Programma van Eisen voor een digitale oplossing ter aanvulling op bron- en contactonderzoek

Versie 0.5, 19 mei 2020

Inhoudsopgave

1 Inleiding

1.1 Over dit document

Dit document beschrijft de eisen aan de app. De eisen zijn toegespitst op de Nederlandse situatie, maar volgen ook de adviezen van de EU op het gebied van Contact Informatie apps[1]. Ze zijn geformuleerd op basis van de bestaande behoeften en inzichten. Technische uitwerking, juridische beoordeling en het realisatietraject zijn geen onderdeel van dit document; die zullen later toegevoegd worden en kunnen aanleiding geven tot aanpassing van de eisen.

De eisen zijn verdeeld over twee categorieën:

- Functionele eisen: wat moet de app doen, welke taken moet de app kunnen vervullen?
- Niet-functionele eisen: aan welke kwaliteitseisen moet de app voldoen?

Eisen met betrekking tot "kwaliteit in gebruik"[2] zijn opgenomen onder de niet-functionele eisen.

De nummers van functionele eisen beginnen met een "F", die van niet-functionele eisen met een "Q". Het is de bedoeling dat deze nummers ongewijzigd blijven na het vaststellen van dit document; eisen die vervallen worden doorgehaald en nieuwe eisen krijgen altijd een nieuw, hoger nummer.

1.2 Definities

Dit document hanteert de volgende definities:

index (case)	bevestigde patiënt COVID-19
bron- en contactonderzoek (BCO)	Het (snel) in kaart brengen van contacten van besmette personen om tijdig maatregelen te nemen en daarmee verdere verspreiding van het virus te voorkomen en het monitoren van locaties of situaties waarin mensen besmet zijn geraakt, om eventuele verheffingen of lokale risico's te signaleren en zo mogelijk extra maatregelen te implementeren.
contact	Persoon die binnen de besmettelijke periode van index case relevante blootstelling heeft gehad. Contacten worden onderscheiden in drie categorieën: 1) huisgenoten, 2) overige nauwe contacten en 3) overige contacten. *NB. In dit document wordt dus met "contacten" niet bedoeld de personen die op de smartphone in een telefoonboek/ contactenlijst zijn opgeslagen.*
contactcode	Een unieke, anonieme code die de app genereert (en meermaals per dag wijzigt) en die als basis dient voor het registreren van mogelijk risicovolle contactmomenten.

1.2 Documenthistorie

v0.1	16 mei 2020	initiële versie, gebruikmakend van "USER STORIES & HAALBAARHEIDSANALYSE: OPLOSSING 1" (v0.1, 24-04-2020) en "Requirements contact tracing app 0.41" (v0.4.1 DRAFT, 15-05-2020)
v0.2	18 mei 2020	tekstuele aanvullingen, scenario's voor procesverloop
v0.3	18 mei 2020	interne review
v0.4	19 mei 2020	schriftelijke review werkgroep verwerkt

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670
[2] Afgeleid van de ISO:IEC-25010-definitie van "quality in use", https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en

2 Doelstellingen

Dit hoofdstuk beschrijft de doelstellingen van de app vanuit een aantal relevante perspectieven: de burger, de infectieziektebestrijding en de overheid.

2.1 Perspectief burger

Burgers kunnen de app installeren met verschillende motieven. De onderstaande lijsten geven enkele mogelijke doelstellingen, beredeneerd vanuit de burger.

Vanuit de geïnfecteerde:

- *"Ik ben besmet met COVID-19 en ik wil zoveel mogelijk voorkomen dat mensen met wie ik in het dagelijks leven relevant contact had, zonder dat ik ze op kan noemen, ook gewaarschuwd worden."* (verantwoordelijkheid nemen naar anderen, contacten informeren)
- *"Ik ben besmet met COVID-19 en ik wil dat mensen met wie ik in het dagelijks leven relevant contact had gewaarschuwd worden, zodat zij snel kunnen handelen."* (verantwoordelijkheid nemen naar anderen, contacten informeren)
- *"In mijn dagelijks leven/ werk kom ik veel in contact met anderen en ik beschouw het als mijn plicht om alle beschikbare middelen te gebruiken."* (verantwoordelijkheid nemen naar anderen)
- "Ik wil bijdragen aan de oplossing voor een groot maatschappelijk probleem." (verantwoordelijkheid nemen)
- "Ik wil bijdragen aan een snellere versoepeling van maatregelen."

Vanuit de gebruiker:

- *"Ik wil zo snel mogelijk op de hoogte zijn van een mogelijke besmetting, zodat ik verdere verspreiding kan voorkomen."*
- *"Ik wil zo veel mogelijk gerustgesteld worden dat ik niet in de buurt van een besmet persoon ben geweest."*
- *"Ik wil bijdragen aan de oplossing voor een groot maatschappelijk probleem."* (verantwoordelijkheid nemen)
- *"Ik wil bijdragen aan een snellere versoepeling van maatregelen."*

Het behalen van persoonlijke voordelen voor burgers en de kwaliteit en betrouwbaarheid van de app zijn van belang voor de adoptie en het langdurige gebruik. De mate waarin de doelen behaald kunnen worden, hangt direct samen met mate waarin (andere) burgers de app adopteren.

2.2 Perspectief infectieziektebestrijding

Vanuit het perspectief van de infectieziektebestrijding is het doel van de app het verkorten van de tijd tussen de identificatie van de index case door een test en het moment waarop personen, die langer dan een bepaalde periode in de buurt geweest zijn, voorzien zijn van een handelingsperspectief en relevante bijbehorende informatie. De app draagt bij aan het informeren van contacten in aanvulling op bestaand bron- en contactonderzoek.

De realisatie en implementatie moeten echter geen nadelig gevolg hebben op de bestaande GGD-processen.

2.3 Perspectief overheid

Het belangrijkste en overkoepelende doel voor de overheid is het bestrijden van de verspreiding van het COVID-19 virus en bevorderen van de volksgezondheid. Hierdoor kunnen de maatregelen op een

verantwoorde manier versoepeld worden. De verwachting is dat naarmate de adoptie groter is, de app een effectiever hulpmiddel is bij het bestrijden van de verspreiding van het virus te beperken.

3 Randvoorwaarden en uitgangspunten

3.1 Randvoorwaarden

Voor nadere uitwerking, realisatie, implementatie en gebruik van de app gelden de volgende randvoorwaarden:

1. De geteste burger wordt altijd als eerste geïnformeerd over de uitslag van de test.
2. Burgers krijgen via de app geen hulp die ze zonder de app niet zouden krijgen.
3. De app functioneert in aanvulling op de reguliere GGD-processen en wordt geïntegreerd waar nodig om een positief testresultaat tot een anonieme contactmelding te laten leiden.
4. De informatie die de app biedt, is actueel en conform de richtlijnen van het RIVM.
5. De oplossing moet zoveel mogelijk voorkomen dat er geen melding van besmettingsrisico wordt gedaan, terwijl dat wel zou moeten.
6. De oplossing moet vals-positieve meldingen zoveel mogelijk voorkomen.
7. De app is beschikbaar op iOS en Android en op alle gangbare, daarmee werkende smartphone-modellen.
8. De app is zo breed mogelijk bruikbaar. De toegankelijkheid van de app is op een zo groot mogelijke relevante doelgroep gericht, door expliciete aandacht voor taal, taalbeheersing en beperkingen.
9. De app is bruikbaar voor burgers met een beperkte belbundel of dataverbinding.
10. De app wordt alleen in productie genomen als is aangetoond dat de app voldoende waarborgen biedt voor het beschermen van privacy.
11. De app dient zo effectief mogelijk te zijn en daartoe wordt een proces ingericht om dat te monitoren. Hiertoe wordt nader onderzoek uitgevoerd om te komen tot normering.
12. De app informeert geen contacten van contacten.
13. De statistische, anonieme data wordt verzameld, echter alleen de data die nodig is om de effectiviteit van de app te monitoren.

3.2 Uitgangspunten

Deze specificatie van de oplossing is gebaseerd op de volgende uitgangspunten:

1. Het overkoepelende doel is de bestrijding van de verspreiding van het COVID-19 virus.
2. De inzet van deze app is tijdelijk en gebonden aan het overkoepelende doel.
3. Om de app effectief te laten functioneren, moet het mogelijk zijn om voldoende betrouwbaar een afstand tussen twee smartphones te bepalen op basis van in smartphones beschikbare technologie (bijvoorbeeld bluetooth).
4. De eisen worden geformuleerd onafhankelijk van een specifieke ontwikkelmethode; indien nodig kunnen eisen later worden omgezet of opgesplitst in bijvoorbeeld 'user stories'.
5. De app biedt geeft geen nadere risicobeoordeling op basis van de verzamelde gegevens of andere medische duiding: de app registreert contactcodes en ontvangt handelingsperspectieven.
6. De nadere uitwerking richt zich primair op een app die geschikt is voor smartphones.
7. De criteria op basis waarvan bepaald wordt of een contact risicovol is en een waarschuwing vereist, worden zoveel mogelijk afgestemd met de buurlanden.
8. De (niet-)functionele eisen worden later aangescherpt op basis van resultaten uit risicoanalyses en de Data Protection Impact Assessment.

4 Overzicht

4.1 Functionele onderdelen

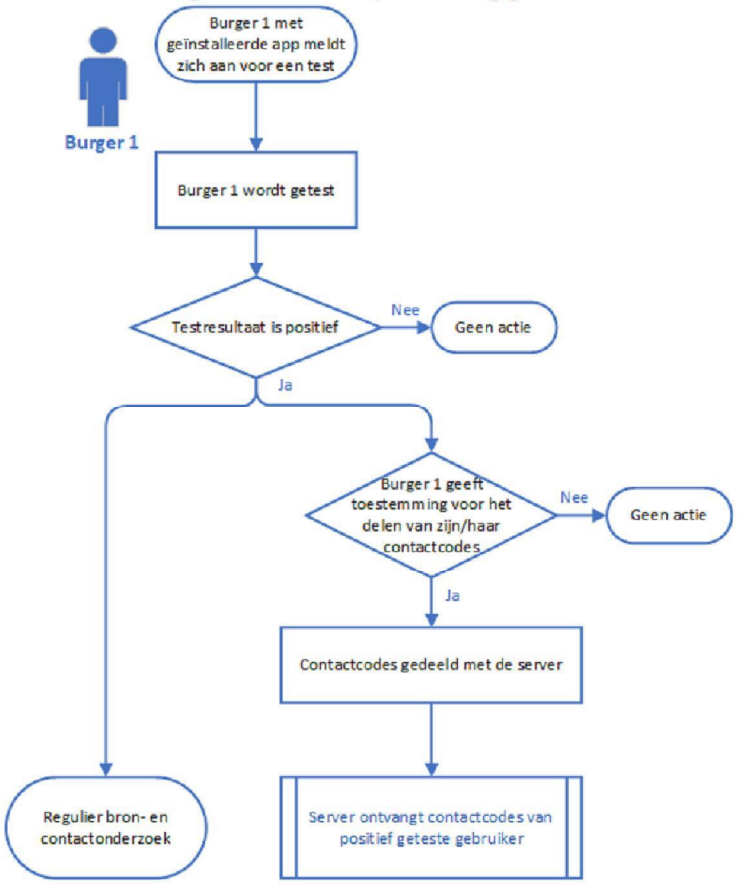
De oplossing vereist twee functionele onderdelen: een mobiele app op de smartphone van de burger en een server die enkel ervoor zorgt dat de contactcodes van de positief geteste burger worden gedeeld.

4.2 Proces

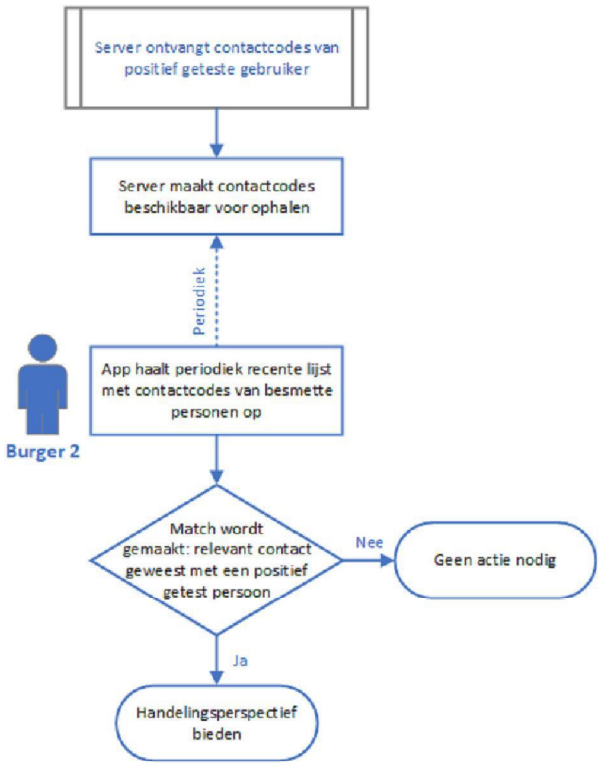
Als de app actief is, verzamelt die contactcodes van alle smartphones die zich voor een bepaalde minimale duur binnen een vastgesteld bereik hebben bevonden (bijvoorbeeld: 15 minuten en 1,5 meter).

Op het moment dat de gebruiker zich heeft laten testen met een positief resultaat, worden na toestemming van de burger, de contactcodes op de server voor een zekere periode opgenomen. Om misbruik te voorkomen kan het melden van een positief testresultaat alleen plaatsvinden na

autorisatie van een aangewezen instantie. Het proces is weergegeven in de onderstaande afbeelding.



De app van een (andere) gebruiker kan dan op basis van die registratie bepalen of de gebruiker in relevant contact is geweest; dit doet de app door periodiek de contactcodes van recente besmettingen op te halen. Dit is gevisualiseerd in de onderstaande afbeelding.



4.3 Relatie met de applicatie Thuisrapportage

Als verlengstuk van het bron- en contactonderzoek wordt ook gewerkt aan een "applicatie Thuisrapportage", waarmee burgers hun (niet anonieme) contactgegevens kunnen verzamelen ten behoeve van het contactonderzoek. De relatie tussen de app en de applicatie Thuisrapportage is beperkt: bij een waarschuwing kan de app de burger het advies geven om de applicatie Thuisrapportage te gebruiken; dit is hieronder schematisch weergegeven.

5 Functionele eisen

Dit hoofdstuk beschrijft de functionele eisen van de app.

5.1 De app

5.1.1 Installeren en aanmelden

F1. Na installatie en voor het eerst opstarten, vraagt de app om toestemming (informed consent[3]) van de gebruiker; indien de gebruiker die toestemming niet direct geeft, kan hij dat later alsnog doen.

F2. Zonder informed consent kan de gebruiker de app niet gebruiken.

F3. De app geeft de gebruiker een unieke, anonieme **contactcode**, die meermaals per dag varieert.

5.1.2 Bedienen

F4. De gebruiker kan de app op elk moment permanent verwijderen, alle verzamelde gegevens worden dan tevens verwijderd van de smartphone.

F5. De app kan tijdelijk worden uitgeschakeld; als de gebruiker later de app weer inschakelt, functioneert die weer volledig, in de tussengelegen periode worden er geen gegevens verzameld en verzonden. Bij tijdelijk uitschakelen krijgt de gebruiker een herinnering om de functionaliteit weer in te schakelen.

5.1.3 Contacten bijhouden

F6. De app verzamelt anonieme contactcodes van alle gebruikers van de app die gedurende een vastgestelde periode (bijvoorbeeld 15 minuten) binnen een vastgestelde afstand (bijvoorbeeld 1,5 meter) zijn geweest en voorziet deze van een datum.

F7. De criteria op basis waarvan de app een contact registreert (periode en afstand) zijn centraal ingesteld en aanpasbaar.

F8. De app verwijdert automatisch alle contactcodes die langer dan 14 dagen geleden zijn verzameld.

5.1.4 Signaleren

F9. De app haalt periodiek, incrementeel, contactcodes van recente besmettingen op van de server.

F10. De frequentie waarmee de app bij de server controleert, is instelbaar en aanpasbaar.

F11. De app waarschuwt de burger automatisch als er een besmettingsrisico is geweest vanwege een relevant contact (bijv. langer dan 15 minuten, binnen 1,5 meter) met een positief geteste burger.

F12. De waarschuwing die de app geeft, moet voldoende en duidelijke informatie bevatten zodat de burger een verstandige beslissing kan nemen (handelingsperspectief). Hieronder valt, ten minste, de tekst van de officiële informatiebrief in digitale vorm. Aanvullend kunnen bijvoorbeeld de volgende adviezen getoond worden: download de thuisrapportage app, neem contact op met huisarts of GGD, blijf thuis en/of vraag een test aan.

F13. De tekst van de waarschuwing is centraal instelbaar en de app haalt deze tekst periodiek op (bijvoorbeeld dagelijks). (Dit is om zo veel mogelijk te voorkomen dat bij gewijzigd beleid updates van de app nodig zijn en er verschillende versies van de app in omloop zijn.)

F14. De app zorgt dat de waarschuwing zo opvallend mogelijk voor de gebruiker is.

---

[3] Naar analogie: "Informed consent is een belangrijk uitgangspunt uit het gezondheidsrecht. Informed consent houdt in dat een patiënt zijn of haar toestemming moet geven voor een medische behandeling of deelname aan (medisch-)wetenschappelijk onderzoek." (bron: Centrum voor ethiek en gezondheid)

5.1.5 Informeren

F15. De app voorziet in een toelichting ten aanzien van het doel van de app.
F16. De app benadrukt zo helder mogelijk dat de app zorgvuldig omgaat met informatie over de gebruiker, zijn contacten en eventuele testresultaten.
F17. De app biedt een lijst met veel gestelde vragen over gebruik van de app en antwoorden daarop met indien mogelijk een chatbot.
F18. De app kan de gebruiker bij vragen over het functioneren van de app doorverwijzen.

5.2 Server en update faciliteiten

Om de app te laten werken, is een server nodig (zie hoofdstuk "Overzicht"). Deze server moet de volgende functionaliteit bieden:

F19. De server slaat tijdelijk contactcodes van besmette personen op na een positieve COVID-19-test.
F20. De server verwijdert contactcodes automatisch na een vooraf ingestelde tijd.
F21. De update faciliteit houdt de criteria op basis waarvan een contact als relevant wordt beoordeeld (periode, afstand) en zorgt dat apps die criteria kunnen ophalen.
F22. De update faciliteit houdt de tekst van de waarschuwing bij, die getoond wordt aan gebruikers van de app, en zorgt dat apps die tekst kunnen ophalen.
F23. De update faciliteit houdt de tekst voor de lijst met veel gestelde vragen bij en zorgt dat app die tekst kunnen ophalen.

6 Niet-functionele eisen

De niet-functionele eisen (kwaliteitseisen) zijn geordend op basis van de standaard voor het specificeren van softwarekwaliteit (ISO/IEC 25010[4]); deze standaard biedt een raamwerk voor de diverse kwaliteitseigenschappen van een systeem. Het model bestaat uit een aantal hoofdcategorieën die nader zijn onderverdeeld. De onderstaande paragrafen beschrijven de eisen met betrekking tot relevante categorieën; definities van de kwaliteitseigenschappen zijn voor leesbaarheid opgenomen bij de betreffende paragrafen.

ISO/IEC 25010 beschrijft ook eigenschappen voor "kwaliteit in gebruik" (quality in use). Gelet op de aard van de app en het belang van een grote adoptie zijn die voor de app relevant. Kwaliteit in gebruik is beschreven in het volgende hoofdstuk.

Q1. De app is een aanvulling op bestaande processen.
Q2. Er is afstemming met buurlanden.
Q3. De app biedt de gebruiker altijd een acceptabel en haalbaar handelingsperspectief.
Q4. De app is ingericht om zo min mogelijk middelen (bijvoorbeeld batterijcapaciteit) te gebruiken.
Q5. De server en gebruikte infrastructuur zijn eenvoudig op en af te schalen.
Q6. De app heeft geen merkbare nadelige invloed op de werking van andere apps, met als uitzondering het mogelijk moeten delen van communicatietechnologie, zoals bluetooth.
Q7. Communicatie tussen de app en de server is gebaseerd op courante en bewezen standaarden.
Q8. De beschrijving van de app in de app stores is zodanig, dat gebruikers uit de doelgroepen het nut en de werking van de app kunnen doorgronden.
Q9. Het ontwerp is beproefd op bruikbaarheid door verschillende doelgroepen.
Q10. Teksten in de app zijn duidelijk en niet langer dan nodig.
Q11. De app biedt een zo beperkt mogelijke flow door de functionaliteit, met zo min mogelijk interactie-elementen.
Q12. De gebruiker kan eenvoudig vaststellen of de app volledig en naar behoren werkt.
Q13. Indien de app niet kan communiceren door uitval van de netwerkverbinding, laat de app hierover een melding zien.
Q14. Indien de app geen contacten kan signaleren door uitval van de benodigde technologie, laat de app hierover een melding zien.
Q15. De gebruikersinterface van de app is ontworpen met een zo plezierig mogelijke gebruikersbeleving en is voorafgaand aan inproductiename daarop getoetst.
Q16. De app kan omgaan met en is beschikbaar in de voor de gebruikers belangrijkste talen.
Q17. De app voldoet, waar relevant, aan de richtlijnen uit de Web Content Accessibility Guidelines (WCAG2.1[5]).
Q18. De app is aantoonbaar bruikbaar door burgers met beperkte digitale vaardigheden en beperkte taalbeheersing.
Q19. De app, de server en update faciliteit zijn voorbereid op het uitvallen van benodigde technologie en kan zonder foutmelding en in beperkte mate functioneren zolang die technologie niet beschikbaar is.
Q20. De app mag geen schade veroorzaken aan de smartphone.
Q21. De server kan na een verstoring de situatie (contactcodes van besmette gebruikers) van een bepaald moment van voor de verstoring herstellen; de maximale periode van verlies is vastgelegd in een SLA.
Q22. Gegevens die worden verwerkt zijn niet tot een individueel persoon herleidbaar.

[4] ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models
[5] https://www.w3.org/TR/WCAG21/

Q23. De app maakt geen gebruik van locatiegegevens.
Q24. De app voldoet aan de Algemene Verordening Gegevensbescherming (AVG).
Q25. De server en daarmee ondersteunde processen voldoen aan de AVG.
Q26. De contactcode is op geen enkele wijze gebaseerd op persoonlijke gegevens.
Q27. Het ontwerp van de app is gebaseerd op de principes van "Privacy by Design"[6].
Q28. Gebruik van de app is pas mogelijk na expliciet informed consent door de gebruiker.
Q29. Het ontwerp en alle programmatuur zijn toegankelijk voor externe verificatie (open source).
Q30. De app voldoet aan de relevante Nederlandse en internationale standaarden voor informatiebeveiliging.
Q31. De app en de server zijn getoetst middels een risicoanalyse, Privacy Impact Assessment (PIA) en een penetratietest en alle daardoor ontdekte kwetsbaarheden zijn opgelost of als risico geaccepteerd.
Q32. Alle in de app getoonde teksten hebben een bronvermelding en zijn vastgesteld door de genoemde bron.
Q33. Het is duidelijk voor de gebruiker dat de app een door de Nederlandse overheid aanbevolen, beheerde en goedgekeurde app is.
Q34. Alle instellingen in de app die snel en regelmatig op basis van het geldende beleid moeten kunnen worden gewijzigd, zijn in te stellen zonder dat een update van de app nodig is.
Q35. Functionaliteit in de app kan worden getest in een testomgeving.
Q36. De communicatie tussen de app en de server kan worden getest in een testomgeving.
Q37. Het installeren van de app moet eenvoudig en laagdrempelig zijn.
Q38. De app is beschikbaar in de gangbare app stores (Google Play Store en de Apple App Store).

[6] https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf