IMPUTABILITÉ

NOTE D'INTERPRÉTATION

Mai 2018

Association
Française des
Hébergeurs
Agréés de
Données de
Santé
à caractère personnel

NOTE D'INTERPRÉTATION – IMPUTABILITÉ

Version du 5 avril 2018

Avant-propos

Ce document est une note d'interprétation telle que prévue par le code de l'AFHADS. Elle porte sur les exigences de contrôle des applications hébergées en matière d'imputabilité.

C'est un guide pratique fondé sur l'expérience. Il ne se substitue pas aux éventuelles exigences qui seraient applicables au titre des futurs référentiels opposables, mais n'est en rien contradictoire avec l'état de ces référentiels tel qu'il est connu à la date de rédaction.

Objectif et fondement

Parmi les exigences portant sur les contrats d'hébergement dans le cas d'un agrément figurait celle de pouvoir présenter à la personne concernée, à sa demande, un historique des accès à ses données personnelles.

Cette exigence a disparu avec le passage à la certification, et ne se retrouve dans aucun autre texte législatif ou réglementaire.

C'est pourtant une mesure efficace dans son principe pour la protection de la confidentialité des données :

- Le contrôle des habilitations d'accès est souvent basé sur des rôles dont l'attribution est bien plus large que le besoin de connaitre les données.
- Même si les accès sont tracés, la quantité des traces est telle qu'il n'est en pratique pas possible de détecter un comportement inapproprié si l'on ne sait pas cibler la personne dont les données ont été compromises.
- Permettre à la personne concernée d'accéder à ces traces est un bon moyen pour qu'un tel ciblage soit possible pour tout un chacun, plutôt que limité à des personnalités identifiables comme particulièrement exposées.

Elle pourrait réapparaitre un jour au travers du futur référentiel opposable d'imputabilité. Celui-ci devrait toutefois être assez différent du texte actuel, qui est plutôt construit dans une logique d'investigation après un incident que de mise à disposition routinière pour les personnes concernées.

Exigences

Contenu des traces

L'objectif de l'imputabilité décrite ici est de détecter des accès inappropriés aux données de santé à caractère personnel (DSCP).

Ceci implique qu'une trace comporte au moins les informations suivantes :

- Une datation du ou des accès tracés
- Un identifiant de l'utilisateur du système hébergé ayant accédé aux DSCP
- Un identifiant de la personne concernée
- Une caractérisation des DSCP accédées
- Le mode d'accès aux DSCP (Création, Modification, Lecture ou Suppression)

Lisibilité

Pour que les traces collectées soient effectives, il est nécessaire qu'elles soient facilement lisibles et interprétables par la personne concernée.

Deux caractéristiques peuvent y faire obstacle :

- La volumétrie des traces
- Le besoin de connaissances particulières pour savoir interpréter les informations tracées

Pour réduire la volumétrie, les traces peuvent être agrégées soit dans le temps, soit sur des populations.

L'agrégation dans le temps consiste à ne présenter qu'une seule trace pour un ensemble d'accès de même nature par la même personne dans une période donnée. La granularité dépendra ici du contexte : une session d'utilisation du système hébergé, une période de temps, un épisode de soins, etc. Si on recourt à ce mécanisme la trace devra présenter explicitement la période concernée et le nombre d'accès durant la période.

L'agrégation par populations permet d'éviter de devoir publier ou restituer des traces individuelles pour chaque personne au sein d'une liste affichée sur un écran ou embarquée dans un rapport. En ce cas les accès aux populations doivent être tracés comme les accès aux individus, ainsi que l'inclusion d'un individu dans une population donnée. Les traces d'accès à ladite population doivent être rendues disponibles à la personne concernée pour toute la période durant laquelle elle en a fait partie.

L'interprétation des informations tracées peut être rendue complexe par la technicité de l'information, ou par le manque de contexte.

La caractérisation des DSCP accédées doit être intelligible et fondée sur leur criticité. Une caractérisation globale en « données administratives » et « données médicales » est par exemple tout à fait recevable.

L'identifiant de l'utilisateur ayant accédé à la donnée est typiquement une information inexploitable sans contextualisation. De plus, il constitue une donnée personnelle sur cet utilisateur qui doit être minimisée. La meilleure solution consiste à présenter :

- Le rôle de l'utilisateur ayant fondé son habilitation à accéder à la donnée.
- Un identifiant local qui pourra être résolu en s'adressant au responsable de traitement en cas de suspicion d'un accès illégitime.

Accessibilité

La personne concernée doit disposer d'un procédé simple, documenté, avec un temps de réponse garanti pour l'obtention des traces d'accès à ses DSCP. Celles-ci devront être fournies dans un format exploitable et par un canal de communication sécurisé.

Le processus de traitement d'une demande d'accès doit être documenté, et garantir que c'est bien à la personne concernée que sont transmises les données de trace.

Intégrité des traces

Pour éviter toute contestation, les traces doivent être signées, au moins en bloc une fois par semaine.

Droits des utilisateurs

Les traces constituent également des données personnelles portant sur les utilisateurs dont les accès sont tracés.

La constitution de ces traces doit être justifiée, que ce soit par la relation contractuelle entre l'utilisateur du service hébergé et le responsable de traitement ou par l'intérêt légitime des personnes concernées par les DSCP accédées. Ce pourra également être ultérieurement par l'obligation légale qui serait introduite par le futur référentiel opposable d'imputabilité.

La mise à disposition de ces données aux personnes concernées représente un motif légitime et impérieux, qui interdit de recourir au droit à l'effacement.

La durée de conservation des traces est calée sur le délai de prescription des actions de droit commun, soit 5 ans. En cas de résiliation du contrat d'hébergement, les traces encore valides font partie des données à transférer au titre de la réversibilité.