Informatieveiligheidscomité

Kamer sociale zekerheid en gezondheid

IVC/KSZG/20/324

BERAADSLAGING NR. 20/174 VAN 7 JULI 2020 MET BETREKKING TOT DE GOEDE PRAKTIJKEN DIE TOEGEPAST DIENEN TE WORDEN DOOR DE MOBIELE APPLICATIES, MET NAME HET VOLDOEN AAN DE CRITERIA OPGESTELD DOOR HET EHEALTH-PLATFORM, TENEINDE TE VOLDOEN AAN NIVEAU 2 (M2) VAN DE VALIDATIEPIRAMIDE

Het Informatieveiligheidscomité,

Gelet op de Verordering (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 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 3°, 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 de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen*;

Gelet op het auditoraatsrapport van het eHealth-platform;

Gelet op het verslag van de heer Bart Viaene;

Beslist op 7 juli 2020, na beraadslaging, als volgt:

I. ONDERWERP VAN DE AANVRAAG

1. MHealthBelgium is een platform dat alle relevante en vereiste informatie over mobiele applicaties voor zorginstellingen, zorgprofessionals en patiënten centraliseert. Het platform gebruikt een validatiepiramide bestaande uit drie niveaus om te beoordelen of de mobiele applicaties voldoen aan de nodige voorwaarden inzake kwaliteit, veiligheid en doeltreffendheid:

- het eerste niveau (M1) bepaalt de basiscriteria. De mobiele applicaties dienen over een CE-markering te beschikken, alsook in overeenstemming te zijn met de regelgeving voor medische hulpmiddelen en de Algemene Verordening Gegevensbescherming. Het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten is verantwoordelijk voor dit niveau.

- het tweede niveau (M2) bepaalt voorwaarden met betrekking tot informatieveiligheid en met betrekking tot de interoperabiliteit met andere mobiele applicaties en ICT-toepassingen binnen de gezondheidszorg, zoals de basisdiensten van het ehealth-platform. Derhalve werd aan het ehealth-platform gevraagd om deze voorwaarden vast te leggen. De mobiele applicaties dienen vervolgens een risicobeoordeling te ondergaan door een onafhankelijke organisatie, teneinde de interoperabiliteit te testen. Ten slotte moeten de mobiele applicaties voldoen aan alle basiscriteria (niveau 1).

- het derde en laatste niveau (M3) is enkel bestemd voor mobiele applicaties die over een aangetoonde gezondheidseconomische meerwaarde beschikken. Mobiele applicaties onder M3 dienen bovendien te voldoen aan alle criteria van niveaus 1 en 2. Het RIZIV, dat verantwoordelijk is voor dit niveau, dient een formeel raamwerk te ontwikkelen voor de financiering van de applicaties.

2. Voor wat betreft het tweede niveau van de validatiepiramide heeft het ehealth-platform reeds een ontwerplijst[1] van 6 criteria vastgesteld:

- App classification;
- Identification of the person in need of care;
- App user authentification;
- Verification of relevant characteristics and relationships of the app user;
- Interoperability;
- Compliance with the general data of protection regulation (GDPR).

Webapplicaties dienen cumulatief aan deze criteria te voldoen, teneinde een "validatiestempel" voor M2 te kunnen bekomen.

3. Het Informatieveiligheidscomité neemt bijgevolg kennis van de criteria.

[1] Zie bijlage voor een meer uitgebreide omschrijving.

II. BEVOEGDHEID

4. Krachtens artikel 46 §1 1° van de wet van 16 januari 1990 *houdende de oprichting en organisatie van een Kruispuntbank de sociale zekerheid* is de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, met het oog op de bescherming van de persoonlijke levenssfeer onder andere belast met het formuleren van de goede praktijken die het nuttig acht voor de uitvoering en de naleving van deze wet en haar uitvoeringsmaatregelen en 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.

5. Het Informatieveiligheidscomité oordeelt bijgevolg dat het bevoegd is.

III. GOEDE PRAKTIJKEN

6. Rekening houdend met de principes van de Algemene Verordening Gegevensbescherming (AVG) en de bepalingen van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*, formuleert de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité de volgende praktijk die door de mobiele toepassingen gerespecteerd dient te worden:

Teneinde te voldoen aan niveau 2 (M2) van de validatiepiramide, dienen de in bijlage opgesomde criteria, opgesteld door het ehealth-platform, cumulatief in acht genomen te worden.

Bart VIAENE

Bijlage: Criteria teneinde te voldoen aan niveau 2 (M2) van de validatiepiramide

OVERVIEW OF THE CRITERIA

CRITERION 1: APP CLASSIFICATION

Depending on the data processed by the app, the app is classified into one of the following three categories:

- Category 1: the application does not process any personal data as defined in the General Data Protection Regulation (GDPR)
- Category 2: the application processes personal data as defined in the General Data Protection Regulation (GDPR) but does not process sensitive personal data as defined in Article 9 GDPR , such as health data;
- Category 3: the app processes sensitive personal data as defined in Article 9 GDPR.

Processing of data by the app not only means the processing of data on the device on which the app is installed, but also the possible processing of data on information systems with which the app continuously or regularly exchanges data.

CRITERION 2: IDENTIFICATION OF THE PERSON IN NEED OF CARE

Apps of category 2 or 3 uniquely identify the person in need of care about whom data are processed through his/her Social Security Identification Number (SSIN)

- during the authentication process of the person in need of care when using the app;
- when processing the personal data about the person in need of care.

CRITERION 3: APP USER AUTHENTICATION

Apps of category 2 or 3, or applications that provide access to data that are processed through an application of category 2 or 3, authenticate the application's user.

This authentication is done

- either by using a method integrated within the Federal Authentication Service (FAS) of a level equal to or higher than the level determined by the Board of Directors of the eHealth platform ;
- or by an authentication system specific to the provider, provided that the three following conditions are met:
  - a registration of the identity takes place on the basis of a one-off use of an authentication method integrated in the FAS of a level that is equal to or higher than the level determined by the Board of Directors of the eHealth platform and
  - the provider's own authentication system meets the requirements for a « substantial » assurance level, as specified in points 2.1, 2.2.1, element 2, 2.2.3, 2.2.4, 2.3.1 (excepting element 1) and 2.4 of the Annex to the Implementing Regulation (EU) 2015/1502 of the EIDAS Regulations and

- the means of authentication used in the provider's own authentication system and its activation process meet the requirements for a « low » assurance level in point 2.2.1, element 1 and point 2.2.2 of the Annex to Implementing Regulation (EU) 2015/1502 of the EIDAS Regulation, and it has been designed in such a way that it can be assumed that it will only be used by the person to whom it belongs.

At this moment, the minimum level in the FAS, determined by Board of Directors of the eHealth platform is level 400.

CRITERION 4: VERIFICATION OF RELEVANT CHARACTERISTICS AND RELATIONSHIPS OF THE APP USER

If the use of apps from category 2 or 3 requires the verification of relevant characteristics or relationships of the app user, these attributes/qualities or relationships are consulted in the relevant authentic sources accessed via the eHealth platform.

This consultation is done

- either via the eHealth platform user and access management system
- or through up-to-date user information provided by the app provider, originating from an authentic source accessible via the eHealth platform.

CRITERION 5: INTEROPERABILITY

If the app itself or information systems on which data originating from the app are processed, exchanges structured personal data with information systems of healthcare actors, such as care providers, care institutions or people in need of care, this exchange takes place via open standards, and preferably via the standards set by the eHealth platform, if available.

CRITERION 6: COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATION (GDPR)

The providers of category 2 or 3 apps confirm that the processing of personal data takes place in accordance with the provisions of the General Data Protection Regulation (GDPR).

In particular, this means that they confirm they

- comply with the principles stated in article 5 of the GDPR , in particular
  - lawfulness, fairness and transparency; purpose limitation;
  - data minimisation;
  - accuracy ;
  - storage limitation;
  - integrity and confidentiality;
- honour the rights of the data subject mentioned in Chapter III of the General Data Protection Regulation (GDPR)
- comply with the special provisions of the General Data Protection Regulation (GDPR) on the processing of sensitive personal data when the application belongs to category 3.

The providers of category 3 apps confirm that they have carried out a data protection impact assessment according to articles 35 and 36 of the General Data Protection Regulation (GDPR) and have made it publicly available, indicating the url where it is available.

In case the communication of personal data by the application requires an authorization from the Information Security Committee according to Chapter VII of the Act of December 13, 2006 containing various provisions concerning health, this communication only takes place after such authorization has been obtained and in accordance with the provisions of this authorization.

_____

GLOSSARY

AUTHENTICATION

The process of verifying whether the identity that an entity claims to have in order to use an electronic service, is the correct identity. The authentication can be done by verifying

- knowledge (e.g. a password);
- possession (e.g. a certificate on an electronically readable card);
- biometric property(ies);
- a combination of one or more of these means.

AUTHENTIC SOURCE

A database made available via the eHealth platform with reliable information about relevant characteristics and / or relevant relationships.

EHEALTH PLATFORM

A public institution that aims

- to optimise the quality and continuity of healthcare delivery and patient safety
- to facilitate the simplification of administrative formalities for all actors in health care
- and to support health policy by organising
- mutual electronic services and information exchange between all actors in health care
- with the necessary guarantees in the field of information security and the protection of privacy

For more information, see https://www.ehealth.fgov.be/ehealthplatform/nl

EIDAS REGULATION

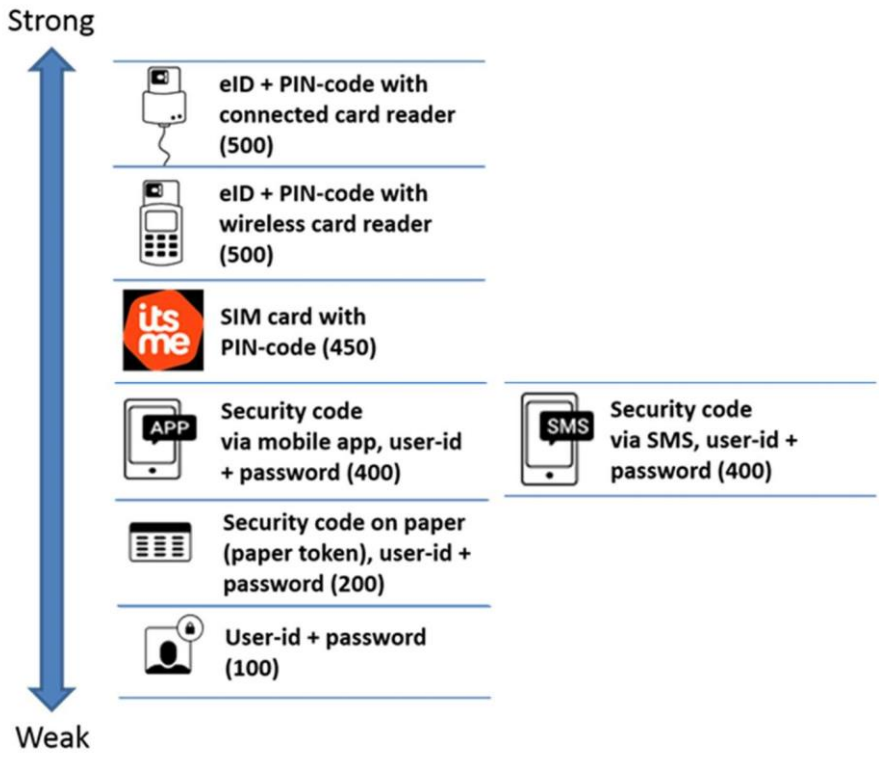
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

See

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002.

FEDERAL AUTHENTICATION SERVICE (FAS)

A service offered by the FPS BOSA that enables users of electronic services to validate their identity by various means with an increasing security level. The FAS is part of CSAM, a service that offers a comprehensive solution for all aspects of user and access management to online government services. See https://iamapps.belgium. be/sma/generalinfo?view=home



GENERAL DATA PROTECTION REGULATION (GDPR)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

REGISTRATION

The process whereby the identity of an entity, a characteristic of an entity or a relationship between entities is determined with sufficient certainty before means are made available on the basis of which the identity, a characteristic or a relationship is authenticated or verified.

RELEVANT CHARACTERISTIC

An attribute of an entity other than the attributes that determine the identity of the entity, such as a capacity, a function in a particular organisation, a professional qualification, that is relevant to determine which access rights to personal data an entity has. One entity can have several relevant characteristics.

RELEVANT RELATIONSHIP

A relationship between an entity and another entity, such as a care relationship between a care provider and a person in need of care, that is relevant to determine which access rights to personal data an entity has. An entity may have several relevant relationships with other entities.

SOCIAL SECURITY IDENTIFICATION NUMBER (SSIN)

A unique identification key per natural person commonly used within the government, social and health sector. For persons included in the National Register, this is the national register number mentioned on the electronic identity card. For all other persons, this is a number that the Crossroads Bank for Social Security assigns and manages in a database, known as the CBSS registers.

VERIFICATION OF A RELEVANT CHARACTERISTIC OR RELATIONSHIP

The process of verifying whether a relevant characteristic or a relevant relationship that an entity claims to have in order to use an electronic service, is effectively an attribute or a relationship of this entity. The verification of a feature or an office can be effected on the basis of

- the same kind of means as used for authentication;
- after entity authentication, by consulting a database (authentic source) in which characteristics or relationships are stored with regard to an identified entity.

INTERPRETATION NOTES

CRITERION 2: IDENTIFICATION OF THE PERSON IN NEED OF CARE

Apps of category 2 or 3 uniquely identify the person in need of care about whom data are processed through his/her Social Security Identification Number (SSIN)

- during the authentication process of the person in need of care when using the app;
- when processing the personal data about the person in need of care.

Use of the SSIN number

Reference	Article	Link
WET VAN 21 AUGUSTUS 2008 HOUDENDE OPRICHTING EN ORGANISATIE VAN HET EHEALTH-PLATFORM Belgisch Staatsblad van 13 oktober 2008 [Gewijzigd bij wet van 19 maart 2013 (Belgisch Staatsblad van 29 maart 2013), bij wet van 10 april 2014 (Belgisch Staatsblad van 30 april 2014), bij wet van 21 juli 2016 (Belgisch Staatsblad van 28 september 2016) bij wet van 5 september 2018 (Belgisch Staatsblad van 10 september 2018)]	Artikel 8 Bij de mededeling van niet-gecodeerde persoonsgegevens aan en door het eHealth-platform worden uitsluitend de identificatienummers bedoeld in artikel 8 van de Wet Kruispuntbank Sociale Zekerheid gebruikt.	https://www.ehealth.fgov.be/ehealthplatform/nl/wet-van-21-augustus-2008houdende-oprichting-enorganisatie-van-hetehealth-platform
LOI DU 21 AOÛT 2008 RELATIVE À L'INSTITUTION ET À L'ORGANISATION DE LA PLATE-FORME EHEALTH Moniteur belge du 13 octobre 2008 [Modifiée par la loi du 10 avril 2014 (Moniteur belge du 30 avril 2014)] et [Modifiée par la loi du 5 septembre 2018 (Moniteur belge du 10 septembre 2018)]	Article 8 Lors de la communication de données à caractère personnel non codées à ou par la plate-forme eHealth, seuls les numéros d'identification visés à l'article 8 de la loi relative à la Banque Carrefour de la sécurité sociale sont utilisés.	https://www.ehealth.fgov.be/ehealthplatform/fr/loidu-21-aout-2008-relativea-linstitution-et-alorganisation-de-la-plateforme-ehealth

This means that every actor that uses at least one of the basic services of the eHealth Platform should use the SSIN number to uniquely identify the patient when the exchange contains non-coded (identifiable) personal data.

Actors in the health sector have been authorized or can be authorized formally to use the SSIN in that respect.

MHEALTH PLATFORMS IDENTIFIED BY EHP NUMBER

The EHP number is an identifier that is issued by the Belgian Federal eHealth platform to an organization/platform. Without a suitable identifier, these organisations/platforms cannot use the basic services of the eHealth platform.

EHP numbers are attributed to organisations who are not known in the eHealth ecosystem and cannot be identified otherwise. When an organisation possesses ex. a NIHII number, this identifier is used.

CONDITIONS FOR OBTAINING AN EHP NUMBER (FOR MHEALTH PLATFORMS)

- M1 compliant;
- commit to using the eHealth basic services. Minimum requirement is the use of the eHealth IAM system and the use of therapeutic relationships and patient consent;
- when using the Token Exchange service, all conditions to use this service must be fulfilled https://www.ehealth.fgov.be/ehealthplatform/file/view/AWRqRnFkRwIvE61VSt9?filename=IAM%20Connect%20Token%20eXchange%20-%20Tech%20Specs%20v1_2%20dd%2002012019.pdf);
- all personal and medical data are encrypted (when stored on the platform);
- security loggings on the platform are obligatory.

HOW TO OBTAIN A EHP NUMBER?

Since this is an exceptional procedure you should contact the Belgian eHealth

platform. Contact ehealthppkb@ehealth.fgov.be