

# Contrat relatif à la sécurité des services numériques et à la protection des données du Centre Hospitalier Régional METZ-THIONVILLE

Contrat n° **DSN-2025-XXX**

Diffusion limitée : DG, DTPBMES, DAGJQ, DALH, DSN, Prestataires

## ENTRE

### Le Centre Hospitalier Régional de Metz-Thionville

Établissement public de santé

Dont le siège est 1, Allée du Château, CS45001, 57085 METZ CEDEX 03

Représenté par son Directeur Général, Monsieur Dominique PELJAK, dûment habilité à cet effet

*Ci-après le « CHR »*

## ET

**NOM**

**ADRESSE DU SOUS-TRAITANT**

Représenté par ..... dûment habilitée à cet effet

*Ci-après le « prestataire »*

Le prestataire et le CHR sont collectivement désignés les « Parties ».

**ONT CONVENU ENSEMBLE DE CE QUI SUIT :**

## Table des matières

### CONTRAT

TITRE I – LES CLAUSES DU CONTRAT .....	3
Clause 1 - Objet et champ d'application.....	3
Clause 2 - Invariabilité des clauses .....	5
Clause 3 - Interprétation .....	5
Clause 4 - Hiérarchie .....	5
TITRE II - OBLIGATIONS DES PARTIES .....	5
Clause 6 - Description du ou des traitements.....	5
Clause 7 - Obligations des parties.....	5
Clause 8 - Assistance au CHR .....	7
Clause 9 - Notification de violations de données à caractère personnel.....	8
TITRE III - DISPOSITIONS FINALES .....	9
Clause 10 - Non-respect des clauses et résiliation .....	9
TITRE IV - CONFORMITES.....	10
ANNEXE I - Plan d'Assurance Sécurité – PAS .....	11
ANNEXE II - RGPD .....	23
ANNEXE III - Réversibilité des données .....	32

# TITRE I – LES CLAUSES DU CONTRAT

## Clause 1 - Objet et champ d'application

Les cases sont à cocher/décocher et/ou à compléter selon le périmètre de la prestation.

a) Les services numériques concernés par le présent contrat sont les suivants :

Nom du service numérique	Description
À renseigner	À renseigner
...	

Ce contrat s'applique à l'ensemble des services numériques, d'un même domaine, pour lesquels le prestataire s'engage sur des mesures identiques pour, par exemple :

- différents modules d'une même solution (dossier patient, ...)
- différents types d'équipements (parc d'échographes, ...)

*Dans le cas d'une modification ultérieure du périmètre avec les mêmes niveaux d'engagement, un avenant sera nécessaire.*

b) La durée du présent contrat qui lie le CHR au prestataire est la suivante :

<b>X</b>	Contrat valide pendant la durée du marché public Durée du marché : du xx/xx/xxxx au xx/xx/xxxx
	Contrat valide pendant la durée de la prestation Durée de la prestation : du xx/xx/xxxx au xx/xx/xxxx
	Autre : à préciser

c) La prestation couverte par le présent contrat est la suivante :

<b>X</b>	Prestation de service pouvant nécessiter l'accès ponctuel à des données soumises au secret professionnel du CHR
	Prestation de service nécessitant l'accès fréquent et systématique à des données soumises au secret professionnel et aux services numériques du CHR
	Hébergement et maintenance de progiciel(s) stockant des données soumises au secret professionnel
	Prestation de conseil ou d'assistance (forfaitaire) visant à traiter des données soumises au secret professionnel pour le compte et sur instruction du CHR

	Mise à disposition de personnels en régie qui pourraient être amené à traiter des données soumises au secret professionnel et accéder aux services numériques pour le compte et sur instruction du CHR
	Autre : à préciser

d) Les missions confiées au sous-traitant pendant la durée du contrat sont les suivantes :

X	Installation de la solution
X	Maintenance corrective et évolutive
X	Gestion des configurations et des correctifs
X	Gestion des incidents techniques
X	Gestion du support utilisateur
X	Formation des utilisateurs
	Gestion des habilitations
	Gestion des enregistrements et des traces informatiques
	Développement sur mesure
	Hébergement des données sur une application en mode SAAS
	Sauvegarde des données
	Renforcement des équipes métiers
	Analyse des données à des fins statistiques
	Autre : à préciser

e) Les présentes clauses contractuelles (ci-après les « clauses ») doivent garantir :

e.1) la conformité avec l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

e.2) la conformité avec l'article 2.II du décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel.

f) Les parties ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016 et de l'article 2.II du décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel.

g) Les annexes I à III font partie intégrante des clauses.

h) Les présentes clauses sont sans préjudice des obligations auxquelles le CHR est soumis en vertu du règlement (UE) 2016/679 et d'autres réglementations en vigueur.

i) Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679.

## **Clause 2 - Invariabilité des clauses**

a) Les parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent.

b) Les parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

## **Clause 3 - Interprétation**

a) Lorsque des termes définis dans le règlement (UE) 2016/679 figurent dans les clauses, ils s'entendent comme dans le règlement en question. Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.

b) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations qui incombent au CHR ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

## **Clause 4 - Hiérarchie**

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

# **TITRE II - OBLIGATIONS DES PARTIES**

## **Clause 6 - Description du ou des traitements**

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du CHR, sont précisés à l'annexe II.

## **Clause 7 - Obligations des parties**

### **7.1 Instructions**

a) Le prestataire ne traite les données soumises au secret professionnel et n'intervient sur les services numériques que sur instruction documentée du CHR, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le prestataire informe le CHR de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le CHR pendant toute la durée de la prestation. Ces instructions doivent toujours être documentées.

b) Le prestataire informe immédiatement le CHR si, selon lui, une instruction donnée par le CHR constitue une violation du règlement (UE) 2016/679 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

## 7.2 Limitation de la finalité

Le prestataire traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement et les missions, telles que définies à l'annexe II, sauf instruction complémentaire du CHR.

## 7.3 Durée du traitement des données à caractère personnel

Le traitement par le prestataire n'a lieu que pendant la durée précisée à l'annexe II.

## 7.4 Sécurité des données et des services numériques

a) Le prestataire s'engage à mettre au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe I pour assurer la sécurité des données soumises au secret professionnel et des services numériques du CHR. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données soumises au secret professionnel ou l'accès non autorisé à de telles données (violation de données soumises au secret professionnel). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.

b) Le prestataire n'accorde aux membres de son personnel l'accès aux données soumises au secret professionnel et aux services numériques du CHR que dans la mesure strictement nécessaire à l'exécution de la prestation. Le prestataire veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

## 7.5 Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le prestataire applique des limitations spécifiques et/ou des garanties supplémentaires.

## 7.6 Documentation et conformité

- a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.
- b) Le prestataire traite de manière rapide et adéquate les demandes du CHR concernant le traitement des données conformément aux présentes clauses.
- c) Le prestataire met à la disposition du CHR toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679. À la demande du CHR, le prestataire permet également la réalisation d'audits dans la limite d'une fois par an et sous réserve du respect par le CHR d'un délai de préavis de trente jours (30) ouvrés, notifié par lettre recommandée avec accusé de réception, des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le CHR peut tenir compte des certifications pertinentes en possession du prestataire.
- d) Le CHR peut décider, et à ses frais, de procéder lui-même à l'audit ou de mandater un auditeur indépendant non concurrent du prestataire et ayant préalablement signé un accord de confidentialité avec le prestataire. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du prestataire dans la limite de 2 jours ouvrés et sont, le cas échéant, effectués moyennant un préavis

raisonnable. Au-delà de 2 jours l'audit sur place, le prestataire se réserve le droit de facturer ces inspections dans ses locaux.

- e) Les parties mettent à la disposition de(s) l'autorité(s) de contrôle compétente(s), dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

## **7.7 Recours à des sous-traitants ultérieurs**

- a) **La liste des sous-traitants ultérieurs autorisés par le CHR figure à l'annexe II pour l'ensemble du contrat.**
- b) Le prestataire n'est pas autorisé à sous-traiter à un sous- traitant ultérieur les opérations de traitement qu'il effectue pour le compte du CHR en vertu des présentes clauses sans l'information écrite spécifique préalable du CHR par voie d'avenant au contrat. Le prestataire soumet la demande d'information spécifique au moins 1 mois avant le recrutement du sous-traitant ultérieur en question.
- c) Lorsque le prestataire recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du CHR), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au prestataire en vertu des présentes clauses. Le prestataire veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679.
- d) À la demande du CHR, le prestataire lui fournit une copie de ce contrat conclu avec le sous- traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous- traitant peut expurger le texte du contrat avant d'en diffuser une copie.
- e) Le prestataire demeure pleinement responsable, à l'égard du CHR, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le prestataire informe le CHR de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
- f) Le prestataire convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le prestataire a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le CHR a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur de renvoyer les données à caractère personnel et de les effacer.

## **7.8 Transferts internationaux**

- a) Tout transfert de données vers un pays tiers ou une organisation internationale par le prestataire n'est effectué que sur la base d'instructions documentées du CHR ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le prestataire est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679.
- b) Le CHR convient que lorsque le prestataire recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du CHR) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le prestataire et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

## **Clause 8 - Assistance au CHR**

- a) Le prestataire informe sans délai le CHR de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le CHR ne l'y ait autorisé.

b) Le prestataire prête assistance au CHR pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations, le prestataire se conforme aux instructions du CHR.

c) Outre l'obligation incombant au prestataire d'assister le CHR en vertu de la clause 8b, le prestataire aide en outre le CHR à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le prestataire :

1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d'impact relative à la protection des données ») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ;

2) l'obligation de consulter l(es) autorité(s) de contrôle compétente(s) préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le CHR ne prenait pas de mesures pour atténuer le risque ;

3) l'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le CHR si le prestataire apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes ;

4) les obligations prévues à l'article 32 du règlement (UE) 2016/679.

d) Les parties définissent à l'annexe I les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au CHR dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

## **Clause 9 - Notification de violations de données à caractère personnel**

En cas de violation de données à caractère personnel, le prestataire coopère avec le CHR et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679, en tenant compte de la nature du traitement et des informations dont dispose le prestataire.

### **9.1 Violation de données en rapport avec des données traitées par le CHR**

En cas de violation de données à caractère personnel en rapport avec des données traitées par le CHR, le prestataire prête assistance au CHR :

a) aux fins de la notification de la violation de données à caractère personnel à l(es) autorité(s) de contrôle compétente(s), dans les meilleurs délais après que le CHR en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques) ;

b) aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du CHR, et inclure, au moins :

1. la nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
2. les conséquences probables de la violation de données à caractère personnel ;
3. les mesures prises ou les mesures que le CHR propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais ;



c) aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

## **9.2 Violation de données en rapport avec des données traitées par le prestataire**

En cas de violation de données à caractère personnel en rapport avec des données traitées par le prestataire, celui-ci en informe le CHR dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

- a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;
- b) les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
- c) ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les parties définissent à l'annexe II tous les autres éléments que le prestataire doit communiquer lorsqu'il prête assistance au CHR aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679.

## **TITRE III - DISPOSITIONS FINALES**

### **Clause 10 - Non-respect des clauses et résiliation**

a) Sans préjudice des dispositions du règlement (UE) 2016/679, en cas de manquement du prestataire aux obligations qui lui incombent en vertu des présentes clauses, le CHR peut donner instruction au prestataire de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le prestataire informe rapidement le CHR s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

b) Le CHR est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

- 1) le traitement de données à caractère personnel par le prestataire a été suspendu par le CHR conformément au point a) et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
- 2) le prestataire est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 ;
- 3) le prestataire ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l(es) autorité(s) de contrôle compétente(s) concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679.

c) Le prestataire est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le CHR que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le CHR insiste pour que ses instructions soient suivies.

d) À la suite de la résiliation du contrat, le prestataire supprime, selon le choix du CHR, toutes les données à caractère personnel traitées pour le compte du CHR et certifie auprès de celui-ci qu'il a procédé à cette

suppression, ou renvoie toutes les données à caractère personnel au CHR et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps.

Le prestataire continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données. L'annexe III précise les engagements des parties en matière de réversibilité.

## **TITRE IV - CONFORMITES**

Les exigences du CHR METZ-THIONVILLE en termes de sécurité et de protection de données sont exposées dans les annexes de ce contrat :

- ANNEXE I : Plan d'Assurance Sécurité – **43 engagements** à compléter
- ANNEXE II : Clauses RGPD – Clauses types à renseigner et **10 engagements** de vérification de conformité
- ANNEXE III : Réversibilité des données – **9 engagements**

**Les annexes I à III font partie intégrante des clauses du présent contrat.**

Fait à METZ,

Le ...../...../ .....

En deux exemplaires originaux, pour être remis à chacune des Parties.

Avis favorable du RSSI / DPO du CHR Albert CRUMBACH	
--	--

Pour le CHR	Pour le prestataire
Pour le Directeur Général et par délégation, Mickael CHOPLIN, Directeur des Services Numériques.  Signature	Son Directeur Général  .....  Signature

## ANNEXE I - Plan d'Assurance Sécurité – PAS

Le prestataire doit **cocher les cases correspondantes et préciser si nécessaire** afin de s'engager **sur 43 mesures de sécurité** en fonction du périmètre du service concerné. :

- 23 **Mesures communes pour tous les services numériques** dont 13 prérequis obligatoires
- 18 **Mesures pour les solutions hébergées dans le Datacenter du CHR ('On-Premise')** dont 6 prérequis obligatoires
- 2 **Mesures pour les solutions dont l'hébergement est externalisé ('Cloud')** obligatoires

Les mesures de sécurité définies dans le présent article sont conformes aux recommandations et aux bonnes pratiques énoncées par les autorités compétentes (ANSSI, CNIL, ANS, etc.) et aux exigences des référentiels ISO 27001:2022 et HDS v2

Ces mesures visent à garantir un niveau de sécurité adapté au risque, et prévoient :

- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

### **Coordonnées de l'Ingénieur Sécurité SI du CHR**

Nom et coordonnées	Cyril PIERRÉ Ingénieur Sécurité Risques Numériques <a href="mailto:dsn.securite@chr-metz-thionville.fr">dsn.securite@chr-metz-thionville.fr</a> 03 87 55 77 94
--------------------	---

### **Coordonnées du référent Sécurité SI / juridique du prestataire**

Nom, fonction et coordonnées	
------------------------------	--

**Important :** Sont considérés comme 'intervenant' toutes les personnes susceptibles de se connecter à distance ou sur le site du client dans le périmètre du présent contrat.

## Mesures communes pour tous les services numériques

### Prérequis obligatoires

#### **ENG1 - Notification d'un abaissement de la sécurité**

Le prestataire s'engage à notifier sans délai au CHR tout changement susceptible d'entraîner une diminution du niveau de sécurité. Cette notification devra inclure des informations précises sur la nature du changement, sa finalité, sa date de mise en œuvre, ainsi que les mesures correctives envisagées ou déjà appliquées.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG2 - Obligation de confidentialité**

Le prestataire s'engage à fournir au CHR, sur demande, les documents démontrant que ses intervenants sont soumis au secret professionnel ou à une obligation de confidentialité.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG3 - Information des intervenants**

Le prestataire s'engage à informer ses intervenants de l'obligation de respecter la « Charte d'utilisation des services numériques pour les prestataires du CHR METZ-THIONVILLE » sur site ou à distance. Il s'engage à fournir, sur demande, les éléments démontrant que cette information a été effectuée avant le début de la prestation.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG4 - Sensibilisation à la sécurité**

Le prestataire s'engage à faire suivre à ses intervenants une session de sensibilisation à la sécurité rappelant les exigences sécurité de la prestation et les bonnes pratiques de sécurité.

**Le prestataire doit fournir une liste des sensibilisations récentes effectuées auprès de ses intervenants en annexe à ce document.** Une mise à jour de ce document pourra être demandée par le CHR.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG5 - Respect des règles de sécurité**

Le prestataire s'engage à veiller à ce que ses intervenants respectent les règles et les directives de sécurité physique dès lors que des interventions dans les locaux du client sont prévues.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

**ENG6 - Gestion des correctifs**

Le prestataire s'engage à installer les dispositifs du service dans des versions stables et à jour de leurs correctifs de sécurité. Les versions installées doivent être des versions supportées.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

**ENG7 - Veille sécurité**

Le prestataire s'engage à fournir des correctifs de sécurité sur les vulnérabilités identifiées dans un délai de 14 jours pour les services exposés sur internet et 60 jours pour les autres.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

**ENG8 - Sécurité des échanges**

Le prestataire s'engage à chiffrer tous les échanges de documents sensibles avec le CHR en utilisant une solution de partage de fichiers professionnelle (Exemple : France Transfert, BluesFiles, NetExplorer, TransfertPro ...). Un lien de dépôt peut être fourni par l'interlocuteur CHR.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

**ENG9 - Gestion des comptes et des mots de passe**

Le prestataire s'engage à être conforme à la « Politique de gestion des comptes et des mots de passe » du CHR, à savoir :

- Mot de passe complexe de 15 caractères et de 3 critères différents minimum (parmi majuscule, minuscule, chiffre, caractère spécial)
- Ce mot de passe ne doit pas être utilisé chez un autre client
- Le mot de passe ne doit pas apparaître en clair (dans un fichier, script, URL, base de données, ...)

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

**ENG10 -Gestion des pertes ou des vols**

Le prestataire s'engage à prévenir sans délai le CHR en cas de vol d'un équipement de l'un de ses intervenants pouvant contenir des identifiants et mots de passe du CHR

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

**ENG11 -Signalement des évènements de sécurité**

Le prestataire s'engage à signaler au CHR sans délai tout événement ou incident pouvant avoir un impact sur la sécurité des données ou des services numériques du CHR, en précisant la nature de l'incident, les mesures immédiates prises pour contourner ou résoudre l'incident et le plan d'action proposé.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

### ENG12 - Droit de propriété intellectuelle

Le prestataire s'engage à fournir la liste exhaustive des licences nécessaires au CHR pour le bon fonctionnement de l'application (à l'exception des licences Oracle, Windows PC/serveurs et Office).

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle. Liste des licences nécessaires : ..... .....
	Non applicable pour le motif suivant : .....

### ENG13 -Documentation attendue

Le prestataire s'engage à fournir les éléments suivants :

- Modalités d'accès au support
- Guide d'utilisation de la solution
- Modèle de matrice des habilitations (par module : rôles et autorisations en lecture, modification, control total)
- Exclusions antivirus sur les postes clients
- Une liste des flux réseaux (Source, Destination, UDP, TCP, Direction, Description)

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage sur cette mesure, sauf pour le ou les point(s) suivant(s) en précisant la mesure alternative pour chacun : .....

## Clauses non-obligatoires mais recommandées :

### ENG14 -Politique de Sécurité :

Le prestataire dispose d'une politique de sécurité (PSSI) du SI qu'il met en œuvre dans le cadre de la prestation et qui pourra être consultée sur demande par le CHR.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### ENG15 -Navigateur Web

Dans le cas d'une application Web, le prestataire s'engage à ce qu'elle soit compatible avec le navigateur 'Microsoft Edge Chromium-based'

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle. Navigateur supporté : .....
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG16 -Chiffrement des flux**

Le prestataire s'engage à ce que tous les flux soient chiffrés en s'appuyant sur les dernières technologies en vigueur : HTTPS, SMTPS, SFTP, LDAPS avec signature, SMB avec signature, ...

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG17 -Protection des mots de passe**

Le prestataire s'engage à s'assurer que les mots de passe portés à la connaissance de son personnel ou de celui de ses prestataires sont stockés exclusivement dans un outil sécurisé de gestion des mots de passe.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG18 -Suppression des comptes génériques**

Le prestataire s'engage à ne pas utiliser de compte générique et à supprimer les comptes par défaut des systèmes, applications et outils d'administration nécessaires à la prestation.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG19 -Journalisation**

Le prestataire s'engage à ce que la solution proposée permette l'extraction des données de journalisation suivantes

- Horodatage des connexions et évaluation de durée
- Opérations réalisées dans l'application
- Attributions, modifications et révocation de droits des utilisateurs.
- Exécution automatique des scripts et tâches planifiées

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG20 -Durée de rétention des journaux**

Le prestataire s'engage à s'assurer que la durée de rétention des journaux soit de 1 an.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG21 -Validation d'un changement**

Le prestataire s'engage à ce que tout changement sur un service numérique fasse l'objet d'un plan de changement validé par la DSN incluant notamment les tests de non-régression et les méthodes de retour arrière en cas d'incident

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG22 -Continuité de service**

Le prestataire s'engage à décrire les mécanismes permettant d'assurer la continuité d'activité s'il s'agit d'un service numérique en haute disponibilité.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG23 -Mesures correctives**

Le prestataire s'engage à mettre en œuvre les mesures correctives identifiées lors d'un audit de sécurité dans les délais requis.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....



## Mesures concernant les services numériques hébergés sur l'infrastructure du CHR (solution on-premise)

### Prérequis obligatoires

#### **ENG24 -Durcissement de la sécurité**

Le prestataire s'engage à ne pas dégrader des mesures de sécurité en place (filtrage réseau, filtrage web, durcissement Windows, EDR, solution antivirus, ...)

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG25 -Annuaire des intervenants**

Le prestataire dispose d'un annuaire complet et récent de ses intervenants. Cet annuaire devra être remis au CHR sur demande.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG26 -Accès à Internet / WAN**

Le prestataire s'engage à ne pas installer de backdoor ou d'autres accès à Internet / WAN sur les équipements installés au CHR

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG27 -Bastion d'accès sécurisé (prérequis obligatoire)**

Le prestataire s'engage à accéder aux ressources administrées en utilisant la solution Bastion d'accès sécurisé du CHR, double authentification avec Microsoft AUTHENTICATOR, dès lors qu'une intervention sur les services numériques du CHR est nécessaire.

À noter que cette mesure est non obligatoire pour l'installation d'un équipement dans les services du CHR mais nécessaire pour toutes les autres interventions (sur site ou à distance).

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

### ENG28 -Base de données

Le prestataire indique le nom du SGBD et la version utilisée.

L'administration de la base et des sauvegardes seront à la charge du CHR pour PostgreSQL, Oracle et SQL Server.

Si un autre SGBD est utilisé, l'administration et la configuration de la base et des sauvegardes seront à la charge du prestataire

Deux Bases de données devront être opérationnelles : une Base de production et une Base de test-formation pour tester les nouvelles versions du logiciel et/ou permettre la formation des utilisateurs sans perturber l'activité.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle. SGBDR utilisé : ..... Version : .....
	Non applicable pour le motif suivant : .....

### ENG29 -Documentation attendue pour une installation On-Premise

Le prestataire s'engage à fournir les éléments suivants :

- Guide d'administration de la solution (installation, supervision, accès aux traces ...)
- Un synoptique de l'infrastructure / de la solution
- Un compte « super administrateur » à disposition de la DSN (OS, BDD, application ...)
- Exclusions antivirus sur les serveurs
- Éléments à superviser
- Une liste des éléments à sauvegarder

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage sur cette mesure, sauf pour le ou les point(s) suivant(s) en précisant la mesure alternative pour chacun : .....

## Clauses non-obligatoires mais recommandées :

### ENG30 -Départ d'un intervenant

Le prestataire s'engage à informer le CHR de tout départ d'un intervenant. Il veille à ce que l'intervenant concerné restitue l'ensemble des informations et des moyens qui lui ont permis d'effectuer sa mission sur les données et les services numériques du CHR.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative :.....
	Non applicable pour le motif suivant : .....

**ENG31 -Liaison avec l'Active Directory**

Le prestataire s'engage à interfacier sa solution et ses outils d'administration à l'annuaire centralisé (Active Directory) du CHR et à respecter les règles de cloisonnement entre compte administrateur et compte utilisateur.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG32 -Gestion des comptes de services**

Le prestataire s'engage à ne mettre en œuvre que des comptes de services permettant une rotation automatique via l'annuaire Active Directory du CHR (compte GMSA)

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG33 -Compte nominatif**

Le prestataire s'engage à fournir au CHR un compte d'administrateur nominatif individuel pour l'ensemble des composants de sa solution (application, serveur, base de données, équipement ...). En cas de départ de la personne concernée, son compte sera supprimé et un nouveau créé pour son remplaçant.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG34 -Limitation des outils et utilitaires**

Le prestataire s'engage à ne pas ajouter d'outils ou d'utilitaires sur les services numériques du CHR, sans accord tracé auprès de la Direction des Services Numériques du CHR, ceci afin de d'éviter d'introduire de nouveaux risques.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG35 -Interrogation des bases de données**

Le prestataire s'engage à fournir au CHR les éléments nécessaires à l'exploitation et à l'interrogation des données

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG36 -Système d'exploitation (Serveurs et clients)**

Le prestataire s'engage à ce que la solution proposée soit compatible avec la dernière version majeure de Windows client et serveur.

Si le prestataire fournit un équipement physique, il s'engage également à y installer la dernière version majeure de Windows.

Dans le cas d'utilisation d'une distribution Linux, le cycle de vie doit être d'au moins 3 ans à partir de la mise en œuvre de la solution.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG37 -Mise à jour du système d'exploitation**

Le prestataire s'engage à ce que la solution ou l'équipement proposé permette l'application des mises à jour mensuelles (Cumulative Update) sur les postes et serveurs concernés.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG38 - Citrix**

Le prestataire s'engage à ce que les applications proposées avec la solution soient déployées via les serveurs Citrix de l'établissement au lieu d'installations individuelles sur les postes de travail.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG39 -Plan d'adressage réseau**

Le prestataire s'engage à respecter les principes suivants : Les PC du CHR sont en DHCP et ceux spécifique à un prestataire (par exemple un automate) sont en IP fixes sur des Vlans dédiés. Les protocoles NetBios et Wins seront désactivés.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG40 -Environnement virtuel**

Le prestataire s'engage à utiliser l'infrastructure de virtualisation VMware vSphere de l'établissement.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**ENG41 - Intervention en mode dégradé**

En cas d'évènement nécessitant un isolement complet à Internet et bloquant la télémaintenance, le prestataire s'engage à fournir une proposition pour une intervention sur site

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

## Mesures concernant les services numériques hébergés chez le prestataire ou son sous-traitant (solution Cloud)

### Prérequis obligatoires

#### **ENG42 -Hébergement de données de santé**

Le prestataire s'engage à être certifié Hébergeur de Données de Santé (HDS) si le service numérique contient des données à caractère personnel hébergé dans le Cloud et à fournir au CHR le certificat correspondant à la solution d'hébergement proposée.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

#### **ENG43 -Hébergement sans données de santé**

Si le prestataire n'est pas certifié HDS, il s'engage à fournir un dossier de sécurité explicitant les mesures de sécurité mises en œuvre.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Non applicable pour le motif suivant : .....

## ANNEXE II - RGPD

### A2.1 - Coordonnées du Responsable de traitement (le CHR)

« Responsable du traitement », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre (RGPD art4.7).

Nom de la personne morale	CHR METZ-THIONVILLE
Adresse :	Hôpital de Mercy, 1 allée du Château CS 45001, 57085 Metz CEDEX 03
Nom et coordonnées du DPO	Albert CRUMBACH <a href="mailto:DPO@chr-metz-thionville.fr">DPO@chr-metz-thionville.fr</a> 03 87 55 37 28

### A2.2 - Coordonnées du sous-traitant (le prestataire)

« sous-traitant », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (RGPD art4.8).

Nom de la personne morale	À renseigner
Adresse :	À renseigner
Nom, fonction et coordonnées de la personne de contact	À renseigner
Nom et coordonnées du DPO	À renseigner

### A2.3 - Nature des opérations réalisées par le prestataire sur les données à caractère personnel pour le compte du responsable de traitement

<b>X</b>	Consultation et utilisation des données (Traitement par le prestataire sur les données, télémaintenance, support, ...)
	Collecte des données (saisie des données, importation des données, ...)
	Enregistrement des données (validation des données dans le système fourni par le prestataire, ...)
	Organisation et structuration des données (intervention sans modification sur les données, ...)
	Conservation des données (sauvegarde ou stockage des données, ...)
	Adaptation ou modification des données (intervention avec modification sur les données, modification par requête ou via IHM, ...)
	Extraction des données (exportation de données partielle ou totale du système, requêtage des données,...)
	Communication ou diffusion des données (communication des données par transmission, interfaces, ...)
	Rapprochement ou interconnexion des données (rapprochement avec des données venant de sources extérieures, transcodage, ...)
	Effacement ou destruction des données (suppression de données dans la base de données, de fichiers, ...)
	Autre : à préciser

### A2.4 - Catégories de personnes concernées

Le traitement de données concerne les catégories de personnes suivantes :

<b>X</b>	Les patients pris en charge par les professionnels de santé du CHR
<b>X</b>	Les professionnels de santé du CHR utilisateurs du SI
	Des tiers : à préciser

### A2.5 - Catégories de données à caractère personnel traitées

Personnes concernées	Catégorie de données	
Patients	Données d'identification / de coordonnées (Nom, Prénom, adresse postale et numérique, nationalité, ...)	<b>X</b>
	Données relatives à la vie personnelle (situation familiale, loisirs, ...) et professionnelle (employeur, fonction, ...)	<b>X</b>
	Données non courantes perçues comme sensibles (coordonnées bancaires, données sur les difficultés sociales ou personnelles, N° SS, .....)	<b>X</b>



Personnes concernées	Catégorie de données	
	Données sensibles relevant des art 9 ou 10 du RGPD (Données de santé à caractère personnel, orientation politique, religieuse, condamnation, ...)	X
	Données de connexion (traces informatiques, identifiant de connexion, ...)	X
	Autres données : à préciser	
Professionnels de santé	Données d'identification / de coordonnées (Nom, Prénom, adresse postale et numérique, nationalité, ...)	X
	Données relatives à la vie personnelle (situation familiale, loisirs, ...) et professionnelle (employeur, fonction, ...)	X
	Données non courantes perçues comme sensibles (coordonnées bancaires, données sur les difficultés sociales ou personnelles, N° SS, .....)	X
	Données sensibles relevant des art 9 ou 10 du RGPD (Données de santé à caractère personnel, orientation politique, religieuse, condamnation, .....)	X
	Données de connexion (traces informatiques, identifiant de connexion, ....)	X
	Autres données : à préciser	
Des tiers : à préciser	Données d'identification / de coordonnées (Nom, Prénom, adresse postale et numérique, nationalité, ...)	X
	Données relatives à la vie personnelle (situation familiale, loisirs, ...) et professionnelle (employeur, fonction, ...)	X
	Données non courantes perçues comme sensibles (coordonnées bancaires, données sur les difficultés sociales ou personnelles, N° SS, .....)	X
	Données sensibles relevant des art 9 ou 10 du RGPD (Données de santé à caractère personnel, orientation politique, religieuse, condamnation, .....)	X
	Données de connexion (traces informatiques, identifiant de connexion, ....)	X
	Autres données : à préciser	

## A2.6 - Durée du traitement

X	Ponctuellement pendant la durée de réalisation de la prestation réalisée (ex. : Uniquement lorsque le personnel du prestataire réalise une intervention de maintenance sur site ou à distance)
X	Systématique pendant toute la durée du contrat (ex. Prestation en régie nécessitant l'accès quotidien aux données)
	Des tiers : à préciser

## A2.7 - Engagement du prestataire (sous-traitant) relatif à l'information à fournir au CHR (responsable de traitement) en cas de violation de données

Le prestataire (sous-traitant) s'engage à fournir toutes les informations nécessaires permettant au CHR (responsable de traitement) de satisfaire aux obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679.

Ainsi, au-delà des informations mentionnées à l'article 8.2, le sous-traitant sera susceptible de fournir des informations complémentaires demandées par l'autorité de contrôle dans le cadre de son téléservice de notification des violations de données [Notifier une violation de données personnelles | CNIL](#).

## A2.8 - Sous-traitants ultérieurs autorisés

Nom de la personne morale	À renseigner
Adresse :	À renseigner
Nom, fonction et coordonnées de la personne de contact	À renseigner
Nom et coordonnées du DPO	À renseigner
Missions sous-traitées par le prestataire	À renseigner
Objet et nature du traitement des données	À renseigner
Durée du traitement :	À renseigner

Nom de la personne morale	À renseigner
Adresse :	À renseigner
Nom, fonction et coordonnées de la personne de contact	À renseigner
Nom et coordonnées du DPO	À renseigner
Missions sous-traitées par le prestataire	À renseigner

Objet et nature du traitement des données	À renseigner
Durée du traitement :	À renseigner

Ajouter des tableaux de sous-traitants si nécessaire

## A2.9 - Vérification de conformité du RGPD

### RGPD1 - DPO

Le soumissionnaire a désigné un délégué à la protection de données ou une personne en charge des sujets « informatique et libertés » qui sera l'interlocuteur du DPO du CHR.

X	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### RGPD2 -Registre des traitements

Pour les activités de traitement sous-traités par le CHR, le soumissionnaire tient à jour un registre des activités de traitement sous-traitées comprenant, a minima les informations précisées à l'article 30 §2 du RGPD.

X	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### RGPD3 - Sous-traitance

Une procédure du soumissionnaire encadre le recours à des sous-traitants ultérieurs. Le contrat respecte les exigences de l'article 28 du RGPD.

X	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

#### RGPD4 - Transfert de données hors UE

Le soumissionnaire s'assure que les opérations de traitement effectuées pour le compte du CHR ne prévoient pas de transfert de données en dehors de la France ou le cas échéant de l'Espace Économique Européen.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

#### RGPD5 - Violation de données

Le soumissionnaire a défini une procédure de notification d'une violation de données à caractère personnel au CHR. La notification doit comporter à minima les informations prévues à l'art. 33 §3 du RGPD.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

#### RGPD6 - Minimisation des données

La solution proposée par le soumissionnaire prévoit de respecter le principe de minimisation des données par des mesures spécifiques telles que la limitation de l'usage des champs commentaires, la limitation des champs de saisie et/ou le masquage de commentaires inappropriés.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

#### RGPD7 - Limitation de la durée de conservation

La solution proposée par le soumissionnaire prévoit de respecter le principe de limitation de la durée de conservation des données par des mesures spécifiques telles que la possibilité de définir une durée de conservation, la possibilité d'archiver automatiquement les données, la possibilité d'anonymiser des données à échange d'utilisation.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### RGPD8 - Qualité des données

La solution proposée par le soumissionnaire prévoit de respecter le principe de qualité des données par des mesures spécifiques telles que la possibilité d'être alerté en cas de perte d'intégrité des données.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### RGPD9 - Respect des droits des personnes

La solution proposée par le soumissionnaire prévoit la possibilité de répondre aux demandes d'exercice des droits des personnes en facilitant l'accès, la modification, la suppression des données et en permettant le gel des données en cas de demande de limitation du traitement. La procédure prévoit l'aide et l'assistance du CHR.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### RGPD10 - Analyse d'Impact sur la Protection des Données

Le soumissionnaire a défini une procédure permettant d'aider le CHR lorsqu'il est dans l'obligation de réaliser une analyse l'impact sur la protection des données (AIPD).

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### A2.10 - Instructions à destination du sous-traitant

Les présentes instructions sont définies par le CHR en sa qualité de Responsable de Traitement au sens de l'art. 4 du RGPD. Elles sont à destination du prestataire en sa qualité de sous-traitant au sens de l'art. 4 du RGPD.

### A2.11 - Instructions relatives aux opérations de traitement sous-traitées

#### Opérations de traitement sous traitées :

Le responsable de traitement définit les opérations de traitement qui doivent être réalisées pour son compte par le sous-traitant. Seules les opérations de traitement définies dans ce contrat doivent être réalisées par le sous-traitant. Toute utilisation des données à d'autres fins que celles définies par le responsable de traitement pourrait constituer un détournement de finalité imputable au sous-traitant.

Il est rappelé qu'en application de l'article L. 4113-7 du code de la santé publique, la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des données personnelles de santé, sont interdites

(même rendues anonymes à l'égard des patients) dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur.

Dans le cas où le sous-traitant rencontrerait des difficultés à réaliser les opérations de traitement sous-traitées, il est tenu d'en informer, sans délai, le responsable de traitement par écrit.

#### Licéité des traitements :

La base légale des activités de traitement est définie par le responsable de traitement seul responsable en la matière est répond à des missions de santé publique qui incombe au CHR. Le sous-traitant n'est pas autorisé à définir une autre base légale pour justifier l'usage de données des personnes concernées.

### **Instructions relatives aux moyens essentiels**

#### Personnes concernées :

Les personnes concernées par les opérations de traitement sont définies par le responsable de traitement dans le cadre de ce contrat. Le sous-traitant n'est pas autorisé à traiter des données d'autres personnes sans une instruction documentée du responsable de traitement.

#### Catégories de données :

Seules les catégories de données définies dans ce contrat doivent être traitées par le sous-traitant. Dans le cas où d'autres catégories de données doivent être traitées à l'initiative du responsable de traitement, le sous-traitant devra attendre une instruction documentée avant toute opération sur ces nouvelles catégories de données.

Au titre du principe de limitation, le sous-traitant n'est pas autorisé à traiter (notamment en les conservant) des données communiquées spontanément par les personnes concernées qui ne seraient pas dans les catégories de données définies dans ce contrat. Le sous-traitant n'est pas autorisé à collecter directement ou indirectement des données qui ne seraient pas dans les catégories de données définies dans ce contrat.

Le sous-traitant est tenu d'informer le responsable de traitement sans délai dans le cas où il serait amené à traiter des catégories de données autres que celles définies dans l'annexe 2 du contrat quelles qu'en soient les circonstances. La collecte de données au-delà de celles définies par le responsable de traitement pourrait constituer une collecte excessive de données au regard de la finalité de traitement imputable au sous-traitant.

#### Durée de conservation des données :

La durée du traitement est définie par le responsable de traitement dans ce contrat. Le sous-traitant n'est pas autorisé à conserver les données au-delà de cette durée sauf si une législation en vertu du droit de l'Union ou du droit national auquel le sous-traitant est soumis l'y oblige.

A l'échéance de la durée définie, le sous-traitant doit apporter la démonstration et la preuve écrite de la destruction effective des données ou, le cas échéant, de leur restitution au responsable de traitement sauf si une législation en vertu du droit de l'Union ou du droit national auquel le sous-traitant est soumis limite cette obligation. Une conservation des données au-delà de la durée définie par le responsable de traitement pourrait constituer un manquement à la durée de conservation imputable au sous-traitant.

#### Destinataires des données :

Le sous-traitant n'est pas autorisé à transmettre des données ou des résultats de traitement à des destinataires ou des tiers différents de ceux définis par le responsable de traitement à moins d'être tenu d'y procéder en vertu du droit de l'Union ou du droit national auquel le sous-traitant est soumis. Le sous-traitant doit informer le responsable de traitement des obligations en question.

Le sous-traitant n'est pas autorisé à transférer des données hors de l'UE sans une instruction documentée du responsable de traitement. Tout transfert de données à un destinataire ou à un tiers non autorisé par le responsable de traitement est un manquement qui pourrait être imputable au sous-traitant.

#### Sécurité des traitements :

Le sous-traitant est tenu de respecter les engagements en matière de sécurité des traitements définis ce contrat et, le cas échéant, d'informer, dans les meilleurs délais, le responsable des traitements dans le cas où les mesures définies ne permettent plus de protéger suffisamment les données. Dans le cas où le responsable de traitement constate des défauts ou des failles dans la sécurité des traitements, le sous-traitant doit y remédier dans les meilleurs délais et apporter la démonstration de l'efficacité des nouvelles mesures mises en œuvre.

### **Instructions relatives aux moyens non-essentiels**

#### Marge de manœuvre du sous-traitant :

Le sous-traitant dispose d'une marge de manœuvre concernant les moyens techniques et organisationnels qui lui permettent de réaliser les opérations de traitements définies dans ce contrat. Le sous-traitant informe le responsable des traitements des moyens non-essentiels qui vont l'aider à réaliser sa mission. Le sous-traitant est tenu d'informer, par écrit, le responsable des traitements dans le cas où des changements dans les moyens mis en œuvre impactent la bonne réalisation des opérations de traitement sous-traitées ou s'ils introduisent des risques pour les droits et les libertés des personnes concernées par les opérations en question.

### **Instructions générales sur la relation avec le responsable de traitement**

#### Echanges documentés :

Le sous-traitant doit systématiquement documenter par écrit les échanges qu'ils seraient amenés à avoir avec le responsable de traitement concernant la réalisation des opérations de traitement sous-traitées et, le cas échéant, des difficultés qu'il rencontre.

#### Nouvelles instructions documentées :

Le responsable de traitement peut être amené à formuler de nouvelles instructions sur la période de validité du contrat qui le lie avec le sous-traitant. Ces instructions seront documentées. Le sous-traitant est tenu de respecter ces nouvelles instructions à moins qu'elles n'entrent pas dans le cadre du contrat le liant avec le responsable de traitement ou si elles constituent une violation du RGPD ou d'autres dispositions du droit de l'Union ou du droit national relatives à la protection des données. Dans ce cas, le sous-traitant doit apporter les justifications relatives à ces constats par écrit, dans les meilleurs délais.

## ANNEXE III - Réversibilité des données

### Coordonnées de l'Ingénieur Sécurité du CHR

Nom et coordonnées	Cyril PIERRÉ Ingénieur Sécurité Risques Numériques <a href="mailto:dsn.securite@chr-metz-thionville.fr">dsn.securite@chr-metz-thionville.fr</a> 03 87 55 77 94
--------------------	---

### Coordonnées du référent Sécurité SI / juridique du prestataire

Nom, fonction et coordonnées	À renseigner
------------------------------	--------------

### A3.1 - Catégories de données concernées par la réversibilité

X	Données de santé collectées et traitées dans le cadre de la prestation
X	Données techniques collectées et traitées dans le cadre de la prestation
X	Données sur le personnel du CHR (coordonnées, etc.)
X	Résultats / livrables de la prestation
X	Enregistrements de conversations téléphoniques
X	Copies temporaires de données
X	Traces informatiques
X	Courriers électroniques
X	Sauvegarde des données
X	Documents remis par le CHR pour réaliser la prestation
	Autre : à préciser

### A3.2 - Catégories de support concernés par la réversibilité

X	Document(s) bureautique(s)
X	Base(s) de données
X	Progiciel(s) métiers
X	Support de stockage de données
X	Espace de stockage dans le Cloud



<b>X</b>	Messagerie
<b>X</b>	Dossiers papiers
	Autre : à préciser

### A3.3 - Engagement du Prestataire

#### REV1 - Restitution des données

Le prestataire s'engage à laisser le choix au CHR sur le moyen technique permettant de restituer les données, fichiers et/ou documents concernés (dépôt sécurisé, support externe, etc.). Il s'engage à restituer les données collectées et traitées par son personnel ou celui de ses sous-traitant dans un délai maximum de 30 jours suivant la cessation des relations contractuelles dans un format lisible et réutilisable par le CHR.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

#### REV2 - Suppression des données

Le prestataire s'engage à supprimer les données, fichiers et/ou documents concernés une fois la restitution validée par le CHR et à fournir le procès-verbal associé dans un délai maximum de 15 jours. En aucun cas le prestataire ne pourra être en mesure de reconstituer les données, fichiers et/ou documents concernés.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

#### REV3 - Gestion des difficultés

Le prestataire s'engage à informer sans délai le CHR dans le cas où des difficultés seraient rencontrées pour restituer ou supprimer les données, fichiers et/ou documents concernés.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**REV4 - Sécurité des données restituées**

Le prestataire s'engage à mettre en œuvre des solutions techniques permettant de garantir la sécurité et la confidentialité des données, fichiers et/ou documents restitués notamment par la mise en œuvre d'une solution de chiffrement.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**REV5 - Confidentialité et secret médical**

Le prestataire s'engage à la mise en œuvre de la réversibilité (restitution, suppression) uniquement par un personnel habilité soumis au secret professionnel ou à un engagement de confidentialité.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

**REV6 - Traçabilité**

Le prestataire s'engage à ce que les phases de restitution et des suppressions des données, fichiers et/ou documents concernés fassent l'objet d'une traçabilité permettant le cas échéant de traiter les incidents et les actes illicites dans le respect de la réglementation en vigueur.

<b>X</b>	Le prestataire s'engage sur cette mesure, elle est déjà opérationnelle.
	Le prestataire s'engage à mettre en œuvre cette mesure dans un délai raisonnable inférieur à 24 mois.
	Mesure alternative : .....
	Non applicable pour le motif suivant : .....

### A3.4 - Engagements du CHR

#### REV7 - Signature du procès-verbal de restitution

Le CHR s'engage à retourner au prestataire le procès-verbal de restitution des données, fichiers et/ou documents concernés signé dès réception. Dans le cas où le CHR ne renvoie pas ce procès-verbal dans un délai de 30 jours suivant son envoi, il est alors considéré comme accepté tacitement, le prestataire pourra alors procéder à la destruction des données.

X	Le CHR s'engage sur cette mesure.
---	-----------------------------------

#### REV8 - Vérification de la qualité des données restituées

Le CHR s'engage à procéder aux vérifications de qualité des données, fichiers et/ou documents restitués dès réception et signaler sans délai au prestataire toute anomalie constatée.

X	Le CHR s'engage sur cette mesure.
---	-----------------------------------

#### REV9 - Sécurité des données

Le CHR s'engage à assurer la sécurité et la confidentialité des données, fichiers et/ou documents concernés dès lors qu'elles ont été restituées par le prestataire et ne pas tenir pour responsable le prestataire d'un quelconque défaut de sécurité qui incomberait au CHR.

X	Le CHR s'engage sur cette mesure.
---	-----------------------------------