

Informatieveiligheidscomité Kamer sociale zekerheid en gezondheid
--

IVC/KSZG/25/324

BERAADSLAGING NR. 14/094 VAN 18 NOVEMBER 2014, GEWIJZIGD OP 28 JULI 2015 EN 4 NOVEMBER 2025, BETREFFENDE DE MEDEDELING VAN GEPSEUDONIMISEERDE PERSOONSGEGEVENS DIE DE GEZONDHEID BETREFFEN DOOR WACHTPOSTEN, DOOR APOTHEKEN AANGESLOTEN BIJ DE KONINKLIJKE APOTHEKERSVERENIGING VAN ANTWERPEN (KAVA) EN DOOR SPOEDDIENSTEN AAN HET CENTRUM VOOR HUISARTSENGENEESKUNDE VAN DE UNIVERSITEIT ANTWERPEN IN HET KADER VAN HET ICAREDATA-PROJECT

Het Informatieveiligheidscomité, kamer sociale zekerheid en gezondheid (hierna “het Comité” genoemd);

Gelet op de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming);

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*;

Gelet op de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*;

Gelet op de definitieve machtigingsaanvragen ontvangen op 13 oktober 2014 en 5 juni 2015 en 30 mei 2025;

Gelet op het auditoraatsrapport van het eHealth-platform;

Gelet op het verslag van de heer Michel Deneyer.

Beslist op 18 november 2014, op 28 juli 2015 en op 4 november 2025, na beraadslaging, als volgt:

I. ONDERWERP VAN DE AANVRAAG

1. Het Centrum voor Huisartsengeneeskunde, Vakgroep Eerstelijns- en Interdisciplinaire Zorg van de Faculteit Geneeskunde en Gezondheidswetenschappen van de Universiteit Antwerpen (CHA-ELIZA) legt het Comité ter goedkeuring de mededeling van gepseudonimiseerde persoonsgegevens door wachtposten en, in een tweede fase, door de apotheken aangesloten bij de Koninklijke Apothekersvereniging van Antwerpen (KAVA), door de spoeddiensten van het Universitair Ziekenhuis Antwerpen en van de twee grootste ziekenhuisketens van Antwerpen en, in een derde fase, door de leverancier van een digitaal zelftriagesysteem voor in het kader van de oprichting van een klinische research gegevensdatabank, *Improve Care and Research Electronic Data Trust Antwerp* (iCAREdata) genaamd.
2. Het doel van het project is om onderzoek naar de zorg buiten de normale werkuren (out-of-hours, OOH) mogelijk te maken en de kwaliteit van OOH-zorg te verbeteren. Momenteel mogen de gegevens van een patiëntencontact in een wachtpost niet langer dan 18 maanden worden bewaard, waardoor ze slechts voor een korte periode beschikbaar zijn voor onderzoek. Door het onderzoeksproject iCAREdata zal het mogelijk zijn om deze gegevens op gepseudonimiseerde wijze langduriger en daardoor diepgaander te kunnen onderzoeken.
3. In een tweede fase laten de persoonsgegevens van de apotheken aangesloten bij KAVA en van een aantal spoeddiensten toe om een duidelijk beeld te krijgen van de geneesmiddelen afgeleverd op voorschrift en van de medische hulp die door de spoeddiensten geboden wordt buiten de normale werkuren.
4. In een derde fase laten de persoonsgegevens van triagesystemen, inclusief zelf-triage of zelf-evaluatie voor de patiënt¹ toe om de zorgvraag mee in kaart te brengen die vooraf gaat aan een zorgcontact (huisartsenwachtpost, apotheek van wacht of spoedgevallen dienst). Vervolgens kan de patiëntenflow doorheen het niet-planbare zorgsysteem in kaart gebracht worden na het doorlopen van triage. Dit stelt in staat om de volgende doeleinden in kaart te brengen: de gevolgen en invloeden van het implementeren van triagesystemen op patiëntencontacten met de niet-planbare zorgvoorzieningen, de effectiviteit en accuraatheid (medische veiligheid) van triage, de naleving van triage adviezen en de impact van triagesystemen (op de werkbelasting in niet-planbare zorgsysteem, op 'oneigenlijke gebruik' van niet-planbare zorgsysteem, op de pathologieverdeling tussen de verschillende diensten en op de zorgvraag).
5. De gepseudonimiseerde persoonsgegevens worden geanalyseerd door onderzoekers van het CHA-ELIZA. Het onderzoek kan worden uitgevoerd op initiatief van CHA-ELIZA of op vraag van externe onderzoekers.

¹ www.moetiknaardedokter.be

6. De benodigde persoonsgegevens worden op automatische wijze ingezameld bij de deelnemende wachtposten in het softwareprogramma van de wachtpost. Hetzelfde softwareprogramma wordt ook gebruikt om de persoonsgegevens in te zamelen bij de apotheken aangesloten bij KAVA en bij de betrokken spoeddiensten. De persoonsgegevens worden vervolgens via de eHealth-box overgemaakt aan het eHealth-platform dat als *trusted third party* (TTP) tussenkomt voor de codering van de identificatiegegevens van de patiënt en de betrokken zorgverleners, alvorens de gepseudonimiseerde persoonsgegevens worden meegedeeld aan het CHA-ELIZA. De patiënten worden geïnformeerd via een affiche in de wachtzaal of aan de ingang van de apotheek en de arts of apotheker kan nadere informatie verstrekken. De patiënt heeft de mogelijkheid om deelname te weigeren en de huisarts of de apotheker kan de weigering registreren in het elektronisch medisch dossier.
7. Volgende gepseudonimiseerde persoonsgegevens die de gezondheid betreffen worden per betrokken patiënt meegedeeld:

Patiëntgegevens:

- het identificatienummer van de sociale zekerheid (INSZ) dat wordt gepseudonimiseerd door de TTP. Indien de patiënt geen INSZ bezit, wordt een nummer door de TTP toegekend.
- geboortedatum van de patiënt, dat wordt gepseudonimiseerd door de TTP.
- geboortjaar patiënt
- geslacht patiënt
- postcode woonplaats patiënt
- code verzekerbaarheid patiënt

Contactgegevens:

- identificatie contact,² gepseudonimiseerd door TTP
- identificatie wachtpost
- datum en tijdstip contact en start behandeling, wijze van contacteren, type contact, urgentieraad
- RIZIVnummer arts die contact behandelt, gepseudonimiseerd door TTP
- Eventuele verwijzing, al dan niet arbeidsongeschiktheid

Morbiditeitsgegevens:

- Diagnose
 - o Datum, contactreden (thesarusterm en code), diagnose (thesaurusterm en code)
 - o Vrij tekstveld met subjectieve klachten patiënt
 - o Vrij tekstveld met vaststellingen onderzoek
- Medicatievoorschriften
 - o Datum, naam medicatie, CNK-code

8. De apotheken zullen de volgende persoonsgegevens betreffende de gezondheid meedelen:

² In het EMD van de wachtpost krijgt ieder contact met een patiënt een nummer toegewezen.

- identificatie van de apotheek;
- RIZIV-nummer van de voorschrijvende arts, gepseudonimiseerd door de TTP;
- INSZ van de patiënt, gepseudonimiseerd door de TTP;
- datum en tijdstip van aflevering van het geneesmiddel;
- CNK-code van het geneesmiddel.

9. De spoeddiensten zullen de volgende gegevens meedelen:

Gegevens met betrekking tot de patiënt:

- INSZ van de patiënt, gepseudonimiseerd door de TTP (als de patiënt geen INSZ heeft, zal de TTP hem een nummer toekennen);
- het geboortjaar van de patiënt;
- het geslacht van de patiënt;
- de postcode van het domicilie van de patiënt;
- de verzekerbaarheidscode van de patiënt.

Contactgegevens:

- identificatie van het contact, gepseudonimiseerd door de TTP;
- identificatie van de spoeddienst;
- RIZIV-nummer van de arts, gepseudonimiseerd door de TTP;
- de datum en het tijdstip van het contact met de spoeddiensten en van het begin van het onderzoek, de wijze van contactname, het type contact en de mate van spoed;
- de eventuele behandeling.

Gegevens inzake morbiditeit:

- diagnose:
 - o de datum, het motief van het contact (term uit de thesaurus en code), diagnose (term uit de thesaurus en code);
 - o vrije tekst met de beschrijving van de subjectieve klachten van de patiënt;
 - o vrije tekst met de vaststellingen voortvloeiend uit het onderzoek;
- geneesmiddelenvoorschriften:
 - o datum, naam van het geneesmiddel, CNK-code.

10. De triagesystemen zullen de volgende gegevens meedelen:

Gegevens met betrekking tot de patiënt:

- geboortedatum van de patiënt, dat wordt gepseudonimiseerd door de TTP.
- geboortjaar van de patiënt;
- geslacht van de patiënt.

Contactgegevens:

- taalcode van de triage;
- wachtpostregio.

Gegevens inzake morbiditeit:

- lichaamsregio met klacht (triage hoofdstuk);
 - aanmeldingsklacht;
 - toegekende urgentiegraad na triage;
 - verwijlsadvies;
 - gegeven advies;
11. Een “comma separated value”-bestand (csv-bestand) wordt aangemaakt op de server of de computer van de wachtposten, van de Koninklijke Apothekersvereniging van Antwerpen (KAVA) die de database van de apotheken beheert, op de server van de spoeddiensten en op de server van de leverancier van het triagesysteem. De KAVA deelt enkel de gegevens mee die betrekking hebben op patiënten die door een wachtpost of door een spoeddienst gezien werden, op basis van de identificatienummers van de patiënten die ontvangen werden tijdens de wachtdienst en die door de deelnemende wachtposten of spoeddiensten meegedeeld werden.
 12. De eerste vier kolommen van het csv-bestand van de wachtpost en spoeddienst bevatten opeenvolgend het INSZ-nummer van de patiënt, het RIZIV-nummer van de arts, de geboortedatum van de patiënt en de identificatiecode van het contact. Deze drie kolommen worden gescheiden door een puntkomma van de volgende kolommen die de medische informatie bevatten. Deze kolommen met medische informatie worden voor verzending geëncrypteerd. Dit csv-bestand wordt beveiligd verzonden naar eHealth voor codering via de eHealthBox. Nadien worden de gepseudonimiseerde bestanden beveiligd verzonden naar de eHealthBox van iCAREdata.
 13. De eerste kolom van het csv-bestand van het triagesysteem bevat de geboortedatum van de gebruiker. Deze kolom wordt gescheiden door een puntkomma van de volgende kolommen die de medische informatie bevatten. Deze kolommen met medische informatie worden voor verzending geëncrypteerd. Dit csv-bestand wordt beveiligd verzonden naar eHealth via het UZA voor codering via de eHealthBox. Nadien worden de gepseudonimiseerde bestanden beveiligd verzonden naar de eHealthBox van iCAREdata.
 14. In deze eHealthBox worden de eerste vier kolommen van het csv-bestand van de zorgverstrekkers en de eerste kolom van het csv-bestand van het triagesysteem gepseudonimiseerd door eHealth. Dit gebeurt met een algoritme dat enkel gekend is door het eHealthplatform. Dit is een reversibel algoritme. De geëncrypteerde velden met medische informatie, kunnen niet gelezen worden door het eHealthplatform aangezien het niet over de sleutel voor decryptie beschikt. Het bestand met gepseudonimiseerde identificatievelden en geëncrypteerde medische velden, wordt op regelmatige tijdstippen opgehaald door de server van de UA vanuit de eHealthBox.
 15. Op de server van de UA worden door de onderzoekersploeg van iCAREdata de medische velden gedecrypteerd, de identificatievelden blijven gepseudonimiseerd.

Met deze werkwijze kan het eHealth-platform geen medische gegevens lezen en kan de onderzoekersploeg van iCAREdata geen gegevens identificeren.

16. Teneinde de heridentificatie aan de hand van de combinatie van gepseudonimiseerde persoonsgegevens te vermijden, wordt een small cells risk analyse uitgevoerd in samenwerking met de Technische cel. Indien nodig zullen bepaalde gepseudonimiseerde persoonsgegevens worden geaggregeerd om te voorkomen dat de betrokkenen zouden kunnen worden geïdentificeerd.
17. Voor het beheer van de iCAREdata-gegevensbank werden twee adviesraden opgericht: een wetenschappelijk comité en een stuurcomité. Het wetenschappelijk comité is samengesteld uit vertegenwoordigers van het CHA-ELIZA (artsen), vertegenwoordigers van de meewerkende wachtposten, van KAVA en de spoeddiensten, een vertegenwoordiger van de UA-Herculesstichting en een patiëntenvertegenwoordiger. Het controleert de ontvankelijkheid en haalbaarheid van onderzoeksvragen. Het weert aanvragers met niet-wetenschappelijke, zuiver commerciële doelstellingen. Het controleert de kwaliteit van de verzamelde gegevens en de geleverde output door iCAREdata. Het stuurcomité is op zijn beurt samengesteld uit de supervisor, promotor, copromotor van het iCAREdata-project, de databeheerder (arts) en de betrokken CHA-leden, evenals een vertegenwoordiger van UA-Herculesstichting. De dataleveranciers kunnen actief of passief deelnemen aan de vergaderingen. Het is verantwoordelijk voor het management van iCAREdata (constructie en onderhoud van de infrastructuur), voor de opvolging van de werking van de infrastructuur (incl. website), beoordeling van de loggings, het financieel management, de feedback naar Herculesstichting, het onderhoud van contacten en het verzorging van de communicatie, de reactie op klachten en het behandelen van aanvragen tot opting-out (onderzoekers, artsen, patiënten, derden), de opvolging van het advies van het wetenschappelijk comité.
18. De gepseudonimiseerde persoonsgegevens van het iCAREdata-project worden wetenschappelijk geanalyseerd op initiatief van onderzoekers binnen het CHA-ELIZA en verbonden aan het iCAREdata-project dan wel op vraag van externe onderzoekers. De externe onderzoekers kunnen enkel de resultaten van de analyses (al dan niet in de vorm van aggregaties) ontvangen. Er worden géén gepseudonimiseerde persoonsgegevens meegedeeld aan externe onderzoekers zonder bijkomende machtiging van de afdeling gezondheid van het Comité.
19. Onderzoekers die niet verbonden zijn aan het CHA-ELIZA, moeten een specifieke aanvraag indienen, waarna een overeenkomst wordt opgesteld met betrekking tot de gevraagde analyses. Deze overeenkomsten worden in beide adviesraden besproken.
20. Het RIZIV-nr. van de betrokken artsen wordt reversibel gepseudonimiseerd. Zodoende kan, via de tussenkomst van het eHealth-platform, tot depseudonimisering worden over gaan doch uitsluitend met betrekking tot het gepseudonimiseerde RIZIV-nr. van de geneesheren in kwestie teneinde de nodige feedback aan de betrokken geneesheer te kunnen verstrekken. Zo kan bijvoorbeeld aan een

individuele arts meegedeeld worden, hoeveel en welke antibiotica hij voorschrijft bij een bepaalde infectie. De onderzoekers hebben op geen enkel ogenblik kennis van de identiteit van de betrokken geneesheren.

21. De gegevensbank van de iCAREdata-project wordt bewaard op een server die zich bevindt in een serverroom op Campus Middelheim van de Universiteit Antwerpen. Deze ruimte is fysiek enkel toegankelijk voor een beperkt aantal ICT medewerkers. De toegang tot de eigenlijke databank is beperkt tot de databeheerder (geneesheer) en een ICT-medewerker (bio-informaticus) van het iCAREdata-project. Ze hebben enkel toegang via een beveiligde verbinding. Veiligheidsloggings betreffende de toegang tot de gegevensbank worden genomen.

II. BEVOEGDHEID

22. Overeenkomstig artikel 42, § 2, 3°, van de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid* vereist iedere mededeling van persoonsgegevens die de gezondheid betreffen, behoudens de voorziene uitzonderingen, een principiële machtiging van de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité.
23. De mededeling van gepseudonimiseerde persoonsgegevens die de gezondheid betreffen door wachtposten aan het CHA-ELIZA met het oog op de samenstelling van een register voor onderzoeksdoeleinden valt niet onder één van voormelde uitzonderingen, en vereist bijgevolg een machtiging van het Comité.
24. Met toepassing van artikel 5, § 1, van de wet *houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren*, is het Comité bevoegd om een machtiging te verlenen voor het gebruik van het rijksregisternummer wanneer het een beslissing neemt omtrent een persoonsgegevensstroom. De verzending van de identificatienummers van de patiënten ontvangen door de wachtposten en de spoeddiensten naar KAVA, zoals beschreven in punt 9, kan aldus worden gemachtigd.

III. BEHANDELING VAN DE AANVRAAG

A. TOELAATBAARHEID

25. De verwerking van persoonsgegevens die de gezondheid betreffen is in principe verboden, overeenkomstig artikel 9, § 1, van de Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (AVG). Dit verbod geldt echter niet, zoals in casu het geval is, wanneer de verwerking noodzakelijk is met het oog op archivering in het algemeen belang,

wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en belangen van de betrokkene.

26. Volgens artikel 5 van de AVG moeten de persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Ze moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden ingezameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.
27. Het doeleinde van de gegevensverwerking is de samenstelling van een databank met gepseudonimiseerde gezondheidsgegevens om wetenschappelijk onderzoek mogelijk te maken. De Universiteit Antwerpen heeft als zelfstandige universiteit overeenkomstig haar statuten onder andere specifieke wetenschappelijke onderzoeksopdrachten te vervullen. Gelet op het voorgaande stelt het Comité dan ook vast dat de beoogde verwerking een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde heeft.

B. MINIMALE GEGEVENSVERWERKING

28. Volgens artikel 5 van de AVG moeten de persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
29. Wat de verzamelde gepseudonimiseerde gezondheidsgegevens betreft, neemt het Comité akte van het feit dat er slechts een beperkt aantal rechtstreeks identificerende persoonsgegevens worden verzameld, meer bepaald het geboortjaar, het geslacht, en de postcode van de woonplaats. Iedere patiënt wordt uniek geïdentificeerd aan de hand van een INSZ dat wordt gepseudonimiseerd door het eHealth-platform. De gezondheidsgegevens zelf beslaan de diagnose en het medicatiegebruik. Het Comité stelt vast dat het beoogde klinisch onderzoek door het CHA-ELIZA wel degelijk specifieke informatie vereist over de incidentie en prevalentie van ziekten en medicatie, evenals gegevens over het contact met de wachtpost of de spoeddienst. De aanvrager stelt dat de beschreven gegevens toelaten dat uiteenlopende onderzoeksvragen betreffende de OOH-zorg kunnen worden behandeld. De meta-analyse van de gegevens kan een beter inzicht geven in de werking van de wachtposten en de spoeddiensten.
30. Een latere verwerking van persoonsgegevens voor wetenschappelijke doeleinden dient in principe plaats te vinden aan de hand van anonieme gegevens. Indien het doeleinde niet kan worden verwezenlijkt met anonieme gegevens, mogen gepseudonimiseerde persoonsgegevens worden verwerkt. Gelet op het feit dat het noodzakelijk is dat een patiënt uniek wordt geïdentificeerd en het noodzakelijk is een

patiënt te kunnen opvolgen in de tijd, is het aanvaardbaar dat met gepseudonimiseerde persoonsgegevens wordt gewerkt.

31. Wat de verwerking van de gepseudonimiseerde persoonsgegevens op vraag van externe onderzoekers betreft, stelt het Comité vast dat de wetenschappelijke analyses die nodig zijn voor het beantwoorden van de onderzoeksvragen door de onderzoekers van het CHA-ELIZA verbonden aan het iCAREdata-project betreft zelf worden uitgevoerd. Iedere mededeling van gepseudonimiseerde persoonsgegevens die de gezondheid betreffen uit de gegevensbank van het iCAREdata-project wordt voorafgaandelijk ter goedkeuring aan het Comité voorgelegd.
32. Gelet op het voorgaande acht het Comité de verwerking van de beoogde persoonsgegevens toereikend, terzake dienend en niet overmatig in het licht van de beoogde doeleinden.

C. OPSLAGBEPERKING

33. Volgens artikel 5, § 1, e) van de AVG moeten persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, § 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking"). De aanvrager voorziet in een bewaartermijn van 30 jaar vanaf de opname in de gegevensbank. Deze bewaartermijn moet toelaten om evoluties in de tijd te bestuderen. De aanvrager stelt dat de OOH-zorg een relatief recent fenomeen is en dat de werking een onvoorziene richting kan nemen. Ook trends in voorschrijfgedrag kunnen enkel na jaren worden bestudeerd. Het Comité aanvaardt dan ook de voorgestelde bewaartermijn.

D. TRANSPARANTIE

34. Overeenkomstig artikel 12 van de AVG moet de verwerkingsverantwoordelijke passende maatregelen nemen opdat de betrokkene informatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt. De informatie moet schriftelijk of met andere middelen, met inbegrip van elektronische middelen indien dit passend is, worden verstrekt.
35. Wanneer de persoonsgegevens niet bij de betrokkene werden verkregen, verstrekt de verwerkingsverantwoordelijke hem/haar alle informatie bedoeld in artikel 14, § 1 en § 2 van de AVG.

36. De aanvrager voorziet in een kennisgeving van de gegevensverwerking aan de betrokkene door middel van een affiche in de wachtzaal of in de apotheek (op een opvallende plaats, duidelijk leesbaar) en de mogelijkheid van nadere informatieverstrekking door de huisarts tijdens de consultatie of door de apotheker. Er wordt in de kennisgeving via de affiche eveneens verwezen naar voorliggende beraadslaging.
37. Het Comité acht de voorziene kennisgeving voldoende.

E. INFORMATIEVEILIGHEID

38. De verwerking van persoonsgegevens die de gezondheid betreffen moet gebeuren onder het toezicht en de verantwoordelijkheid van beroepsbeoefenaar in de gezondheidszorg. Het Comité stelt vast dat er een arts werd aangesteld die verantwoordelijk is voor de verwerking van de persoonsgegevens die de gezondheid betreffen. Het Comité herinnert er aan dat de beroepsbeoefenaar in de gezondheidszorg en zijn aangestelden of gemachtigden bij de verwerking van persoonsgegevens tot geheimhouding verplicht zijn.
39. Krachtens artikel 5, § 1, f) van de AVG moeten persoonsgegevens, door het nemen van passende technische of organisatorische maatregelen, op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwelijkheid). Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.
40. Om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te garanderen, moet iedere instelling die persoonsgegevens bewaart, verwerkt of meedeelt afhankelijk van de context en de aard van de persoonsgegevens maatregelen nemen in de volgende elf actiedomeinen die betrekking hebben op de informatieveiligheid: veiligheidsbeleid; aanstelling van een functionaris voor gegevensbescherming; organisatorische en menselijke aspecten van de veiligheid (vertrouwelijkheidsverbintenis van het personeel, regelmatige informatieverstrekking en opleidingen ten behoeve van het personeel inzake bescherming van de privacy en veiligheidsregels); fysieke veiligheid en veiligheid van de omgeving; netwerkbeveiliging; logische toegangs- en netwerkbeveiliging; loggings, opsporing en analyse van de toegangen; toezicht, nazicht en onderhoud; systeem van beheer van de veiligheidsincidenten en de continuïteit (backup-systemen, fault tolerance-systemen, ...); naleving en documentatie. Het Comité neemt akte van het feit dat de aanvrager bevestigt dat een functionaris voor gegevensbescherming werd aangesteld. De lokalen waar de gepseudonimiseerde persoonsgegevens worden opgeslagen zijn beveiligd en zijn slechts toegankelijk voor daartoe gemachtigde personen. De toegang 'on-campus' via het netwerk tot de server

is strikt geregeld en gebeurt op basis van IP adres en accountgegevens. De gebruikte protocollen worden, waar mogelijk, beveiligd door middel van SSL. Remote toegang tot de server is enkel mogelijk via SSL VPN-toegang en op grond van specifieke toegangsrechten. De toegang wordt eveneens gelogd. De server is voorzien van redundante onderdelen: dubbele voeding, RAID technologie, automatische monitoring van hardware en het nemen van backups.

41. Het Comité herinnert eraan dat krachtens artikel 9 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens de verwerkingsverantwoordelijke de volgende bijkomende maatregelen neemt bij de verwerking van genetische, biometrische of gezondheidsgegevens:
 - 1° hij of, in voorkomend geval, de verwerker wijst de categorieën van personen die toegang hebben tot de persoonsgegevens aan waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig wordt omschreven;
 - 2° hij of, in voorkomend geval, de verwerker houdt de lijst van de aldus aangewezen categorieën van personen ter beschikking van de bevoegde toezichthoudende autoriteit;
 - 3° hij zorgt ervoor dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen.
42. Het Comité acht het noodzakelijk eraan te herinneren dat het Centrum voor Huisartsengeneeskunde, Vakgroep Eerstelijns- en Interdisciplinaire Zorg van de Faculteit Geneeskunde en Gezondheidswetenschappen van de Universiteit Antwerpen (CHA-ELIZA) sedert 25 mei 2018 de bepalingen en de principes moet naleven van Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). Deze instanties moeten tevens de bepalingen naleven van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Om deze redenen besluit,

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

dat de mededeling van de persoonsgegevens zoals beschreven in deze beraadslaging toegestaan is mits er wordt voldaan aan de in deze beraadslaging vastgestelde maatregelen ter waarborging van de gegevensbescherming, in het bijzonder de maatregelen op het vlak van doelbinding, minimale gegevensverwerking, opslagbeperking en informatieveiligheid.

Het eHealth-platform wordt gemachtigd om het verband tussen het gepseudonimiseerd nummer en het reële identificatienummer te bewaren gelet op het longitudinaal karakter van het project. Bovendien wordt het eHealth-platform gemachtigd om tot depseudonimisering over te gaan doch uitsluitend met betrekking tot het gepseudonimiseerde RIZIV-nr. van de artsen in kwestie teneinde de nodige feedback aan de betrokken arts te kunnen verstrekken. Hierbij mogen nooit (al dan niet gepseudonimiseerde) persoonsgegevens betreffende de individuele patiënten worden meegedeeld.

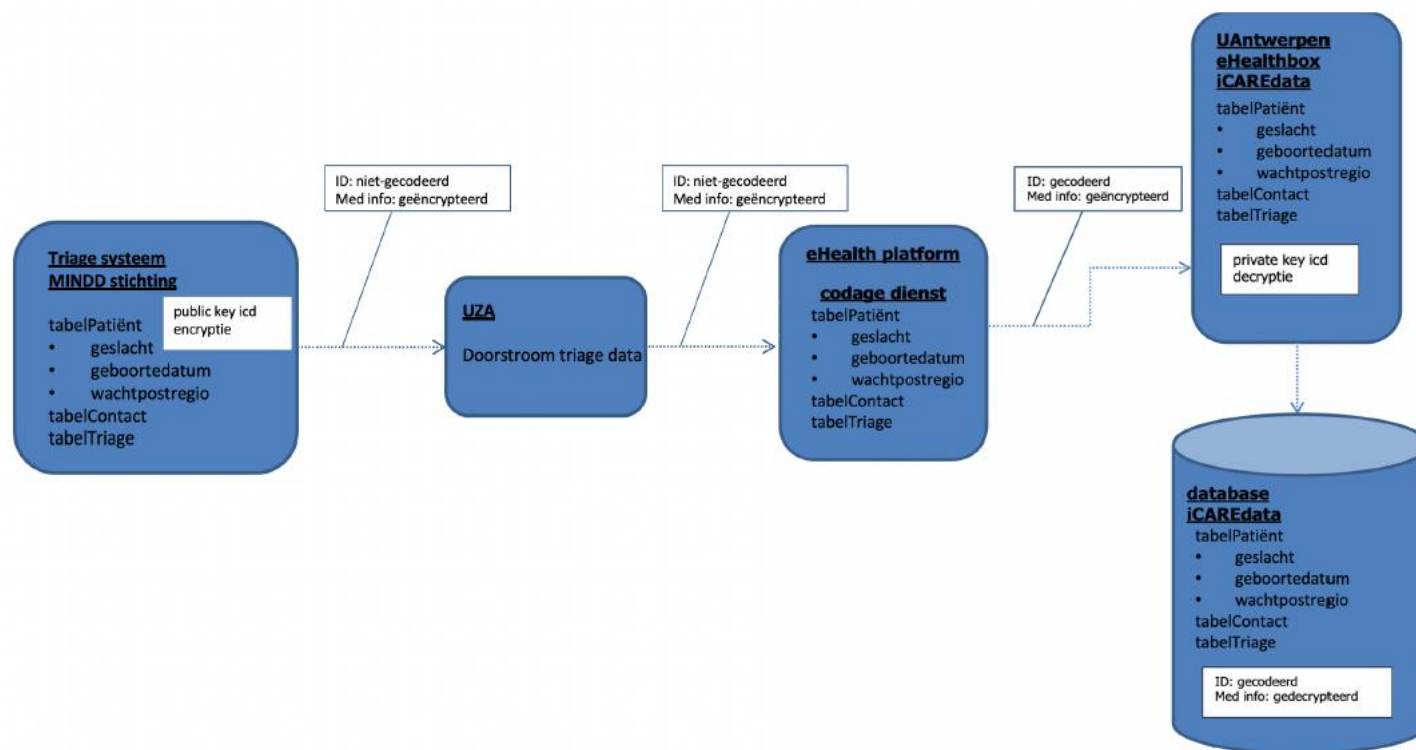
De wijzigingen van deze beraadslaging die door het informatieveiligheidscomité werden goedgekeurd op 4 november 2025 treden in werking op 20 november 2025.

Michel DENEYER
Voorzitter

De zetel van de kamer Sociale Zekerheid en Gezondheid van het Informatieveiligheidscomité is gevestigd in de kantoren van de Kruispuntbank van de Sociale Zekerheid, op het volgende adres: Willebroekkaai 38 – 1000 Brussel (tel. 32-2-741 83 11).

Bijlage: schematische voorstelling stroom

Schematische voorstelling extra datastroom betreffende de triagesystemen



Schematische voorstelling van alle datastromen

