9. Notifier en cas de violation des données

Que faire en cas de violation des données ?

> *Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».*
>
> Article 4.12 du règlement général sur la protection des données

Le Règlement Général de Protection de Données (RGPD) exige du responsable du traitement et du sous-traitant d'être vigilants à la sécurité du traitement des données à caractère personnel et ce, en mettant en place des mesures de sécurités adéquates afin de prévenir toute violation de données.

➡ **En d'autres termes, une violation de données est la perte, le vol, la divulgation ou la destruction d'une donnée à caractère personnel, de manière intentionnelle ou accidentelle, mais également l'indisponibilité de la donnée.**

Que faire en cas de violation de données à caractère personnel ?

Le praticien doit inscrire l'incident dans son registre d'incidents. Le registre d'incidents est un document qui reprend tous les incidents en lien avec les traitements.

Si la violation de données à caractère personnel engendre un risque pour la vie privée du patient (vol de laptop non crypté, hacking) le praticien est tenu de la notifier à l'Autorité de Protection de Données (APD), dans un délai de 72 heures calendaires à partir de la prise de connaissance via le formulaire disponible sur le site suivant : **Notifier une fuite de données | Autorité de protection des données**. Au-delà des 72 heures calendaires, il faudra motiver votre retard. Dans le cas où la violation engendre un risque élevé d'atteinte de la vie privée du patient, il faudra également la notifier au patient sauf exception prévue par le RGPD (Article 34.3 du Règlement Général de Protection de Données (RGPD)).

Risque pour le patient ?

Absence de Risque	Risque	Risque élevé
Il y a une brèche technique (panne des réseaux, panne d'électricité, ou un hacking stoppé à temps,…) Et cela **ne viole pas la vie privée du patient**	Il y a eu violation des données (vol de laptop non crypté, hacking, …) Et cela **risque de violer la vie privée du patient**	Il y a eu violation des données Et cela **engendre un risque élevé d'atteinte à la vie privée du patient**
Inscription de l'incident technique dans le registre des incidents.	Notification à l'APD dans les 72h courantes + Inscription dans le registre des incidents.	1. Notification à l'APD dans les 72h courantes 2. Notifier le/les patient(s)concerné(s)* 3. Inscription dans le registre des incidents.

* Exceptions prévues par le RGPD (article 34, 3)

Concrètement

Sécurisez au maximum les données de votre patientèle afin d'éviter tout risque de violation de données

Prévoyez, dans le contrat de sous-traitance, l'obligation de sécurité à charge du sous-traitant, en ce compris, une obligation de notification au responsable du traitement dans un délai déterminé (par exemple 24h à partir de la connaissance)

Tenez à jour un registre des incidents de toutes les violations de données à caractère personnel

Évaluez le risque

Notifiez l'APD dans les 72h max. à partir de la connaissance de la violation en cas de risque d'atteinte à la vie privée de votre patient

Informez le patient de cette violation en cas de risque élevé d'atteinte de sa vie privée