

	Procédure	Référence : PROC/00055
	Charte d'utilisation des services numériques pour les prestataires du CHR METZ-THONVILLE <i>Diffusion publique</i>	Version : 02
		Date de publication : 01/09/2023
		Date prochaine révision : 27/07/2027

La mise à jour de ce document est garantie sur Intranet – Veuillez régulièrement à l'actualisation de vos éditions papier.
Pour toute information sur ce document, merci de contacter les rédacteurs et/ou le service qualité.

OBJET

Le CHR Metz-Thionville met à la disposition de personnels habilités des informations, des outils informatiques (PC, stations, logiciels, etc.), des moyens de communication (messageries, accès Internet, assistants personnels numériques, etc.), ainsi que des données (bases de données, images, vidéos, etc.). Ces services numériques et ces données sont indispensables au bon fonctionnement du CHR, de ses métiers et de ses fonctions et ils contribuent à la réalisation de ses missions de santé public.

Ces services numériques et ces données font partie du patrimoine immatériel et matériel du CHR. A cet égard, toute information émise, reçue ou stockée sur n'importe quel support (papier, électronique, ...) est, et demeure la propriété du CHR.

Tout prestataire utilisateur de ces services numériques et de ces données doit respecter les règles de sécurité et de bonne conduite : l'imprudence, la négligence ou la malveillance pouvant avoir des conséquences graves particulièrement dans le cadre de la prise en charge des patients.

Ces services numériques et ces données étant exposés à de nombreux risques en termes de sécurité (accidents, erreurs, malveillances, etc.), la présente charte s'inscrit dans le cadre de la Politique de Sécurité du Système d'Information (PSSI) du GHT Lorraine Nord, élaborée pour définir les principes et règles de sécurité. Elle est de ce fait un document de référence pour l'établissement.

Elle précise les règles et précautions que les prestataires du CHR doivent respecter afin de garantir un usage fiable et sécurisé des données et ressources des services numériques auxquelles ils sont amenés à accéder pour réaliser leurs missions.

DOMAINE D'APPLICATION

Cette charte s'applique au prestataire et ses sous-traitants disposant d'un accès aux services numériques et aux données du CHR dans le cadre de leurs missions.

Ces prestataires disposent de droits d'accès, parfois étendus, aux services numériques du CHR leur permettant de réaliser les missions qui leur sont confiées et peuvent être amenés à avoir accès à des informations ou des données présentant un caractère confidentiel et soumis à un secret professionnel.

ABREVIATIONS

- **CHR** : Centre Hospitalier Régional de METZ-THONVILLE
- **DSI** : Direction du Système d'Information
- **GHT** : Groupement Hospitalier de Territoire
- **Prestataires** : prestataire et ses sous-traitants

DOCUMENTS ASSOCIES

- [PROC/00054](#) : Contrat relatif à la sécurité des services numériques et à la protection des données du Centre Hospitalier Régional METZ-THONVILLE

REFERENCES

- **RGPD** : Le Règlement (UE) 2016/679 ; Règlement Général sur la Protection des données

DEVELOPPEMENT

Article 1 - Les droits des prestataires

En application des consignes qui leur ont été transmises par le CHR, les prestataires peuvent prendre toute disposition nécessaire afin d'assurer la bonne réalisation de leur mission dans les limites et selon les directives définies par le CHR.

En outre, ils ne peuvent être contraint à enfreindre la loi : par conséquent, ils doivent refuser de faire un contrôle ou une action qui ne respectent pas les obligations légales en vigueur ou les droits élémentaires des utilisateurs, ainsi que toute action qui pourrait compromettre la sécurité des services numériques du CHR.

Article 2 - Obligation de confidentialité

Les prestataires sont soumis à une obligation de confidentialité (secret professionnel) et de non-divulgence liée à leurs activités. Pour rappel :

- l'Article 226-13 du code pénal dispose « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. » ;
- l'Article 121-1 du code pénal dispose « Nul n'est responsable pénalement que de son propre fait. ».

En conséquence :

- Les permissions attribuées aux prestataires ne sont utilisées que pour mener à bien les tâches qui leur sont confiées. Ils veillent à ce que les tiers non-autorisés n'aient pas connaissance de telles informations ;
- Les prestataires prennent connaissance des informations contenues dans les services numériques ou donnent accès à celles-ci seulement dans le cadre de leurs fonctions et/ou sur demande explicite de la DSI ;
- Le devoir de réserve et le principe de neutralité leur imposent l'interdiction absolue de faire de sa fonction l'instrument d'une propagande quelconque ;
- Les outils mis à sa disposition par le CHR ne sont utilisés que dans un but professionnel, tout usage à titre personnel ou privé est interdit ;
- Ils s'engagent à ne pas faire état ni utiliser les informations qu'ils peuvent être amenés à connaître dans le cadre de leurs fonctions ;
- L'accès ou la prise en main, à distance, sur le poste de travail d'un utilisateur est interdit sauf si l'autorisation explicite de ce dernier a été donnée ;
- Ils ont le devoir de ne pas abuser de leurs éventuelles prérogatives ; les actions qu'ils réalisent doivent être faites non seulement en toute transparence mais aussi de manière proportionnelle et adaptée à la finalité de leurs missions ;
- Ils s'efforcent d'éviter tout conflit pouvant exister entre leurs intérêts et ceux du CHR, ils informent le CHR de tout conflit d'intérêt dans lequel ils pourraient être impliqués pouvant altérer l'efficacité de leurs missions ;
- Ils veillent au respect de la politique et des directives relatives à la protection des données à caractère personnel du CHR et de la loi dite « informatique et libertés ».

L'obligation de confidentialité est applicable pendant toute la durée de la mission et au-delà, sans limite de durée que ce soit dans la sphère professionnelle ou privée.

Article 3 - Continuité des activités du prestataire

En toutes circonstances, la continuité du service et de la prestation doit être assurée.

Ils sont donc tenus d'assurer le suivi de leurs postes :

- Ils formalisent les procédures qu'ils gèrent pour que soit assurée cette continuité de service ;
- Ils documentent leurs actions et interventions de telle sorte que les personnels du CHR ne soient pas dans un état de dépendance en cas d'absence ou lorsqu'ils quittent leurs fonctions ;
- Ils collaborent et coopèrent avec la DSI du CHR en cas d'incidents de sécurité ;
- Ils sont tenus de suivre les procédures préalablement définies par le CHR.

Article 4 - Respect des bonnes pratiques

Les prestataires observent strictement les règles de sécurité et les limites fixées à leurs interventions :

- Ils limitent leurs actions aux services numériques dont ils ont la charge et dans le respect de la finalité de leurs missions. Ils modifient les configurations et les droits d'accès uniquement dans les cas préalablement définis par le CHR ;
- Ils ont le devoir d'informer le CHR de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des services numériques. De même ils s'engagent à l'informer de toute opération inhabituelle nécessitant l'accès à des données sensibles et des motifs les y autorisant conformément à l'exercice de leurs missions (sauf au cas où la discrétion des opérations est imposée par les autorités judiciaires) ;
- Ils ont l'obligation de refuser la réalisation de toute requête leur paraissant inappropriée ou contraire à la réglementation, en justifiant leurs raisons auprès du demandeur et en informant immédiatement la DSI du CHR ;
- Dans le cadre de la conduite de leurs missions et vis-à-vis des ressources à leur charge (serveurs, bases de données, postes de travail utilisateurs, etc.), ils utilisent les logiciels faisant partie des standards approuvés par le CHR. Toute installation de logiciel ne faisant pas partie de ces standards doit faire l'objet d'une autorisation préalable de la DSI du CHR.

Article 5 - Notification d'incident de sécurité et de violation de données

Les prestataires doivent tenir informé le CHR des incidents de sécurité et vulnérabilités des services numériques rencontrés dans l'exercice de leurs missions : tentatives d'intrusion, virus détectés, matériels obsolètes, saturation de ressources informatiques, plan de reprise/continuité d'activité non opérationnel, etc...

Ils doivent signaler tout incident de sécurité (règle de sécurité violée, charte de bon usage non respectée ...) et toutes autres activités pouvant avoir un impact légal ou réglementaire ou bien induisant un risque (technique, juridique, financier, image de marque...) pour le CHR. Ainsi :

- Ils informent sans délai la DSI du CHR de toute faille ou incident de sécurité qu'ils pourraient découvrir ou dont ils pourraient avoir connaissance ;
- Ils coopèrent avec la DSI en cas d'incident de sécurité impliquant les services numériques qu'ils administrent ou utilisent dans le cadre de leurs missions ;
- Ils préservent, conservent et sauvegardent les « traces » ou tout élément nécessaire à la résolution d'un incident et à toute investigation ultérieure.
- Ils informent sans délai le DSI du CHR de toute violation de données entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données ou l'accès non autorisé à de telles données.

Article 6 - Identification et authentification du prestataire

Les prestataires s'assurent de la protection des droits d'accès liés à leurs fonctions qui leur sont attribués par le CHR.

Ils observent les règles de sécurité en vigueur visant à protéger l'utilisation des comptes et des droits d'accès qui leur ont été attribués. Ils veillent notamment à la protection des postes de travail à partir desquels ils exercent leurs fonctions et à la gestion des identifiants et mots de passe des comptes :

- Les mots de passe utilisés doivent être complexes et changés régulièrement conformément à la politique de sécurité des mots de passe du CHR ;
- Il est rappelé que les droits confiés (et par conséquent les couples identifiant/mot de passe associés) sont nominatifs, confidentiels et non cessibles ;
- Ils utilisent leurs comptes uniquement pour les activités et besoins directement liés aux tâches dont ils ont la charge.

Des contrôles des traces de connexion ou des sessions de connexion peuvent être effectués par la DSI en cas d'incident ou à titre préventif.

Article 7 - Sensibilisation et formations

Dans le cadre de la sécurité des services numériques et des données, les prestataires s'engagent :

- à sensibiliser et former son personnel avant toute mission réalisée pour le compte du CHR ;
- à contribuer à la sensibilisation des utilisateurs du CHR.