Déclaration sur l'honneur
(Cercle de Confiance - Circle-of-Trust - CoT)

Introduction

Dans un contexte de communication croissante de données de santé, en provenance et à destination d'une organisation active dans le domaine de la santé, des soins et du bien-être, il est nécessaire de garantir la sécurité des informations, raison pour laquelle le principe du " **Circle-of-Trust - CoT** " a été défini.

Un "Circle-of-Trust" est accordé à une organisation active dans le domaine de la santé, des soins et du bien-être qui prend et applique des mesures de sécurité de l'information à différents niveaux, en ce qui concerne ses utilisateurs de données, afin que d'autres établissements de soins et/ou prestataires de soins et/ou autorités, et le citoyen concerné, puissent raisonnablement être sûrs que ces mesures de sécurité sont respectées et n'aient pas à les organiser ou à les contrôler eux-mêmes[1]

Pour qu'une organisation active dans le domaine de la santé, des soins et du bien-être soit considéré comme Circle of Trust, elle doit répondre aux 13 critères validés dans un règlement approuvé par le Comité de gestion de la plateforme eHealth le 13 septembre 2022, et par le Comité de sécurité de l'information le 5 juillet 2022 (Délibération 19/166). Elle doit prendre les mesures nécessaires pour se conformer à ces critères. Ces critères peuvent être consultés sur le portail de la plateforme eHealth ***https://www.ehealth.fgov.be/ehealthplatform/fr/reglements*****.**

C'est l'autorité d'agrément ou l'autorité avec laquelle l'organisation active dans le domaine de la santé, des soins et du bien-être a conclu un accord (gestionnaire des informations la concernant dans la base de données de référence CoBRHA) [2] qui enregistre le "statut CoT" dans CoBRHA[3] dès qu'une organisation active dans le domaine de la santé, des soins et du bien-être déclare qu'elle respecte les 13 critères applicables au principe du Circle-of-Trust.

---

[1] Article 1er de la Délibération n° 19/166 du 1er octobre 2019, modifiée le 6 juillet 2021, relative au 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

[2] L'administration qu'une organisation de soins reconnaît ou avec laquelle l'organisation de soins a un accord et qui publie votre capacité et vos données dans CoBRHA. Cela peut inclure : l'INAMI, le SPF Santé Publique, VAZG, Iriscare, Aviq, DSL, ...). Cette administration enregistre le drapeau "COT" dans CoBRHA lorsqu'une organisation active dans le domaine de la santé, des soins et du bien-être déclare qu'elle remplit les 13 critères

[3] CoBRHA: base de données de référence unique du fédéral et des entités fédérées, hébergée par la Plateforme eHealth, regroupant les données d'identification de tous les prestataires et acteurs de soins individuels et institutionnels et alimentée par toutes les sources authentiques du pays

Le contrôle du respect du règlement CoT et de la Délibération n° 19/166 du 1er octobre 2019, modifiée le 6 juillet 2021, et en particulier le contrôle du respect du règlement général sur la protection des données[4] et des règles de protection des personnes physiques à l'égard du traitement des données à caractère personnel qui sont à la base de ce règlement, est effectué par l'autorité de contrôle (l'Autorité de Protection des Données ou une autre autorité de contrôle). L'enregistrement de l'adhésion au Circle-of-Trust peut être retiré par une autorité d'agrément à la demande d'une autorité de contrôle compétente, si les missions ou les obligations découlant du règlement CoT ne sont pas remplies ou pas respectées par l'organisation active dans le domaine de la santé, des soins et du bien-être concernée. L'impact potentiel est que l'organisation active dans le domaine de la santé, des soins et du bien-être n'aura plus accès à la lecture/écriture de certaines informations d'un ou plusieurs services eSanté, et devra soumettre une nouvelle demande d'adhésion au Circle-of-Trust.

Cette révocation ne pourra être effectuée qu'après qu'une autorité de contrôle en matière de sécurité de l'information, ayant suivi un processus élaboré par cette autorité[5], confirme que l'organisation active dans le domaine de la santé, des soins et du bien-être ne respecte plus les conditions imposées en matière de sécurité de l'information telles que visées dans les règlements du CoT.

[4] 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 sur la protection des données).
[5] Il est prévu que l'organisation active dans le domaine de la santé, des soins et du bien-être concernée aura d'abord la possibilité de remplir ses obligations et pourra être entendue en cas de conflit.

Déclaration

En signant ce document, je certifie que l'organisation respecte la réglementation relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, et qu'elle se conforme aux 13 critères ci-dessous qui s'appliquent au principe du Circle-of-Trust.

J'accepte que le non-respect des 13 critères par l'organisation puisse entraîner la révocation de l'enregistrement du Circle-of-Trust.

L'organisation s'engage à assurer de manière continue le respect des éléments repris dans la déclaration. Elle s'engage à vérifier à chaque modification substantielle de ses processus - notamment informatiques - que l'ensemble des critères repris dans le présent document sont bien respectés et à signaler immédiatement si elle n'est plus en mesure de respecter ces critères.

Nom de l'organisation active dans le domaine de la santé, des soins et du bien-être:

.....

Adresse: .....

.....

Données de contact du responsable:

.....

Adresse mail: .....

N° Tel: .....

Données de contact du délégué à la protection des données:

Adresse mail: .....

N° Tel: .....

Numéro(s)[6] avec lequel l'organisation active dans le domaine de la santé, des soins et du bien-être est connue dans CoBRHA:

N° INAMI: .....

HCO-nr.: .....

[6] Le numéro de l'organisation individuelle active dans le domaine de la santé, des soins et du bien-être doit être mentionné ici : par exemple, le service de soins à domicile, l'hôpital, l'établissement de réadaptation, le centre de soins résidentiels, la maison de soins psychiatriques, le service d'aide à domicile, ... Plus d'un numéro est possible si différentes organisations individuelles relèvent de la même structure

N° INAMI: .....

HCO-nr.: .....

N° INAMI: .....

HCO-nr.: .....

Le n° BCE de l'organisation active dans le domaine de la santé, des soins et du bien-être:

Nom de l'autorité d'agrément:

.....

.....

Seuls les titulaires de fonctions enregistrées dans l'organisation active dans le domaine de la santé, des soins et du bien-être, tels que connus dans la Banque Carrefour des Entreprises, peuvent signer ce document. En l'absence de signature ou de signature d'un titulaire de fonction non-enregistré, ce document sera déclaré irrecevable par l'autorité reconnue de l'organisation active dans le domaine de la santé, des soins et du bien-être

Date: .....

Nom: .....

Qualité: .....

Signature du responsable:

Ce formulaire doit être envoyé à l'autorité d'agrément. L'organisation active dans le domaine de la santé, des soins et du bien-être doit être en mesure de prouver à tout moment à l'autorité compétente en matière de protection des données qu'il respecte la protection de la vie privée.

L'autorité d'agrément n'est pas compétente pour contrôler l'organisation active dans le domaine de la santé, des soins et du bien-être, que ce soit pour le respect de la vie privée, pour résoudre les problèmes et les litiges, ou pour traiter les plaintes relatives à la vie privée. Lorsqu'une plainte est reçue par une autorité d'agrément, elle est transmise à une autorité de contrôle.

Pour chacune des 13 cases ci-dessous, veuillez indiquer si les systèmes (couplés) utilisés pour la prestation de soins et l'aide au patient, en ce compris la facturation, dans votre organisation y satisfont. Si vous ne cochez pas une ou plusieurs cases, ce document sera déclaré irrecevable par l'autorité d'agrément de votre organisation active dans le domaine de la santé, des soins et du bien-être.

☐ 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[7].

☐ 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.

☐ 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 cadre 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.

☐ 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

[7] Cela inclut également les autres données personnelles que l'établissement de soins doit échanger afin de pouvoir remplir sa mission de soins

- 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 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 Plateforme 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.

☐ 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, ou de l'exclusion de l'utilisateur de l'accès, ces caractéristiques, relations ou exclusion sont consultées

- soit dans les sources authentiques définies par le Comité de gestion de la Plateforme 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 Plateforme 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.
  - la banque de données de la Plateforme eHealth avec les exclusions des prestataires de soins de l'accès aux données à caractère personnel relatives à un utilisateur de soins déterminé.

☐ 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 Plateforme eHealth, ou d'un organe de contrôle, suite à une plainte, qu'une reconstitution complète puisse avoir lieu dont 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 Plateforme eHealth.

☐ 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 exécutent. 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.

☐ 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.

☐ 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 base de données de référence 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 des organes de contrôle.