Protection des données : L'ultimatum du 25 mai 2018

Les Professionnels de Santé face à la cybercriminalité

Pour les médecins et leur société d'exercice
Une nouvelle obligation professionnelle

Généralisation à tous les professionnels de santé

Une nouvelle réglementation, prendra effet le 25 mai 2018 : le Règlement Général sur la Protection des Données (RGPD), voté par le parlement européen en avril 2016.

Le RGPD a pour objet de **renforcer le droit à la confidentialité pour les individus et à la protection des données personnelles, en définissant des exigences de sécurité et les activités de traitement qui leur sont associées.**
Ce Règlement s'appliquera de la même manière dans les 28 États membres de l'Union Européenne (UE 2016 / 679) **à toutes les entreprises et particulièrement les professions de santé.**

- Le 1er octobre 2017 la DGS – la Direction Générale de la santé - a également imposé un plan d'action pour réduire le cyber-risque, à tous les Professionnels de Santé.

Ces nouvelles réglementations créent de nouvelles responsabilités pour vous en tant que chefs d'entreprise ainsi qu'un nouveau devoir : celui de notifier les éventuelles victimes suite à une cyber attaque.

Tous les professionnels de Santé, individuel, en société ou en établissements de soins se voient ainsi responsabilisés.

Il faut rappeler qu'en cas de plainte de la part d'un patient dont les données médicales ont été piratées, le professionnel de santé risque une peine qui peut aller jusqu'à 5 ans d'emprisonnement et 300.000 € d'amende (art. 226-17 Code pénal).

La sécurisation des systèmes informatiques de vos cabinets est donc cruciale.

Comme tous les professionnels de la santé vous allez devoir respecter notamment les obligations suivantes :

- **Obligation de déclaration ou notification dans les 72 h** en cas de perte ou de vol (même supposé) de données personnelles pour toutes les entreprises y compris les professions libérales, **sous peine d'amende de 2% de votre CA**
- **Les professionnels de santé doivent informer leur Agence Régionale de Santé (ARS)**
- **Obligation de se mettre en conformité à la politique informatique et libertés**

Vous devrez mettre en place un **« registre des traitements mis en œuvre », prouvant la politique de confidentialité et la sécurisation des données de votre société.**

MEDIRISQ vous propose un contrat d'assurance spécifique pour apporter les réponses juridiques et techniques appropriées face à la nouvelle réglementation et en réponse à la cyber criminalité.

www.MEDIRISQ.fr
Email : contact@medirisq.fr

04 76 70 9000

Février 2018,

Le contrat d'assurance des Professionnels de Santé face à la cybercriminalité

Afin de vous aider et vous accompagner MEDIRISQ apporte aux Professionnels de santé une solution d'assurance cyber-risques complète, simple et accessible **à partir de 314.33 € TTC/an.**

Pourquoi faut-il s'assurer :

- **Forte augmentation de la cybercriminalité :**

Entre 2015 et 2016 il y a eu 2.5 fois plus de cyber attaques et 4 fois plus de cyber extorsions.
Au deuxième trimestre 2016, près de 90 % des attaques «ransomware» ont visé des établissements de santé dans le monde (source Lexsi).

- **Pour couvrir les conséquences financières de cette cybercriminalité** (garanties à partir de 100 000 € jusqu'à 1million d'€)
- Une cyber-attaque peut avoir un impact direct sur votre exercice comme sur les finances de votre entreprise (**Coût moyen : 127 € / dossier reconstitué et temps perdu : en moyenne 9 semaines)**
- **Pour répondre à une des obligations du RGPD**
- **Pertes de données définitives** s'il n'y a pas d'archivage électronique efficace
- **Frais de reconstitution de données**
- **Frais de décontamination virale**
- **Frais supplémentaires d'exploitation** (personnel, utilisation d'équipement extérieur)
- **Honoraires d'experts** pour identifier l'origine et les circonstances d'un sinistre, **Frais de recours**
- **Éventuelles rançons en crypto-monnaie (bitcoins, monéro), et en €uros**

Les cabinets médicaux sont concernés

Comme tous professionnels de santé, **les données médicales des patients sont sensibles et recherchées.**
Les dossiers médicaux sont des mines d'informations personnelles.

La valeur des données de santé et des numéros de sécurité sociale dépasse très largement celle des coordonnées bancaires.

- **Chantage pour obtenir de l'argent en échange de la non-publication des données dérobées.**
- **Revente des numéros de sécurité sociale et des coordonnées bancaires des patients sur le marché parallèle.**
- **Revente des informations exfiltrées à partir des dossiers médicaux des patients à d'autres organismes du secteur qui peuvent les exploiter.**

Chaque professionnel de santé doit être **sûr à 100 % de sa sécurité** car les **logiciels connectés sont des portes d'entrée pour les pirates informatiques.**

Il est important de **former le personnel** car les négligences humaines sont le **plus souvent à l'origine des failles de sécurité.**

Les établissements de santé et les entreprises du secteur médical sont des proies faciles car leurs investissements en matière de sécurité informatique restent encore insuffisants pour les mettre hors d'atteinte.

Les professionnels de santé vont devoir mettre en place une véritable politique de protection de données (plan de continuité d'activité et de reprise d'activité en cas de cyber-attaque), mais aussi s'assurer que ces solutions répondent aux risques potentiellement encourus.

Ils vont devoir s'entourer d'experts en cas de suspicion de cyber-attaque afin de permettre d'évaluer correctement l'impact et les conséquences.

Nos Services

Un service d'assistance et de gestion de crise 24h/7j

- **Un coordinateur de crise spécialisé en cybercriminalité**
- **Des prestations sélectionnées selon les cas de cyber attaque qui font le relais afin de gérer la problématique :**
  - **Expertise informatique** : désignation d'un expert pour enquêter et mesurer l'étendue d'une violation et pour éviter un futur incident
  - **Frais légaux** : frais de consultation d'avocat ou de conseil juridique
  - **Veille internet** : surveillance internet sur l'utilisation de données suspectées volée
  - **Notification et assistance téléphonique :** notification d'une atteinte à la réputation des données personnelles dérobées et mise à disposition d'une assistance téléphonique

Des garanties d'assurance pour préserver la continuité de l'activité

- **Responsabilité civile**
- **Responsabilité liée au contenu d'un site internet**
- **Enquêtes administratives :** frais de défense lorsque l'enquête est menée par la CNIL
- **Pénalités PCI-DSS :** en cas de violation des Normes de Sécurité PCI-DSS (Payment Card Industry Data Security Standard, standard de sécurité des données pour l'industrie des cartes de paiement)
- **Relations Publiques :** frais de communication nécessaires suite à l'atteinte à l'image
- **Cyber extorsion :** paiement sous contrainte
- **Frais de reconstitution des données :** atteinte ou incapacités à accéder à une donnée protégée
- **Perte d'exploitation :** au cours de la période d'interruption et pour une durée de 60 jours

Notre Solution

MEDIRISQ vous propose un contrat d'assurance adapté aux Professionnels de santé pour répondre à vos nouvelles obligations professionnelles et faire face à la cybercriminalité

Une souscription simplifiée :

Il suffit de nous retourner le formulaire joint après avoir parfaitement répondu à toutes les questions, à MEDIRISQ - 11 place Victor Hugo - CS 10630 - 38000 GRENOBLE - Cedex 1

Février 2018,

Nos conseils

- Utilisez systématiquement des pare-feux et des antivirus pour vos ordinateurs fixes et mobiles
- Séparez les usages personnels des usages professionnels
- Attention à l'escroquerie aux faux RIB
- Ne cliquez pas sur une pièce jointe ou un lien si vous ne connaissez pas l'émetteur
- Sauvegardez vos données sur un disque dur externe et conservez le dans un autre lieu
- Utilisez 2 disques durs externes, un pour les jours pairs et un pour les jours impairs
- Effectuez régulièrement des restaurations de vos disques durs afin de vérifier l'état des sauvegardes
- Mettez à jour régulièrement vos logiciels sur des sites officiels
- Cryptez toutes vos données sensibles
- Utilisez des mots de passe avec de nombreux caractères variés
(Majuscule, minuscule, chiffre, caractères spéciaux)
ex : GhT10càrMDQ38 (J'AI ACHETÉ 10 CYBER RISQUES A MÉDIRISQ 38)
- Ne conservez aucune liste de codes secrets sur votre ordinateur ou smartphone
- Formez votre personnel
- Cryptez toutes vos données sensibles
- Retirez, protégez et rangez votre carte CPS sans votre code personnel
- N'utilisez aucun wifi public (gare, hôtel, aéroport)
- Utilisez les services d'un expert informatique
- Contactez MEDIRISQ et assurez-vous !

Proposition d'assurance Cyber Risques

Offre dédiée aux PROFESSIONNELS DE SANTE

Contrat cyber risques proposé par MEDIRISQ, sis 11 place Victor Hugo – 38000 Grenoble, SAS au capital de 10 000 € - RCS Grenoble 531317030 – Code APE 6622Z – www.orias.fr – N° 11 061 847
Contrat souscrit auprès de la Compagnie Axeria iard sis 27 rue Maurice Flandin - CS 53713 - 69444 LYON CEDEX 03, S.A. au capital de 38 000 000 € - RCS Lyon 352 893 200 - N° Siret 352 893 200 00027 - Entreprise régie par le Code des Assurances Autorité de Contrôle Prudentiel et de Résolution – 61, Rue Taitbout – 75436 PARIS Cedex 09.