Comité de sécurité de l'information

Chambre sécurité sociale et santé

CSI/CSSS/20/324

DÉLIBÉRATION N° 20/174 DU 7 JUILLET 2020 RELATIVE AUX BONNES PRATIQUES À APPLIQUER AUX APPLICATIONS MOBILES, À SAVOIR RÉPONDRE AUX CRITÈRES ÉTABLIS PAR LA PLATE-FORME EHEALTH, AFIN DE SATISFAIRE AU NIVEAU 2 (M2) DE LA PYRAMIDE DE VALIDATION

Le Comité de sécurité de l'information,

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (Règlement général relatif à la protection des données ou AVG);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu la loi du 3 décembre 2017 *relative à la création de l'Autorité de protection des données*, en particulier l'article 114, modifié par la loi du 25 mai 2018 ;

Vu la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, en particulier l'article 42, § 2, 3°, modifié par la loi du 5 septembre 2018 ;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, notamment l'article 97;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant dispositions diverses* ;

Vu le rapport d'auditorat de la Plate-forme eHealth ;

Vu le rapport de monsieur Bart Viaene ;

Émet, après délibération, la décision suivante, le 7 juillet 2020:

I. OBJET DE LA DEMANDE

1. MHealthBelgium est une plateforme qui centralise toutes les informations utiles et pertinentes au sujet des applications mobiles destinées aux patients, professionnels de soins ou institutions de soins. La plateforme utilise une pyramide de validation à 3 niveaux pour évaluer si les applications mobiles satisfont aux conditions requises en matière de qualité, de sécurité et d'efficacité:

- le premier niveau (M1) définit les critères de base. Les applications mobiles doivent disposer d'un marquage CE ainsi qu'être conformes à la réglementation sur les dispositifs médicaux et au Règlement général sur la protection des données. L'Agence fédérale des médicaments et des produits de santé est responsable pour ce niveau.

- le deuxième niveau (M2) définit les conditions relatives à la sécurité de l'information et à l'interopérabilité avec d'autres applications mobiles et applications informatiques au sein des soins de santé, telles les services de base de la Plate-forme eHealth. C'est pourquoi il a été demandé à la Plate-forme eHealth de définir ces conditions. Les applications mobiles doivent ensuite être soumises à une évaluation des risques par une organisation indépendante, aux fins de tester l'interopérabilité. Enfin, les applications mobiles doivent satisfaire à l'ensemble des critères de base (niveau 1).

- le troisième et dernier niveau (M3) est réservé aux applications mobiles offrant une plus-value au niveau de l'économie de la santé. Les applications mobiles de niveau 3 doivent par ailleurs répondre à tous les critères du niveau M1 et du niveau M2. L'INAMI qui est responsable pour ce niveau doit développer un cadre formel pour le financement des applications.

2. En ce qui concerne le deuxième niveau de la pyramide de validation, la Plate-forme eHealth a déjà fixé un projet de liste[1] de 6 critères:

- 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).

Les applications web doivent répondre à ces critères de manière cumulative, afin d'obtenir un « cachet de validation » pour le niveau M2.

3. Le Comité de sécurité de l'information prend par conséquence connaissance des critères.

[1] Voir l'annexe pour une description plus détaillée.

II. COMPÉTENCE

4. En vue de l'article 46, §1, 1° de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-Carrefour la sécurité sociale*, la chambre sécurité sociale et santé du Comité de sécurité de l'information est, en vue de la protection de la vie privée, notamment chargée de formuler les bonnes pratiques qu'elle juge utiles pour l'application et le respect de la présente loi et de ses mesures d'exécution et des dispositions fixées par ou en vertu de la loi visant à la protection de la vie privée à l'égard des traitements de données à caractère personnel relatives à la santé.

5. Le Comité de sécurité de l'information estime par conséquent qu'il est compétent.

III. BONNES PRATIQUES

6. Compte tenu des principes du RGPD et des dispositions de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, la chambre sécurité sociale et santé du Comité de sécurité de l'information formule les pratiques suivantes qui doivent être respectées par les applications mobiles.

Afin de satisfaire au niveau 2 (M2) de la pyramide de validation, les critères énumérés en annexe qui ont été déterminés par la Plate-forme eHealth doivent être respectés de manière cumulative.

Bart VIAENE

Annexe: critères à respecter pour satisfaire au niveau 2 (M2) de la pyramide de validation

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

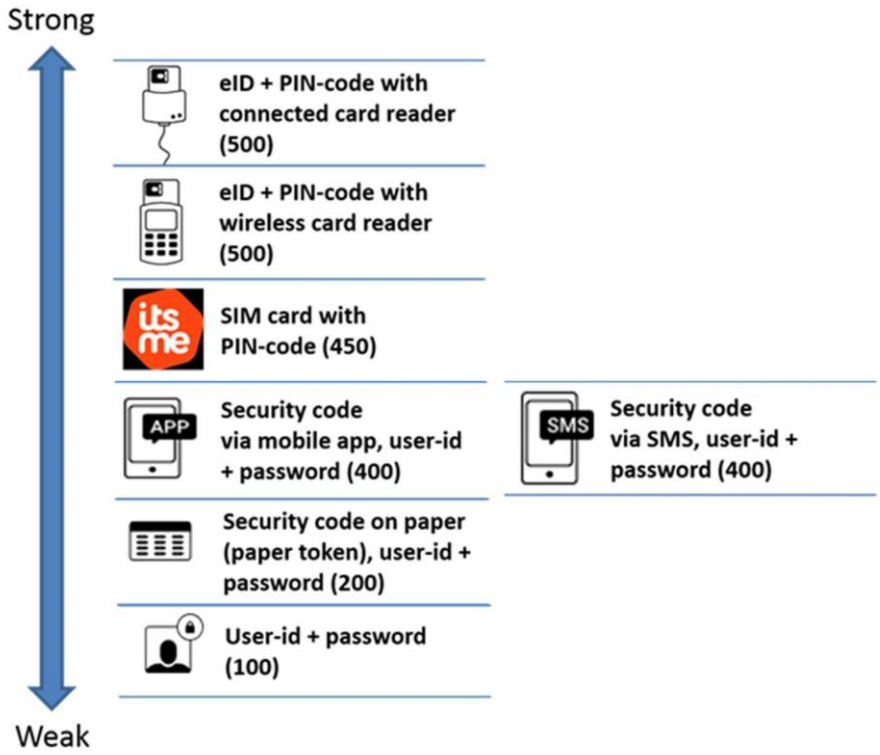
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on 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