Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/23/206

BERAADSLAGING NR. 10/085 VAN 21 DECEMBER 2010, LAATST GEWIJZIGD OP 7 DECEMBER 2021 EN 12 MEI 2023, MET BETREKKING TOT DE ORGANISATIE VAN DE MEDEDELING VAN ELEKTRONISCHE AMBULANTE VOORSCHRIFTEN IN HET KADER VAN RECIP-E EN DE WEBTOEPASSING PARIS

Het Informatieveiligheidscomité;

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 of AVG);

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 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, in het bijzonder artikel 114, gewijzigd bij de wet van 25 mei 2018;

Gelet op de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid*, in het bijzonder artikel 42 §2 2° a), gewijzigd bij de wet van 5 september 2018;

Gelet op de wet van 5 september 2018 *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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,* in het bijzonder artikel 97;

Gelet op beraadslaging nr. 12/047 van 19 juni 2012 laatst gewijzigd op 18 april 2017 en 18 juli 2017 met betrekking tot de geïnformeerde toestemming van een betrokkene met de elektronische uitwisseling van zijn persoonsgegevens die de gezondheid betreffen en de wijze waarop deze toestemming kan worden geregistreerd

Gelet op artikel 11 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*;

Gelet op de beraadslaging nr. 10/085 van 21 december 2010 en de gewijzigde versies van 15 december 2015, 16 januari 2018 en 7 december 2021;

Gelet op het auditoraatsrapport van het eHealth-platform van 1 december 2021;

Beslist op 12 mei 2023, na beraadslaging, als volgt:

I. VOORWERP VAN DE AANVRAAG

i. RECIP-E

1. Het Rijksinstituut voor ziekte- en invaliditeitsverzekering (hierna genoemd: *"het RIZIV"*) implementeert met het project Recip-e het gebruik van het elektronische ambulante voorschrift. In de eerste fase bestond het doel van het project er in het in België ontwikkelde model voor elektronische ambulante voorschriften in de praktijk te brengen, te testen in een aantal regio's en aan de hand van deze ervaringen de nationale uitrol ervan voor te bereiden. In de huidige fase is de nationale uitrol van Recip-e volop bezig voor wat huisartsen en apothekers betreft. Tevens wordt het elektronisch ambulant voorschrift vanuit een ziekenhuis geïmplementeerd. Tot slot is Recip-e ook beschikbaar voor tandartsen en vroedvrouwen enerzijds en kinesitherapeuten en verpleegkundigen anderzijds respectievelijk als voorschrijvers en uitvoerders van een voorschrift.

2. Gelet op het juridisch kader van het elektronische ambulante voorschrift zoals voorzien in artikel 42 van de gecoördineerde wet van 10 mei 2015 betreffende de uitoefening van gezondheidszorgberoepen, is het vereist dat de elektronische ambulante voorschriften op elektronische wijze kunnen worden uitgewisseld tussen de zorgverlener die het voorschrift heeft aangemaakt en de zorgverlener die door de patiënt is gekozen om het voorschrift uit te voeren.

3. Om de benodigde architectuur voor de uitwisseling van de elektronische ambulante voorschriften te organiseren, heeft het Comité van de verzekering voor geneeskundige verzorging van het RIZIV in 2009 een publieke oproep voor een technische partner gelanceerd. Deze oproep werd beantwoord door de vzw Recip-e, waarvan de leden bestaan uit diverse wettelijk erkende representatieve beroepsorganisaties van zorgverleners[1]. Deze vzw heeft overeenkomstig haar statuten de volgende doelstellingen:
   - het optreden als contractuele partner voor het pilootproject "Ambulant elektronisch voorschrift";
   - het begeleiden, realiseren en beheren van het Recip-e systeem voor het elektronisch voorschrift voor de diverse zorgberoepen;
   - het optreden als overlegorgaan met het oogmerk zoveel mogelijk gezamenlijke standpunten in te nemen inzake het elektronisch voorschrijven, binnen de bredere context van ICT in de gezondheidszorg, inclusief het ontwikkelen van concepten en modellen.

[1] Algemene Pharmaceutische Bond / Association Pharmaceutique Belge, Belgische vereniging van artsensyndicaten / Association Belge des Syndicats Médicaux, Vereniging der Coöperatieve Apotheken van België / Office des Pharmacies coopératives de Belgique, KARTEL (ASGB – GBO – MoDeS) / CARTEL (ASGB – GBO – SBGS/SBMS), AADM, AXXON, Nationaal Verbond van Katholieke Vlaamse Verpleegkundigen en Vroedvrouwen, Verbond der Vlaamse Tandartsen.

4. In het kader van het voormelde project heeft de vzw Recip-e de volgende architectuur voor de uitwisseling van elektronisch ambulante voorschriften tussen de betrokken actoren uitgewerkt, meer bepaald tussen een voorschrijver *buiten* een ziekenhuis en de verstrekker van de voorgeschreven zorg dan wel tussen een voorschrijver *in* een ziekenhuis en een verstrekker van de voorgeschreven zorg.

5. De elektronische Recip-e gegevensstroom voor de uitwisseling van elektronisch ambulante voorschriften bestaat *in concreto* uit vier verschillende stromen:
   - van de voorschrijver naar de Recip-e tijdelijke opslag;
   - van de tijdelijke opslag naar de verstrekker van de voorgeschreven zorg;
   - eventuele feedback vanwege de zorgverlener naar de voorschrijver;
   - eventuele verwittiging vanwege de voorschrijver aan een zorgverstrekker dat een voorschrift in aantocht is, indien de patiënt dit wenst.

6. Gedurende een beperkte tijd blijft tijdens de nationale uitrol nog een papierstroom bestaan. De actuele voorschriften, afgedrukt op papier, met daaraan toegevoegd een uniek identificatienummer per voorschrift (in barcodeformaat en in leesbare tekst), worden door de voorschrijver aan de patiënt gegeven die het op zijn beurt aflevert aan de zorgverstrekker van zijn keuze en met de correcte competentie (apotheker voor geneesmiddelenvoorschriften, kinesitherapeuten voor kine-voorschriften en verpleegkundigen voor verpleegkundige voorschriften). Daarnaast bestaat er ook een gedematerialiseerde weg. De voorschrijver print het voorschrift niet af. De apotheker kan ook met eID/ rijksregisternummer alle openstaande voorschriften ophalen of een App wordt aangeboden en het specifieke voorschrift wordt opgehaald analoog als met papier.

7. Het voorschrift zal op elektronische wijze worden aangemaakt door de voorschrijver, zijnde een arts of een tandarts of een vroedvrouw, door middel van zijn software. Ingeval de voorschrijver een ambulant voorschrift niet in zijn eigen praktijk maar in een ziekenhuis aanmaakt, zal de software waarmee dat gebeurt de EMD software van het ziekenhuis zijn. Het voorschrift dient conform te zijn aan de geldende wettelijke bepalingen. Het Comité wijst erop dat de huidige beraadslaging zich beperkt tot de evaluatie van de verwerking van persoonsgegevens in het kader van de elektronische mededeling van het voorschrift en niet zal ingaan op de samenstelling van het elektronisch ambulante voorschrift zelf.

8. Wat de authenticatie van de voorschrijver betreft, vraagt de softwaremodule van de voorschrijver via het eHealth platform een SAML-token aan voor een sessie. De geldigheidsduur van de sessie is beperkt in de tijd. Dit SAML-token fungeert als bewijs voor de systemen dat de gebruiker een geldige voorschrijver is. Identificatie-informatie wordt enerzijds verkregen via het 'Holder-of-Key'[2] certificaat dat de gebruiker van de toepassing authentiseert en dat door eHealth uitgereikt is. Dit certificaat bevat de identiteit van de verantwoordelijke voor het beheer van de toepassing. Anderzijds wordt ook identificatie-informatie verkregen via de identificatie (INSZ) van de voorschrijver zelf die de sessie opstartte.

[2] Holder of Key: technisch certificaat dat delegatie van de identiteit aan dit lokaal geïnstalleerd certificaat mogelijk maakt.

9. Een onderscheid dient hier te worden gemaakt tussen enerzijds een ambulant medisch voorschrift dat gemaakt wordt op het systeem van een individuele voorschrijver en anderzijds een ambulant medisch voorschrift dat gemaakt wordt vanuit een ziekenhuis, opgesteld vanuit een ziekenhuissysteem (EMD).

9.1. In de eerste situatie wordt door middel van de artsensoftware de identificatie-informatie van de voorschrijver verkregen via zijn identificatie (INSZ), hetzij door middel van zijn/haar eID (met ingave van de PIN code), hetzij door middel van het persoonlijke encryptiecertificaat (eHealth-certificaat) en de bijhorende private sleutel (die hier dan dienst doen als middel voor de authenticatie van de identiteit van de titularis), toegekend door het eHealth-platform. Voor deze laatste methode dient de gebruiker een paszin voor zijn private sleutel in te geven.

9.2. In de situatie van een ambulant medisch voorschrift dat binnen een ziekenhuis wordt opgemaakt voor uitvoering buiten het ziekenhuis (bijvoorbeeld in een publieke apotheek), staat het ziekenhuis garant voor de naspeurbaarheid van de correcte en éénduidige identificatie van de voorschrijver met betrekking tot elk voorschrift dat binnen het ziekenhuis gemaakt werd. Het ziekenhuis dat via het 'Holder-of-Key'-certificaat verantwoordelijk en aansprakelijk is voor het beheer van de (voorschrijf)toepassing, garandeert te allen tijde de correcte identificatie-informatie van de voorschrijver van een bepaald voorschrift te bewaren en deze onomstotelijk te kunnen aantonen, indien daarom gevraagd wordt. De identificatie van de voorschrijver van elk uniek voorschrift wordt gewaarborgd volgens het concept van vertrouwenscirkels[3] en door de combinatie van de beschikbare identificatie-informatie in enerzijds het 'Holder-of-Key' certificaat dat de eigenaar van de toepassing authentiseert, en anderzijds het toegangs- en loggingsbeheer vanwege het ziekenhuis en de voorschrijversidentiteit (natuurlijk persoon) die zich in het vercijferde gedeelte van het voorschrift bevindt en door het ziekenhuis kan ontcijferd worden.

De logging in het ziekenhuis dient het unieke Recip-e identificatienummer (RID) te bevatten van elk ambulant voorschrift dat werd verzonden. Door de Recip-e voorschriften (analoog aan de intra-muros voorschriften) na toepassing van de hashingfunctie in het ziekenhuis periodiek te groeperen in een 'timestamp bag' vooraleer deze aan de dienst voor elektronische datering van het eHealth-platform aan te bieden, wordt gewaarborgd dat het voorschrift niet meer onmerkbaar gewijzigd kan worden na de toepassing van de elektronische datering.

Zowel het ziekenhuis zelf als de controle-instanties beschikken over de mogelijkheid om de elektronische voorschriften nadien opnieuw te hashen en na te gaan of het hashresultaat overeenkomt met het hashresultaat dat door het eHealth-platform elektronisch werd gedateerd en ondertekend. Indien dit het geval is, dan heeft men de zekerheid dat het voorschrift niet werd gewijzigd

9.3. De authenticatie van de identiteit van de voorschrijver van een ambulant voorschrift binnen het ziekenhuis moet verlopen volgens de authenticatiemethodes die werden beschreven in het "Protocol houdende de voorwaarden en de modaliteiten volgens welke een elektronisch

[3] Circles-of-trust: een geheel van methodologische en technische afspraken tussen vertrouwde partijen die informatie onweerlegbaar beveiligen.

document met precisie kan worden geassocieerd aan een referentiedatum en ene referentietijdstip en het niet meer onmerkbaar kan worden gewijzigd, in het kader van het elektronisch ziekenhuisvoorschrift". Het Sectoraal comité[4] heeft een positief advies aan dit protocol verleend[5].

Dit betekent dat ieder ziekenhuis de nodige procedures moet vastleggen om een correcte identificatie en authenticatie van de voorschrijver te garanderen. Hierbij kan slechts worden voorzien in twee soorten van authenticatieprocedures, meer bepaald een authenticatie door middel van gebruikersnaam en paswoord dan wel door middel van het authenticatiecertificaat op de elektronische identiteitskaart of een ander certificaat dat voldoet aan de bepalingen van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten.

Aangaande de authenticatie door middel van gebruikersnaam en paswoord specificeert het protocol dat de gebruikersnaam en het paswoord strikt persoonlijk en niet overdraagbaar dienen te zijn. Het paswoord kan eenmalig of meermaals gebruikt worden. Indien het paswoord meermaals kan worden gebruikt, dient de voorschrijver het paswoord zo snel mogelijk na de ontvangst en in elk geval bij het eerste gebruik ervan te wijzigen. Indien het paswoord meermaals kan worden gebruikt, dient de voorschrijver nadien dit paswoord te wijzigen op regelmatige tijdstippen.

Het protocol wijst er op dat een veilig paswoord idealiter is samengesteld uit 15 tekens en minstens uit 8 tekens. Een paswoord kan hetzij eenmalig worden gebruikt doordat het bij elk gebruik wordt berekend op basis van een "challenge" (dynamisch paswoord), hetzij meermaals wordt gebruikt (statisch paswoord). Een paswoord dat meermaals kan worden gebruikt, bevat alfanumerieke karakters en symbolen, geplaatst in een volgorde die niet makkelijk kan worden geraden. Elke voorschrijver dient ervoor te zorgen dat het gekozen paswoord voldoet aan deze eisen. Elke voorschrijver is zelf aansprakelijk in de gevallen waarin een paswoord wordt achterhaald en / of misbruikt.

Elke voorschrijver dient zorgvuldig om te gaan met zijn gebruikersnaam en paswoord en is tot geheimhouding ervan gehouden. Elke voorschrijver is aansprakelijk voor elk al dan niet geoorloofd gebruik ervan, met inbegrip van elk gebruik door derden.

Indien een voorschrijver kennis heeft van verlies van zijn gebruikersnaam en / of paswoord of van elk ongeoorloofd gebruik door derden van zijn gebruikersnaam en / of paswoord, of een dergelijk verlies of ongeoorloofd gebruik vermoedt, dient hij onmiddellijk alle nodige maatregelen te treffen en de informatieveiligheidsconsulent binnen het ziekenhuis op de hoogte te brengen.

Zo spoedig mogelijk na de ontvangst van de melding en binnen de grenzen van de redelijkheid, worden alle mogelijke inspanningen geleverd om verder misbruik te voorkomen.

[4]Heden de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité genaamd.

[5] Advies nr. 11/01 van 15 februari 2011 van het Sectoraal comité van de sociale zekerheid en van de gezondheid.

Elke voorschrijver blijft aansprakelijk voor alle rechtmatig gebruik van zijn gebruikersnaam en/of paswoord en, ingevolge nalatigheid, alle onrechtmatig gebruik van zijn gebruikersnaam en/of paswoord dat heeft plaatsgevonden vóór het tijdstip waarop de gebruikersnaam en het paswoord geïnactiveerd werden.

10. Eens het elektronisch voorschrift is gecreëerd, wordt het, na authenticatie van de geactiveerde voorschrijverssoftware en na authenticatie van de voorschrijvende arts zelf, door de lokale software voorbereid vooraleer het kan worden verzonden naar het centrale systeem van Recip-e.

11. De voorbereiding van het elektronisch voorschrift gebeurt als volgt. Het elektronisch voorschrift wordt door de softwaremodule van de voorschrijver versleuteld door middel van de basisdienst versleuteling van het eHealth-platform, zodat het enkel zal kunnen worden geopend en gelezen door een bevoegd persoon, zijnde de voorschrijver van het voorschrift zelf, de patiënt of een bevoegde zorgverlener die door de patiënt wordt gekozen om het voorschrift uit te voeren. Aan het versleutelde voorschrift wordt vervolgens de volgende administratieve informatie toegevoegd:
    - de referentie van de sleutel die gebruikt werd bij de versleuteling, teneinde de sleutel te kunnen opvragen uit het sleuteldepot;
    - de code van het documenttype, namelijk een code die aanduidt of het al dan niet een geneesmiddelenvoorschrift betreft, een code die aanduidt of het geneesmiddelenvoorschrift informatie over de verzekerbaarheid vereist, en een code die aanduidt of het geneesmiddelenvoorschrift informatie over de aanwezigheid van een voorafgaande machtiging van een adviserend arts vereist;
    - het nationaal identificatienummer van de sociale zekerheid (INSZ) van de patiënt en het identificatienummer van de voorschrijver. Hierbij wordt onderscheid gemaakt tussen ambulant voorschrift gemaakt door (a) individuele voorschrijver resp. (b) door een voorschrijver in een ziekenhuis:
        a) Ingeval een ambulant voorschrift gemaakt door een individuele voorschrijver is het identificatienummer van de voorschrijver het INSZ dan wel het RIZIV-nummer van de voorschrijver.
        b) Ingeval een ambulant voorschrift gemaakt door een voorschrijver in een ziekenhuis, is het identificatienummer van de voorschrijver het identificatienummer van het ziekenhuis. Het ziekenhuis draagt de verantwoordelijkheid om (door middel van haar intern gebruikersbeheer) de identiteit van de voorschrijver verbonden aan dit voorschrift, te allen tijde éénduidig aan te kunnen tonen.

12. Alvorens het versleutelde voorschrift en de administratieve informatie worden overgemaakt aan het centrale systeem van Recip-e, wordt het geheel nogmaals versleuteld zodat enkel het centrale systeem van Recip-e de twee componenten kan ontcijferen (zonder het versleutelde voorschrift zelf te kunnen ontcijferen welteverstaan). Vervolgens worden een aantal veiligheidscontroles uitgevoerd om te verzekeren dat het voorschrift daadwerkelijk afkomstig is van de betrokken voorschrijver. Wanneer één van deze controles negatief is, wordt een foutmelding teruggestuurd naar de voorschrijverssoftware. Ingeval de veiligheidscontroles een positief resultaat kennen, wordt de boodschap verwerkt, waarbij een

identificatienummer, uniek voor ieder voorschrift, wordt toegevoegd. Het resulterende bericht wordt vervolgens naar het centrale systeem van Recip-e verzonden.

13. Het centrale systeem van Recip-e kan het bericht vervolgens verwerken:
    - het voor Recip-e bestemde gedeelte, namelijk het versleutelde voorschrift dat samen met de administratieve informatie nogmaals werd versleuteld, kan door het Recip-e centrale systeem worden ontcijferd, waardoor (enkel) de administratieve informatie kan worden gelezen door het Recip-e systeem;
    - het versleuteld voorschrift wordt opgeslagen, het wordt onderworpen aan een tijdsregistratie door middel van de basisdienst van het eHealth-platform[6] en er wordt een veiligheidslogging uitgevoerd;
    - voor zover het voorschrift correct geregistreerd kan worden in het centrale systeem van Recip-e, wordt het document-identificatienummer het unieke Recip-e identificatienummer. Dit is vereist om een correct opgeslagen elektronisch voorschrift te kunnen afdrukken;
    - het eHealth-platform logt wie (met gebruik van het RIZIV-nummer van de betrokkenen), wanneer en voor welk administratief gedeelte een transactie heeft verricht, alsook de eventuele foutmeldingen. Het eHealth-platform logt in geen geval het versleutelde voorschrift zelf.

14. Om het elektronisch medisch voorschrift vervolgens op te halen uit het centrale Recip-e systeem, werden de volgende procedures uitgewerkt.

15. Tijdens de huidige fase van het Recip-e project is de uitvoerder van een voorschrift steeds een apotheker. In de toekomst zal ook een verpleegkundige of kinesitherapeut een voor hen bedoeld voorschrift kunnen ophalen. Bij het aanbieden van eID/ INSZ-nummer wordt een therapeutische relatie aangemaakt met de patient/ het bestaan ervan geraadpleegd bij de uitvoerder.

    In noodgevallen is het mogelijk om toegang te verkrijgen tot de gegevens op de centrale Recip-e server zonder validatie van de therapeutische of zorgrelatie, of uitsluitingen. Dit wordt de “break the glass” uitzonderingsprocedure genoemd. Recip-e zal de mogelijke ‘noodgevallen’ (redenen voor Break-the-Glass) voorzien in de specificaties naar de softwarehuizen waarbij de zorgverlener zelf dient aan te geven in welke noodsituatie hij zich bevindt en waarbij ook wordt gesteld dat de zorgverlener zelf de therapeutische relatie achteraf terug moet aanmaken als die nog niet bestond. De zorgverlener moet formeel verklaren dat de procedure enkel wordt gebruikt in een noodgeval en dat hij er de verantwoordelijkheid voor draagt. De toegang wordt dan onmiddellijk verleend aan de zorgverlener zonder de therapeutische of zorgrelatie na te gaan of uitsluitingen te controleren. Het aantal keren dat Break-the-Glass werd toegepast en de tijdstippen waarop, samen met de reden ervoor en de betrokken apotheek, zullen eveneens afzonderlijk gelogd worden in de veiligheidslog waarop controle kan worden uitgeoefend. Deze mogelijkheid wordt enkel

[6] Zie beraadslaging nr. 10/045 van 15 juni 2010 van de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid met betrekking tot de toepassing van de basisdienst elektronische datering door het eHealth-platform.

aangeboden aan zorgverleners die toegang kunnen krijgen tot de centrale Recip-e server door het authenticatiecertificaat dat uitgereikt wordt door eHealth.

Deze uitzonderingsprocedure moet gepaard gaan met enkele waarborgen: de zorgverlener moet een reden opgeven waarom deze noodprocedure wordt gebruikt, zodat een a posteriori controle door iedere belanghebbende partij mogelijk zal zijn. De zorgverlener moet daarnaast de therapeutische relatie achteraf manueel aanmaken en deze asynchroon gemaakte therapeutische relatie synchroniseren wanneer de dienst opnieuw beschikbaar is.

Een monitoring van de asynchroon gecreëerde break-the-glass therapeutische relaties wordt geïmplementeerd. Het aantal keren dat zulke manuele post-BreaktheGlass aktie plaatsvond, kan a posteriori opgevraagd worden bij de organisatie die de therapeutische relatie databank beheert. Daarnaast zal Recip-e via monitoring bij alle betrokken service providers in de keten (NIC, Rijksregister, eHealth Platform, KSZ, netwerkprovider) verifiëren of de reden voor een Break-the-Glass noodprocedure terecht was, met name of er wel degelijk een onbeschikbaarheid in de keten was op het moment dat het voorschrift incl. aanmaak van therapeutische relatie uitgevoerd moest worden.

16. Bij opstart van het systeem van de apotheek wordt de softwaremodule van de apotheek via een eHealth systeem-certificaat geauthentiseerd. Dit certificaat authentiseert de apotheek en heeft een verantwoordelijke (titularis van de officina) die via authentieke bronnen gelinkt kan worden met dit certificaat. Deze persoon is met name verantwoordelijk voor het correcte gebruik van het certificaat en het beheer van de private sleutel, alsook voor de handelingen die worden uitgevoerd bij het gebruik van dit certificaat.

17. De sessie kan worden opgestart door elke apotheker die in de officina onder de verantwoordelijkheid van de titularis werkzaam is. Om een sessie te kunnen opstarten, dient de apotheker zich te authentiseren via de elektronische identiteitskaart (met ingave van de PIN-code), hetzij – in een eerste fase – door middel van het persoonlijke encryptiecertificaat en de bijbehorende private sleutel (die hier dan dienst doen als middel voor de authenticatie van de identiteit van de apotheker), toegekend door het eHealth-platform.

18. Op basis van het unieke Recip-e identificatienummer van het elektronisch voorschrift dat wordt uitgelezen via de barcode die zich bevindt op het afgedrukte voorschrift dat de patiënt in de apotheek overhandigt, kan de apothekerssoftware een versleutelde aanvraag naar het centrale systeem van Recip-e versturen om het elektronische voorschrift dat aan dit unieke identificatienummer is verbonden, op te halen. Het eHealth-platform valideert of deze aanvraag van een geldige en erkende apotheek afkomstig is, waarna het Recip-e systeem de aanvraag kan ontcijferen en de toegangsrechten valideert op basis van (1) de precieze rol van de uitvoerder van het voorschrift (meegestuurd via de aanvraag) en (2) het type voorschrift.
De uitvoerder van het voorschrift verifieert bovendien in de digitale verwerking van het elektronisch voorschrift of de patiënt nog levend of dood is (via MyCareNet systeem). Dit gebeurt buiten Recip-e om, maar wel vóór de aflevering van een product. Aan de kant van voorschrijver wordt bij de aanmaak van het voorschrift eveneens geverifieerd of de patiënt nog levend of dood is (via zijn software). Dit gebeurt eveneens buiten Recip-e om, maar wel voordat het product aan die persoon wordt voorgeschreven.

19. Wanneer de autorisatieprocedure correct is verlopen, zal Recip-e het versleutelde voorschrift terugsturen naar de betrokken apotheek. De sleutel om het versleutelde voorschrift te ontcijferen, wordt vervolgens bij het sleuteldepot bij het eHealth-platform opgevraagd. Indien de aanvrager effectief geautoriseerd kan worden om toegang te verkrijgen tot de sleutel, wordt de sleutel naar de uitvoerders-softwaremodule verstuurd, waarna het elektronische voorschrift met de ontvangen sleutel ontcijferd kan worden.

20. Na het uitvoeren van het voorschrift archiveert de uitvoerder het voorschrift, samen met de sleutel en de uitgevoerde tijdsregistratie. Het Recip-e centrale systeem wordt vervolgens gewaarschuwd door de software van de uitvoerder dat het voorschrift uitgevoerd en gearchiveerd is.

21. Een functie is voorzien op het centrale Recip-e systeem opdat de patiënt zijn/haar persoonlijke medische voorschriften kan raadplegen via externe platformen. Wanneer de patiënt zich authentiseert aan de hand van zijn eID of een evenwaardig goedgekeurd systeem, kan hij/ zij de lijst van voorschriften met de unieke Recip-e identificatienummers raadplegen. De patiënt heeft desgewenst de mogelijkheid om een voorschrift te beheren (revoceren, …). en privacymaatregelen op zijn/haar voorschriften toe te passen (VISI-vlag) zodat de apotheker bij aanbieden van eID/INSZ-nummer alleen de voorschriften ziet waarop de patiënt geen privacymaatregel zette. De patiënt kan zelf de VISI-vlag zetten of kan ook vragen aan de voorschrijver om de VISI-vlag te zetten met zijn toestemming. De patiënt (of de volmachthouder) kan ook een voorschrift reserveren bij een specifieke apotheker en kan zijn eigen contactgegevens meegeven.

    Er moet vermeden worden dat het gebruik van deze functie door de patiënt het risico zou inhouden dat de gegevens voor andere doeleinden worden gebruikt dan de raadpleging en het beheer van de persoonlijke medische voorschriften door de patiënt. Het RIZIV heeft een toepassing VIDIS ontwikkeld waarmee deze functies door de patiënt kunnen worden gebruikt op een wijze dat de hoger vermelde risico's worden vermeden. Andere patiëntenkanalen kunnen de patiënt na authenticatie leiden naar de toepassing VIDIS.

    Het rechtstreeks aanroepen van elektronische geneesmiddelenvoorschriften via API's door andere toepassingen dan deze van de zorgverleners die de geneesmiddelen afleveren of VIDIS wordt niet toegestaan omwille van het risico dat deze gegevens toegankelijk zouden zijn voor aanbieders van de private en/of commerciële patiëntenkanalen en zouden kunnen worden gebruikt voor andere doeleinden dan de aflevering van de geneesmiddelen of de visualisatie en het beheer van de persoonlijke medische voorschriften van de patiënt.

22. De geldigheid van de voorschriften wordt beheerd door Recip-e. Enkel geldige voorschriften worden aan de apotheker getoond. Er wordt bovendien voorzien dat voorschrijvers elkaars voorschriften kunnen consulteren, mits er een therapeutische relatie is met de patiënt en een geïnformeerde toestemming van de patiënt, verleend via het formulier van geïnformeerde toestemming betreffende de elektronische uitwisseling van persoonsgegevens die de gezondheid betreffen, zoals goedgekeurd door de afdeling gezondheid van het Sectoraal

comité van de sociale zekerheid en van de gezondheid[7]bij beraadslaging nr. 12/047 van 19 juni 2012.

23. De voorschriften worden gedurende een maximum van 1 jaar na aanmaak bijgehouden op de Recip-e server. Echter, van zodra een voorschrift door een zorgverlener wordt opgehaald (en nog geldig is) dan wel gerevoceerd wordt door de betrokken patiënt of zorgverlener, wordt voornoemd voorschrift verwijderd van de server. Enkel metadata (zonder inhoud van de voorschriften) worden bijgehouden omwille van traceringsredenen.

24. De verpleegkundige zal de elektronische voorschriften ook kunnen raadplegen. Bovendien heeft eveneens de patiënt toegang tot zijn eigen voorschriften. Ten slotte kan de mandaathouder (na elektronisch toekennen van deze rol door de patiënt) toegang hebben tot de voorschriften van de patiënt. De patiënt kan evenwel bepaalde toegangen beperken voor de mandaathouder.

ii. PARIS

25. Om elke voorschrijver de mogelijkheid te bieden om elektronische voorschriften aan te maken buiten het Elektronisch Medisch Dossier (in afwachting van een veralgemeend gebruik van het EMD), stelt de overheid in afwachting van een veralgemeend gebruik van het EMD gratis een (web)toepassing ter beschikking die een minimale service biedt: "PARIS" (Prescription & Autorisation Requesting Information System).

PARIS wordt ter beschikking gesteld aan sporadische voorschrijvers of voorschrijvers die zich in een situatie bevinden waarin ze (tijdelijk) geen toegang hebben tot hun softwarepakket voor het beheer van het patiëntendossier of tot het informaticasysteem van het ziekenhuis, of die (nog) niet beschikken over een Elektronisch Medisch Dossier (d.w.z. een softwarepakket voor het beheer van het patiëntendossier). PARIS zal aan deze doelgroep ook de mogelijkheid bieden om elektronische voorschriften aan te maken buiten het Elektronisch Medisch Dossier (EMD). De toepassing is aldus nuttig voor huisartsen, specialisten, tandartsen en vroedvrouwen die zich in een situatie bevinden waarin ze (tijdelijk) geen toegang hebben tot hun softwarepakket voor het beheer van het patiëntendossier of tot het informaticasysteem van het ziekenhuis, bijvoorbeeld tijdens huisbezoeken, bezoeken in woonzorgcentra, tijdens een consultatie in het ziekenhuis of die (nog) niet beschikken over een Elektronisch Medisch Dossier, zijnde een softwarepakket voor het beheer van het patiëntendossier, of die daar geen behoefte aan hebben. Dit zijn bijvoorbeeld sommige categorieën van specialisten, voorschrijvers die nog enkel een beperkte praktijk hebben of het beroep niet meer in de klassieke zin van het woord uitvoeren (die werkzaam zijn bij de ziekenfondsen, in de administratie, in het onderwijs, klinisch biologen, anatoom-pathologen, etc.) en oudere voorschrijvers op het einde van een actieve praktijk.

26. De voorschrijver kan de volgende functionaliteiten van het Recip-e systeem gebruiken:
- een voorschrift aanmaken;

[7] Nu de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité genaamd.

- de lijst van voorschriften raadplegen, aangemaakt door de voorschrijver, maar die nog niet zijn afgeleverd;
- een voorschrift annuleren dat nog niet afgeleverd werd;
- een notificatie versturen naar een individuele apotheker;
- de feedback van apothekers raadplegen over af te leveren voorschriften.

27. PARIS biedt geen minimale service aan voor de elektronische machtigingsaanvragen voor geneesmiddelen waarvoor de CIVARS-toepassing reeds operationeel is.

II. BEVOEGDHEID VAN HET COMITE

28. Artikel 11 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* bepaalt dat elke mededeling van persoonsgegevens door of aan het eHealth-platform, behoudens enkele uitzonderingsgevallen, een principiële machtiging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité vereist.

29. Voorts is de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité ingevolge artikel 42, § 2, 3°, van de wet van 13 december 2006 houdende diverse bepalingen betreffende gezondheid bevoegd voor het verlenen van een principiële machtiging met betrekking tot elke mededeling van persoonsgegevens die de gezondheid betreffen, behoudens de voorziene uitzonderingen.

30. Artikel 46, § 1, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid* bepaalt bovendien dat de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité belast is met het verzekeren van het toezicht op de naleving van de door of krachtens de wet vastgestelde bepalingen tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens die de gezondheid betreffen. Daarbij kan zij alle aanbevelingen formuleren die zij nuttig acht en bijdragen tot het oplossen van principiële problemen of geschillen.

31. Het Comité stelt verder vast dat de aanvrager bij de mededeling van het elektronische ambulante voorschrift het gebruik van het INSZ van zowel de voorschrijver als van de patiënt voorziet, hetgeen het gebruik van ofwel het rijksregisternummer ofwel het identificatienummer toegekend door de Kruispuntbank van de Sociale Zekerheid impliceert.

Krachtens artikel 15 §3 van de hogervermelde wet van 15 januari 1990 kan de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, voor zover deze een beraadslaging moet verlenen voor een mededeling van persoonsgegevens, in voorkomend geval eveneens een beraadslaging verlenen voor het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen door de betrokken instanties indien dat noodzakelijk is in het kader van de beoogde mededeling.

Overeenkomstig artikel 5, §1 van de wet van 5 mei 2014 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, kan het Comité eveneens uitspraak doen over het gebruik van het rijksregisternummer telkens als over een gegevensstroom of verwerking van persoonsgegevens wordt beslist.

Het gebruik van het identificatienummer van de sociale zekerheid, voor zover toegekend door de Kruispuntbank van de Sociale Zekerheid, is vrij overeenkomstig artikel 8, § 2, van de hogervermelde wet van 15 januari 1990.

32. Artikel 42 van de gecoördineerde wet van 10 mei 2015 betreffende de uitoefening van gezondheidszorgberoepen bepaalt de criteria waaraan een geldig voorschrift moet voldoen. Hierbij wordt vermeld dat het voorschrift gedagtekend wordt op papier of op elektronische wijze aan de hand van een procedure die goedgekeurd wordt door het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid.[8] Bovendien dient het voorschrift te worden ondertekend ofwel wordt de identiteit van voorschrijver geauthentiseerd aan de hand van een procedure die goedgekeurd wordt door het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid.[9] Het Comité dient zich bijgevolg uit te spreken over de procedure om het voorschrift op elektronische wijze te dagtekenen en de procedure om de identiteit van de voorschrijver te authentiseren.

33. Het Comité acht zich bevoegd om zich uit te spreken over de verwerking van persoonsgegevens in het kader van het project Recip-e en de webtoepassing PARIS.

III. BEHANDELING TEN GRONDE

A. TOELAATBAARHEID

34. De verwerking van persoonsgegevens is enkel toegelaten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en is de verwerking van persoonsgegevens die de gezondheid betreffen in principe verboden.[10]

35. Het verbod is niet van toepassing indien de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen.[11]

36. Het Comité stelt vast dat de mededeling van de versleutelde elektronische voorschriften door de voorschrijver aan het centrale systeem van Recip-e voldoet aan de voorwaarden van de uitzondering op het voormelde verbod zoals opgenomen in artikel 9 lid 2 h) GDPR.

[8] Heden de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité genaamd.
[9] Heden de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité genaamd.
[10] Art. 9, lid 1 GDPR.
[11] Art. 9 lid 2 h) GDPR.

B. FINALITEIT

37. Overeenkomstig art. 5, b) van de GDPR is de verwerking van persoonsgegevens enkel toegelaten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

38. Met de beoogde verwerking van persoonsgegevens in de projecten Recip-e en PARIS heeft het RIZIV tot doel het gebruik van de elektronische ambulante voorschriften mogelijk te maken, zoals omschreven in randnummers 1, 2, 3, 25 en 26. Het RIZIV heeft als openbare instelling van sociale zekerheid de wettelijke opdracht de 'verplichte verzekering' te organiseren, te beheren en te controleren[12]. Dit houdt onder andere in dat het de regels voor de terugbetaling van geneeskundige prestaties en geneesmiddelen opstelt en de tarieven ervan bepaalt. Meer specifiek behoort het tot de bevoegdheden van de dienst voor geneeskundige verzorging om de voorwaarden te bepalen waaronder de geneeskundige verstrekkingen kunnen worden terugbetaald.

39. Het Comité acht het in hoofde van het RIZIV en de vzw Recip-e effectief gerechtvaardigd om de voor het gebruik van het elektronische ambulante voorschrift vereiste infrastructuur uit te werken en stelt daarbij vast dat de beoogde verwerking welbepaalde en uitdrukkelijk omschreven doeleinden heeft.

C. PROPORTIONALITEITSPRINCIPE

40. Overeenkomstig art. 5, b) en c) van de GDPR dienen de persoonsgegevens toereikend, ter zake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.

41. De persoonsgegevens die bij de mededeling van het elektronische ambulante voorschrift zullen worden verwerkt, zijn: enerzijds het elektronische ambulante voorschrift zelf dat de naam en de voornaam van de patiënt, de coördinaten van de voorschrijver en de informatie betreffende de voorgeschreven geneesmiddelen of verstrekkingen bevat en anderzijds het administratieve gedeelte dat het INSZ van de patiënt evenals het INSZ dan wel het RIZIV-nummer van de voorschrijver bevat.

42. Het elektronische voorschrift zelf wordt versleuteld aan de hand van de basisdienst versleuteling voor onbekende bestemmeling van het eHealth-platform. Dit betekent dat van zodra het elektronische voorschrift is aangemaakt, het bericht wordt versleuteld zodat enkel een beperkt aantal personen het bericht kunnen ontcijferen en het voorschrift kunnen lezen, meer bepaald de voorschrijver zelf, de andere voorschrijvers, de betrokkene op wiens naam het voorschrift is gemaakt, de volmachthouder en de zorgverlener die door de betrokkene wordt gevraagd om het voorschrift uit te voeren of te consulteren. Het centrale systeem van Recip-e dat de versleutelde voorschriften bewaart nadat ze op correcte wijze zijn aangemaakt, kan bijgevolg op geen enkele wijze kennis nemen van de inhoud van het voorschrift.

[12] Wet van 14 juli 1994 betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen, gecoördineerd op 14 juli 1994, *B.S.* 27 augustus 1994.

43. Aangezien de eenduidige identificatie van zowel de patiënt als de voorschrijver van primordiaal belang is, wordt voorzien dat in het administratieve gedeelte dat het versleuteld voorschrift vergezelt, de patiënt wordt geïdentificeerd aan de hand van zijn INSZ en de voorschrijver wordt geïdentificeerd aan de hand van zijn INSZ dan wel RIZIV-nummer.

44. De aanvrager stelt dat het gebruik van de voormelde identificatienummers noodzakelijk is enerzijds om de patiënten toe te laten om in het centrale systeem van Recip-e de voorschriften die op hun naam zijn voorgeschreven te consulteren en in te trekken, en anderzijds om de vereiste veiligheidsloggings correct te kunnen laten uitvoeren.

45. Algemeen gesteld acht het Comité het inderdaad aangewezen dat eenduidige identificatienummers zoals het INSZ worden gebruikt om de patiënt en de voorschrijver te identificeren in het administratieve gedeelte bij de communicatie van dergelijke versleutelde berichten. Het Comité stelt vast dat hoewel er persoonsgegevens die de gezondheid betreffen zouden kunnen worden afgeleid uit de combinatie tussen de identificatienummers van de patiënt en de voorschrijver, deze verwerking van persoonsgegevens eveneens noodzakelijk is teneinde aan een aantal specifieke verplichtingen te kunnen voldoen. Zo is de verwerking van deze identificatienummers noodzakelijk voor de verplichte uitvoering van veiligheidsloggings, om de berichten aan de juiste ontvangers te kunnen overmaken (routering genaamd) en voor de praktische uitwerking van bepaalde wettelijk voorziene rechten van de betrokkenen, zoals het recht op inzage. Deze verwerking van persoonsgegevens vereist evenwel dat de veiligheidsmaatregelen, zoals verder besproken, een garantie bieden dat de gegevens in kwestie met de meest strikte confidentialiteit worden behandeld. De verwerking van de identificatienummers is ook slechts toegestaan voor de vermelde doeleinden inzake het beheren van veiligheidsloggings, routering en organisatie van de wettelijke voorziene rechten van de betrokkenen, zoals het recht op inzage.

46. Het Comité acht de persoonsgegevens die zullen worden verwerkt in het kader van het Recip-e en het PARIS project relevant, evenredig en niet buitensporig.

47. Persoonsgegevens moeten 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.

48. Voor zover ze niet worden opgehaald door een zorgverlener (en nog geldig zijn) of niet worden gerevoceerd door de betrokken patiënt of zorgverlener, worden de versleutelde voorschriften gedurende maximum één jaar in het centrale systeem van Recip-e bewaard.

49. Het is voorzien dat de elektronische voorschriften na aflevering aan de uitvoerder door deze laatste worden bewaard conform de wettelijke bepalingen. Nadat een elektronisch voorschrift is opgevraagd en uitgevoerd, wordt het in het centrale systeem van Recip-e opgeslagen versleutelde elektronische voorschrift verwijderd. De veiligheidsloggings worden door het centrale systeem van Recip-e gedurende een periode van 30 jaar bewaard.

50. Indien het centrale systeem van Recip-e zou worden gebruikt om een versleuteld bericht (feedback) te verzenden tussen de uitvoerder van het voorschrift en de voorschrijver, wordt voorzien dat het versleuteld bericht slechts zolang wordt bewaard tot het eerstvolgend

ogenblik dat een voorschrijver een sessie opent en het bericht kan worden afgeleverd. Zodra afgeleverd, worden de feedbackberichten onmiddellijk en definitief uit het centrale systeem van Recip-e verwijderd.

51. Gelet op het voorgaande acht het Comité de voorziene bewaartermijnen aanvaardbaar.

D. BEVEILIGING EN CONFIDENTIALITEIT

52. Overeenkomstig art. 9, lid 3 van de GDPR mogen persoonsgegevens betreffende de gezondheid enkel worden verwerkt onder het toezicht en de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg. Hoewel dit strikt genomen niet wordt vereist, verdient het volgens het Comité de voorkeur dat dergelijke gegevens worden verwerkt onder de verantwoordelijkheid van een arts[13], hetgeen *in casu* het geval is.

53. De aanvrager moet, overeenkomstig art. 5, f) van de GDPR, alle gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens. 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.

54. Overeenkomstig de referentiemaatregelen voor de bescherming van iedere verwerking van persoonsgegevens opgesteld door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer dient iedere verantwoordelijke voor de verwerking, afhankelijk van de aard en de omvang van de verwerking, in het kader van deze verplichting specifieke maatregelen te nemen, zoals het opstellen van een veiligheidsplan, het aanstellen van een veiligheidsconsulent, het garanderen van de fysieke bescherming van de persoonsgegevens en de beveiliging van de netwerken, het voorzien in een adequaat gebruikers- en toegangsbeheer, het installeren van loggings- en opsporingsmechanismen, het regelmatig valideren en verifiëren van de technische of organisatorische veiligheidsmaatregelen, het beschikken over een beheersplan voor veiligheidsincidenten en over een volledige, gecentraliseerde en bijgewerkte documentatie[14].

55. *In casu* wordt voorzien dat de basisdienst gebruikers- en toegangsbeheer van het eHealth-platform wordt gebruikt voor de authenticatie en autorisatie van de verschillende gebruikers van het Recip-e en het PARIS project, meer bepaald de voorschrijver, de uitvoerder en de betrokkene zelf. De verwerking van persoonsgegevens door het eHealth-platform in het kader van het gebruikers- en toegangsbeheer werd reeds gemachtigd door het Comité[15]. Bij

[13] Het Comité heeft deze voorkeur opgesteld in paragraaf 61 van haar beraadslaging nr. 07/034 van 4 september 2007 *m.b.t. de mededeling van persoonsgegevens aan het Federaal Kenniscentrum voor de Gezondheidszorg met het oog op het onderzoek 2007-16-HSR "Onderzoek naar mogelijke financieringsmechanismen voor het geriatrisch dagziekenhuis*", www.privacycommission.be.

[14] http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

[15] Beraadslaging nr. 09/008 van 20 januari 2009, gewijzigd op 16 maart 2010 en op 15 juni 2010, van het sectoraal comité van de sociale zekerheid en van de gezondheid met betrekking tot de toepassing van het geïntegreerd

ambulante voorschriften die binnen een ziekenhuis worden opgemaakt logt het ziekenhuis éénduidig de identiteit van de arts die een specifiek ambulant voorschrift voorgeschreven heeft.

56. Gelet op artikel 42 van de gecoördineerde wet van 10 mei 2015, keurt het Comité uitdrukkelijk de voorziene authenticatiemethodes evenals het gebruik van de basisdienst 'elektronische datering' van het eHealth-platform voor de dagtekening van de elektronische ambulante voorschriften goed.

57. Voor de versleuteling van het elektronische voorschrift voor de mededeling tussen de voorschrijver en de uitvoerder enerzijds, en voor de versleuteling van het versleutelde bericht en de administratieve informatie voor de mededeling tussen de voorschrijver en het centrale systeem van Recip-e anderzijds, zal gebruik worden gemaakt van de basisdienst versleuteling voor onbekende bestemmeling van het eHealth-platform. De versleuteling van eventuele feedbackberichten zal gebeuren aan de hand van een versleuteling voor bekende bestemmeling.

58. Het Recip-e en het PARIS project voorzien eveneens dat de nodige veiligheidsloggings zullen worden uitgevoerd, eveneens door het gebruik van de basisdiensten van het eHealth-platform. Bij deze logging worden de volgende gegevens bewaard: welke handeling wordt gesteld (overmaken van wie de handeling stelt (aan de hand van het INSZ), met betrekking tot welke persoon (eveneens aan de hand van het INSZ) en wanneer de handeling werd gesteld.

59. Tot slot neemt het Comité akte van het feit dat voor beide projecten een afzonderlijke veiligheidsconsulent werd aangesteld, wiens identiteiten het Comité mocht vernemen.

gebruikers- en toegangsbeheer door het ehealth-platform bij de uitwisseling van persoonsgegevens, www.privacycommission.be.

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 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.

Dat de machtiging wordt verleend tot de verwerking van persoonsgegevens voor de elektronische uitwisseling van het elektronische ambulante voorschrift in het kader van Recip-e en de webtoepassing PARIS en de machtiging tot het gebruik van het rijksregisternummer voor die doeleinden.

Gelet op artikel 42 van de gecoördineerde wet van 10 mei 2015 betreffende de uitoefening van gezondheidszorgberoepen, keurt het Comité uitdrukkelijk de voorziene authenticatiemethodes evenals de voorziene methode voor dagtekening van de elektronische ambulante voorschriften goed.

Bart VIAENE
Voorzitter