Juridische aspecten van het digitaal verkrijgen van toestemming (consent) bij NIET-WMO-plichtig onderzoek.

Inventarisatie gemaakt binnen de LCRDM taakgroep Digitaal Consent door:
Rob Gommans, Elize Vlainic, Maarten Goldberg, Lolke Boonstra, Iris Kist, Martin Frank

Mei-oktober 2020

Conclusies uit de inventarisatie.

1. Identificatie heeft geen juridische grondslag, vastleggen van toestemming van de betrokkene wel. (Zie pag 2 voor achtergrond informatie)

2. Bewijslast voor consent ligt bij onderzoeker, zorg dat je aan de VSGO voldoet en dit vastlegt

3. Er is geen juridische grondslag gevonden om de mate van identificatie vast te leggen die heeft plaatsgevonden

4. Bij geen noodzaak om de specifieke persoon vast te leggen, is de mate waarin het wel gedaan wordt aan onderzoeker en instelling, waarbij eventueel nog aanvullende regels voor het type onderzoek kunnen gelden (discipline specifiek). (Zie pag 5 voor achtergrond informatie)

5. Het is niet zinvol om landelijke standaard procedures of werkwijzes te ontwikkelen, het eigen beleid van de instelling en toetsing door de ethische commissie en het verschil tussen disciplines vraagt om maatwerk

Achtergrondinformatie

Ad 1 verplichting tot identificatie

Het gaat om niet WMO-plichtig onderzoek waarbij toestemming noodzakelijk is (vanuit organisatorische, ethische en/of juridische grondslagen).

Waarom identificeren? De 'zwaarste' redenen en procedures eerst

1. Om achteraf bewijs te hebben dat een specifiek persoon zijn/haar toestemming gegeven heeft en mogelijkheid om toestemming achteraf weer in te trekken (recht om vergeten te worden)
Identificatie methodes onder meer iDIN, ReadID, IRMA

2. Omdat een instituut- of onderzoeksveld-specifieke gedragscode dat vereist.
Identificatie methodes onder meer iDIN, ReadID, IRMA

3. Om zeker te weten dat je met een specifiek persoon te maken hebt (om vooraf/tijdens onderzoek te verifiëren dat persoon X is wie hij/zij zegt dat hij/zij is).

- Video/audio verbinding
- Participant Identification Code (i.e., hash/checksum)
- Identificatie methodes zoals iDIN, ReadID, IRMA

Mogelijkheid tot legitimatie/identificatie:

- Verificatie middels e-mail adres of IP adres is niet afdoende. Een persoon kan meerdere e-mailadressen/IP adressen hebben.

- Verificatie middels captcha, video of audioverbinding

- Query/response procedure via authenticator app.

iDIN, ReadID of IRMA

- iDIN: identificatie/authenticatie via bank. Is men bereid dit te doen? Angst dat bank inzage heeft in andere persoonsgegevens d.m.v. deelname aan onderzoek. Werkt niet/onvoldoende bij personen < 18 jaar en bij mensen zonder bankrekening (buitenlandse deelnemers)

- ReadID: identificatie/authenticatie middels paspoort/rijbewijs en smartphone. Opslaan van hash over identificatie data om achteraf nog te kunnen verifiëren dat pesoon X echt destijds toestemming gegeven heeft.

- IRMA: zelf geen identificerende partij, middels andere partij, bijvoorbeeld via Gemeente. Kluis met persoonsgegevens wordt op telefoon opgeslagen, "zware" procedure voor "slechts" het geven van toestemming voor deelname aan onderzoek. Werkt niet met buitenlandse deelnemers, business model ontbreekt nog.

4. Om zeker te weten dat een unieke persoon deelneemt (voorkomen dat iemand vaker deelneemt).

- Video/audio verbinding

- Query/response procedure via authenticator app

Unieke (onetime) link in survey

5. Om zeker te weten dat je met een persoon te maken hebt.

    ◦ E-mail

    ◦ Captcha

    ◦ Query/response

    ◦ Video/audio verbinding

Vraag naar use cases: In welke situatie vraag je bij niet WMO plichtig onderzoek naar een identificatie van de proefpersoon en waarom?

- Feedback RUG (Psychologie)

Bij onderzoek s zeker niet altijd sprake van identificatie van deelnemers, maar regelmatig toch wel. Hierbij doel ik op identificatie op naam of evt indirecte identificatie door een pseudoniem te vragen (code, zoals gebruikt binnen SONA of Prolific bijv).

Echter naar mijn weten wordt er eigenlijk nooit om legitimatie gevraagd, inderdaad net zoals bij offline onderzoek niet gebruikelijk is (want vaak niet nodig?). De naar mijn weten enige uitzondering hierop is dat mensen om hun BSN gevraagd kunnen worden zodat ze uitbetaald kunnen worden. Opmerking daarbij: Een BSN of IBAN wordt wel gevraagd voor uitbetaling maar niet gecontroleerd op echtheid via een ID

Bij Sona werkt het als volgt: een student wordt ingevoerd in de Sona-pool na formele inschrijving bij Psychologie. Als je komt opdagen bij een experiment is een ID niet nodig. Je moet je wel identificeren bij de Sona-administratie als er dingen rechtgezet moeten worden.

- Feedback Radboud Universiteit Nijmegen, Faculteit Sociale Wetenschappen

Proefpersonen worden niet geïdentificeerd. Proefpersonen wordt gevraagd naar SONA/Prolific ID of naam, afhankelijk van de manier van werving. Op het toestemmingsformulier slaan we iha alleen daad van toestemming met time stamp op. Uitzondering zijn longitudinaal onderzoek en bij mogelijke toevalsbevindingen. In deze gevallen slaan we wel een naam op op het toestemmingsformulier, alsmede aanvullende contactgegevens in andere databases. Gegevens worden ingevuld/genoemd door proefpersoon en worden niet extra geverifieerd. Tbv betaling wordt ook soms naam en soms ook adres en banknummer opgeslagen op de financiële formulieren, wederom zoals aangeleverd door de proefpersoon. Het is niet meer toegestaan om hiervoor BSN op te slaan. Deze gegevens worden opgeslagen en bewaard door de financiële afdeling van de Faculteit.

Reactie taakgroep

- Geen juridische plicht voor legitimeren/identificeren.
- Verzoek tot inzage in identificatiebewijs is toegestaan (om identiteit vast te stellen), maar individu hoeft hier niet aan mee te werken.
- Kopie identificatiebewijs maken is niet toegestaan.
- Geen juridische grondslag voor verwerken BSN nummer.

Verdere aandachtspunten (niet uitgewerkt)

Bij offline onderzoek vindt ook meestal geen identificatie plaats.

Wat als een wettelijke vertegenwoordiger ook toestemming moet geven?

Hoe zit het met Recht op vergetelheid?

Participant Identification Code (i.e., hash/checksum)

Online bronnen:

https://www.digitaleoverheid.nl/dossiers/identiteit/

https://wetten.overheid.nl/BWBR0033181/2012-07-12

https://readid.com/

https://www.nictiz.nl/programmas/eid-in-de-zorg/

https://communities.surf.nl/artikel/remote-vetting-voor-surfsecureid

Ad 4-: Bewijslast en mate van identificatie

Wat moet er wel en niet als bewijs worden vastgelegd indien consent (nWMO) digitaal verkregen wordt?

Vraag naar use cases: *Beschikken jullie over praktijkvoorbeelden waarbij in overleg met jullie is overgegaan tot het digitaal verkrijgen van consent van nWMO-plichtig onderzoek en of dit consent vervolgens op een bepaalde manier moest worden vastgelegd?*

Feedback FG Leiden "De eisen daaraan hangen van de omstandigheden af. Gaat het alleen om het eenmalig afnemen van een vragenlijst dan zijn de eisen laag, vinkje op de elektronische vragenlijst.

Gaat het om terugkoppeling dan moeten we er vrij zeker van zijn dat we het aan de juiste persoon terugkoppelen

Gaat het om toestemming voor bijvoorbeeld inzage in het medisch dossier dan kan dat op dit moment nog niet elektronisch, dan zit je nl op minimaal op het niveau van digid of een gekwalificeerde elektronische handtekening. Het bewijzen van elektronische toestemming staat bij ons nl nog in de kinderschoenen ."

"De verificatie of de gegevens echt van de betrokken is voor research van groot belang maar vaak minder voor de betrokkenen aangezien verkeerde info meestal geen invloed heeft op de betrokkenen. Die scheve verhouding heeft zeker invloed hoe zaken ingeregeld zijn aangezien hoge eisen aan identificatie vaak ook weer response verlagend zijn. Maar dat is inderdaad vaak impliciet."

Feedback EC Leiden (?)

"Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

Wat dat in de praktijk inhoudt is moeilijk te zeggen, maar ik denk dat we met deze wettelijke bepaling niet al te formalistisch moeten omgaan resp. vooral naar een praktisch werkbare oplossing moeten zoeken. Ideaal zou natuurlijk zijn dat toestemming elektronisch wordt gegeven en dat zo'n voorziening is ingebed in een systeem waartoe de betrokkene alleen toegang heeft als deze zich aan de hand van diens BSN of op andere wijze heeft geïdentificeerd. Dan komt natuurlijk al snel toestemming geven via het patientenportaal in beeld..."

Feedback van RUG

De enige cases die ik tegengekomen ben als deelnemer zijn de PsyCorona en de Lifelines vragenlijsten die je persoonlijk toegestuurd worden via de e-mail en waar je in de startpagina van de vragenlijst gevraagd wordt of je echt mee wilt doen (klikken op ok is consent). De antwoorden worden gekoppeld aan de reeds verzamelde data. Ik vermoed (maar heb dat niet kunnen vinden) dat bij PsyCorona mijn e-mailadres de link is. En binnen Lifelines mijn geboortedatum (want daar wordt naar gevraagd). Ik vermoed dat die alleen in combinatie met mijn e-mail uniek genoeg is om als identificatie gebruikt te worden.

Een ander "open" voorbeeld dat wellicht gebruikt kan worden door jullie werkgroep (bekeken vanuit een Europees perspectief) is wellicht de NDAR database (https://healthdata.gov/dataset/national-database-autism-research-ndar NDAR is een (Amerikaanse) database met Autisme gerelateerde data waarbij het systeem "NDA GUID" gebruikt wordt: "a universal subject ID that allows researchers to

share data specific to a study participant without exposing personally identifiable information (PII) and makes it possible to match participants across labs and research data repositories. (...)

Meer over NDA GUID staat op: https://nda.nih.gov/training/module?trainingModuleId=training.data-submission&slideId=slide.guid

Reactie taakgroep

Zoals we zelf eerder besproken hebben is BSN wel een zwaar middel en een patiëntenportaal is niet voor handen bij niet medisch onderzoek, dus ik vind het zelf lastig wat we hiermee kunnen, behalve natuurlijk dat er een wettelijke grondslag lijkt te zijn voor het kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

Het is mij niet duidelijk in hoeverre het aantonen dat de betrokkene die toestemming heeft gegeven ook daadwerkelijk degene is over wie die de persoonsgegevens verstrekt hiertoe behoort.

(Brengt dit dan toch een wettelijke grondslag voor identificatie met zich mee en daarmee een eerdere discussie weer ter tafel? Ik kon niet vinden in hoeverre de bevestiging dat de betrokkene daadwerkelijk degene is van wie toestemming verkregen is, gekeken naar: https://europadecentraal.nl/onderwerp/informatiemaatschappij/gegevensbescherming-en-de-avg/rechtmatigheid-en-transparantie/toestemming/ en https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf

Wellicht pagina 15 en 23 extra interessant, maar iets dat al eerder door een FG onder ons bekeken is? Pag 25 benoemt een tekst rondom hoe de manier waarop toestemming verkregen wordt en de manier waarop het ingetrokken moet worden niet teveel van elkaar mogen verschillen. Impliciet wordt in deze tekst daardoor al aangegeven in welke mate het vastleggen van de toestemming al voldoende zou kunnen zijn – en nog veel implicieter dat daardoor identificatie ook alleen in die mate nodig zou hoeven zijn? –:

“Artikel 7, lid 3 van de AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat het intrekken van toestemming door de betrokkene even eenvoudig moet zijn als het geven ervan. De AVG stelt niet dat het geven en intrekken van informatie altijd plaats moet vinden door middel van dezelfde handeling. Wanneer toestemming echter wordt verkregen via elektronische middelen, door middel van slechts één muisklik, veeg of toetsenaanslag, moet de betrokkene deze toestemming, in de praktijk, ook even eenvoudig kunnen intrekken. Indien toestemming wordt verkregen door het gebruik van een dienstspecifieke gebruikersinterface (bijvoorbeeld via een website, een app, een gebruikersaccount, de interface van een IoT-apparaat of via e-mail), lijdt het geen twijfel dat de betrokkene zijn of haar toestemming moet kunnen intrekken via dezelfde elektronische interface, omdat overschakelen naar een andere interface enkel voor het intrekken van toestemming buitensporige moeite zou kosten. Voorts moet de betrokkene zijn of haar toestemming kunnen intrekken zonder nadeel. Dit betekent onder meer dat een verwerkingsverantwoordelijke het mogelijk moet maken dat toestemming kosteloos of zonder verslechtering van het serviceniveau wordt ingetrokken51 .”

Pas vanaf pag. 32 wordt het specifiek voor wetenschappelijk onderzoek, maar ook daar weer de focus op de toestemming van de betrokkene, niet de mate van identificatie van de betrokkene.

Tijdens overleg

Aantonen/vastleggen hoe je het doet, daarbij wel in ogenschouw genomen dat cliënt vrij, specifiek en ondubbelzinnig diens toestemming heeft gegeven. – Artikel 4 11 AVG: vrijwillig, specifiek, geïnformeerd, ondubbelzinnig (VSGO)

Organisatie (indien verwerkingsverantwoordelijk) is accountable

Voor identificatie: organisatie zit in principe goed indien aanpak/overwegingen goed gedocumenteerd. Dit verschilt per instelling en per type onderzoek. Maar indien binnen onderzoek identificatie nodig wordt geacht is er geen juridische grondslag om die identificatie vast te leggen. Alleen wel dat de betrokkene consent heeft gegeven.

Maar niet altijd vast te leggen wie een persoon is zonder te hebben gezien, en daarmee dus niet of de betrokkene de persoon in kwestie is

Transparantie en accountability zijn het belangrijkste.