*Le présent questionnaire a pour but de permettre une étude préliminaire de tarification sans engagement ni de l'Etablissement, ni de l’Assureur. L'assurance ne peut être accordée qu'après accord formel des parties sur les conditions de garanties, de tarif et de franchises.*

**l’établissement : Activités et données**

**Etablissement**

Etablissement : Centre Hospitalier de Sens

Adresse : 1, avenue Pierre de Coubertin

Code postal : 89100 Commune : Sens

Téléphone : 03 86 86 15 15 E-mail : [dsi@ch-sens.fr](mailto:dsi@ch-sens.fr), [rssi@ch-sens.fr](mailto:rssi@ch-sens.fr) , [dpo@ght-nordyonne.fr](mailto:dpo@ght-nordyonne.fr)

Numéro FINESS : 890970569 Numéro SIRET : 268 900 230 00015

**Activités**

Selon les critères applicables de l’activité :

Montant EPRD principal et annexes / ~~Budget principal et annexes / Chiffre d’affaires~~\* (dernier chiffre connu) : 150 335 594€ *\* rayer les mentions inutiles*

Suivant la nature de vos activités :

Nombre cumulé annuel\* de séjours, journées et séances (dernier chiffre connu) :

séjours (RSS) : 32 638 ; journées PMSI : 95 399 dont 13 476 séances

Nombre de lits (équivalent) : 771 Nombre de places : 53

Nombre\* de consultations, d’analyses, de diagnostic ou d’interventions :

consultations : 38841 ; interventions : 7132

Faites-vous partie d’un GHT : Non Oui comme « support » Oui comme « membre »

Faites-vous partie d’un GCS : Non Oui

Faites-vous partie d’un groupe d’établissements privés interconnectés informatiquement : Non Oui

**Données**

Nombre de collaborateurs : 1484 , et nombre de préposés utilisateurs du SI  : 1484

Proportion d'employés permanents vs temporaires Tous Beaucoup Peu

Ratio de turnover du personnel Faible Moyen Elevé

Natures des données sensibles

Données administratives : état civil, coordonnées, …

Données de santé

Données bancaires

Autres données à caractère personnel : précisez

Données relatives à la propriété intellectuelle (exemple : essais cliniques, recherches impliquant la personne humaine)

Vos données sont-elles hébergées chez un tiers hébergeur OUI NON

Si oui, est-il certifié Hébergeur de Donnée de Santé OUI NON

Nom du (ou des) hébergeurs : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pouvez-vous fournir le registre RGPD de vos traitements OUI NON

Nombre d'individus distincts ayant été admis dans votre établissement au cours des 28 dernières années (selon votre meilleure estimation) : 290 000

Effectuez-vous des prestations informatiques pour le compte de Tiers (notamment Hébergement ou exploitation) ? OUI NON

Si oui, précisez leur nature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Les mesures de sécurité mises en place**

|  |  |  |
| --- | --- | --- |
|  | **ORGANISATION DE LA SECURITE** |  |
| A.05.1.1 | Avez-vous élaboré et mis en œuvre une politique de sécurité de l’information formelle, applicable à l’ensemble de l’organisation et disponible en permanence à tous les employés et les prestataires externes concernés? | OUI NON |
| A.06.1.1 | Avez-vous désigné une personne responsable de la sécurité de l'information (par exemple, le « RSSI » Responsable de la Sécurité des Systèmes d’Information)? | OUI NON |
| A.18.1.4 | Avez-vous désigné une personne responsable de la protection des données à caractère personnel (Un « DPO » Data Protection Officer)? | OUI NON |
| A.06.1.3 | Avez-vous une liste à jour des autorités et des contacts externes à informer en cas d’incident de sécurité informatique? | OUI NON |
|  | Avez-vous engagé un programme de réduction des risques technologiques | NON  OUI (informel)  OUI (formel) |

|  |  |  |
| --- | --- | --- |
|  | **SECURITE DES RESSOURCES HUMAINES** |  |
| A.07.2.2 | Offrez-vous au moins une formation annuelle pour sensibiliser vos utilisateurs (employés et prestataires) à la sécurité et pour les préparer à être plus résilients et vigilants face au phishing ? | NON  aux internes uniquement  aux internes et prestataires |
|  | Les soignants sont-ils invités à déclarer des évènements indésirables lorsqu’ils sont causés par des problèmes techniques impliquant l’informatique | NON  OUI (sensibilité faible)  OUI (sensibilité forte) |
|  | Votre équipe informatique dispose-t-elle des compétences nécessaires pour opérer toutes les technologies présentes dans votre établissement (IT, OT, dispositifs médicaux) | NON  OUI (IT uniquement)  OUI (tout) |
|  | **CLASSIFICATION** |  |
| A.08.1.1 | Maintenez-vous à jour un inventaire complet (cartographie) des composantes du système d'information (matériels informatiques fixes et nomades, dispositifs médicaux connectés, applications métiers et logiciels (y compris OS)) ?  Nombre approximatif de postes de travail (1), serveurs (2), automates « OT » (3) et dispositifs médicaux (4) | OUI NON  (1) 900  (2) 300  (3) 150  (4) 500 |
| A.08.2.1 | Classifiez-vous les informations par rapport à leur confidentialité? | OUI NON |
| A.08.2.2 | Les procédures d'étiquetage des informations sont-elles mises en œuvre conformément au système de classification ci-dessus? | OUI NON |
| A.08.2.3 | Donnez-vous des conseils sur la manière de gérer les informations classifiées? | OUI NON |
| A.08.3.1 | Limitez-vous l'accès aux informations confidentielles stockées sur des supports amovibles tels que les périphériques de stockage externes (clés USB ou disques durs, par exemple), ou bien les cryptez-vous ? | OUI NON |
| A.08.3.2 | Détruisez-vous de manière sécurisée les supports contenant des informations sensibles s’ils ne sont plus utilisés? | OUI NON |
|  | **CONTROLE D’ACCES** |  |
| A.09.1.2 | Limitez-vous les privilèges des employés et des utilisateurs externes sous réserve du "besoin d'en connaître" (en particulier l'accès aux données sensibles, telles que les données personnelles et de santé)? | NON  OUI (internes uniquement)  OUI (internes et externes) |
| A.09.2.2 | Avez-vous mis en place un processus formel pour la gestion (attribution et révocation) des droits d’accès? | OUI NON |
| A.09.2.3 | Interdisez-vous les droits d'administrateur local sur les postes de travail pour les utilisateurs ? | OUI NON |
| A.09.2.5 | Révisez-vous les droits d'accès des utilisateurs au moins une fois par an ? | OUI NON |
| A.09.2.6 | Révoquez-vous tous les accès systèmes, les comptes et les droits associés après la cessation d'emploi des utilisateurs (y compris les employés, les employés temporaires, les entrepreneurs ou les fournisseurs) ? | OUI NON |
| A.09.4.3 | Avez-vous mis en place une politique de mots de passe imposant l'utilisation de mots de passe longs et complexes dans votre organisation ? (Les mots de passe longs et complexes sont définis comme étant : huit caractères ou plus ; ne comprenant pas de mots inclus dans les dictionnaires ; sans caractères consécutifs identiques, entièrement numériques ou entièrement alphabétiques). | OUI NON |
|  | A quelle fréquence les mots de passe des utilisateurs doivent-ils impérativement être changés? (Si > à 90 jours merci de préciser la fréquence) : 1 an | <90jours >90jours |
|  | Encouragez-vous l’utilisation d’authentification double facteur (carte CPS, token matériel ou virtuel) | NON  OUI (parfois)  OUI (souvent) |
|  | Avez-vous un process de revue et analyse des « bris de glaces » | N/A  NON  OUI |
|  | Gardez-vous à disposition un ensemble d’identifiants génériques « de proximité » utilisés lorsque du personnel nouveau arrive (ex : nouveaux praticiens ou internes) | N/A  NON  OUI |
|  | Les mots de passe par défaut sont-ils changés avant mise en production des systèmes technologiques (IT, OT, dispositifs médicaux) | NON  OUI (IT uniquement)  OUI (toutes technologies) |
|  | Avez-vous implémenté la traçabilité des accès et actions effectuées sur les systèmes (à minima connexion/déconnexion nominatives) | NON  OUI (éclaté)  OUI (centralisé)  OUI (centralisé et protégé) |
|  | Avez-vous mis en place des moyens mécaniques ou de protection physiques de protection contre le vol d’équipements pour l’ensemble du parc (IT, OT, dispositifs médicaux) | N/A  NON  OUI (IT uniquement)  OUI (partout) |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | **CHIFFREMENT** |  |
| A.10.1.1 | Toutes les informations confidentielles stockées sur les appareils mobiles (p. ex. téléphones intelligents et ordinateurs portables) sont-elles chiffrées ? | NON  OUI (portables uniquement)  OUI (tous dispositifs) |
|  | Autorisez-vous vos employés à utiliser leur ordinateur personnel pour effectuer certaines de leurs missions (BYOD) | N/A  NON  OUI (parfois)  OUI (souvent) |
|  | Autorisez-vous vos employés à effectuer certaines de leurs missions depuis leur domicile | N/A  NON  OUI (parfois)  OUI (souvent) |
| A.10.1.2 | Avez-vous développé et mis en place une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques et des certificats? | OUI NON |
|  | **SECURITE DES OPERATIONS** |  |
| A.11.1.2 | Tenez-vous une liste du personnel (employés, fournisseurs et visiteurs) ayant un accès autorisé à vos locaux et aux zones de sécurité sensibles ? | OUI NON |
| A.12.1.2 | Avez-vous mis en place des procédures de gestion du changement pour les systèmes critiques? | OUI NON |
| A.12.1.4 | L'environnement informatique pour le développement et les tests est-il séparé de l'environnement informatique de production? | OUI NON |
| A.12.2.1 | Utilisez-vous une protection contre les logiciels malveillants pour tous les postes de travail et ordinateurs portables, passerelles de messagerie, proxies Web, et sont-ils mis à jour automatiquement ? | NON  OUI (postes de travail uniquement)  OUI (tous équipements) |
|  | Utilisez-vous une protection contre les intrusions (« EDR ») pour les postes de travail et serveurs | NON  OUI (postes de travail uniquement)  OUI (serveurs uniquement)  OUI (tous équipements) |
|  | Les réseaux sans fil couvrent-ils tous les bâtiments | NON  OUI (bâtiments médicaux)  OUI (partout) |
| A.12.3.1 | Effectuez-vous des sauvegardes régulières au moins hebdomadaires des données critiques de l’établissement | OUI NON |
|  | Certaines données critiques ne sont-elles pas sauvegardées de façon au moins hebdomadaire ?  Identifiez les le cas échéant : \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Aucune  Certaines, identifiées |
|  | Assurez-vous un export et une conservation qui garantisse que les sauvegardes ne seront pas compromises par un même événement physique ou logique que les données critiques ?  Quotidiens  Hebdomadaires  Mensuels  Moins d’une fois par mois ou jamais  Identifiez la méthode : \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| A.12.4.1 | Produisez-vous et consultez-vous régulièrement des journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les erreurs et les événements liés à la sécurité de l'information (au moins pour vos pare-feu et votre contrôleur de domaine)? | OUI NON |
| A.12.5.1 | Avez-vous mis en place un processus centralisé d'installation de logiciels? | OUI NON |
| A.12.6.1 | Appliquez-vous les mises à jour et correctifs de sécurité aux systèmes et applications informatiques critiques dans un délai d'au plus 1 mois après leur publication ? | OUI NON |
|  | Appliquez-vous les mises à jour et correctifs de sécurité aux systèmes et applications informatiques non critiques dans un délai d'au plus 3 mois après leur publication ? | OUI NON |
|  | Par qui sont effectuées les opérations de maintenance concernant les équipements « OT » et les dispositifs médicaux | Personne  les fabricants  prestataire tiers  service interne |
| A.12.6.2 | Par qui sont effectuées les opérations de maintenance concernant votre autocommutateur téléphonique (PABX) | Personne  les fabricants  prestataire tiers  service interne |
| A.13.1.1 | Recevez-vous des bulletins d’information concernant les problématiques de sécurité de vos technologies « OT » et dispositifs médicaux | OUI NON |
| A.13.1.2 | Surveillez-vous votre réseau et identifiez-vous les événements de sécurité? | OUI NON |
| A.13.1.3 | Des systèmes reliés à Internet (p. ex. serveurs Web et messagerie) sont-ils autorisés à initier du trafic vers votre réseau de confiance (même via zone démilitarisée (DMZ) ou depuis un fournisseur tiers)? | OUI NON |
| A.13.2.3 | Cryptez-vous les communications confidentielles (par exemple les e-mails sécurisés avec SMIME (Secure Multipurpose Internet Mail Extensions) ou SMTP-over-TLS (Simple Mail Transfer Protocol Secure)) ? | OUI NON |
| A.14.1.2 | Votre serveur Web crypte-t-il les données confidentielles (p. ex. HTTPS) ? | OUI NON |
|  | *NA si pas de serveur web* |  |

|  |  |  |
| --- | --- | --- |
| A.14.2.8 | Testez-vous les fonctionnalités de sécurité au cours du cycle de développement des systèmes d’information, y compris mises à jour de sécurité informatique ? | OUI NON |
| A.14.3.1 | Tenez-vous compte d'exigences de confidentialité lorsque vous utilisez des données opérationnelles pour des tests en vous assurant que tous les détails sensibles sont protégés par leur suppression ou substitution? | NON  OUI (données anonymisées)  OUI (données protégées) |
|  | **GESTION DES FOURNISSEURS** |  |
| A.15.1.1 | Avez-vous identifié et documenté tous vos fournisseurs importants (y compris les fournisseurs de services tiers)? | OUI NON |
| A.15.1.2 | Les accords avec des fournisseurs de services tiers exigent-ils un niveau de sécurité correspondant à votre propre norme de sécurité de l'information? | OUI NON |
| A.15.2.1 | Surveillez-vous les activités des fournisseurs de services tiers à la recherche d’événements de sécurité afin de maintenir un niveau de sécurité des informations convenu? | OUI NON |
|  | Les accords avec les fournisseurs de services « SaaS » exigent-ils un niveau de sécurité correspondant à votre propre norme de sécurité de l'information? | OUI NON |
|  | Les accords avec les fournisseurs de services Cloud exigent-ils un niveau de sécurité correspondant à votre propre norme de sécurité de l'information? | OUI NON |
| A.16.1.1 | Etes-vous interconnectés avec des fournisseurs tiers dans le cadre du déploiement du « Dossier Médical Partagé » ou similaire | OUI NON |
| A.16.1.2 | Tous vos employés et fournisseurs tiers connaissent-ils la ligne de compte rendu des événements liés à la sécurité des informations? | OUI NON |
| A.16.1.3 | Les employés et les sous-traitants sont-ils tenus de signaler toute faille identifiée en matière de sécurité de l'information (pas encore un incident ou un événement) dans les systèmes ou les services? | OUI NON |
| A.16.1.5 | Avez-vous établi une procédure d'escalade pour les incidents de sécurité de l'information ? | OUI NON |
| A.16.1.6 | Utilisez-vous les connaissances acquises lors de l'analyse et de la résolution d'incidents de sécurité de l'information pour réduire la probabilité ou l'impact d'impacts futurs? | OUI NON |
|  | Etes-vous interconnecté avec des établissements tiers dans le cadre d’activités de télémédecine ou similaire | OUI NON |
|  | Etes-vous interconnecté avec des établissements tiers dans le cadre d’activités médicales partagées (radiologie, pharmacie, …) ou similaire | OUI NON |
| A.17.1.1 | Avez-vous effectué une analyse d'impact sur l’activité de l’établissement (Bilan d’Impact sur l’Activité - BIA)? | OUI NON |
| A.17.1.2 | Avez-vous mis en place un dispositif de gestion de la continuité des activités (Plan de Secours Informatique (PSI) et d’un Plan de Continuité d'Activité (PCA)) qui traite spécifiquement des cyber incidents? | OUI NON |
|  | Mettez-vous à jour vos PSI et PCA au moins une fois par an? | OUI NON |
| A.17.1.3 | Testez-vous vos PSI et PCA au moins une fois par an? | OUI NON |
| A.17.2.1 | Vos installations de traitement de l'information (c.-à-d. tout système, service ou infrastructure, ou emplacement physique qui les abrite) sont-elles mises en œuvre de façon redondante ? | OUI NON |
|  | Disposez-vous d’une équipe dédiée à la réponse sur incidents de sécurité | NON  OUI (HO)  OUI (astreinte)  OUI (24/7) |
|  | **GESTION DE LA CONFORMITE** |  |
| A.18.1.1 | Avez-vous mis en place une procédure pour vous conformer en permanence à toutes les exigences légales, réglementaires et contractuelles pertinentes en matière de protection de la vie privée? | OUI NON |
| A.18.1.3 | Avez-vous publié des directives sur la conservation, le stockage, la manipulation et la destruction de documents et d'informations? | OUI NON |
| A.18.2.3 | Analysez-vous régulièrement les systèmes critiques (y compris par tests d'intrusion ou par évaluations de vulnérabilités) - soit par vous-même, soit par un tiers - en particulier à chaque fois que de nouveaux systèmes sont introduits et à la suite de changements ? | OUI NON |
|  | Les recommandations issues du dernier rapport d’audit :  Ont été mises en œuvre intégralement (recommandations critiques traitées en priorité)  Sont partiellement mises en œuvre (recommandations critiques traitées exclusivement)  Ne sont pas mises en œuvre |  |

**Antériorités**

|  |  |  |
| --- | --- | --- |
|  | **Antécédents d’assurance** |  |
|  | L’établissement a-t-il été titulaire d’un contrat comportant l’une ou l’autre des garanties demandées ? | OUI NON |
|  | Si oui, ce contrat comportant l’une ou l’autre des garanties demandées a-t-il fait l’objet d’une résiliation ou d’un non renouvellement par l’assureur ? | OUI NON |
|  | Si oui, indiquer le motif exact, le nom de la Société, le numéro de contrat : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  | **Historique des incidents de sécurité** |  |
|  | Au cours des trois dernières années, avez-vous été confronté à un incident de cybersécurité significatif (violation de la sécurité informatique, corruption du système ou perte de données, frais de notification) ? | Jamais  Tous les ans Tous les mois  Tous les jours |
|  | Si oui, précisez la nature de l’incident : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  | Et ses conséquences financières : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  | Au cours des trois dernières années, avez-vous fait l’objet d’une violation de données à caractère personnel ayant entrainé une notification aux personnes concernées ? | OUI NON |
|  | Si oui, indiquer le nombre de réclamations associées : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  | et leurs conséquences financières (coût de la notification et de l’indemnisation du préjudice) : \_\_\_\_\_\_\_\_\_\_\_\_ |  |

|  |  |
| --- | --- |
| Au cours des trois dernières années, avez-vous été confronté à une perturbation des activités de soins consécutive à un problème informatique (pannes, bugs, lenteurs) que les utilisateurs ont pu résoudre? | Jamais  Tous les ans  Tous les mois  Tous les jours |
| Au cours des trois dernières années, avez-vous été confronté à une perturbation des activités de soins consécutive à un problème informatique (pannes, bugs, lenteurs) nécessitant une intervention du service informatique ? | Jamais  Tous les ans  Tous les mois  Tous les jours |