PANNE INFORMATIQUE OU CYBER-INCIDENT



Continuer à soigner au cabinet, sans aggraver l'incident
(Plan de Continuité d'Activité / PCA)

1 - Réagir immédiatement

Étape 1 : Diagnostic

SCÉNARIO A : Bug ou panne logicielle/internet

Signes évocateurs

> Un seul poste ou logiciel touché (vérification auprès de vos confrères et/ou collaborateurs)
> Message d'erreur du logiciel, lenteur
> Panne annoncée par l'éditeur ou le prestataire
> Coupure Internet ou électrique, lecteur de carte hors service
> Aucun fichier modifié ou devenu illisible

1. Redémarrer le poste
2. Si le problème persiste : appeler l'éditeur ou le prestataire informatique (cf. page 3)
3. Sortir le matériel de secours (cf. page 3)

SCÉNARIO B : Suspicion de cyberattaque

Signes évocateurs

> Écran bloqué, message de rançon
> Fichiers illisibles, chiffrés, renommés
> Plusieurs postes touchés en même temps
> Comportement anormal : souris qui bouge seule, mots de passe refusés ou modifiés, antivirus désactivé, courriels envoyés à votre insu
> Alerte de l'éditeur ou de l'hébergeur signalant une attaque

Ne jamais banaliser l'incident !

1. **Ne pas éteindre** les machines (pour préserver les preuves techniques)
2. **Débrancher le câble réseau** (ethernet) ou couper le wi-fi ; déconnecter les sauvegardes externes
3. **Noter l'heure** de découverte et les symptômes observés
4. Alerter le **prestataire informatique** et le **17cyber.gouv.fr**
5. **Ne pas payer** de rançon. Prévenir son **assureur**[1]
6. Sortir le **matériel de secours**

[1] *Certains contrats d'assurance (notamment de local professionnel) incluent un service d'assistance informatique en cas d'incident cyber voire l'intervention d'un prestataire spécialisé.*

2 - Consulter en mode dégradé

1. **Trier** : identifier les patients prioritaires (urgences, pathologies chroniques)
2. **Reconstituer l'agenda dès que possible** (si possible grâce à des sauvegardes en amont)
3. **Accéder aux services socles si internet fonctionnel**. Si scénario B, alors utiliser un appareil **non compromis et hors réseau du cabinet**
4. **Tracer** : noter examen, conclusions et prescriptions sur support papier ou informatique non compromis
5. **Facturer** : en mode dégradé SESAM-Vitale avec pièces justificatives via SCOR ; à défaut, feuille de soins papier (conserver une copie)

Les services socles, des alliés dans la crise (si internet fonctionnel)

Avant la crise : alimenter et consulter

> Envoyer au DMP chaque document remis au patient : ordonnances, comptes rendus, vaccinations, courriers d'adressage…

> Actualiser et verser le VSM (Volet de Synthèse Médicale), surtout pour les patients chroniques

> Chaque vendredi faire une impression de votre agenda de la semaine suivante

Pendant la crise : consulter

> dmp.fr : antécédents, allergies, traitements de fond, VSM, dernières ordonnances, résultats et comptes rendus

> MSSanté : résultats et courriers reçus

> AmeliPro (e-CPS ou lecteur CPS de secours) : droits du patient et prescriptions sécurisées

Si internet non fonctionnel : demander à chaque patient d'apporter ses derniers courriers, ordonnances et résultats d'examens.

3 - Sortie de crise et retour à la normale

Une fois le système rétabli :

> **En cas de cyber-incident, vérifier ou faire vérifier** l'intégrité du système (antivirus, journaux) **avant** de reconnecter les postes **+ changer tous les mots de passe**

> **Régulariser** : saisir ou scanner dans le logiciel métier les données recueillies sur papier puis les verser au DMP

> **Déclencher** les facturations différées

> **CNIL** : finir de compléter la notification initiale si besoin et tenir à jour le registre des violations

> **Reconstituer le matériel de secours**

4 - Matériel de secours

Classeur de secours : identifié, rangé dans un lieu connu de tous, sécurisé mais simple d'accès, permettant **5 à 10 jours** d'activité. Ordonnances et Cerfa **à commander à l'avance** sur AmeliPro.
+ sauvegardes régulières de votre agenda et de vos logiciels s'ils ne sont pas en SaaS.

Document	Quantité suggérée (pour 1 médecin)	Stock vérifié le
Ordonnances	2 blocs classiques + 1 bloc sécurisé (stupéfiants) + 1 bloc bi-zone	.....
Feuilles de soins	250 exemplaires (si le lecteur de carte est hors service)	.....
Arrêts de travail	1 à 2 liasses de 25 exemplaires (sécurisés)	.....
Certificats AT/MP	20 à 30 exemplaires	.....
Protocoles de soins ALD	5 à 10 exemplaires	.....
Dossier patient vierge	250 fiches d'examen simplifiées (prise de notes manuscrite)	.....
Et aussi	Une copie de cette fiche, une feuille pour le suivi de facturation différée, l'affiche « Informations patients » (§7), la copie du contrat avec votre prestataire informatique	.....

+/- outils informatiques de secours (hors réseau) : PC, imprimante, accès internet séparé (point d'accès 4G/5G) voire clé USB (modèles Word/PDF d'ordonnances types et de courriers d'adressage)

5 - Numéros utiles à compléter

Contact	Nom / n° de contrat	Contact
Prestataire informatique		
Éditeur du logiciel métier (support)		
Assureur (cyber / RCP)		
Fournisseur d'accès Internet		
Banque		
17Cyber : assistance aux victimes 24h/24 7j/7		17cyber.gouv.fr
Centre de Réponse aux Incidents Cyber Nouvelle-Aquitaine du lundi au vendredi, 9h-17h		0 805 29 29 40
CNIL : notifier une violation		notifications.cnil.fr/notifications/index

6 - Déclarer à la CNIL dans les 72 heures

Point de vigilance

Même si votre logiciel est en SaaS (hébergé en ligne), vous restez responsable du traitement. L'éditeur est sous-traitant : il doit vous alerter dans les meilleurs délais (art. 33.2 RGPD), mais la notification à la CNIL vous incombe.

Y a-t-il violation de données ?

> Toute atteinte à la confidentialité (fuite, accès non autorisé), à l'intégrité (altération, chiffrement) ou à la disponibilité (données inaccessibles, même temporairement) de données personnelles.

Faut-il déclarer ?

> Oui !

Dans quel délai ?

> Dans les 72 h de la découverte ; au-delà, il faudra justifier le retard.

N.B. : la notification peut être réalisée en deux temps : initiale dans les 72 h puis complémentaire.

Comment ?

> Téléservice notifications.cnil.fr/notifications/index

+ consigner l'incident dans le registre interne des violations.

7 -Information des patients

Afficher dans le cabinet la page **« Information patients - Panne informatique & continuité de vos soins »** du kit de résilience ANS.

Télécharger le kit de résilience de l'ANS

Point de vigilance

Une information individuelle est aussi nécessaire en cas de violation à risque élevé pour les droits et libertés des personnes concernées.

Retrouvez toutes nos fiches sur