Reglement tot vaststelling van de criteria voor de toepassing van een cirkel van vertrouwen door een organisatie in het kader van de uitwisseling van gezondheidsgegevens

DOEL VAN HET REGLEMENT

De verwerking van persoonsgegevens, inzonderheid van persoonsgegevens m.b.t. de gezondheid, dient te geschieden met de nodige maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer. Een belangrijk aspect daarvan is de waarborg dat de persoonsgegevens enkel worden verwerkt

- voor rechtmatige doeleinden en
- door personen die, voor het bereiken van die doeleinden, nood hebben aan de verwerking van persoonsgegevens m.b.t. de betrokkene.

In een systeem van gedeelde verwerking van persoonsgegevens door tal van actoren, vereist het bieden van dergelijke waarborg een duidelijke vastlegging van de verantwoordelijkheden van elkeen.

Dit reglement wil hiertoe bijdragen door het preciseren van het concept van 'cirkels van vertrouwen'. Een 'cirkel van vertrouwen' is een groep gebruikers van een organisatie, waarvoor die organisatie zelf op een aantal vlakken informatieveiligheidsmaatregelen organiseert en de correcte naleving ervan bewaakt, zodat andere organisaties er redelijkerwijze kunnen op betrouwen dat deze informatieveiligheidsmaatregelen worden nageleefd en deze maatregelen dus zelf niet meer moeten organiseren of bewaken.

Cirkels van vertrouwen kunnen worden georganiseerd door tal van organisaties, zoals ziekenhuizen, organisaties belast met indicatiestellingen in het kader van BelRAI, ziekenfondsen, edm.

Opdat andere organisaties dan de organisatie die een cirkel van vertrouwen instelt, daarin rechtmatig vertrouwen zouden kunnen hebben, worden criteria vastgelegd waaraan elke organisatie die dergelijke cirkel van vertrouwen wenst te organiseren, moet voldoen. Deze criteria verwijzen maximaal naar reeds bestaande Europese en Belgische regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). Zij doen geen afbreuk aan deze regelgeving, die ten volle blijft gelden, maar preciseren in een aantal gevallen de wijze waarop aan deze regelgeving dient te worden voldaan.

De criteria zelf nemen de vorm aan van een reglement. Bij sommige criteria wordt voor een goede verstaanbaarheid toelichting verstrekt. Die toelichting is louter informatief.

OVERZICHT VAN DE CRITERIA

THEMA 1: RECHTMATIGHEIDS- EN DOELBINDINGSBEGINSEL

CRITERIUM 1: REGISTER VAN DE VERWERKINGSACTIVITEITEN

De organisatie beschikt voor de verwerkingsactiviteiten m.b.t. zorgvragers over een register van de verwerkingsactiviteiten zoals bedoeld in artikel 30 van de Algemene Verordening Gegevensbescherming (AVG), waarin de rechtmatige verwerkingsdoeleinden van de verwerkingsactiviteiten staan vermeld.

CRITERIUM 2: PRECISERING VAN DE RECHTSGRONDEN VOOR DE VERWERKING VAN BIJZONDERE CATEGORIËEN VAN PERSOONSGEGEVENS

Voor de verwerking van bijzondere categorieën van persoonsgegevens, bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG), m.b.t. zorgvragenden, vermeldt het register van de verwerkingsactiviteiten de rechtsgrond(en) bedoeld in artikel 9, 2. van de AVG op basis waarvan de bijzondere categorieën van persoonsgegevens worden verwerkt.

THEMA 2: EVENREDIGHEIDSBEGINSEL

CRITERIUM 3: VERWERKINGSBEPERKING

De persoonsgegevens m.b.t. zorgvragenden, in het bijzonder de bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG), kunnen enkel worden verwerkt door gebruikers die deze in hoofde van hun functie moeten kunnen verwerken voor de rechtmatige verwerkingsdoeleinden beschreven in het register van de verwerkingsactiviteiten. De verwerkingsmogelijkheden worden voldoende fijnmazig gemoduleerd, zodat elke gebruiker slechts de persoonsgegevens kan verwerken m.b.t. de zorgvragenden waarvoor dit in hoofde van zijn functie nodig is en over de tijdsperiode waarvoor dit in hoofde van zijn functie nodig is.

THEMA 3: GEBRUIKERS- EN TOEGANGSBEHEER

CRITERIUM 4: AUTHENTICATIE VAN DE IDENTITEIT VAN DE GEBRUIKER

De organisatie authentiseert de identiteit van de natuurlijke persoon die de bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. Van de Algemene Verordening Gegevensbescherming (AVG) verwerkt (de 'gebruiker').

Deze authenticatie geschiedt

- hetzij met een middel geïntegreerd in de Federal Authentication Service (FAS) van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform;
- hetzij door een authenticatiesysteem eigen aan de organisatie
    - mits een registratie van de identiteit geschiedt aan de hand van een eenmalig gebruik van een authenticatiemiddel geïntegreerd in de FAS van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform en
    - mits het authenticatiesysteem eigen aan de aanbieder voldoet aan de voorwaarden voor een betrouwbaarheidsniveau 'substantieel' zoals gepreciseerd in de punten 2.1., 2.2.1. element 2, 2.2.3., 2.2.4., 2.3.1. (met uitzondering van element 1) en 2.4. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening en
    - mits het authenticatiemiddel gebruikt in het authenticatiesysteem eigen aan de aanbieder en het activeringsproces ervan voldoet aan de voorwaarden voor een betrouwbaarheidsniveau 'laag' in punt 2.2.1. element 1 en punt 2.2.2. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening, en het zodanig is ontworpen dat het kan worden verondersteld slechts te worden gebruikt door de persoon aan wie het toebehoort.

Op dit ogenblik is het minimumniveau in de FAS vastgesteld door het Beheerscomité van het eHealth-platform niveau 400 voor natuurlijke personen handelend als zorgverstrekker en niveau 350 voor natuurlijke personen handelend als zorgvrager.

Toelichting
Het eenmalig gebruik van een authenticatiemiddel geïntegreerd in de FAS om de identiteit van de gebruiker te registreren houdt niet in dat de FAS zelf daartoe moet worden gebruikt. De elektronische identiteitskaart kan bijvoorbeeld ook gewoon worden opgevraagd om de foto visueel te vergelijken met de houder van de kaart, of uitgelezen aan de hand van een eigen implementatie van de betrokken organisatie. Het authenticatiesysteem eigen aan de organisatie moet voldoen aan de voorwaarden voor het betrouwbaarheidsniveau 'substantieel' van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening, met dien verstande dat het authenticatiemiddel wel een authenticatiemiddel mag zijn dat gebruikt maakt van slechts één authenticatiefactor (bvb. gebruikersnummer en paswoord).

CRITERIUM 5: VERIFICATIE VAN RELEVANTE KENMERKEN EN RELATIES VAN DE GEBRUIKER

Indien de elektronische verwerking van bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG) de verificatie vereist van relevante kenmerken of relaties van de gebruiker, of van de uitsluiting van de gebruiker tot toegang, worden deze kenmerken, relaties of uitsluitingen geraadpleegd

- hetzij in de betrokken authentieke bronnen vastgelegd door het Beheerscomité van het eHealth-platform
- hetzij in een gegevensbank van de organisatie of van een gezondheidsnetwerk waarvan de organisatie deel uitmaakt en die, waar nodig, gesynchroniseerd is met kwaliteitsvolle informatie uit de authentieke bronnen vastgelegd door het Beheerscomité van het eHealth-platform.

Het Beheerscomité heeft tot op heden het gebruik vastgelegd van de volgende authentieke bronnen:

- Cobrha
- de gegevensbank bij de ziekenfondsen m.b.t. de houders van een Globaal Medisch Dossier.
- de gegevensbank bij het eHealth-platform met de uitsluitingen van zorgverstrekkers tot toegang tot persoonsgegevens m.b.t. een bepaalde zorgvrager.

Toelichting
Het is van groot belang dat de informatie die wordt gebruikt m.b.t. relevante kenmerken van een gebruiker of van de relaties van de gebruiker met bvb. zijn organisatie of de zorgvragende kwaliteitsvol en up to date is. Daartoe zijn zgn. authentieke bronnen uitgebouwd, zoals Cobrha of de gegevensbank van de houders van een Globaal Medisch Dossier bij de ziekenfondsen. Het is van belang dat de kwaliteitsvolle en up to date informatie die beschikbaar is in deze authentieke bronnen wordt gebruikt, hetzij door de betrokken authentieke bron rechtstreeks te raadplegen, hetzij door de eigen gegevensbank van de organisatie ermee waar nodig te synchroniseren.

THEMA 4: LOGGING

CRITERIUM 6: INTERNE LOGGING

De elektronische toegang tot persoonsgegevens wordt gelogd. Het logbeheer moet minimaal beantwoorden aan de volgende doelstellingen

- toelaten snel en eenvoudig te kunnen bepalen welke natuurlijke persoon, wanneer en op welke manier toegang heeft verkregen tot welke persoonsgegevens m.b.t. welke persoon;
- de persoon die persoonsgegevens heeft verwerkt en de persoon waarover persoonsgegevens zijn verwerkt eenduidig kunnen identificeren;

- de noodzakelijke tools ter beschikking hebben om toe te laten de loggegevens uit te baten door de geautoriseerde personen;
- de loggegevens minstens 10 jaar bewaren.

CRITERIUM 7: AUDITTRAIL

Indien de elektronische verwerking van persoonsgegevens de toegang inhoudt tot persoonsgegevens verwerkt door derden, wordt ervoor gezorgd dat bij onderzoek, op initiatief van het eHealth-platform, of van een toezichtsorgaan, naar aanleiding van een klacht, een volledige reconstructie kan geschieden die ertoe strekt te bepalen welke natuurlijke persoon toegang heeft gehad tot welke soorten persoonsgegevens m.b.t. welke personen, wanneer en op welke manier. Onder coördinatie van het eHealth-platform worden methoden afgesproken die deze volledige reconstructie mogelijk maken.

THEMA 5: INFORMATIE, VORMING, SENSIBILISERING, CONTROLE EN SANCTIES

CRITERIUM 8: INFORMATIE, VORMING EN SENSIBILISERING

De organisatie stelt de nodige policies op om uitvoering te geven aan de criteria vermeld in dit document, stelt deze op een algemeen toegankelijke wijze ter beschikking van alle gebruikers die deel uitmaken van de cirkel van vertrouwen, biedt hierover een gepaste permanente vorming aan aan deze gebruikers en sensibiliseert hen voortdurend tot het naleven van de policies.

CRITERIUM 9: INTERNE CONTROLE

De organisatie organiseert een regelmatige interne controle op de naleving van de criteria vervat in dit document en de policies die er uitvoering aan geven. De organisatie bewaart de resultaten van deze interne controle gedurende 2 jaar. De organisatie voorziet in afschrikwekkende sancties t.a.v. gebruikers die deel uitmaken van de cirkel van vertrouwen die de criteria of de policies die eraan uitvoering geven niet naleven.

THEMA 6: NALEVING BERAADSLAGINGEN INFORMATIEVEILIGHEIDSCOMITE

CRITERIUM 10: NALEVING BERAADSLAGINGEN INFORMATIEVEILIGHEIDSCOMITE

De organisatie bevestigt alle maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer na te leven die zijn voorzien in de toepasselijke beraadslagingen van het Informatieveiligheidscomité.

THEMA 7: HANDHAVING

CRITERIUM 11: OPNAME IN DE AUTHENTIEKE BRON COBRHA ALS ORGANISATIE DIE EEN CIRKEL VAN VERTROUWEN ORGANISEERT

De organisatie meldt schriftelijk aan de beheerder van de haar betreffende informatie in de authentieke bron Cobrha dat zij een cirkel van vertrouwen instelt overeenkomstig de voorwaarden vermeld in dit document, en bevestigt daarbij te voldoen aan elk van deze voorwaarden. In de authentieke bron Cobrha wordt door deze beheerder vermeld dat de organisatie een cirkel van vertrouwen heeft ingesteld.

CRITERIUM 12: OPENBARE DOCUMENTATIE

De organisatie publiceert op haar website op een begrijpbare wijze de verwerkingsdoeleinden waarvoor ze persoonsgegevens m.b.t. zorgvragenden verwerkt en de policy waarmee uitvoering wordt gegeven aan het evenredigheidsbeginsel.

CRITERIUM 13: EXTERNE CONTROLE

De organisatie houdt het verwerkingsregister en de documenten en policies die ze voor de naleving van deze voorwaarden uitwerkt, evenals de resultaten van de interne controle, ter beschikking van de toezichtsorganen.

BIJLAGE: GLOSSARIUM

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

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.

Zie https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679

AUTHENTICATIE VAN DE IDENTITEIT

Het proces waarbij wordt nagegaan of de identiteit die een entiteit beweert te hebben om gebruik te kunnen maken van een elektronische dienst, de juiste identiteit is. De authenticatie van de identiteit kan geschieden op basis van een controle van

- kennis (vb. een paswoord);
- bezit (vb. een certificaat op een elektronisch leesbare kaart);
- biometrische eigenschap(pen);
- een combinatie van één of meerdere van deze middelen.

AUTHENTIEKE BRON

Een gegevensbank met betrouwbare informatie over relevante kenmerken en/of relevante relaties, die toegankelijk is via de basisdienst gebruikers- en toegangsbeheer van het eHealth-platform.

CIRKEL VAN VERTROUWEN

Een cirkel van vertrouwen is een groep gebruikers van een organisatie waarvoor de organisatie zelf op een aantal vlakken informatieveiligheidsmaatregelen organiseert en de correcte naleving ervan bewaakt, zodat andere organisaties er redelijkerwijze kunnen op betrouwen dat deze informatieveiligheidsmaatregelen worden nageleefd en deze maatregelen dus zelf niet meer moeten organiseren of bewaken.

COBRHA (COMMON BASE REGISTRY FOR HEALTHCARE ACTORS)

CoBRHA (Common Base Registry for HealthCare Actors) is de gemeenschappelijke gegevensbank van de openbare instellingen die bevoegd zijn voor de erkenning van de actoren in de gezondheidszorg in België. Deze gegevensbank is een geconsolideerde authentieke bron die een antwoord biedt op 3 vragen met betrekking tot een actor in de gezondheidszorg:

1. Wie is de actor in de gezondheidszorg ?

   De actor kan een individuele beroepsbeoefenaar in de gezondheidszorg zijn (bv. arts, verpleegkundige, …) of een zorginstelling (bv. ziekenhuis, rusthuis, ...).

2. Wat mag de actor doen ?

   Voor een zorginstelling stemt dit overeen met de erkende activiteiten van deze instelling (bv. algemeen ziekenhuis, intensive care, SMUR/MUG, ...). Voor een beroepsbeoefenaar stemt dit overeen met de erkende beroepen en specialisaties van deze persoon (diploma, visum, ...).

3. Welke verantwoordelijkheden heeft de actor ?

   De verantwoordelijkheden van de actor in de gezondheidszorg stemmen overeen met zijn rollen, eventueel ten aanzien van een andere actor in de gezondheidszorg (bv. hoofdgeneesheer in een ziekenhuis).

EIDAS-VERORDENING

Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG en de Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

Zie https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32014R0910

EHEALTH-PLATFORM

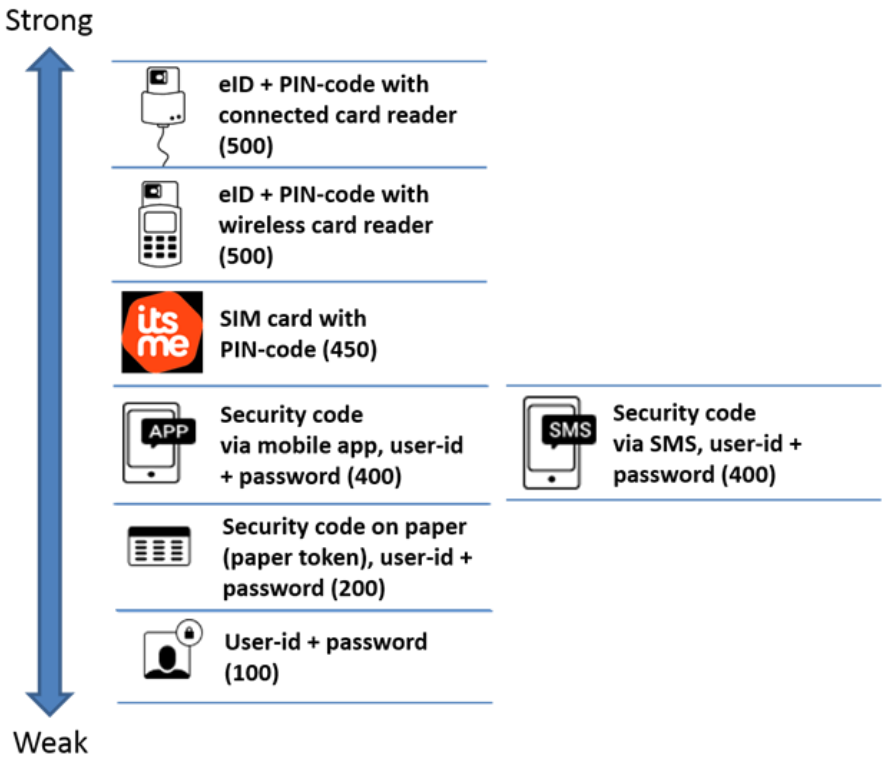
Een overheidsinstelling die tot doel heeft om

- door een onderlinge elektronische dienstverlening en informatie-uitwisseling tussen alle actoren in de gezondheidszorg
- georganiseerd met de nodige waarborgen op het vlak van de informatieveiligheid en de bescherming van de persoonlijke levenssfeer
- de kwaliteit en de continuïteit van de gezondheidszorgverstrekking en de veiligheid van de patiënt te optimaliseren
- de vereenvoudiging van de administratieve formaliteiten voor alle actoren in de gezondheidszorg te bevorderen
- en het gezondheidsbeleid te ondersteunen.

Voor meer informatie, zie https://www.ehealth.fgov.be/ehealthplatform/nl

FEDERAL AUTHENTICATION SERVICE (FAS)

Een dienst aangeboden door de FOD BOSA aan de hand waarvan gebruikers van elektronische diensten hun identiteit kunnen authentiseren via verschillende middelen met stijgend veiligheidsniveau. De FAS is een onderdeel van CSAM, een dienst die een algemene oplossing biedt voor alle aspecten van gebruikers- en toegangsbeheer voor online overheidsdiensten. Zie https://iamapps.belgium.be/sma/generalinfo?view=home



GEBRUIKER

De gebruiker is de persoon die persoonsgegevens verwerkt.

IDENTIFICATIENUMMER SOCIALE ZEKERHEID (INSZ)

Unieke identificatiesleutel per natuurlijk persoon die wordt gebruikt in de overheids-, sociale- en gezondheidssector. Voor de personen opgenomen in het Rijksregister is dit het rijksregisternummer dat vermeld staat op de elektronische identiteitskaart. Voor de andere personen is dit een nummer dat de Kruispuntbank van de Sociale Zekerheid toekent en beheert in een gegevensbank, de KSZ-registers.

INFORMATIEVEILIGHEIDSCOMITE

Het Informatieveiligheidscomité ingesteld bij wet van 5 september 2018, dat o.a. bevoegd is om een principiële machtiging te verstrekker voor elke mededeling van persoonsgegevens door of aan het eHealthplatform.

Voor meer informatie, zie https://www.ehealth.fgov.be/ehealthplatform/nl/wet-van-21-augustus-2008-houdende-oprichting-en-organisatie-van-het-ehealth-platform, meer bepaald artikel 11.

RELEVANT KENMERK

Een attribuut van een entiteit, ander dan de attributen die de identiteit van de entiteit bepalen, zoals een hoedanigheid, een functie in een bepaalde organisatie, een beroepskwalificatie, ..., die relevant is om te bepalen welke toegangsrechten tot persoonsgegevens een entiteit heeft. Een entiteit kan verschillende relevante kenmerken hebben.

RELEVANTE RELATIE

Een relatie tussen een entiteit en een andere entiteit, zoals een zorgrelatie tussen een zorgverstrekker en een zorgvragende, die relevant is om te bepalen welke toegangsrechten tot persoonsgegevens een entiteit heeft. Een entiteit kan verschillende relevante relaties met andere entiteiten hebben.

REGISTRATIE

Het proces waarbij de identiteit van een entiteit, een kenmerk van een entiteit of een relatie tussen entiteiten met een voldoende zekerheid wordt vastgesteld vooraleer middelen ter beschikking worden gesteld aan de hand waarvan de identiteit, een kenmerk of een relatie worden geauthentiseerd of geverifieerd.

UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE EIDAS-VERORDENING

Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

Zie https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ%3AJOL_2015_235_R_0002

VERIFICATIE VAN EEN RELEVANT KENMERK OF RELATIE

Het proces waarbij wordt nagegaan of een relevant kenmerk of een relevante relatie die een entiteit beweert te hebben om gebruik te kunnen maken van een elektronische dienst, effectief een kenmerk of een relatie van deze entiteit is. De verificatie van een kenmerk of een mandaat kan geschieden op basis van

- dezelfde soort middelen als deze gebruikt voor de authenticatie van de identiteit;
- na authenticatie van de identiteit van een entiteit, door de raadpleging van een gegevensbank (authentieke bron) waarin kenmerken of relaties m.b.t. een geïdentificeerde entiteit worden opgeslagen.