Procédure Gestion des violations de données

Date de modification	Type de modification	Version	Date d'application
13/12/2024	Relecture du document	2	20/12/2024
28/10/2020	Création du document	1	04/11/2020

SOMMAIRE

-/-

Page

Rédaction	Validation	Approbation
Nom		
Fonction : Référent RGPD	Fonction : RAQ & GDR	Fonction : Directrice
Visa :	Visa :	Visa :

Procédure Gestion des violations de données

1. Introduction

Les entités du groupe Ramsay Santé s'engagent à gérer les données à caractère personnel en totale observation des dispositions du Règlement général sur la Protection de Données.

Le présent document décrit les processus à suivre par le personnel de ces entités en cas de constatation ou de suspicion de violation de données à caractère personnel. Une violation de données à caractère personnel recouvre **tout incident de sécurité, d'origine malveillante ou non, intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité des données personnelles**. C'est lorsque des données personnelles sont de manière accidentelle ou illicite : détruites, perdues, altérées, divulguées, consultées ou rendues indisponibles par une personne non-autorisée ou un incident technique.

N.B. : L'indisponibilité d'une donnée devient une violation dès lors qu'elle a un impact sur une personne concernée.

Le RGPD dispose que les violations de données à caractère personnel doivent faire l'objet d'une notification auprès des personnes concernées en cas de risque avéré. Dans certains cas, les autorités (Commission Nationale Informatique et Liberté, Agence Nationale pour la Sécurité des Systèmes d'Information, Agence Régionale de Santé).

En cas de détection d'une violation de données à caractère personnel, il convient de qualifier l'incident pour en mesurer la portée, en déterminer le niveau de gravité et en conséquence le niveau de communication extérieure/déclaration nécessaire.

Le respect de la présente procédure permettra d'assurer aux entités du groupe que la violation soit :

- Limitée autant que faire se peut ;
- Diagnostiquée et estimée ;
- Adressée.

2. Le périmètre

Le périmètre organisationnel est limité à celui de l'établissement. L'ensemble des données à caractère personnel doit être considéré, en revanche, en cas de caractère informatique.

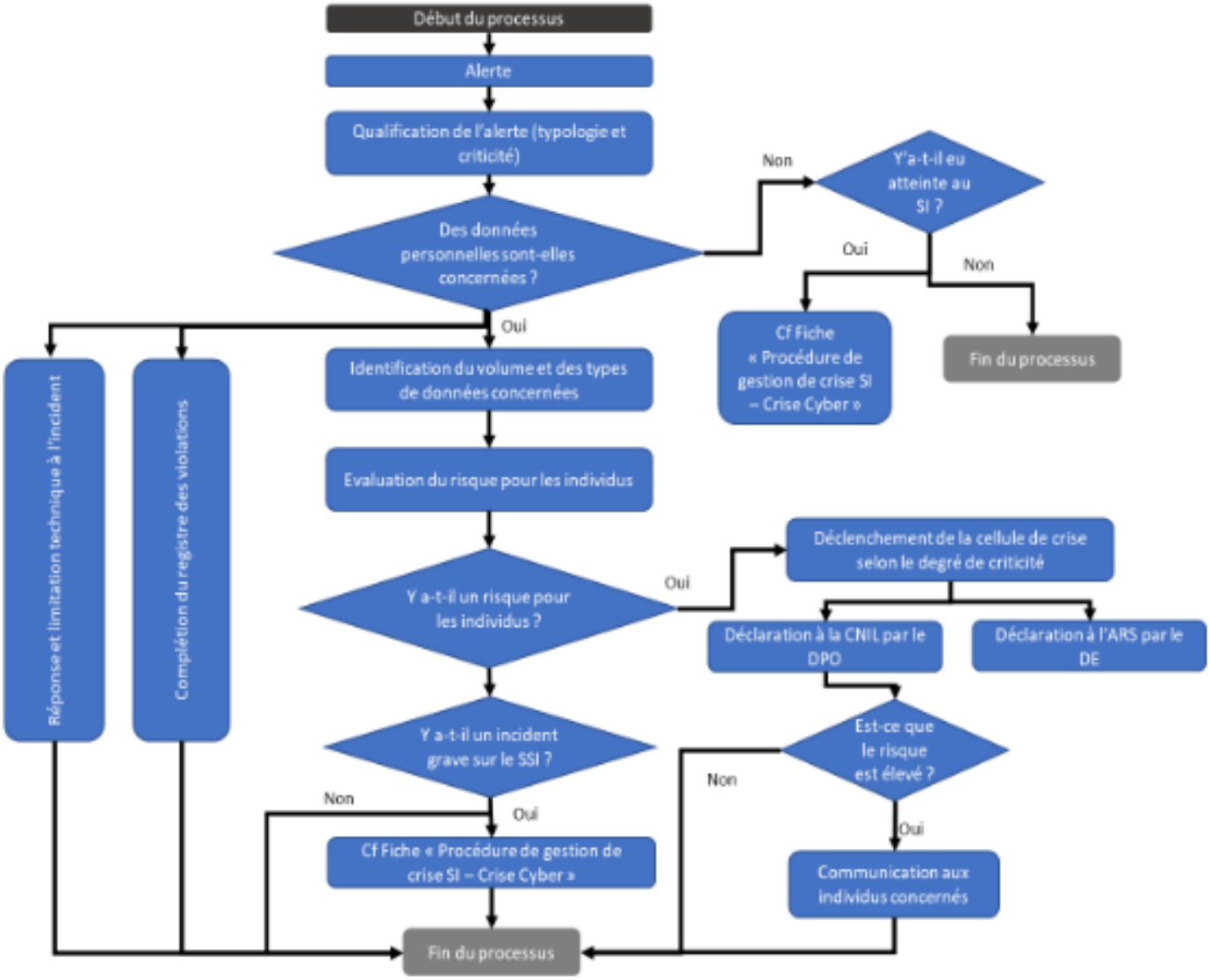
3. Démarche Globale

La démarche globale de gestion des incidents, est la suivante :

- Alerte
- Qualification
- Réponse / Notification
- Clôture : bilan et plan d'action

Le détail de ces étapes est décrit au chapitre suivant.

4. Les acteurs et la matrice des flux



Détails des étapes :

4.1 Alerte

En cas de constatation ou de suspicion forte de violation de données à caractère personnel, tout membre de Ramsay Santé doit alerter le plus rapidement possible, et dans la limite de 24 heures, au moins une des personnes suivantes :

- Le Correspondant RGPD de l'entité
- Tout membre de l'encadrement de l'entité

L'alerte doit être effectuée par tout canal possible (oral, téléphone) et devra être systématiquement doublée d'un envoi de message électronique pour une bonne description et traçabilité de l'incident. Le DPO groupe ( ) doit être systématiquement en copie de ce message.

Les informations à fournir sont idéalement les suivantes :

- Quand la violation est-elle survenue (date et heure) ?
- Description de la violation (nature des informations concernées)
- Cause de la violation (si connue) ou à défaut la façon dont elle a été constatée

- Quels systèmes, si applicable, sont concernés
- Quel(s) service(s) sont impactés
- Une action corrective a–t-elle été immédiatement mise en œuvre ?
- Une éventuelle action de communication a-t-elle été réalisée à propos de l'alerte ?

4.2 Qualification

En cas de détection d'une fuite de données à caractère personnel, il convient de qualifier l'incident pour en mesurer la portée, en déterminer le niveau de gravité et en conséquence le niveau de communication extérieure/déclaration nécessaire. Les acteurs de la qualification sont le correspondant RGPD, le DPO groupe en support et toute autre personne susceptible d'y concourir.

Les critères à considérer pour déterminer si une **violation de données à caractère personnel** a eu lieu sont les suivantes :

- La violation porte-t-elle réellement sur des données à caractère personnel ?
- L'information à caractère personnel constitue-t-elle une donnée sensible ?
- S'agit-il :
    - D'un accès non autorisé ?
    - D'une communication/diffusion non autorisée ?
    - D'une perte, avec suspicion de récupération frauduleuse ?
    - D'une indisponibilité de la donnée ayant un impact pour des patients / collaborateurs ?

Si la qualification n'aboutit pas à déterminer que des données à caractère personnel sont concernées, et s'il apparaît que la cause de la crise est liée au système d'information, il convient de se référer à la fiche « Procédure de gestion de crise SI – Crise cyber ».

4.3 Identification et évaluation du risque

Pour déterminer la **sévérité** de la violation, les critères suivants doivent être examinés :

- Le type et l'étendue des informations personnelles concernées
- Le nombre d'individus concernés
- Les données sont-elles protégées par un mécanisme de sécurité (chiffrement ou mot de passe) ?
- La catégorie de personnes ayant obtenu accès à la donnée
- La nature et la sévérité du risque, avéré ou potentiel, encouru par les personnes concernées
- L'attention des médias ou des parties prenantes est-elle susceptible d'être attirée ?

Il n'y a pas de réponse de principe à une violation de données et chaque incident doit être traité au cas par cas en déterminant les circonstances et les risques associés pour y apporter la réponse appropriée.

4.4 Actions à mener

4.4.1 Déclenchement de la cellule de crise

Si les premières constatations amènent à considérer que la crise présente un risque important pour les personnes physiques, les biens ou l'image de l'établissement ou du groupe, le déclenchement de la **cellule de crise** s'avère nécessaire. Le déclenchement de cette cellule peut être réalisé même en l'absence d'impact sur les données à caractère personnel.

Fonction	Prénom/Nom	Téléphone	Téléphone portable	Statut (Titulaire / Suppléant / Optionnel)
Cellule de Sécurité Sanitaire (CSS)				**Obligatoire** peut prendre en charge le lien avec la communication ou d'autres services externes à la DSI
Directeur de l'établissement ou cadre d'astreinte				**Obligatoire**
Directeur de la Production et de l'Exploitation				**Facultatif** Si sujet informatique
Directeur des SI Groupe				**Facultatif** Si sujet informatique
Responsable Sécurité des SI Groupe				**Facultatif** Si sujet informatique
Directeur à la Protection des Données				**Facultatif** En cas d'impact sur des données à caractère personnel
Correspondant RGPD de l'établissement				**Facultatif** En cas d'impact sur des données à caractère personnel

Les étapes suivantes doivent être considérées et mises en œuvre par la Cellule de Crise :

- Si ça n'a pas déjà été fait, **mettre un terme immédiat à la violation**. Les actions correctrices peuvent inclure :
  - La récupération des données à caractère personnel en cause,
  - La coupure des accès non autorisés,
  - L'arrêt ou l'isolation des systèmes compromis.
- **Evaluer les risques** découlant de la violation, en collectant toute information ou indice disponible ;
- **Faire appel** et échanger avec le personnel compétent pour évaluer correctement les circonstances techniques et/ou organisationnelles de la violation. Eventuellement, faire appel à une ressource externe experte.
- **Déterminer si un risque grave** pour les personnes concernées est possible.
- **Déterminer si la violation doit être rapportée** à une instance publique (CNIL, ARS, …) et si les **personnes affectées doivent être notifiées**.

4.4.2 Déclaration à la CNIL par le DPO

La communication auprès de l'autorité de contrôle française doit être réalisée dans un délai de 72H. Seul le DPO groupe est habilité à la réaliser. La déclaration contient *à minima* les éléments suivants :

- 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 (DPO ou autre) ;
- Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

4.4.3 Déclaration à l'ARS

Les évènements indésirables graves doivent être signalés sans délai à l'Agence Régionale de Santé (ARS). Cette déclaration est faite par le directeur de l'établissement, avec l'approbation de la Cellule de Crise, par le biais du portail concernant le signalement des évènements sanitaires indésirables figurant à l'adresse suivante : https://signalement.social-sante.gouv.fr/.

Le directeur de l'établissement peut désigner une personne déléguée responsable du signalement des incidents.

Les incidents graves concernent les évènements ayant pour effet de générer une situation exceptionnelle au sein de l'établissement, et notamment :

- Les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins ;
- Les incidents ayant des conséquences sur la **confidentialité ou l'intégrité des données de santé** ;
- Les incidents portant atteinte au fonctionnement normal de l'établissement.

4.4.4 Communication aux Personnes concernées

En cas de risque élevé pour les personnes concernées, le directeur d'établissement devra informer, en termes clairs et simples, les utilisateurs touchés par l'incident. Cette communication sera réalisée avec l'avis et en parfaite collaboration des acteurs impliqués de la cellule de crise.

Dans le cas où la communication aux personnes concernées exigerait des efforts disproportionnés (quantité trop importante, impossibilité de les contacter individuellement), une communication publique peut être envisagée :

- Publication d'un encart sur le site Internet de l'établissement
- Publication d'un encart sur le site Internet du groupe
- Publication d'un encart sur le portail Ramsay Services
- Communiqué de presse
- De la forme de communication appropriée.

La CNIL pourra demander au responsable de traitement ne l'ayant pas fait, d'effectuer cette communication.

4.5 Autres déclarations

Il est possible qu'il soit nécessaire de procéder à des déclarations de l'incident auprès d'autres instances (ANSSI, notamment). Celles-ci seront réalisées conjointement avec le RSSI.

4.6 Complétion du registre des violations

Toutes les violations doivent être inscrites dans deux registres internes maintenus :

- à l'échelon local, par le Correspondant RGPD
- à l'échelon groupe, par le Délégué à la Protection des Données

L'incident doit systématiquement faire l'objet d'un bilan qui sera inscrit aux registres mentionnés ci-dessus.

Il convient également de déterminer un plan d'action pour éviter que le même incident se reproduise.

Ces étapes seront réalisées conformément à la méthodologie groupe ACRES.

4.7 Gestion de crise : Réponse et limitation technique à l'incident

En parallèle des actions relatives à la conformité au RGPD, les équipes SI sont en charge de la réponse technique aux incidents, en collaboration avec toutes les parties prenantes nécessaires (DSI, managers, Communication, RETEX…). Ces actions sont pilotées par la Cellule de crise.