



Livre blanc Altevia Tech

Édition cabinets Médicaux

Cybersécurité
et cabinets médicaux

Protéger les données de santé, garantir la continuité des soins, assumer la responsabilité médicale

Préambule

Dans un cabinet médical, la confiance est essentielle.
Elle repose sur la qualité des soins, le secret médical, la disponibilité des informations et la continuité de la prise en charge des patients

Aujourd'hui, cette confiance dépend aussi fortement du système informatique.

Dossiers patients, logiciels métiers, imagerie, prescriptions, télétransmission et échanges sécurisés sont devenus indispensables au fonctionnement quotidien.

La cybersécurité n'est plus un sujet technique secondaire.
Elle est devenue une composante directe de la responsabilité médicale et de la continuité des soins.

Ce livre blanc s'adresse aux dirigeants de cabinets médicaux et aux professionnels de santé qui souhaitent

- comprendre les risques réels
- structurer une approche claire
- assumer un cadre durable et maîtrisé
- sans alourdir la pratique médicale ni perturber les soins.

L'informatique comme outil de continuité des soins

Un cabinet médical moderne dépend de son système informatique pour

- l'accès aux dossiers patients
- la gestion des rendez vous
- la prescription et la facturation
- la télétransmission et les échanges avec les organismes
- la coordination avec d'autres professionnels de santé

L'activité médicale est continue, sensible et souvent sous contrainte de temps.

La moindre indisponibilité peut entraîner

- un retard de prise en charge
- une impossibilité d'accéder à l'historique médical
- une désorganisation du cabinet
- un risque pour le patient

**Dans ce contexte, l'informatique n'est plus un support.
C'est un outil critique de continuité des soins.**

La nature spécifique des risques cyber pour les cabinets médicaux

Des données parmi les plus sensibles

Les cabinets médicaux manipulent

- des données de santé
- des informations personnelles confidentielles
- des éléments relevant du secret médical

Ces données font partie des données les plus sensibles et les plus réglementées.

Une exposition médicale et juridique directe

Un incident informatique peut provoquer

- une violation du secret médical
- une indisponibilité des dossiers patients
- une mise en cause de la responsabilité du praticien
- des sanctions réglementaires
- une perte de confiance durable des patients

Dans un cabinet médical, un incident cyber peut avoir des conséquences humaines, médicales et juridiques.

Les fausses certitudes les plus répandues

Ce que beaucoup de cabinets pensent

De nombreux cabinets pensent être protégés car

- leur logiciel métier est conforme
- ils ont un antivirus
- ils effectuent des sauvegardes
- ils n'ont jamais connu d'incident

Ces éléments sont nécessaires mais très insuffisants.

Ce que montrent les incidents réels

La majorité des incidents graves surviennent dans des environnements

- mal configurés
- mal sauvegardés
- mal compris par les utilisateurs
- sans responsabilité clairement définie

**La cybersécurité ne se résume pas à la conformité des outils.
Elle repose avant tout sur une organisation claire et assumée.**

Le changement de paradigme nécessaire

La cybersécurité efficace repose sur trois principes fondamentaux.

La simplicité

- Un système simple, fiable et compris par l'équipe médicale est plus sécurisé qu'un environnement complexe mal maîtrisé.

L'intégration

- La sécurité doit être intégrée aux usages médicaux, sans ralentir la pratique ni la prise en charge des patients.

La responsabilité: quelqu'un doit assumer clairement

- le bon fonctionnement
- la sécurité
- la continuité
- la réaction en cas d'incident

La cybersécurité est un cadre de responsabilité médicale à poser, pas une contrainte technique à subir.

Questions clés pour les dirigeants de cabinets médicaux

Pouvez vous répondre clairement à ces questions

- vos savez vous où sont stockées les données de santé de vos patients ?
- pouvez vous accéder aux dossiers en cas d'incident informatique ?
- les accès aux dossiers sont ils strictement maîtrisés ?
- les sauvegardes sont elles réellement exploitables ?
- savez vous qui intervient en cas de problème ?
- la continuité des soins est elle garantie ?
- vous sentez vous serein sur ce sujet ?

Si ces réponses ne sont pas immédiates, le risque existe déjà.

L'approche Altevia Tech pour les cabinets médicaux

Altevia Tech accompagne les cabinets médicaux avec une approche pensée pour la réalité des soins

- Claire
- Progressive
- sans jargon inutile
- orientée responsabilité et sérénité.

Nous prenons en charge l'ensemble du système informatique

- la gestion du parc informatique
- le support utilisateurs
- la supervision continue
- les sauvegardes et la continuité d'activité
- la gestion des accès et des identités

La cybersécurité est intégrée par défaut.

Elle s'adapte aux contraintes médicales sans perturber la pratique.

Objectif

- un système fiable
- des équipes opérationnelles
- une continuité garantie
- un dirigeant serein

Nous assumons la responsabilité du bon fonctionnement de votre informatique.

Une méthode progressive et adaptée au terrain

Notre démarche repose sur une progression maîtrisée

- identifier les risques concrets
- stabiliser le socle
- définir une trajectoire pragmatique
- superviser et améliorer dans le temps

Vous démarrez simplement.

Nous sécurisons sans interrompre les soins.

Conclusion

La cybersécurité dans un cabinet médical n'est pas une contrainte supplémentaire.

C'est une condition de qualité, de sécurité et de responsabilité médicale.

Un cabinet médical qui maîtrise son informatique

- protège ses patients
- respecte le secret médical
- assure la continuité des soins
- travaille sereinement

Avec Altevia Tech, vous faites le choix

- d'un partenaire responsable
- d'un cadre clair
- d'une sécurité intégrée
- d'une informatique qui soutient la pratique médicale.



Prochaines étapes

Un diagnostic cybersécurité confidentiel pour cabinets médicaux

- une analyse factuelle
- des priorités claires
- une vision maîtrisée

Pour en discuter

contact@altevia-tech.com
www.altevia-tech.com