## Gestion des risques numériques : un enjeu majeur

Outre la paralysie du système informatique qui entraîne un blocage de l’activité et des pertes financières, les cyberattaques exposent les professionnels de santé à un autre risque majeur : la modification ou la perte de confidentialité des données médicales, strictement personnelles et à forte valeur.

Mais au-delà du simple impact technique ou financier, des conséquences en termes d’image et de crédibilité sont également à craindre. Une cyberattaque peut nuire à la réputation du cabinet et engendrer une perte de confiance de la patientèle.

De plus, si les dossiers médicaux ont été divulgués, il peut également y avoir des conséquences juridiques puisque les patients ont le droit d’exiger des dommages et intérêts.

Pour minimiser les risques de cyberattaque et leurs conséquences, les professionnels de santé doivent aujourd’hui redoubler de vigilance à tous les niveaux. Parmi les bons réflexes à adopter, vérifier que son contrat multirisque professionnel couvre les cyber-risques et augmenter son niveau de garantie, le cas échéant.

**Quelques règles essentielles de cybersécurité**

* Ayez recours à des prestataires compétents en la matière pour paramétrer vos serveurs et outils informatiques (ordinateur, smartphone, réseau au sein du cabinet…) ;
* Assurez-vous du chiffrage systématique des données personnelles en ligne ;
* Utilisez une [messagerie sécurisée de santé](https://www.macsf.fr/Nos-produits-services/services-et-formations-macsf/lifen-la-messagerie-securisee-de-sante) pour tout échange avec un autre professionnel de santé ou votre patient ;
* Ne laissez pas un tiers compléter, sous votre login, des éléments dans le dossier patient informatisé ;
* Si vous utilisez une messagerie électronique standard ou des messageries instantanées, assurez-vous que ces messageries sont sécurisées et adaptées à votre utilisation professionnelle ;
* Evitez un accès libre à votre ordinateur ou votre téléphone sur lesquels pourraient être stockées des données médicales. Un verrouillage automatique de vos ordinateur/téléphone après un court délai et un chiffrement des données sensibles sont des précautions utiles.

**Adopter une bonne "cyber-hygiène"**en intégrant dans les habitudes de travail quotidiennes :

* l’utilisation de mots de passe forts ;
* l’interdiction stricte d'ouvrir des e-mails et des liens inconnus ;
* l’activation permanente des protections antivirales par pare-feu au travail et encore plus à la maison. Le risque est particulièrement important avec l’augmentation du télétravail.

**A lire aussi sur macsf.fr :["Coronavirus et l’obligation de protection des données de santé"](https://www.macsf.fr/actualites/Coronavirus-et-RGPD" \o "" \t "_blank)**

<https://www.macsf.fr/actualites/Coronavirus-et-RGPD>

<https://www.macsf.fr/actualites/les-cybercriminels-s-attaquent-aux-professionnels-de-sante>