

# GUIDE DE CONFORMITÉ D'UN CONTRAT INFORMATIQUE CABINET MÉDICAL

- DIX POINTS À VÉRIFIER -



Un document réalisé par



En partenariat avec



Ce guide a été conçu à l'occasion de la première édition de la Journée de l'Exercice Médical Libéral (JEML), organisée en 2025 à Poitiers par l'URPS ML NA. Pensée comme un temps fort d'échanges et de montée en compétences à destination des médecins libéraux en exercice ou en devenir, la JEML a pour objectif de leur fournir des repères concrets dans un contexte de numérisation croissante où **la cybervigilance est devenue un enjeu majeur de l'exercice médical libéral.**

Ce document s'inscrit dans cette logique opérationnelle : il prolonge les apports de l'atelier Cybervigilance en proposant **un outil pratique, directement mobilisable pour sécuriser les relations contractuelles avec les prestataires informatiques.**

## POURQUOI CE GUIDE ?

Le cabinet médical repose sur un système informatique sensible. Un contrat mal défini expose le médecin à des risques majeurs. L'objectif de ce guide est d'aider à vérifier que toutes les clauses essentielles figurent dans le contrat avec un prestataire informatique (infogérant ou éditeur), et que les responsabilités de chacun sont explicitement encadrées.

**Les éléments qu'il convient de vérifier dans tout contrat relèvent des 10 catégories suivantes :**

## 1. PÉRIMÈTRE ET RESPONSABILITÉS

- Le **périmètre** exact des services du prestataire informatique est listé
- Ce qui n'est pas couvert** est clairement indiqué
- Les logiciels métier** gérés ou non sont précisés
- Le prestataire a une **obligation de conseil** explicitement mentionnée
- Les responsabilités du prestataire et du médecin** sont écrites explicitement

### Pourquoi c'est important ?

Un manque de précision crée des zones grises : lors d'un incident, le prestataire peut refuser d'intervenir ou facturer massivement.

Par ailleurs : un certain nombre de contrats ne distingue pas la maintenance corrective (résolution de panne) de la maintenance évolutive (améliorations, mises à niveau).

Sans distinction claire, le prestataire peut facturer des interventions essentielles en supplément.

## 2. GESTION DES INCIDENTS ET DES CYBERATTAQUES

**Délais d'intervention garantis** pour les incidents critiques (*incident qui affecte sérieusement la confidentialité, l'intégrité ou la disponibilité, surtout lorsqu'il touche des données de santé ou empêche d'exercer la médecine en conditions normales*)

**Délais d'intervention** précisés pour incidents majeurs et mineurs

**Horaires** d'intervention, **astreinte** (si prévue), **coûts**

**Procédure opérationnelle** en cas de cyberattaque :

- isolement des machines
- analyse
- restauration
- accompagnement déclaratif CNIL

**Modalités de communication** pendant un incident (numéro d'urgence, escalade)

### Points faibles fréquents

Les contrats ne mentionnent pas la remédiation en cas de cyberattaque. Sans formalisation, la prise en charge peut être refusée.

## 3. MISES À JOUR ET CORRECTIFS

- **Mises à jour de sécurité** incluses dans le contrat
- **Mises à jour automatiques ou planifiées**
- Engagement sur le **délai d'application des patchs critiques**
- **Mise à jour du système d'exploitation** (Windows, iOS, serveurs)
- **Vérification de compatibilité** avec les logiciels métiers

### Alerte

La non mise à jour des systèmes d'exploitation, logiciels, équipements de sécurité peut être une faille exploitée par les attaquants. Le médecin doit savoir si la mise à jour incombe au prestataire ou si cela relève de sa responsabilité.

Certains prestataires n'appliquent les mises à jour que sur demande du cabinet, sans informer clairement de la mise à disposition de ces nouvelles versions : cela revient souvent à ne jamais les appliquer.

Exiger une clause de mise à jour systématique par le prestataire.

## 4. SAUVEGARDES

- **Sauvegardes quotidiennes** prévues et types de sauvegardes précisés
- **Sauvegardes chiffrées**
- **Hébergement certifié HDS** (hébergeur de données de santé à caractère personnel)
- **Nombre de versions** conservées défini
- **Test de restauration** prévu au contrat (au moins semestriel)
- **Procédure de restauration** documentée

### Point critique

Une sauvegarde non testée n'est pas une sauvegarde.

### Écueil typique

Si le prestataire sous-traite à un hébergeur non certifié sans l'indiquer clairement : cela constitue un risque juridique majeur.

### Alerte supplémentaire

En réseau ou en USB, une sauvegarde externe ne doit pas rester branchée en permanence : une sauvegarde non isolée risque d'être inutilisable en cas de ransomware.

### Recommandation

Réaliser, a minima, une restauration de sauvegarde annuelle, avec preuve de sa bonne exécution et avoir une copie de sa sauvegarde isolée du bureau informatique ou hors ligne.

## 5. SÉCURITÉ DU RÉSEAU ET DES ACCÈS

- ▣ Feuilles **Firewall** installé et maintenu par le prestataire
- ▣ Feuilles **Accès WiFi séparés** (pro / privé / patients)
- ▣ Feuilles **VPN** pour accès distant
- ▣ Feuilles **Authentification forte** par Pro Santé Connect ou par double authentification (2FA) pour les services critiques
- ▣ Feuilles **Comptes utilisateurs individuels** (pas de comptes partagés)
- ▣ Feuilles **Gestion des droits** (pas d'accès administrateur inutile)

### Recommandation

Si le professionnel médical dispose d'un compte administrateur, il sera nécessaire de le sécuriser et de ne l'utiliser que pour effectuer des tâches d'administration.

## 6. ANTIVIRUS ET PROTECTION AVANCÉE

- ▣ Feuilles **Antivirus professionnel** installé sur tous les postes
- ▣ Feuilles **Supervision centralisée** par le prestataire
- ▣ Feuilles **Protection contre les logiciels malveillants** incluse
- ▣ Feuilles **Alertes automatiques** remontées au cabinet et au prestataire et **traitement systématique de ces alertes.**

### Alerte

Certains prestataires installent un antivirus mais ne supervisent rien. Sans supervision, les alertes critiques peuvent rester non traitées pendant un délai certain.

## 7. PARC INFORMATIQUE : DOCUMENTATION FOURNIE

- 🍃 **Inventaire complet** du matériel et des versions logicielles
- 🍃 **Schéma réseau**
- 🍃 **Politique de sauvegarde** écrite
- 🍃 **Liste des sous-traitants** du prestataire
- 🍃 **Liste des comptes et accès techniques** (sous enveloppe scellée)
- 🍃 **Rapport d'intervention** périodique prévu (annuel ou trimestriel)

### Alerte

En l'absence d'un inventaire et d'un schéma réseau mis à jour, il est impossible de détecter des failles, des appareils obsolètes ou des matériels non sécurisés laissés actifs.

## 8. HÉBERGEMENT DES DONNÉES

- 🍃 **L'hébergeur est certifié HDS** (preuve fournie)
- 🍃 **Localisation des serveurs** précisée (France ou en Europe)
- 🍃 **Sous-traitance encadrée et transparente**
- 🍃 **Clause RGPD** : rôle du prestataire et des sous-traitants éventuels clairement indiqué

### Alerte

La liste des hébergeurs certifiés HDS est disponible sur le site officiel suivant :

<https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies>

La mention « données stockées dans le cloud » est insuffisante : il faut une preuve HDS.

## 9. ASPECTS FINANCIERS

- ☛ **Ce qui est inclus** dans le forfait est clair
- ☛ **Ce qui est facturé** en plus est listé
- ☛ **Modalités de facturation** des interventions hors forfait
- ☛ **Durée d'engagement** raisonnable (12 mois ou reconduction tacite)
- ☛ **Conditions de résiliation** simples et sans verrouillage
- ☛ **Accès aux données garanti** en cas de rupture du contrat

### Alerte

Certains contrats incluent des frais de sortie prohibitifs ou rendent la récupération des données dépendante d'un « forfait de transfert ». C'est illégal si aucune alternative raisonnable n'est proposée.

## 10. SORTIE DE CONTRAT

- ☛ **Procédure de réversibilité** écrite
- ☛ **Récupération des données** dans un format standard prévue
- ☛ **Effacement sécurisé**, par l'ancien prestataire, prévu (après la récupération des données)
- ☛ **Accompagnement au transfert** prévu (optionnel mais recommandé)

### Alerte

Exiger un délai maximum pour la récupération des données (ex. 15 jours). Certains prestataires pourraient être tentés de ralentir le changement de fournisseur.



⋮ POUR NOUS SUIVRE ET EN SAVOIR +



[urpsml-na.org](https://urpsml-na.org)



[@URPS Médecins Libéraux Nouvelle-Aquitaine](https://www.linkedin.com/company/urps-medecins-liberaux-nouvelle-aquitaine)



[@UrpsMedecinsNouvelleAquitaine](https://www.youtube.com/channel/UCUrpsMedecinsNouvelleAquitaine)