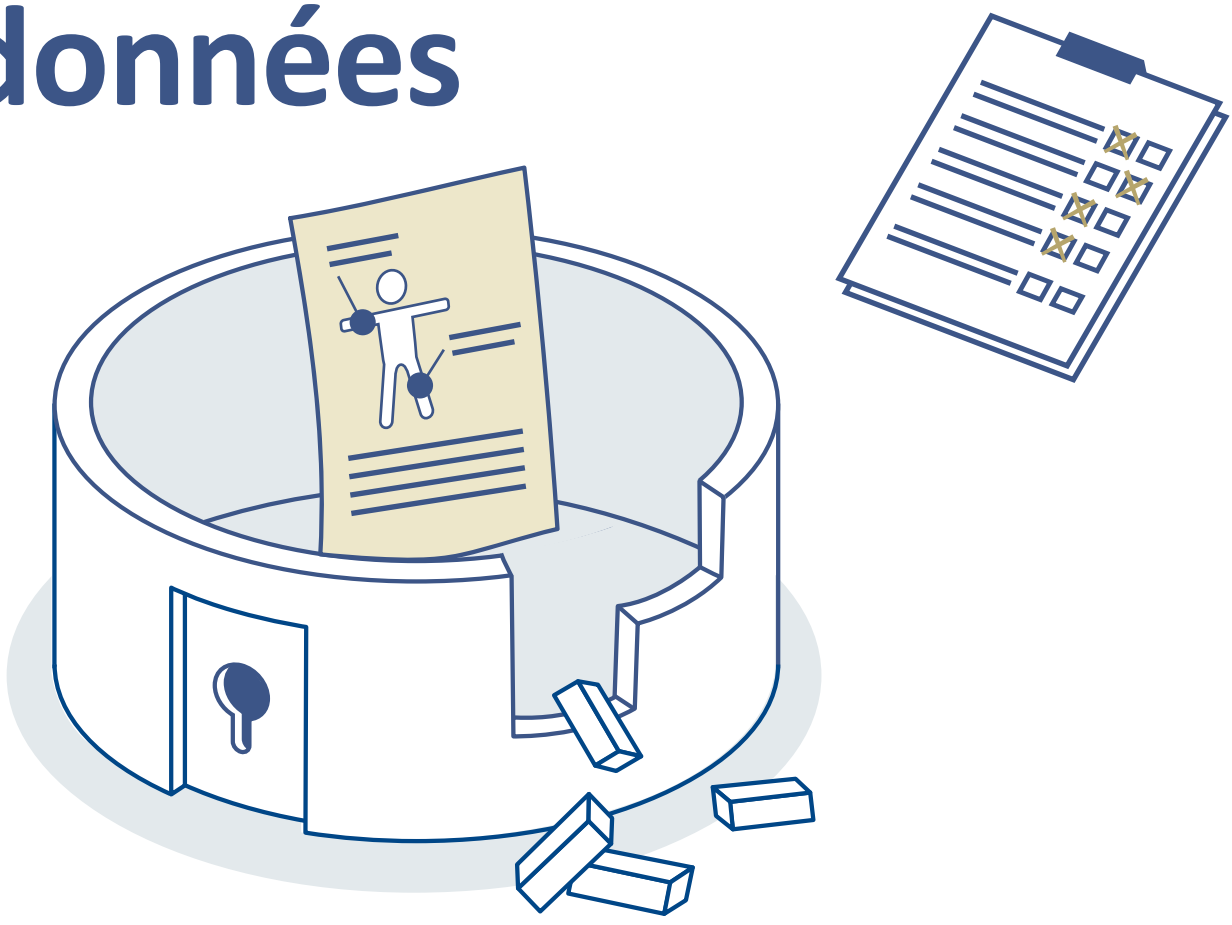
Liste de contrôle et déroulement de la procédure en cas de violation de la protection des données



Version du 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Table des matières

1 Généralités

Le présent document a pour but d'aider à la préparation et au traitement des violations de la sécurité des données et de garantir le respect des exigences légales. Outre les définitions de la violation et de l'obligation d'annoncer, le document comprend également une liste de contrôle relative à la préparation ainsi qu'une procédure relative à la gestion d'un événement.

Concernant les thèmes pour lesquels la loi n'a pas édicté de prescriptions, des recommandations ont été formulées quant à la marche à suivre. Afin d'éviter les redondances par rapport aux Exigences minimales pour la sécurité informatique des cabinets médicaux, qui prévoient des recommandations et des mesures en cas d'incidents de sécurité, il est parfois renvoyé aux différentes recommandations (R) et mesures (M-XX.XX) pour la sécurité informatique.

1.1 Définition de la violation de la sécurité des données

Tout comme en matière de sécurité de l'information, la sécurité des données vise à protéger, par des mesures appropriées, les données personnelles contre la perte de confidentialité, d'intégrité ou de disponibilité.

Selon la loi sur la protection des données, il y a violation de la sécurité des données

— lorsque des données personnelles sont perdues, effacées, détruites ou modifiées de manière accidentelle ou illicite, ou lorsqu'elles sont divulguées ou rendues accessibles à des personnes non autorisées, par exemple en cas de perte d'un support de données tel qu'un ordinateur portable, un CD, une clé USB, etc. ou de destruction de données par un événement naturel tel qu'une inondation, un incendie ; ou en cas d'attaque par phishing.

Les indices d'une possible violation de la sécurité des données sont par exemple :

— effraction dans le cabinet médical,
— incendie.

1.2 Obligation d'annoncer

Lorsque la violation de la sécurité des données présente un risque élevé pour les personnes concernées, elle doit [1] être annoncée au Préposé fédéral à la protection des données et à la transparence (PFPDT). Selon la loi, le risque est élevé lorsque la violation de la sécurité des données compromet vraisemblablement les droits fondamentaux ou la personnalité des personnes concernées.

Voici quelques exemples de risques élevés :

— Les serveurs du cabinet médical sont attaqués et l'on suppose que les agresseurs ont eu accès à toutes les données sur la santé de la patientèle.
— Un dysfonctionnement technique a engendré l'effacement de toutes les données sur santé de la patientèle et la sauvegarde ne peut pas être restaurée.
— Les données de la patientèle sont transmises à des tiers par e-mail sans consentement et de manière non chiffrée.

[1] https://www.edoeb.admin.ch/edoeb/fr/home.html

1.3 Liste de contrôle

La liste de contrôle ci-après vise à vous aider à déterminer les points qu'il serait judicieux de définir de manière préventive. En cas de violation (soupçonnée) de la sécurité des données, des étapes importantes de la procédure sont ainsi déjà clarifiées et les décisions à prendre déjà définies.

Désignation de la personne responsable (responsable de la sécurité des données)

En cas de violation de la sécurité des données, en particulier lorsqu'une obligation d'annoncer selon le chiffre 1.2 est indiquée, le propriétaire du cabinet médical doit être informé immédiatement et les mesures requises doivent être mises en œuvre conjointement avec lui.

Par analogie avec la mesure M-10.01 des Exigences minimales pour la sécurité informatique des cabinets médicaux D3, il convient de désigner une personne responsable en cas de violation de la sécurité des données (ci-après personne responsable de la sécurité des données). Il peut s'agir de la même personne qui a déjà été désignée pour les incidents de sécurité selon les exigences minimales pour la sécurité informatique (cf. également R1 des Exigences minimales pour la sécurité informatique des cabinets médicaux D3).

Aide-mémoire sur la violation de la sécurité des données

Il est recommandé d'élaborer au préalable un aide-mémoire destiné à aider le personnel à identifier une violation de la sécurité des données. L'aide-mémoire pourrait en outre inclure des exemples d'indices d'une violation de la sécurité des données. Le ch. 1.1 Définition de la violation de la sécurité des données ci-avant peut servir d'aide.

Il est par ailleurs recommandé, dans le présent aide-mémoire, de définir des consignes concrètes à l'attention du personnel et de le sensibiliser davantage (cf. ch. 2. Procédure en cas de violation de la sécurité des données ci-après).

Documentation

La loi sur la protection des données prévoit qu'une violation de la sécurité des données doit être documentée par la personne responsable de la sécurité des données lorsque la violation doit être annoncée.

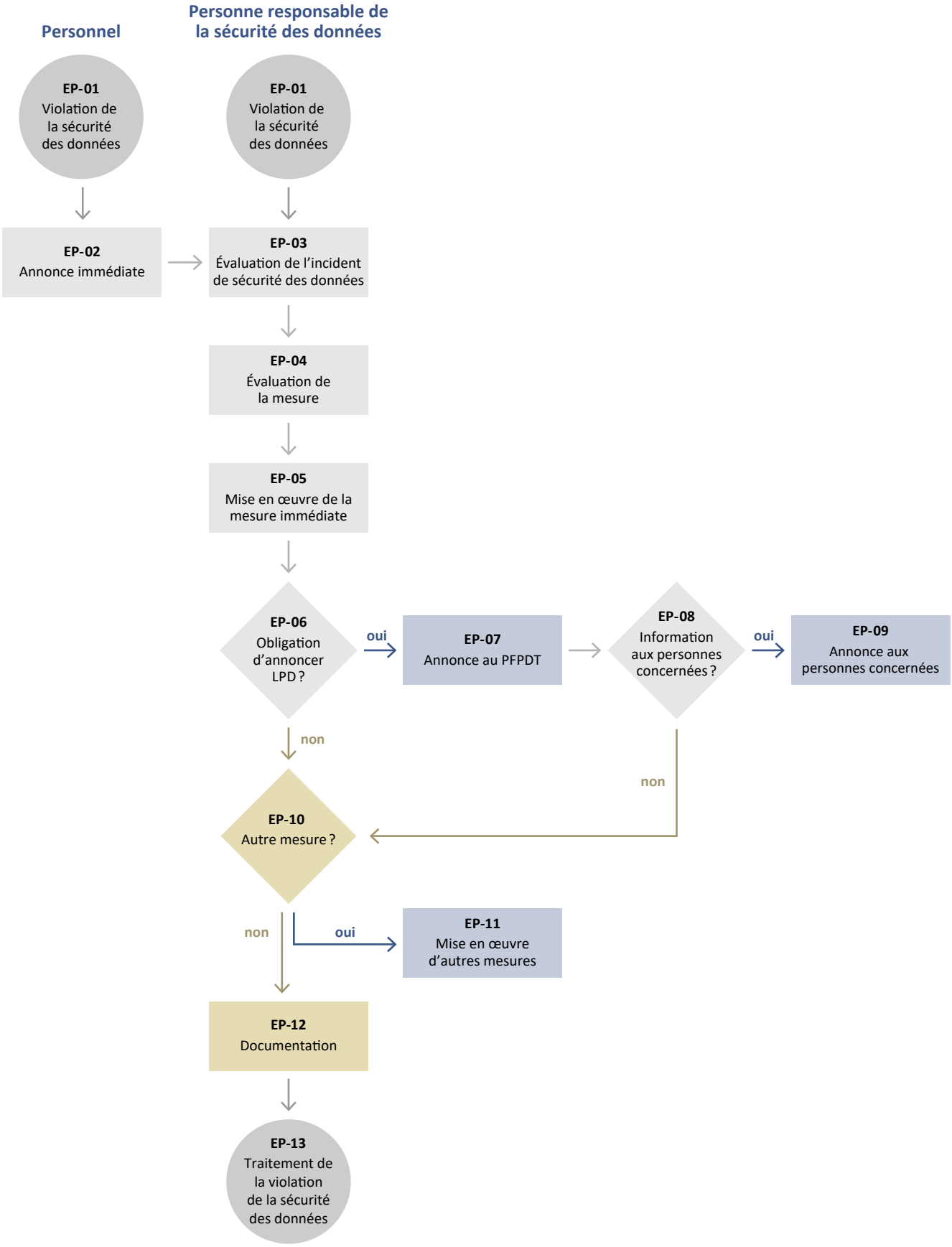
La documentation contient au moins :

— tous les faits liés à la violation de la sécurité des données (cf. également ci-après ch. 2. Procédure en cas de violation de la sécurité des données, étape de la procédure « EP-07, Annonce au PFPDT »),
— les conséquences de la violation de la sécurité des données ainsi que
— les mesures prises pour limiter ou éliminer la violation de la sécurité des données.

Lorsque la violation de la sécurité des données n'est pas soumise à annonce, il est recommandé de documenter en plus le motif pour lequel il a été renoncé à l'annonce.

La documentation doit être conservée pendant au moins deux ans à compter de la date de la violation de la sécurité des données, conformément à l'ordonnance sur la protection des données.

2 Procédure en cas de violation de la sécurité des données



Étape de la procédure (EP)	Tâche	Description de la tâche
EP-01	Violation de la sécurité des données	La sécurité des données a été violée et la violation a été identifiée par la personne responsable de la sécurité des données ou par une ou un membre du personnel (cf. ch. 1.1 Définition de la violation de la sécurité des données ci-avant).
EP-02	Annonce immédiate	Si une collaboratrice ou un collaborateur a identifié une violation (potentielle) de la sécurité des données, la personne responsable de la sécurité des données (cf. ch. 1.3 Liste de contrôle, section « Désignation de la personne responsable ») doit en être immédiatement informée.
EP-03	Évaluation de la violation de la sécurité des données	La personne responsable de la sécurité des données évalue l'annonce et la violation présumée de la sécurité des données. Pour l'évaluation, il est possible de recourir à la mesure M-10.03 des Exigences minimales pour la sécurité informatique des cabinets médicaux.
EP-04	Évaluation des mesures	La personne responsable de la sécurité des données évalue la violation de la sécurité des données sur la base du risque prévisible puis détermine les mesures nécessaires au traitement de la violation. Lors de la définition des mesures, il est possible de distinguer les mesures immédiates visant à maîtriser l'incident de celles visant à traiter sur le long terme la cause et l'incident.
EP-05	Mise en œuvre des mesures immédiates	Si des mesures immédiates ont été définies dans EP-04, elles sont directement mises en œuvre pour limiter la violation de la sécurité des données (p. ex. isolation ou mise hors service de certains services ou systèmes).
EP-06	Obligation d'annoncer LPD ?	La personne responsable de la sécurité des données examine dans un deuxième temps si la violation de la sécurité des données est susceptible d'engendrer un risque élevé pour les personnes concernées (cf. ci-avant 1.2 Obligation d'annoncer) et, partant, s'il existe une obligation d'annoncer au PFPDT.
EP-07	Annonce au PFPDT	En cas d'obligation d'annoncer, l'annonce au PFPDT doit être préparée. La loi sur la protection des données prévoit que l'annonce au PFPDT d'une violation de la sécurité des données doit contenir au moins les éléments suivants : — la nature de la violation de la sécurité des données (p. ex. destruction des données, vol des données, etc.) ; — la date et la durée de la violation, si elles sont connues ; — les catégories et le nombre approximatif de données personnelles concernées, dans la mesure du possible ; — les catégories et le nombre approximatif de personnes concernées, dans la mesure du possible ; — les conséquences de la violation de la sécurité des données, y compris les éventuels risques pour les personnes concernées (p. ex. impossibilité d'accès aux dossiers médicaux ne permettant qu'une traçabilité partielle du traitement, ce qui engendre un risque potentiel pour la santé de la personne concernée ; la publication des dossiers médicaux sur le darknet, ce qui met en danger la personnalité des personnes concernées) ; — les mesures prises ou envisagées pour remédier au défaut ou en atténuer les conséquences (p. ex. restauration de la sauvegarde de données numériques) ; et — le nom et les coordonnées d'une personne de contact. S'il n'est pas possible de communiquer toutes les informations en même temps, les informations restantes peuvent être mises à la disposition du PFPDT par étapes et dans un délai raisonnable. **Remarque :** Un registre des activités de traitement établi au préalable pourrait fournir une aide pour identifier les catégories de personnes et de données concernées par la violation de la sécurité des données (cf. à ce propos le guide et le modèle de registre des activités de traitement).

EP-08	Information aux personnes concernées ?	La personne responsable de la sécurité des données évalue s'il y a lieu d'informer les personnes concernées par la violation de la sécurité des données. Les personnes concernées sont à informer : — lorsqu'il est nécessaire de prendre des mesures de protection (p. ex. modification des données d'accès telles que les mots de passe) ou — lorsque le PFPDT l'exige. La personne responsable de la sécurité des données peut restreindre ou différer l'information des personnes concernées, ou y renoncer dans les cas suivants : — lorsqu'un intérêt prépondérant l'exige ; — lorsque l'information est interdite en vertu d'une obligation légale de garder le secret ; — lorsque l'information est impossible ou exige des efforts disproportionnés ou — lorsque l'information de la personne concernée peut être garantie de manière équivalente par une communication publique.
EP-09	Annonce aux personnes concernées	S'il est apparu lors de l'EP-08 qu'il est nécessaire d'informer les personnes concernées, il convient de préparer une annonce de la violation de la sécurité des données. L'annonce contient au moins les indications suivantes : — la nature de la violation de la sécurité des données (p. ex. destruction des données, vol des données, etc.) ; — les conséquences de la violation de la sécurité des données, y compris les éventuels risques pour les personnes concernées (p. ex. perte de l'accès aux dossiers médicaux ne permettant qu'une traçabilité partielle du traitement, ce qui engendre un risque potentiel pour la santé des personnes concernées ; la publication des dossiers médicaux sur le darknet, ce qui compromet la personnalité des personnes concernées) ; — les mesures prises ou envisagées pour remédier au défaut ou en atténuer les conséquences (p. ex. restauration de la sauvegarde en cas de perte de données numériques) ; — le nom et les coordonnées d'une personne de contact.
EP-10	Autres mesures ?	Une fois les mesures immédiates mises en œuvre et l'application de l'obligation d'annoncer au PFPDT et aux personnes concernées, préalablement examinée puis, le cas échéant, satisfaite, il y a lieu de déterminer si d'autres mesures sont nécessaires, lesquelles pourront toutefois être mises en œuvre à moyen ou long terme (voir aussi EP-04).
EP-11	Mise en œuvre d'autres mesures	S'il s'est avéré que d'autres mesures étaient nécessaires, celles-ci peuvent être mises en œuvre (cf. également M-10.07 et M-10-08 des Exigences minimales pour la sécurité informatique des cabinets médicaux).
EP-12	Documentation	La personne responsable de la sécurité des données documente dans tous les cas la violation de la sécurité des données (cf. ch. 1.3 Liste de contôle, section « Documentation » ci-avant).
EP-13	Traitement de la violation de la sécurité des données	Une fois les mesures nécessaires mises en œuvre, l'éventuelle annonce effectuée et la violation de la sécurité des données documentée, la procédure est close.

Impressum
Edition: FMH – Fédération des médecins suisses, Berne
Publication: mars 2023
www.fmh.ch