met een centrale oplossing waarbij procesmatig en stapsgewijs (workflows) besmettingen en contacten kunnen worden beheerd, wordt deze capaciteit vergroot en eenduidig en overzichtelijk gemaakt. Het is voor ons vanaf hier niet waarneembaar in hoeverre het proces van het invullen van bovengenoemde formulieren door de GGD's door de genomen maatregelen AVG-conform is ingericht. Met Panorama wordt dit proces louter digitaal gemaakt en werkprocesmatig ondersteund. In de kern zullen het proces en de actoren niet hoeven te veranderen. Wel dient aanvullend gekeken te worden in hoeverre het voldoet aan de wet AVG dan ook hier geborgd kan worden. Wij stellen voor hierover verder van gedachten te wisselen.

Het operationeel ondersteunen van besmettingsonderzoek, contactopsporing en uitbraak management is een belangrijke aanvulling op de voorgenomen inzet van apps. Op dit moment wordt, ook via de media waarneembaar, gedacht aan apps die op basis van nabijheid van mobiele telefoons anoniem waarschuwingen aan elkaar doorgeven. Voordeel hiervan is dat AVG wordt gerespecteerd. Nadeel is dat dit geen waterdichte oplossing is door de beperkingen van de nabijheidstechnologie en de niet volledige dekking van de Nederlandse bevolking met smartphones.

Werkwijze/Technisch

De oplossing draait in een (lokale) cloud en er kan via een webbrowser rol-gebaseerd worden ingelogd en gewerkt.

Privacy & Security

IBM Clouds zijn weliswaar niet NEN751x maar wel HIPAA gecertificeerd, en voldoen aan de hoogste vorm van Security¹. V.w.b. AVG is de oplossing rol-gebaseerd en derhalve wordt desgewenst alleen medisch en verder daartoe geëigend personeel toegang gegeven tot persoonlijke/medische informatie, zoals ook nu bij de GGD en het Contact registratieformulier.

Doorlooptijden

Doorlooptijd voor het in gereedheid brengen van de COVID-19 versie van Panorama bedraagt maximaal 6 weken. Panorama is al in gebruik voor COVID-19, o.a. in geheel Canada en een aantal landen in het Midden-Oosten. Indien voorgeschreven kan de oplossing binnen twee weken in een lokale (Nederlandse) cloud worden geïnstalleerd. Geschat wordt dat dan maximaal 4 weken nodig is om de oplossing precies af te stellen naar de Nederlandse situatie en gebruikers, en om het system als geheel te testen en de gebruikers te instrueren.

¹ <https://www.ibm.com/support/pages/ibm-iso-management-system-certifications>

Oplossing 4 - Immunoproof

Bijdrage digitale oplossing

ImmunoProof is een op blockchain gebaseerde oplossing voor het registreren en aantonen van iemands immuniteit, voor in dit geval COVID-19. Op dit moment wordt voor de NHS in het Verenigd Koninkrijk een oplossing gebouwd door o.a. ons IBM Innovatie Centrum in Groningen, om onomstotelijk, volledig veilig en met waarborging voor de privacy (voldoet aan AVG) te kunnen bewijzen als individu dat je immuun bent getest op COVID-19.

ImmunoProof is ontwikkeld om snelle implementatie te garanderen met behoud van vereiste beveiligings- en privacy-normen. De oplossing is ontworpen op basis van de volgende ontwerpprincipes:

- Privacy & Security by design
- Digital experience - human-centered design
- Decentralized approach for rapid scaling
- Minimal integration (initially) for speed

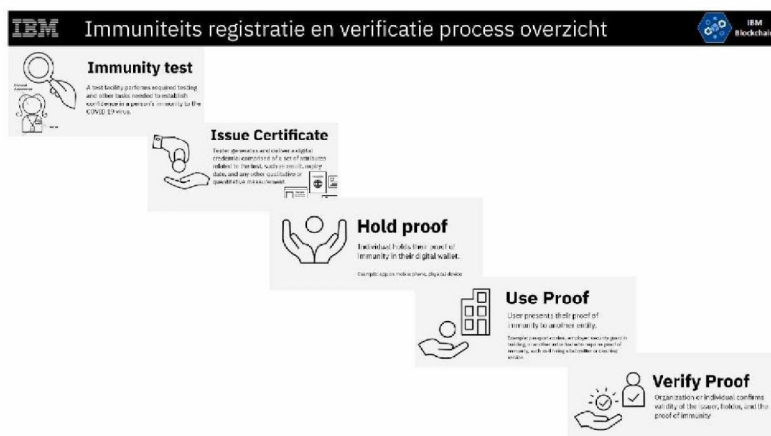
Immuniteitstest: Een daartoe bevoegde instantie/specialist voert een immuniteitstest uit d.m.v. het aantonen van antistoffen in het bloed.

Certificaat-afgifte: Bij positieve uitslag geeft de daartoe bevoegde persoon/specialist in een beveiligde omgeving (shared blockchain ledger) een versleuteld certificaat af, dat benodigde kenmerken bevat (zoals resultaat, pseudoniem versleuteld persoonsID, duur immuniteit).

Bewaar bewijs: het individu met immuniteit bewaart zijn/haar bewijs in een digitale kluis (wallet) in een app op de telefoon.

Gebruik bewijs: Het individu met immuniteit laat het bewijs op daartoe geëigende momenten en plaatsen zien (betreden gebouw, vliegtuig, school, medische locatie, e.d.).

Verifieer bewijs: Een daartoe geëigende persoon (toegangscontrole) verifieert het bewijs i.c.m. een persoons-eigenschap.



Wat draagt het bij aan oplossen van het probleem?

Sommige maatregelen voor intelligente lockdown worden langzaam losgelaten en er wordt voortgang gemaakt met testen voor aantonen van immuniteit. Zeker mensen met vitale beroepen, zoals leraren, medisch personeel, gezagshandhavers die al dan niet COVID-19 hebben gehad en met aantoonbare immuniteit, zullen langzaam weer gaan deelnemen aan het dagelijks leven. Het is dan belangrijk dat onderscheid gemaakt kan worden tussen mensen met en zonder immuniteit, zodat absolute zekerheid bestaat en kan worden aangetoond dat de mensen in vitale beroepen hun zo belangrijke functies weer veilig kunnen uitvoeren.

Werkwijze/Technisch

De eerste keer dat een persoon getest wordt, krijgt deze een unieke willekeurige code in de vorm van een QR-code (bijvoorbeeld op een visitekaartje). Deze code, in combinatie met de geboortedatum van de persoon, vormt vanaf dat moment de unieke toegangssleutel tot de testgegevens omtrent immuniteit. Doordat de combinatie op de blockchain onleesbaar wordt opgeslagen in de vorm van een onomkeerbare *hash digest* (conform industriestandaarden voor wachtwoorden), zijn de testgegevens niet op andere wijze te herleiden tot een persoon. Het is mogelijk om de gegevens zelf versleuteld op te slaan voor een extra laag beveiliging.

De persoon kan de QR-code bewaren in een app (iOS, Android) of op papier (techniekonafhankelijkheid bevordert inclusiviteit). Een derde partij die wil verifiëren of de persoon positief heeft getest op antilichamen, vraagt om de QR-code te tonen en controleert de geboortedatum (eventueel bevestigd door identiteitsbewijs). Door de code te scannen en de geboortedatum in te vullen op een app of mobiele website krijgt de controleur toegang tot een sterk samengevat extract van de testresultaten (op *need-to-know* basis).

Privacy & Security

Wie mag verifiëren, kan beperkt worden door middel van gebruikersaccounts. De combinatie van geboortedatum (iets wat je bent) en de unieke code (iets wat je hebt) biedt naar onze mening een goede balans tussen privacy, gebruiksvriendelijkheid en security. De persoon heeft immers altijd zelf de volledige controle over het al dan niet delen van de eigen gegevens, zonder dat het systeem, een administrator of een derde partij de link met een fysiek persoon kan leggen. Blockchaintechnologie zorgt voor een veilige opslag.

De gebruikte Blockchain is:

- Privé en met Permissie (*permissioned* blockchain variant),
- Niet te kraken (*tamper proof*),
- Onveranderlijk en met volledig verifieerbare herkomst (*provenance*),
- Veilig en anoniem bij data-overdracht naar de app,
- Controleerbaar,
- Schaalbaar door gebruik van mobiele app als bewijsdrager.

Bij het ontwerpen van de oplossing wordt zo veel mogelijk aansluiting gezocht bij principes van privacy en security by design, en Self-Sovereign Identity (SSI¹). Zo kunnen we niet alleen snel een oplossing uitrollen gebaseerd op de huidige stand van de techniek, maar voorzien we ook een pad naar toekomstige standaarden rondom identiteit. ImmunoProof is hiermee sneller en eenvoudiger te implementeren dan een volledige Self-Sovereign Identity oplossing. Daarnaast kan ImmunoProof in de toekomst gemigreerd worden naar een volledige Self-Sovereign Identity oplossing.

Doorlooptijden

De gekozen oplossing is snel te implementeren. Verwacht wordt dat de applicatie eind van deze week gereed is voor user testing. Wij verwachten de oplossing de tweede helft van April operationeel te hebben, waarbij IBM heel snel kan schalen. IBM heeft veel ervaring in het grootschalig uitrollen van applicaties.

¹ <https://dutchblockchaincoalition.org/usecases/self-sovereign-identity-ssi>