OG IT CONSULTING

RESPONSABILITÉ DU DIRIGEANT · NIS2 · DONNÉES DE SANTÉ

**LIVRE BLANC · CYBER 2026**

PME SANTÉ

# Vous vous croyez couverts. Soyons-en sûrs.

Données patients, savoir-faire et responsabilité du dirigeant : ce que les dirigeants du secteur santé (labos, soins, biotech, medtech, éditeurs) ne peuvent plus repousser en 2026.

*OG IT Consulting est un cabinet d'aide à la décision des dirigeants face aux enjeux cyber et IA. Nous éclairons votre exposition réelle, votre responsabilité personnelle et votre assurabilité cyber, là où le DSI, l'hébergeur, l'assureur et l'avocat ne voient chacun qu'une partie.*

Lecture : 9 minutes. · Édition juin 2026. · Réservé aux dirigeants.

CHAPITRE 00

# Le dirigeant qui se croyait couvert.

Prenez le dirigeant d'un laboratoire de biologie, d'un hôpital ou d'une clinique, d'un EHPAD, d'un acteur de la pharma ou de la biotech, d'un fabricant de dispositifs médicaux ou d'un éditeur de logiciel de santé. Il héberge ses données chez un Hébergeur de Données de Santé certifié. Il a un prestataire informatique. Il a une assurance. De son point de vue, le sujet cyber est traité.

Sauf que l'hébergement certifié HDS protège l'endroit où vivent les données, pas l'usage que votre organisation en fait. Le prestataire exploite, il n'arbitre pas votre niveau de risque. L'assurance ne rembourse que ce que le contrat n'a pas exclu, et la liste des exclusions est plus longue qu'on ne le croit. Et personne, dans cette chaîne, ne porte une vision d'ensemble de votre exposition réelle ni de votre responsabilité de dirigeant.

> **La donnée de santé est l'une des plus convoitées du marché noir. Et la PME de santé est l'une des moins préparées et des moins assurées. Vous croyez être couvert parce que vous êtes hébergé. Ce n'est pas la même chose.**

Ce livre blanc n'est pas là pour vous faire peur, ni pour vous vendre une assurance. Il vous donne la lecture que personne ne vous donne, parce que chacun de vos interlocuteurs ne regarde qu'un morceau du tableau. À la fin, vous saurez si vous êtes réellement couvert, ou si vous le croyez seulement.

**Que vous soyez un laboratoire, un hôpital, une clinique, un EHPAD, un acteur de la pharma ou de la biotech, un fabricant de dispositifs médicaux ou un éditeur, le risque prend une forme différente. La responsabilité, elle, reste la même : la vôtre.**

CHIFFRES CLÉS

# Ce que disent les chiffres en 2026.

**749**
incidents de sécurité déclarés dans le secteur de la santé en 2024, en hausse de 29 % en un an, dans 558 établissements.

**20 M€ ou 4 %**
du chiffre d'affaires annuel mondial : sanction maximale du RGPD, applicable aux données de santé (sensibles).

**0,2 %**
des PME françaises sont couvertes par une cyberassurance, contre 84 % des grandes entreprises.

**Rançongiciel**
la menace la plus impactante du secteur ; les incidents liés ont progressé de 28 % en un an (Observatoire ANS 2024).

**1,5 M€**
amende CNIL après la fuite des données médicales d'environ 500 000 personnes.

*Sources : Observatoire des incidents de sécurité des SI santé et médico-social 2024, Agence du Numérique en Santé / CERT Santé, et CERT-FR (CERTFR-2024-CTI-010) ; RGPD, article 83 ; AMRAE, étude LUCY ; CNIL, délibération SAN-2022-009 du 15 avril 2022 (Dedalus Biologie).*

**À RETENIR**

## Cinq vérités que les dirigeants de la santé découvrent trop tard.

Le secteur de la santé est l'un des plus ciblés et des plus régulés. Voici cinq vérités que trop de dirigeants ne mesurent qu'une fois l'incident survenu.

1. **Hébergé chez un HDS ne veut pas dire protégé.** La certification HDS sécurise l'hébergement, pas vos postes, vos accès, vos sauvegardes ni vos usages internes. C'est une brique, pas un bouclier.

2. **Une attaque n'arrête pas que des données, elle stoppe votre activité.** Selon votre métier : les soins et les rendez-vous, la chaîne d'analyse du laboratoire, la production pharmaceutique, ou la plateforme dont vos clients dépendent. Et pour les structures de soins, la sécurité des patients elle-même.

3. **La donnée de santé se monnaie, et se sanctionne.** Volée, elle se revend cher. Mal protégée, elle expose à une sanction RGPD pouvant atteindre 4 % du chiffre d'affaires mondial. Deux fois perdante.

4. **La première cible, c'est vous.** Avant le DSI ou le DPO, c'est le dirigeant dont la responsabilité est engagée. NIS2 place la gestion du risque cyber au niveau de la direction.

5. **La décision se porte au plus haut niveau.** Le DSI, le DPO et l'hébergeur initient et alertent. Ils ne décident pas du risque acceptable et ne maîtrisent pas votre assurabilité cyber. C'est au dirigeant d'arbitrer.

**Le point commun de toutes les organisations de santé frappées : elles se croyaient couvertes. Souvent, des alertes existaient et n'avaient pas été traitées au bon niveau.**

CHAPITRE 01

# Pourquoi le cyber rattrape les dirigeants de la santé en 2026.

Quatre forces convergent en même temps. Leur combinaison change la nature du problème, et de la décision.

## 1. L'attaque n'arrête pas des données. Elle arrête votre activité.

Un rançongiciel qui se propage bloque tout, mais pas la même chose selon votre métier : le dossier patient et la facturation pour un établissement de soins, la chaîne d'analyse et les automates pour un laboratoire, la production pour un industriel pharmaceutique, la plateforme que vos clients utilisent pour un éditeur. L'attaque interrompt les soins, fige vos résultats, stoppe vos lignes ou prive vos clients de leur outil. Et pour les structures de soins, elle touche en plus la sécurité des patients. Le secteur l'a appris dans la douleur, avec des organisations contraintes de revenir au papier pendant des semaines.

> TÉMOIGNAGE PUBLIC
>
> *« Nous sommes revenus au papier, au fax pour communiquer quand c'était possible sur des lignes analogiques. Il a fallu former le personnel le plus jeune à l'usage du fax. »*
>
> Thierry Gamond-Rius, directeur du Centre Hospitalier Intercommunal de Haute-Comté (Pontarlier), après la cyberattaque d'octobre 2025. Rapporté par France 3.

## 2. L'assurance n'est plus un transfert de risque. C'est un examen.

Le marché de la cyberassurance a basculé. L'obtention ou le renouvellement d'une cyberassurance est désormais conditionné au respect d'exigences techniques et organisationnelles de plus en plus strictes : authentification multifacteur, sauvegardes testées, détection sur les postes, plan de continuité. L'assureur ne couvre plus le risque, il vérifie d'abord que vous le maîtrisez.

## 3. Vos tutelles, vos partenaires et le RGPD vous auditent.

Le secteur de la santé est l'un des plus régulés. Hébergement certifié HDS, obligations RGPD renforcées sur les données sensibles, exigences des ARS, des donneurs d'ordre hospitaliers et des partenaires. La cybersécurité est devenue un préalable contractuel et réglementaire, pas une option que l'on traite après.

## 4. NIS2 transfère la responsabilité au dirigeant.

La directive NIS2, transposée par la loi Résilience attendue à l'été 2026, couvre le secteur de la santé et place la gestion du risque cyber au niveau de l'organe de direction. Le dirigeant approuve, supervise, se forme, et sa responsabilité peut être engagée. Les sanctions atteignent 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour les entités essentielles, et s'ajoutent au risque RGPD propre aux données de santé.

**Avant, une attaque égalait une amende pour l'établissement. Désormais, une attaque qui révèle une absence de pilotage met en cause la direction. « Je ne savais pas » n'est plus une défense. C'est devenu une faute.**

CHAPITRE 02

# Pourquoi c'est une décision de dirigeant, pas de DSI.

Le réflexe est de renvoyer le cyber à la technique, ou au DPO. C'est l'erreur qui coûte le plus cher. Chacun de vos interlocuteurs fait bien son métier, mais ne voit qu'une partie du tableau.

- Le DSI ou le prestataire installe, configure, exploite. Il ne décide pas du risque résiduel acceptable et ne maîtrise pas votre assurabilité cyber.
- Le DPO veille à la conformité RGPD. Il ne chiffre pas votre exposition économique ni la continuité de vos soins.
- L'hébergeur HDS sécurise l'hébergement. Il ne répond pas de vos postes, de vos accès, ni de vos usages internes.
- L'assureur place une police. Il ne vous dit pas si votre dispositif tient face à ses propres exigences.
- L'avocat sécurise vos contrats. Il ne vous donne pas la lecture d'ensemble de votre risque.

**Chacun fait bien sa partie. Personne ne fait l'arbitrage d'ensemble. Pourtant, c'est exactement l'arbitrage qui est demandé au dirigeant, et à lui seul.**

## Le rôle d'OG IT Consulting.

**1 ÉCLAIRER**
votre exposition réelle, en langage de dirigeant.

**2 ARBITRER**
les investissements : la meilleure protection au meilleur coût.


**4 TENIR**
la trajectoire : la maîtrise se construit dans la durée.

**3 PROUVER**
le dossier opposable à vos assureurs, vos tutelles, votre responsabilité.

**Une fonction de chef d'orchestre, pas de musicien supplémentaire.**

CHAPITRE 03

# Le coût réel d'une attaque : le calcul que peu de dirigeants osent faire.

Que vous coûterait réellement un mois d'arrêt ? La plupart des dirigeants de la santé n'en connaissent pas le montant. Pourtant, cette réponse conditionne leur capacité à absorber une crise.

> **Chiffre d'affaires annuel ÷ 12 × nombre de mois d'interruption. À cela s'ajoute, pour la santé, le risque RGPD sur les données sensibles, jusqu'à 4 % du chiffre d'affaires mondial. La question n'est plus le montant de la rançon, c'est : suis-je capable de survivre à l'arrêt et à la sanction ?**

## Les frais auxquels on ne pense pas.

Au-delà de la rançon éventuelle, l'addition comprend :

- la perte d'activité, jour par jour
- l'expertise et la remédiation informatique
- les honoraires juridiques
- la notification à l'ANSSI, à la CNIL et aux patients
- la surprime ou le refus d'assurance au renouvellement
- les dommages réclamés en cascade par vos partenaires
- le vol de votre R&D, de vos données d'essais ou de votre savoir-faire
- la communication de crise
- le temps dirigeant englouti pendant des mois

Le coût réel atteint souvent **deux à trois fois le coût visible**.

## La confiance des patients, l'actif le plus fragile.

Une fuite de données de santé touche au plus intime. La confiance perdue ne se rachète pas avec une indemnité. Pour une PME de santé, c'est parfois la perte la plus durable.

CHAPITRE 04

# Ce que votre police couvre, et ce qu'elle ne couvre presque jamais.

Une police cyber se présente comme un produit unique. En réalité, trois exclusions majeures créent souvent un écart entre la protection perçue et la protection réelle.

## Exclusion 1. La faute de gestion.

Si votre dispositif déclaré n'est pas réellement appliqué, sauvegarde jamais testée, double authentification incomplète, alertes restées sans réponse, l'assureur peut invoquer la fausse déclaration et réduire l'indemnisation. La preuve qui sauve, ce sont les journaux et les comptes rendus de test, pas la conviction.

## Exclusion 2. Les sanctions et la perte de confiance.

Les amendes administratives, dont les sanctions RGPD, ne sont pas toujours assurables ou sont fortement limitées. Et la perte de patients ou de contrats après un incident n'est généralement pas couverte. Le contrat couvre la reconstruction, pas la confiance perdue.

## Exclusion 3. Les dommages de long terme.

Les frais de communication de crise sont couverts. Le coût réel arrive plus tard : réputation, partenariats qui s'éloignent, recrutements qui patinent. Des coûts indirects étalés sur six à dix-huit mois, jamais provisionnés.

> **Et la responsabilité personnelle du dirigeant ? La cyberassurance ne la couvre pas forcément. Les exclusions sont à vérifier ligne par ligne avec votre assureur. C'est l'angle mort le plus dangereux.**

CHAPITRE 05

# Les cas qui doivent vous alerter.

## Cerballiance, 2026 (laboratoires) : l'attaque par la chaîne fournisseur.

Le réseau de biologie médicale Cerballiance (groupe Cerba HealthCare, 700 laboratoires, 28 millions de patients par an) a vu, début 2026, l'intrusion passer par le serveur d'un prestataire externe. Données exposées : état civil, identifiants, comptes rendus d'analyses, numéros de sécurité sociale. Signalé à la CNIL, à l'ANSSI et à l'ARS. Et c'était une récidive après un incident similaire en 2025. La faille n'était pas chez eux, mais chez leur prestataire : c'est tout l'enjeu de la chaîne fournisseur.

## Hôpital Ramsay de la Loire, Saint-Étienne, 2025 (clinique) : le vol de données patients.

Entre fin juin et début juillet 2025, une cyberattaque sur cet établissement privé a exposé les données personnelles de plus de 126 000 patients. L'établissement a indiqué qu'il s'agissait quasi exclusivement de données administratives, mais certains patients ont vu fuiter leur motif d'hospitalisation. Le parquet de Paris a saisi l'office anti-cybercriminalité. Même un grand groupe privé n'est pas à l'abri ; une PME de santé l'est encore moins.

## Le secteur dans son ensemble : une cible qui ne désenfle pas.

En 2024, 749 incidents de sécurité ont été déclarés dans le secteur de la santé et médico-social, en hausse de 29 % sur un an, répartis dans 558 établissements. Le rançongiciel reste la menace la plus impactante. Si les grands établissements se défendent mieux, les structures plus petites et le médico-social restent exposés.

## Dedalus Biologie, 2022 (éditeur de données) : la sanction qui tombe.

À la suite d'une fuite ayant exposé les données médicales d'environ 500 000 personnes, dont des informations parmi les plus sensibles, la CNIL a prononcé une sanction de 1,5 million d'euros. Fait marquant : des alertes sur le niveau de sécurité, y compris de l'ANSSI, étaient restées sans réponse. L'illustration parfaite du « on se croyait couverts ».

## Pierre Fabre, 2021 (pharma) : la production à l'arrêt et l'extorsion.

Le laboratoire pharmaceutique a été frappé par le rançongiciel REvil, avec une rançon initiale de 25 millions de dollars. L'entreprise a dû stopper une partie de sa production et renvoyer des salariés chez eux. Pour un acteur de la pharma ou de la biotech, l'attaque ne menace pas que des données : elle stoppe la production et vise un savoir-faire qui vaut des années de R&D.

*Sources : usine-digitale et Orange (Cerballiance, 2026) ; Le Monde Informatique et presse spécialisée (Pierre Fabre, REvil, 2021) ; CNIL, délibération du 15 avril 2022 (Dedalus Biologie) ; franceinfo (Hôpital Ramsay de la Loire, Saint-Étienne, 2025) ; France 3 Bourgogne-Franche-Comté (CH de Pontarlier, 2025) ; Observatoire des incidents de sécurité des SI santé et médico-social 2024 (CERT Santé / Agence du Numérique en Santé).*

CHAPITRE 06

## Cinq questions à poser avant qu'il ne soit trop tard.

Trois à votre assureur, deux à vous-même. Posez-les avant la signature, au renouvellement, et surtout si vous pensez ne pas en avoir besoin.

1. **Quel est le coût précis d'une interruption majeure dans mon établissement, en euros et en jours, sécurité des patients comprise ?**
2. **Que dit exactement ma police sur ma responsabilité personnelle de dirigeant, et sur les sanctions RGPD ?**
3. **Quelles exclusions de ma cyberassurance me concernent vraiment, données de santé comprises ?**
4. **Mon dispositif déclaré est-il réellement appliqué et prouvable, au-delà de l'hébergement HDS ?**
5. **Quel est l'investissement minimum pour passer du « je crois » au « je sais » ?**

> **Si ces questions vous mettent mal à l'aise, c'est sain. C'est la première étape pour reprendre le contrôle. Et non, nous ne vendons pas d'assurance.**

CHAPITRE 07

## Reprendre la main, sans précipitation.

Si ce livre blanc vous a légèrement mis mal à l'aise, c'est que son objectif est atteint. La lucidité est la première des protections. Vous n'avez pas besoin de tout régler demain. Vous avez besoin de savoir où vous en êtes vraiment, avant qu'un incident ne le décide à votre place.

Le bon ordre n'est pas d'acheter une assurance ou un outil dans l'urgence. C'est d'abord d'y voir clair : votre exposition réelle, votre responsabilité, vos angles morts. Le reste découle de cette clarté.

La meilleure façon de commencer ne coûte rien : reprenez les cinq questions de ce document et répondez-y honnêtement, avec votre comité de direction. Partout où vous ne savez pas répondre par un chiffre précis, vous avez trouvé votre point de départ.

# Vous vous croyez couverts. Soyons-en sûrs.

Parlons de votre exposition réelle, sans jargon et sans engagement.


**VOTRE INTERLOCUTRICE**

**Radia OURO-GBELE**

Founder & Managing Director

**CONTACT**

**contact@og-it-consulting.com**

**+33 6 69 50 78 02**

Paris, France · og-it-consulting.com


OG IT CONSULTING