Précisions concernant la « Déclaration sur l'honneur COT »

Contexte

Les administrations et cabinets des autorités fédérale et régionales ont récemment fixé les modalités relatives au fonctionnement et aux exigences d'un « Circle of Trust ».

Ces modalités sont expliquées dans le présent document.

Qu'est-ce qu'un « Circle of Trust » ?

Un « Circle of Trust » est un concept basé sur la cryptographie. Cela signifie essentiellement que, dans un contexte donné (en l'occurrence : l'écosystème eSanté), des parties (en l'occurrence : des applications et systèmes) se fient au fait que chaque partie prend les bonnes mesures en matière d'accès aux données, d'enregistrement et d'utilisation des données. Ces mesures portent, par exemple, sur une bonne gestion des utilisateurs, sur une gestion élaborée des accès permettant uniquement aux utilisateurs légitimes d'accéder aux systèmes et données, ou sur un logging et un historique des accès aux différents systèmes.

En d'autres termes : dans un contexte donné, différents systèmes se font confiance en matière de confidentialité et gestion des utilisateurs.
Une application espère qu'un autre système procédera à tous les contrôles nécessaires et qu'un contrôle supplémentaire de la part de l'application en particulier sera inutile.

Pourquoi un « Circle of Trust » ?

L'écosystème eSanté est un vaste système d'applications et de données médicales accessibles à un grand nombre d'utilisateurs.
Précisément parce qu'il existe tant de systèmes différents et que les données traitées renferment en général des informations médicales, sensibles ou des données à caractère privé, il est le plus souvent indispensable pour une application de s'assurer que seuls des utilisateurs habilités y aient accès. Concrètement, cela signifie qu'une application intègre elle-même une gestion des accès complexe (p. ex. en mettant en place un contrôle des accès à deux étapes, en installant un appareil hardware spécifique ou en utilisant un mot de passe complexe).
Pour un utilisateur qui utilise différents systèmes et qui doit passer par un contrôle des accès spécifique à chaque système, cela peut être source de difficultés inextricables, avec comme conséquence une perte de temps considérable. Cela peut même au final donner lieu à un contrôle de moins bonne qualité si p. ex. l'utilisateur note ses codes d'accès quelque part ou utilise partout le même code.

Le principe du « Circle of Trust » vise à y remédier. Ce principe fonctionne comme suit :

- Une organisation (p. ex. un établissement de soins) confirme de façon explicite, via une déclaration formelle, que les collaborateurs (et autres utilisateurs) peuvent avoir accès aux applications de l'organisation grâce à une bonne gestion des accès, comprenant logging, historique et gestion des exceptions (procédures « Break the Glass »).
- Cette déclaration formelle est enregistrée à un endroit accessible pour d'autres systèmes et applications.

- Si un utilisateur de l'organisation, via une application de cette organisation, veut accéder à un autre système, le système « destinataire » pourra consulter à l'endroit identifié si l'organisation a enregistré la déclaration « COT ».
- Si tel est le cas, le système « destinataire » pourra donner l'accès à l'utilisateur sans vérifier lui-même l'accès.
- Cela représente un gros avantage à la fois pour l'utilisateur (« Single-Sign-on ») et pour le système « destinataire » (pas de contrôle complexe des accès à développer).

Certains systèmes peuvent même limiter l'accès aux seuls utilisateurs d'organisations qui ont fait enregistrer la déclaration COT.

Qu'entend-on par « Déclaration sur l'honneur COT » ?

La « Déclaration sur l'honneur COT » est la façon dont une organisation peut déclarer qu'elle applique toutes les dispositions du RGPD (notamment une gestion stricte des accès) et que les règles complémentaires fixées pour l'écosystème eSanté (entre autres via le Comité de gestion eHealth) sont intégralement suivies.

Les règles complémentaires pour l'écosystème eSanté sont notamment le consentement éclairé pour le partage des données, les règles relatives à la relation thérapeutique et aux exclusions, la matrice d'accès, etc.

La « Déclaration sur l'honneur COT » est signée par le représentant légal de l'organisation.
Il incombe à l'organisation de soit signer à nouveau ce document, soit de le révoquer si les circonstances changent, p. ex. en cas de reprise ou de fusion, en cas de modification des applications utilisées, etc.