Fiche 7.

Notification des violations de données à caractère personnel

Check-list des bonnes pratiques à respecter :

- → Je tiens un registre de toutes éventuelles violations de données à caractère personnel qui se sont réalisées sous ma responsabilité ;
- → Je notifie à l'Autorité de Protection des Données (APD), endéans les 72 heures, toute violation de données susceptible de présenter un risque d'atteinte à la vie privée pour mes patients ;
- → Lorsqu'il existe un risque élevé d'atteinte à la vie privée de mes patients, je les informe, sans retard déraisonnable, de la violation de leurs données personnelles.
- → Pour éviter tout incident et violation de données à caractère personnel, je veille à minimiser les risques et à sécuriser suffisamment les données personnelles de mes patients ;
- → Je conscientise mon personnel et établis une procédure afin de réagir correctement et rapidement à un incident de sécurité.

L'une des nouvelles exigences introduites par le RGPD est **l'obligation de notifier les violations de données à caractère personnel**. Mais quels sont les contours de cette nouvelle obligation et quels sont les bons réflexes à avoir ?

Qu'est-ce qu'une « violation de données à caractère personnel » ?

Le RGPD définit une violation de données à caractère personnel comme « *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* »[1].

Se produit une violation de données à chaque fois que des données personnelles sont perdues, volées, détruites, corrompues ou divulguées de manière illicite ou accidentelle, en ce compris lorsqu'une personne accède aux données ou les transmet sans y être autorisée.

De manière plus générale, il s'agit de toute brèche de sécurité, d'origine malveillante ou non, se produisant de manière intentionnelle ou non, qui a comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité des données à caractère personnel.

Pour qu'il y ait violation de données au sens du RGPD, **2 conditions** doivent être réunies :

1. Vous avez mis en œuvre **un traitement de données à caractère personnel** ;
2. Ces données ont fait l'objet d'une « **violation** » (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite).

Quelques exemples de violation de données :

- Suppression accidentelle de données médicales qui n'ont pas été préalablement sauvegardées (*violation de disponibilité*) ;
- Perte d'une clef USB non cryptée contenant une copie de données relatives à une catégorie de patients (*violation de disponibilité*) ;
- Vol de dossiers patients (*ex : mallette volée ou oubliée*) lorsqu'ils contiennent des données à caractère personnel (*violation de confidentialité et de disponibilité*) ;
- Accès non autorisé par un employé à certains dossiers patients ou de façon plus large à votre logiciel métier (*violation de confidentialité*) ;
- Accès illégitime à des données de santé par un membre non habilité du personnel d'un de vos sous-traitants (*violation de confidentialité*) ;
- Modification non autorisée des résultats obtenus dans le cadre d'une recherche médicale (*violation d'intégrité*) ;
- Cas de *hacking* ou de *randsomware* (*violation de confidentialité, d'intégrité et disponibilité*).

[1] Article 4. 12 du RGPD.

Quelles sont vos obligations si vous constatez ou suspectez une violation ou une fuite de données à caractère personnel ?

En tant que prestataire de soins collectant et traitant des données à caractère personnel relatives à vos patients, vous êtes tenu, conformément aux articles 33 et 34 du RGPD, de mettre en place des mesures pour **prévenir les violations de données** et **réagir de manière appropriée en cas d'incident de sécurité**, c'est-à-dire de mettre fin à la violation et minimiser ses effets.

Par cette nouvelle obligation de sécurité, le RGPD entend **éviter qu'une violation cause des dommages ou des préjudices aux personnes concernées** *(à savoir, les patients).*

Concrètement, cela implique que vous :

1. Notifiez la violation de données à l'Autorité de Protection des Données (APD) ;
2. Informiez les personnes concernées, si nécessaire ;
3. Teniez, dans tous les cas, un registre interne des incidents.

Toute violation des données doit-elle être notifiée à l'APD ?

Non. Seules les violations des données à caractère personnel qui présente « **un risque »** pour la protection de la vie privée des patients doivent être notifiées à l'APD.

- Comment déterminer le risque ?

Il n'existe pas dans le RGPD de définition précise de la notion de « risque » ou de « risque élevé ». L'APD estime toutefois que dans la mesure où la violation de données s'est produite, il convient d'**évaluer la gravité et la probabilité de survenance des conséquences de cette violation de données**[2].

Il convient, à cet effet, de prendre en compte les circonstances spécifiques de la violation dont le type de violation (*confidentialité, disponibilité, intégrité*), la nature, le volume et la sensibilité des données (*données de santé, données génétiques, données biométriques, etc.*), le nombre et type de personnes concernées, les possibilités d'identification des personnes, les caractéristiques du responsable du traitement et la gravité des conséquences.

⇨ Il vous appartient donc de faire une **évaluation au cas par cas** de la gravité des conséquences pour vos patients.

Ce ne sera en définitive que lorsque la violation de données « **peut avoir des conséquences néfastes sur la vie privée** » de vos patients que vous êtes tenu de notifier la violation de données à caractère personnel à l'APD.

[2] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf

☝ **Vous ne devez donc pas faire de notification à l'APD, s'il ne résulte pas d'indisponibilité ni d'altération des données, ni de brèche dans la confidentialité des données.** Ainsi, aucune notification ne devra être faite en cas de perte d'une clé usb suffisamment chiffrée, si vous disposez toujours d'une copie des données perdues.

- ## Dans quel délai ?

Vous disposez de **72 heures** pour notifier à l'APD la violation ou la fuite des données. Soyez attentifs qu'il ne s'agit pas de 3 jours ouvrables, mais de **3 jours « calendrier »**, tout retard devant nécessairement être justifié[3].

Le délai de 72 heures commence à courir **à compter du moment où vous avez pris connaissance de la violation des données**. Par exemple, lorsque vous vous apercevez de la perte de votre clé usb ou d'une intrusion illégitime à vos dossiers patients, lorsqu'une personne vous signale avoir reçu des données qui ne lui étaient pas destinées ou encore lorsque votre sous-traitant vous signale une fuite de données.

En pratique, vous devez être en mesure de **prouver** à quel moment vous avez pris connaissance de la violation dès lors qu'il s'agit du point de départ du délai de notification. Une première **investigation** rapide pourra être nécessaire afin de recueillir des éléments permettant de confirmer la réalité de la fuite de données. Vous devez ainsi indiquer les faits concernant la fuite des données, ses effets et les mesures que vous avez prises pour y remédier, de manière à permettre à l'APD de vérifier le respect du RGPD[4].

- ## Quel est le rôle de votre sous-traitant ?

Votre sous-traitant a l'obligation de vous notifier toute violation ou fuite de données, dans les meilleurs délais, après en avoir pris connaissance[5].

Dès que votre sous-traitant a pris connaissance de la fuite de donnée, vous êtes supposé en avoir aussi pris connaissance. C'est pourquoi, il est recommandé que **votre sous-traitant vous informe immédiatement de toute violation de données ayant eu lieu**. Il est donc important de prévoir cette modalité dans votre **contrat de sous-traitance** et de vous assurer que votre sous-traitant vous apportera toute l'aide pour enquêter, atténuer et remédier à la violation de données. Il est également possible d'envisager dans le contrat que vous avez avec votre sous-traitant qu'il appartient à ce dernier de réaliser, en votre nom, la notification à l'APD de la fuite de données intervenue dans son périmètre.

- ## Que doit contenir la notification ?

La notification à l'APD doit contenir *a minima* les éléments suivants[6] :

[3] Article 33, § 1 du RGPD.
[4] Article 33, §5 du RGPD.
[5] Article 33, § 2 du RGPD.
[6] Article 33, § 3 du RGPD.

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les coordonnées de la personne à contacter (vos coordonnées et/ou celles du DPO);
- et, les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

- Quelle procédure suivre ?

La notification d'une fuite de données à l'APD se fait au moyen d'un formulaire *ad hoc* en ligne que vous pouvez retrouver sur le site internet de l'APD.

Un mode d'emploi vous est proposé sur notre site (http://www.e-santewallonie.be/rgpd) en vue de vous aider à réaliser en bonne et due forme cette notification à l'APD.

Les patients impactés doivent-ils être aussi prévenus ?

PAS TOUJOURS. Ce n'est que lorsqu'il existe un risque **élevé** d'atteinte à la vie privée de vos patients que vous devez les informer de la violation de leurs données[7].

Vous ne devez toutefois pas informer votre patient d'une violation de ses données[8]:

(1) Si vous démontrez qu'il n'existe **aucun risque**.

- *Ex : les ordinateurs portables dérobés sont verrouillés à l'aide d'un mot de passe sécurisé et les informations sont cryptées. De plus, un back-up récent a été réalisé*.

(2) Si vous avez pris certaines **mesures correctives garantissant que le risque n'est plus susceptible de se matérialiser**.

- *Ex : une mesure a été prise à l'égard de l'individu ayant pu consulter illicitement les données à caractère personnel, et ce, avant qu'il n'ait pu faire un usage abusif des données*.

(3) Si la communication exige des **efforts disproportionnés**.

- *Ex : un grand nombre de patient sont concernés par la violation des données, dans ce cas il est plutôt procédé à une communication publique (via la presse par exemple).*

Dans le cadre d'une de ces exceptions, vous êtes tenu **de documenter les différents éléments qui vous ont amené à considérer qu'il ne fallait pas notifier la violation au**

[7] Article 34, § 1 du RGPD.
[8] Article 34, §3, a) b) et c) du RGPD

patient, en indiquant notamment les faits relatifs à la violation de données, ses conséquences et les mesures prises pour y remédier[9].

- Dans quel délai ?

La communication de la violation des données à la/aux personne(s) concernée(s) doit être réalisée "***dans les meilleurs délais***"[10].

En pratique, le délai de notification peut varier en fonction de la nécessité d'atténuer un risque immédiat de dommage (notification immédiate) ou de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation de données ou la survenance de violations similaires (délai plus long)[11].

- Quelles informations communiquer au patient ?

Si une violation de données est constatée et présente un risque ***élevé*** pour les patients, vous devez être transparent vis-à-vis d'eux et décrire, en des **termes clairs et simples** :

- la nature de la violation des données à caractère personnel,
- les conséquences probables de la violation,
- les coordonnées de la personne à contacter (vos coordonnées et/ou celles du DPO)
- et vous devez également exposer les mesures prises pour remédier à la violation et pour limiter les conséquences négatives de la violation[12].

La notification devrait être effectuée en coopération étroite avec l'APD, dans le respect des directives de cette dernière[13].

Que doit contenir le registre des incidents ?

En tout état de cause, **toute violation de données**, de quelle que nature qu'elle soit et indépendamment du risque qu'elle représente pour les patients, doit être dûment documentée dans un registre interne pouvant se présenter sous la forme d'un fichier Excel.

Exemple de canevas :

Date de la constatation de la violation ?	Description de la violation ?	Risque élevé/ moyen/faible ?	Mesure prises ?	Notification à l'APD ?	Notification à la personne concernée ?

[9] Article 33, §5 du RGPD.
[10] Article 34, § 1 du RGPD.
[11] Considérant 86 du RGPD.
[12] Article 34, § 2 du RGPD.
[13] Considérant 86 du RGPD.

En bref, que devez-vous faire en cas de violations de données ?

Pour les personnes concernées, la violation de données implique :	AUCUN RISQUE	UN RISQUE	UN RISQUE ELEVE
Inscription dans le registre des incidents	X	X	X
Notification à l'APD, dans un délai maximal de 72h		X	X
Information aux patients concernés, dans les meilleurs délais, hors cas particuliers.			X

Quels sont les pouvoirs de l'APD en cas de violation de données ?

A la suite d'une violation de données qui lui serait notifiée, l'APD aura pour premier réflexe d'ouvrir **une enquête**. Si son investigation peut se limiter à la violation des données, elle peut aussi viser l'ensemble de votre mise en conformité avec le RGPD. En cas de notification d'une fuite de données trop tard ou de façon incomplète ou en cas de non conformité avec l'ensemble des exigences du RGPD, l'investigation de l'APD pourrait aboutir à la décision d'infliger une **amende administrative**.

En outre, en parallèle à l'enquête menée par l'APD, les personnes victimes d'une violation de données à caractère personnel pourraient également **se tourner vers la justice** en vue de réclamer tantôt la cessation d'un traitement illégal tantôt l'indemnisation de leur préjudice.

Toutefois, **l'enjeu réel pour vous n'est pas tant d'éviter les sanctions administratives mais plutôt de préserver la continuité de votre activité lorsque vous êtes face à une violation de donnée** et par voie de conséquence d'éviter d'être pointé comme un « mauvais élève » par l'APD.

Pour ce faire, quelques bons réflexes à adopter seraient de :

- **sécuriser suffisamment les données de vos patients**, non seulement pour éviter les violations de données mais aussi pour éviter qu'une violation de données présente un risque *élevé*, ce qui impliquerait une notification aux personnes concernées ;
- **conscientiser votre personnel,** d'une part pour éviter tout incident et, d'autre part, dans la situation où un incident surviendrait malgré tout, pour que votre personnel sache immédiatement comment réagir et qui avertir ;
- **établir une procédure afin de réagir correctement et rapidement**, en documentant les différentes actions à entreprendre.

Pour e-santéwallonie,
Emeraude Camberlin, Juriste

Annexe : Check-list de synthèse

1. Y a-t-il eu une fuite de données à caractère personnel ?

Si un incident de sécurité implique un risque de fuite de données à caractère personnel, mais qu'aucune donnée n'a été rendue publique ou n'a été transmise à la mauvaise personne, il s'agira toujours d'un incident. Dans ce cas, il est de votre devoir de le recenser dans votre **registre des incidents**, mais aucune notification à l'APD ni aux patients concernés par la violation des données ne sera nécessaire.

2. S'il y a eu effectivement fuite de données, y a-t-il un risque d'atteinte à la vie privée ?

Si des données se sont retrouvées en dehors des zones protégées de votre cabinet, il est toujours possible que, grâce aux mesures de protection mises en place, il n'y ait eu **aucun risque**. Ce serait le cas si les données personnelles de vos patients étaient correctement cryptées et ne pourraient donc pas être utilisées par des tiers.

En revanche, s'il existe **un risque** pour les patients concernés par la violation de leurs données à caractère personnel, vous devez **évaluer le risque** d'atteinte au respect de leur vie privée. Il s'agira toujours d'une analyse au cas par cas.

3. Quel est le risque d'atteinte à la vie privée pour les patients impliqués?

Une fois la violation des données avérée, vous devez évaluer la gravité des conséquences pour vos patients et la probabilité de survenance des conséquences de cette violation de données.

Ex 1 : Si vous veniez à égarer de manière accidentelle une base de données dans laquelle vous recensez le nom de vos patients, leurs caractéristiques personnelles ainsi que leurs pathologies respectives considérées comme particulièrement sensibles, à des fins de recherches cliniques par exemple, il existe un **risque** d'atteinte à la vie privée pour vos patients. Ainsi, vous devez notifier cette fuite à l'APD dans les 72 heures. Vous devez par ailleurs inscrire cette violation de données dans votre registre des incidents et prendre toutes les mesures nécessaires pour atténuer le risque.

Ex 2 : Dans la situation où votre plateforme d'agenda en ligne (dans lequel figurent les noms, prénoms, adresses de contact et motifs de consultation de vos patients) venait à être piratée par des tiers mal attentionnés, il existe là encore un **risque** d'atteinte à la vie privée de vos patients. Vous devez donc en informer l'APD, sans oublier de renseigner cette violation de données dans votre registre interne des incidents.