# Réagir à un incident

> **Référentiel BTS — BC3 / C3.6** « Se prémunir et réagir face aux incidents numériques ».

> **L'essentiel :** face à un incident, les premières minutes comptent. Trois réflexes : **isoler**, **alerter**, **ne rien détruire**. Et une règle : on **ne gère pas seul**, on applique une procédure décidée à froid.

# Objectif

À la fin de cette page, vous savez :

- exécuter les premiers gestes face à un incident numérique ;
- dire qui prévenir, dans quel ordre, et dans quels délais ;
- distinguer l'incident technique de la **violation de données personnelles**.

# Reconnaître qu'il se passe quelque chose

Signaux qui doivent déclencher l'alerte, même en cas de doute :

- des fichiers **renommés ou illisibles**, une note de rançon à l'écran ;
- l'ordinateur **anormalement lent**, des fenêtres qui s'ouvrent seules, un curseur qui bouge seul ;
- une **connexion inconnue** signalée sur un compte, ou un mot de passe qui ne fonctionne plus ;
- des **messages partis de votre boîte** que vous n'avez pas écrits ;
- un **document envoyé au mauvais destinataire**, un **téléphone ou un portable perdu** ;
- un patient qui signale avoir reçu un message étrange « de votre part ».

>

> Le pire réflexe est le silence. Beaucoup d'incidents s'aggravent parce que la personne qui a cliqué a eu honte de le dire. **Le cabinet doit poser explicitement qu'un signalement rapide ne sera jamais reproché** — c'est une règle de management autant que de sécurité, et elle doit être dite à l'équipe avant l'incident, pas après.

# Les premiers gestes

**1. Isoler** — déconnecter le poste concerné du réseau : câble réseau débranché, Wi-Fi coupé. Objectif : empêcher la propagation aux autres postes et au serveur.

**2. Ne pas éteindre** (sauf consigne contraire d'un professionnel) — l'extinction peut détruire des traces utiles à l'analyse. Isoler ≠ éteindre.

**3. Ne rien « nettoyer »** — ne pas supprimer les fichiers suspects, ne pas vider les journaux, ne pas réinstaller dans la précipitation. Ce sont des **preuves**, nécessaires pour comprendre l'étendue et pour la plainte.

**4. Alerter** — le responsable désigné dans le cabinet, puis le prestataire informatique ou l'éditeur.

**5. Tracer** — noter par écrit, au fil de l'eau : **date et heure**, ce qui a été constaté, par qui, ce qui a été fait. Ce journal sera indispensable pour la CNIL, l'assurance et la plainte.

**6. Changer les mots de passe** concernés — **depuis un autre poste**, sain.

# Qui prévenir

| Destinataire | Quand | Pourquoi |
|---|---|---|
| **Responsable interne / dirigeant** | Immédiatement | Il décide et engage la structure. |
| **Prestataire informatique / éditeur** | Immédiatement | Diagnostic, endiguement, restauration. |
| **CNIL** | **Sous 72 h** après en avoir pris connaissance, si des **données personnelles** sont touchées et que le risque pour les personnes n'est pas négligeable | Obligation légale (notification de violation de données). |
| **Les personnes concernées** (patients) | Sans délai, si le risque est **élevé** pour elles | Obligation légale ; leur permettre de se protéger. |

| Destinataire | Quand | Pourquoi |
|---|---|---|
| **Dépôt de plainte** (police, gendarmerie) | Rapidement | Nécessaire pour l'assurance, et pour l'action pénale. |
| **cybermalveillance.gouv.fr** | En parallèle | Aide au diagnostic, annuaire de prestataires de proximité. |
| **CERT Santé / ARS** | Selon le statut de la structure | Le signalement des incidents graves de sécurité des SI relève de l'article **L. 1111-8-2** du code de la santé publique, dont le champ (établissements de santé, médico-sociaux, laboratoires…) est précisé par le décret n° 2022-715 du 27 avril 2022. Une petite structure libérale n'entre pas nécessairement dans ce champ, mais peut solliciter l'appui du CERT Santé. |
| **Assureur** | Selon le contrat, souvent sous quelques jours | Déclaration de sinistre, garantie cyber le cas échéant. |

> ⚠ Le délai de **72 h** vers la CNIL court **à partir du moment où la structure a connaissance** de la violation — pas à partir de la fin de l'analyse. En cas d'incertitude sur l'ampleur, on notifie et on complète ensuite.

# Incident technique ou violation de données ?

Les deux ne se recouvrent pas :

- Un serveur qui tombe en panne sans fuite ni perte est un **incident technique** : pas de notification CNIL, mais un enjeu de **continuité d'activité**.
- Un compte rendu envoyé au mauvais patient est une **violation de données** sans la moindre attaque informatique.
- Un rançongiciel est **les deux à la fois** : indisponibilité **et**, très souvent, fuite de données.

La qualification détermine les obligations. Elle se documente dans le **registre des violations**, que toute structure doit tenir — même pour les incidents non notifiés à la CNIL (voir *Formation métier — Données de santé & réglementation*).

# Après : le retour d'expérience

Un incident correctement traité se termine par une analyse à froid, en équipe :

1. **Par où est-ce entré ?**
2. **Qu'est-ce qui a fonctionné** dans notre réaction, et **qu'est-ce qui a manqué** (numéro introuvable, sauvegarde non testée, personne ne savait qui prévenir) ?
3. **Quelles mesures** on met en place, avec un responsable et une date.
4. **Mise à jour de la procédure**, et information de toute l'équipe.

# À retenir

- **Isoler, ne pas éteindre, ne rien effacer, alerter, tracer.**
- **72 h** pour notifier la CNIL en cas de violation de données personnelles à risque.
- **Déposer plainte** et conserver les preuves.
- Un incident se **documente** et se **débriefe** : c'est ce qui évite le suivant.
- Signaler vite doit être **encouragé**, jamais sanctionné.

# Sources

- Le cadre législatif — Portail du CERT Santé
- Article L. 1111-8-2 du code de la santé publique — Légifrance

---

Revision #5
Created 2026-09-15 17:24:24 UTC by Antoine
Updated 2026-09-16 07:03:15 UTC by Antoine