Règlement fixant les critères en vue de l'application d'un cercle de confiance par une organisation dans le cadre de l'échange des données de santé

OBJECTIF DU RÈGLEMENT

Le traitement de données à caractère personnel, en particulier de données à caractère personnel relatives à la santé, doit intervenir dans le respect des mesures relatives à la sécurité de l'information et à la protection de la vie privée. Un aspect essentiel dans ce contexte est la garantie que les données à caractère personnel sont uniquement traitées

- pour des finalités légitimes et
- par des personnes qui, pour pouvoir réaliser ces finalités, ont besoin de traiter des données à caractère personnel relatives à la personne concernée.

Dans un système de traitement mutualisé de données à caractère personnel par de nombreux acteurs, l'offre de ce type de garantie requiert que les responsabilités de chacun soient clairement définies.

Le présent règlement entend y contribuer en précisant le concept des 'cercles de confiance'. Un 'cercle de confiance' est un groupe d'utilisateurs d'une organisation pour lequel cette organisation prend elle-même, à plusieurs niveaux, des mesures relatives à la sécurité de l'information et en surveille le respect correct, de sorte que d'autres organisations puissent raisonnablement avoir confiance que ces mesures de sécurité de l'information sont respectées et qu'elles ne doivent pas les organiser ou les surveiller elles-mêmes.

Les cercles de confiance peuvent être organisés par de nombreuses organisations telles les hôpitaux, les instances chargées de l'évaluation des besoins dans le cadre de Belrai, les mutualités, etc.

Pour que des organisations autres que l'organisation qui met en place un cercle de confiance, puissent légitimement y faire confiance, des critères sont fixés auxquels doit satisfaire toute organisation qui souhaite organiser ce type de cercle de confiance. Ces critères renvoient, dans toute la mesure du possible, à la législation belge et européenne actuelle telle le Règlement général sur la protection des données (RGPD). Ils ne portent pas préjudice à cette réglementation qui reste pleinement en vigueur, mais ils précisent dans certains cas comment il y a lieu de satisfaire à cette réglementation.

Les critères mêmes se concrétisent sous la forme d'un règlement. Pour une bonne compréhension, des précisions sont apportées à certains critères. Ces précisions sont données à titre purement indicatif.

LISTE DES CRITÈRES

THÈME 1: PRINCIPE DE LÉGITIMITÉ ET DE LIMITATION DE LA FINALITÉ

CRITÈRE 1: REGISTRE DES ACTIVITÉS DE TRAITEMENT

L'organisation dispose, pour les activités de traitement concernant les demandeurs de soins, d'un registre des activités de traitement tel que visé à l'article 30 du Règlement général sur la protection des données (RGPD), qui mentionne les finalités de traitement légitimes des activités de traitement.

CRITÈRE 2: PRÉCISION DES FONDEMENTS POUR LE TRAITEMENT DE CATÉGORIES SPÉCIFIQUES DE DONNÉES À CARACTÈRE PERSONNEL

Le registre des activités de traitement mentionne, pour le traitement de catégories spécifiques de données à caractère personnel visées à l'article 9, 1, du Règlement général sur la protection des données (RGPD), concernant les demandeurs de soins, le(s) fondement(s) visé(s) à l'article 9, 2, du RGPD permettant le traitement des catégories spécifiques de données à caractère personnel.

THÈME 2: PRINCIPE DE PROPORTIONNALITÉ

CRITÈRE 3: LIMITATION DU TRAITEMENT

Les données à caractère personnel relatives aux demandeurs de soins, en particulier les catégories spécifiques de données à caractère personnel visées à l'article 9, 1, du Règlement général sur la protection des données (RGPD) peuvent uniquement être traitées par des utilisateurs qui doivent pouvoir les traiter, dans le chef de leur fonction, pour les finalités de traitement légitimes telles que décrites dans le registre des activités de traitement. Les possibilités de traitement sont modulées de façon suffisamment détaillée, de sorte que tout utilisateur ne puisse traiter que les seules données à caractère personnel relatives aux demandeurs de soins pour lesquels ce traitement est nécessaire dans le cadre de sa fonction et pendant la période pendant laquelle ce traitement est nécessaire dans le cadre de sa fonction.

THÈME 3: GESTION DES ACCÈS ET DES UTILISATEURS

CRITÈRE 4: AUTHENTIFICATION DE L'IDENTITÉ DE L'UTILISATEUR

L'organisation authentifie l'identité de la personne physique qui traite les catégories spécifiques de données à caractère personnel visées à l'article 9, 1, du Règlement général sur la protection des données (RGPD) (l'utilisateur').

Cette authentification intervient soit

- par un moyen intégré dans le Federal Authentication Service (FAS) d'un niveau identique ou supérieur au niveau fixé par le Comité de gestion de la Plate-forme eHealth;
- par un système d'authentification propre à l'organisation
  - à condition qu'un enregistrement de l'identité soit effectué au moyen d'un usage unique d'un moyen d'authentification intégré dans le FAS d'un niveau identique ou supérieur au niveau fixé par le Comité de gestion de la Plate-forme eHealth et
  - à condition que le moyen d'authentification propre à l'organisation satisfasse aux conditions d'un niveau de garantie « substantiel », tel que précisé dans les points 2.1., 2.2.1 élément 2, 2.2.3., 2.2.4., 2.3.1. (à l'exception de l'élément 1) et 2.4. de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS et
  - à condition que le moyen d'authentification utilisé dans le système d'authentification propre à l'organisation et que son processus d'activation satisfassent aux conditions d'un niveau de garantie « faible », tel que précisé dans les points 2.2.1. élément 1, et 2.2.2.de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS et qu'il ait été conçu de la sorte que l'on peut présumer qu'il ne sera utilisé que par la personne à laquelle il appartient.

Actuellement, le niveau minimal dans le FAS fixé par le Comité de gestion de la Plate-forme eHealth est le niveau 400 pour les personnes physiques agissant en tant que prestataire de soins et le niveau 350 pour les personnes physiques agissant en tant que demandeur de soins.

Précision
L'usage unique d'un moyen d'authentification intégré dans le FAS afin d'enregistrer l'identité de l'utilisateur n'implique pas que le FAS même doive être utilisé à cet effet. La carte d'identité électronique peut par exemple aussi être demandée pour comparer visuellement la photo avec le détenteur de la carte ou lue au moyen d'une implémentation propre à l'organisation concernée. Le système d'authentification propre à l'organisation doit satisfaire aux conditions du niveau de garantie « substantiel » de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS, en ce sens que le moyen d'authentification peut effectivement être un moyen d'authentification qui fait usage de seulement un facteur d'authentification (par exemple, numéro d'utilisateur et mot de passe).

CRITÈRE 5: VÉRIFICATION DES CARACTÉRISTIQUES PERTINENTES ET DES RELATIONS DE L'UTILISATEUR

Si le traitement électronique de catégories spécifiques de données à caractère personnel visées à l'article 9, 1, du Règlement général sur la protection des données requiert la vérification de caractéristiques pertinentes ou de relations de l'utilisateur, ces caractéristiques ou relations sont consultées

- soit dans les sources authentiques définies par le Comité de gestion de la Plate-forme eHealth
- soit dans une banque de données de l'organisation ou d'un réseau de santé dont l'organisation fait partie et qui est, le cas échéant, synchronisée avec les informations de qualité provenant des sources authentiques définies par le Comité de gestion de la Plate-forme eHealth.

Le Comité de gestion a jusqu'à présent défini l'utilisation des sources authentiques suivantes :

- Cobrha
- la banque de données des mutualités en rapport avec les détenteurs d'un Dossier Médical Global.

Précision
Il est essentiel que les informations utilisées en rapport avec les caractéristiques pertinentes d'un utilisateur ou des relations de l'utilisateur avec par exemple son organisation ou le demandeur des soins soient de qualité et à jour. C'est dans cette optique qu'ont été développées des sources dites authentiques, telles Cobrha ou la banque de données des détenteurs d'un Dossier médical global auprès des mutualités. Il est primordial que ces informations à jour et de qualité qui sont disponibles dans ces sources authentiques soient utilisées, soit en consultant directement la source authentique concernée, soit en synchronisant, le cas échéant, la banque de données de l'organisation par rapport à ces sources authentiques.

THÈME 4: LOGGINGS

CRITÈRE 6: LOGGING INTERNE

L'accès électronique aux données à caractère personnel fait l'objet d'une prise de traces (logs). La gestion des logs doit au moins répondre aux objectifs suivants

- permettre de déterminer rapidement et de manière aisée quelle personne physique a eu accès à quelles données à caractère personnel relatives à quelle personne, à quel moment et de quelle manière;
- pouvoir identifier de manière univoque la personne qui a traité des données à caractère personnel et la personne concernant laquelle les données à caractère personnel sont traitées;
- mettre les outils nécessaires à la disposition afin de permettre une exploitation des données de logging par des personnes autorisées;

- conserver les données de logging au moins pendant 10 ans.

CRITÈRE 7: AUDIT TRAIL

Si le traitement électronique de données à caractère personnel implique l'accès à des données à caractère personnel traitées par des tiers, il y a lieu de garantir, en cas d'investigation à l'initiative de la Plate-forme eHealth, ou d'un organe de contrôle, suite à une plainte, qu'une reconstitution complète puisse avoir lieu dans le but est de déterminer quelle personne physique a eu accès à quels types de données à caractère personnel concernant quelles personnes, à quel moment et de quelle manière. Des méthodes permettant cette reconstitution complète sont décidées sous la coordination de la Plate-forme eHealth.

THÈME 5: INFORMATION, FORMATION, SENSIBILISATION, CONTRÔLE ET SANCTION

CRITÈRE 8: INFORMATION, FORMATION ET SENSIBILISATION

L'organisation rédige les directives nécessaires afin d'exécuter les critères prévus dans le présent document, les met à la disposition, d'une manière généralement accessible, de l'ensemble des utilisateurs qui font partie du cercle de confiance, offre une formation permanente adéquate à ces utilisateurs et les sensibilise en permanence concernant le respect des directives.

CRITÈRE 9: CONTRÔLE INTERNE

L'organisation organise un contrôle interne régulier quant au respect des critères contenus dans le présent document et des directives qui les exécute. L'organisation conserve les résultats de ce contrôle interne pendant 2 ans. L'organisation prévoit des sanctions dissuasives vis-à-vis des utilisateurs qui font partie du cercle de confiance qui ne respecteraient pas les critères ou les directives qui les exécutent.

THÈME 6: RESPECT DES DÉLIBÉRATIONS DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

CRITÈRE 10: RESPECT DES DÉLIBÉRATIONS DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

L'organisation assure respecter l'ensemble des mesures relatives à la sécurité de l'information et à la protection de la vie privée qui sont contenues dans les délibérations applicables du Comité de sécurité de l'information.

THÈME 7: VÉRIFICATION

CRITÈRE 11: ENREGISTREMENT DANS LA SOURCE AUTHENTIQUE COBRHA EN TANT QU'ORGANISATION METTANT EN PLACE UN CERCLE DE CONFIANCE

L'organisation signale, par écrit, au gestionnaire des informations la concernant dans la source authentique Cobrha qu'elle met en place un cercle de confiance, conformément aux conditions mentionnées dans le présent document, et confirme à cet égard qu'elle satisfait à chacune de ces conditions. Dans la source authentique Cobrha, il est mentionné que l'organisation a mis en place un cercle de confiance.

CRITÈRE 12: DOCUMENTATION PUBLIQUE

L'organisation publie sur son site web, en des termes compréhensibles, les finalités du traitement pour lesquelles elle traite des données à caractère personnel relatives aux demandeurs de soins ainsi que la politique portant exécution du principe de proportionnalité.

CRITÈRE 13: CONTRÔLE EXTERNE

L'organisation tient le registre des activités de traitement et les documents et politiques qu'elle élabore en vue du respect de ces conditions, ainsi que les résultats du contrôle interne, à la disposition du Comité de sécurité de l'information et des organes de contrôle.

ANNEXE : GLOSSAIRE

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

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.

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

AUTHENTIFICATION DE L'IDENTITÉ

Le processus permettant de vérifier que l'identité qu'une entité prétend posséder pour pouvoir faire appel à un service électronique, est l'identité exacte. L'authentification de l'identité peut intervenir sur la base d'un contrôle

- des connaissances (p.ex. un mot de passe);
- d'une possession (p.ex. un certificat sur une carte lisible par la voie électronique);
- d'une ou des caractéristiques biométriques;
- d'une combinaison d'un ou plusieurs de ces moyens.

SOURCE AUTHENTIQUE

Une banque de données qui contient des informations fiables sur les caractéristiques pertinentes et/ou les relations pertinentes, qui est accessible via le service de base de gestion des utilisateurs et des accès de la Plate-forme eHealth.

CERCLE DE CONFIANCE

Un cercle de confiance est un groupe d'utilisateurs d'une organisation pour lequel l'organisation même prend, à plusieurs niveaux, des mesures relatives à la sécurité de l'information et en surveille le respect correct, de sorte que d'autres organisations puissent raisonnablement avoir confiance que ces mesures de sécurité de l'information sont respectées et qu'elles ne doivent pas les organiser ou les contrôler elles-mêmes.

COBRHA (COMMON BASE REGISTRY FOR HEALTHCARE ACTORS)

CoBRHA (Common Base Registry for HealthCare Actors) est la banque de données commune des institutions publiques compétentes pour l'agrément des acteurs des soins de santé en Belgique. Cette banque de données est une source authentique consolidée offrant une réponse à 3 questions relatives à un acteur des soins de santé.

1. Qui est l'acteur dans les soins de santé?

   L'acteur peut être un professionnel des soins de santé individuel (p.ex. médecin, infirmier, ...) ou un établissement de soins (p.ex. hôpital, maison de repos, ...).

2. Qu'est-ce que l'acteur peut faire?

   Pour un établissement de soins, cela correspond aux activités agréées de cet établissement (p.ex. hôpital général, soins intensifs, SMUR/MUG, ...). Pour un professionnel des soins de santé, cela correspond aux professions agréées et aux spécialisations de cette personne (diplôme, visa, ...).

3. Quelles sont les responsabilités de l'acteur?

   Les responsabilités de l'acteur des soins de santé correspondent à ses rôles, éventuellement à l'égard d'un autre acteur des soins de santé (p.ex. médecin en chef dans un hôpital).

RÈGLEMENT EIDAS

Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE et Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

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

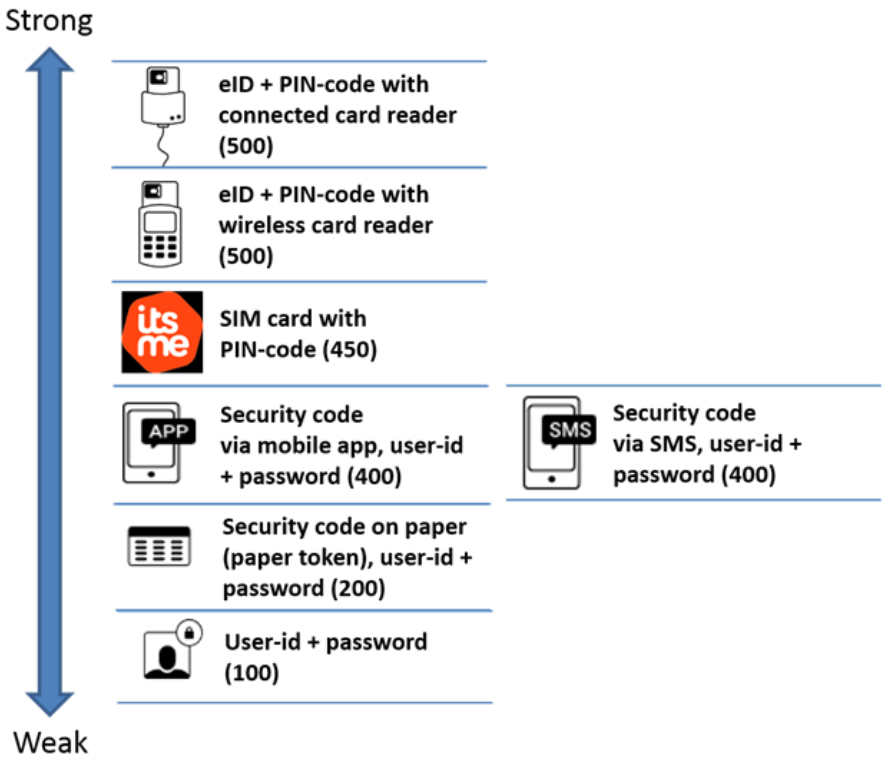
PLATE-FORME EHEALTH

Une institution publique qui a pour mission

- par une prestation de services et un échange d'information mutuels électroniques entre tous les acteurs des soins de santé
- organisés avec les garanties nécessaires en ce qui concerne la sécurité de l'information, la protection de la vie privée du patient
- d'optimaliser la qualité et la continuité des prestations de soins de santé et la sécurité du patient
- de simplifier les formalités administratives pour tous les acteurs des soins de santé
- de soutenir la politique en matière de soins de santé

Pour plus d'informations, voir https://www.ehealth.fgov.be/ehealthplatform/fr

Un service offert par le SPF BOSA permettant aux utilisateurs de services électroniques d'authentifier leur identité par différents moyens dont le niveau de sécurité est croissant. Le FAS fait partie du CSAM, un service offrant une solution générale pour tous les aspects de la gestion des utilisateurs et des accès pour les services publics en ligne. Voir https://iamapps.belgium.be/sma/generalinfo?view=home



UTILISATEUR

L'utilisateur est la personne qui traite des données à caractère personnel.

NUMÉRO D'IDENTIFICATION DE LA SÉCURITÉ SOCIALE (NISS)

Clé d'identification unique par personne physique utilisée dans les secteurs public, social et de la santé. Pour les personnes enregistrées dans le Registre national, il s'agit du numéro de registre national qui est mentionné sur la carte d'identité électronique. Pour les autres personnes, il s'agit d'un numéro qui est attribué par la Banque Carrefour de la sécurité sociale et géré dans une banque de données, appelée registres BCSS.

COMITÉ DE SÉCURITÉ DE L'INFORMATION

Le Comité de sécurité de l'information institué par la loi du 5 septembre 2018, qui est notamment compétent pour rendre une autorisation de principe pour toute communication de données à caractère personnel par la Plate-forme eHealth ou à la Plate-forme eHealth.

Pour plus d'informations, voir https://www.ehealth.fgov.be/ehealthplatform/fr/loi-du-21-aout-2008-relative-a-linstitution-et-a-lorganisation-de-la-plate-forme-ehealth, en particulier l'article 11.

CARACTÉRISTIQUE PERTINENTE

Un attribut d'une entité autre que les attributs qui déterminent l'identité de l'entité tels qu'une qualité, une fonction dans une organisation déterminée, une qualification professionnelle, ... qui est significative pour la détermination des droits d'accès d'une entité à des données à caractère personnel. Une entité peut avoir différentes caractéristiques pertinentes.

RELATION PERTINENTE

Une relation entre une entité et une autre entité telle qu'une relation de soins entre un prestataire de soins et un demandeur de soins, qui est pertinente pour la détermination des droits d'accès d'une entité à des données à caractère personnel. Une entité peut avoir différentes relations pertinentes avec d'autres entités.

ENREGISTREMENT

Le processus permettant de déterminer avec suffisamment de certitude l'identité d'une entité, une caractéristique d'une entité ou une relation entre entités avant la mise à la disposition de moyens permettant d'authentifier ou de vérifier l'identité, une caractéristique ou une relation.

RÈGLEMENT D'EXÉCUTION (UE) 2015/1502 DU RÈGLEMENT EIDAS

Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

Voir https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32015R1502&from=FR

VÉRIFICATION D'UNE CARACTÉRISTIQUE OU D'UNE RELATION PERTINENTE

Le processus permettant de vérifier que la caractéristique pertinente ou la relation pertinente qu'une entité prétend posséder afin de pouvoir faire appel à un service électronique, est effectivement une caractéristique ou une relation de cette entité. La vérification d'une caractéristique ou d'un mandat peut intervenir sur la base

- du même type de moyens que ceux utilisés pour l'authentification de l'identité;
- après authentification de l'identité d'une entité, par la consultation d'une banque de données (source authentique) enregistrant les caractéristiques ou les relations relatives à une entité identifiée.