AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

Annexe 1 – questionnaires fournisseurs

Statut : validé Classification : publique Version : V2.0 – 17/11/2021

Table des matières

Objet et usage des questionnaires

Les outils et services informatiques des professionnels de santé en exercice libéral constituent des ensembles de plus en plus complexes qui mettent en jeu de multiples composants souvent interdépendants. Aussi est-il fortement recommandé de faire appel à des professionnels de l'informatique pour l'installation et la maintenance régulière de ces outils, ou pour la fourniture de téléservices et d'autres services dématérialisés.

Dans ce contexte, et dans la mesure où vous conservez dans tous les cas une responsabilité quant à la protection et à l'usage des données à caractère personnel qui vous ont été confiées, il est essentiel que chacun de vos fournisseurs de service informatique (désignés ci-après « fournisseurs » ou « professionnels informatiques ») garantisse un service dont les modalités vous permettent de respecter vos obligations en matière de sécurité des systèmes d'information et de protection des données à caractère personnel, notamment en ce qui concerne la disponibilité de vos outils et services informatiques, ainsi que la confidentialité, l'intégrité et la disponibilité des données à caractère personnel, de santé ou autres.

Les professionnels informatiques qui interviennent pour votre compte se doivent de réaliser leurs prestations de service en conformité avec les exigences légales et réglementaires applicables. Les questionnaires qui suivent n'ont pas vocation à décrire l'ensemble de ces exigences, mais listent un ensemble non exhaustif de points d'attention qu'il est recommandé à tout professionnel de santé en exercice libéral de vérifier afin de s'assurer que chacun de ses fournisseurs de service informatique prend en compte les problématiques de sécurité de façon suffisamment large.

Dans les cas où les moyens informatiques vous sont fournis par un établissement de santé, ces points d'attention doivent également être pris en compte par ce dernier.

- Quatre questionnaires vous sont proposés ci-après en fonction de la nature du service assuré par chacun de vos fournisseurs de service informatique.
- En tant que professionnel de santé en exercice libéral (ou « professionnel de santé »), vous êtes invité à faire remplir les questionnaires qui vous concernent par chaque fournisseur de service, si possible en étant vous-même présent afin d'obtenir toute explication utile le cas échéant.
  Le fournisseur de service doit indiquer pour chaque point d'attention s'il s'y conforme dans le cadre du service informatique fourni, ou s'il ne s'y conforme pas. Quand la fourniture de service n'est pas conforme, il est fortement recommandé de demander au fournisseur de modifier sa prestation de service et/ou ses pratiques afin de respecter les attentes formulées pour le point d'attention concerné s'il n'est pas indiqué comme étant optionnel (son respect restant néanmoins recommandé).
- Il est fortement recommandé que le fournisseur de service s'engage formellement sur l'exactitude de ses réponses en datant et signant le questionnaire renseigné.

Questionnaire 1 : Points généraux applicables à toute fourniture de service informatique

Ce questionnaire concerne tout type de fourniture de service informatique, et doit être renseigné dans tous les cas.

Le fournisseur doit indiquer dans la colonne Conformité : « OUI » si la prestation de service considérée est conforme à la formulation du point d'attention, et « NON » si ce n'est pas le cas, ou le cas échéant « N/A » si le sujet du point d'attention sort du cadre de la prestation de service considérée (exemple : les points d'attention relatifs à la sous-traitance ultérieure).

Point d'attention	Conformité
Le fournisseur est une entité dotée de la personnalité morale, soumise au droit d'un état membre de l'Union Européenne, de façon à pouvoir être tenu juridiquement responsable de sa prestation de service.	
Un contrat écrit est conclu entre le professionnel de santé et son fournisseur avant l'exécution de la prestation de service.	
Le contrat précise le périmètre de la prestation de service réalisée et détermine la répartition des rôles et responsabilités entre le professionnel de santé et le fournisseur au regard de la mise en œuvre de ladite prestation.	
Le fournisseur a connaissance du cadre légal et règlementaire applicable au secteur sanitaire, social et médico-social, en tient compte dans les prestations de service qu'il assure pour le professionnel de santé, et atteste que les services qu'il lui fournit sont conformes à ce cadre.	
Le fournisseur, lorsqu'il traite des données à caractère personnel, s'engage à respecter les dispositions générales relatives à la protection des données personnelles et des données de santé.	
Le fournisseur a, en sa qualité de prestataire de service, un devoir de conseil vis-à-vis du professionnel de santé.	
Le fournisseur a informé le professionnel de santé du recours à un ou plusieurs sous-traitants éventuels dans le cadre de la réalisation de la prestation de service (ci-après dénommée « sous-traitance ultérieure »). Chaque sous-traitance ultérieure est encadrée par un contrat qui comporte notamment les mentions suivantes : les activités sous-traitées, l'identité et les coordonnées du sous-traitant, les dates du contrat de sous-traitance, la répartition des rôles et responsabilités entre le fournisseur et son sous-traitant.	
Si le fournisseur recourt à la sous-traitance, il s'est assuré que chaque sous-traitant ultérieur : ► respecte les obligations du contrat conclu entre le professionnel de santé et le fournisseur ; ► présente des garanties suffisantes quant à la mise en œuvre de mesures techniques, juridiques et organisationnelles adaptées à la prestation de service.	
Le fournisseur a souscrit une assurance couvrant sa responsabilité civile en cas de dommages causés au professionnel de santé et sur le périmètre de sa prestation de service.	
Le fournisseur :	
► S'interdit de traiter les données métier de son client, et en particulier les données à caractère personnel dont les données de santé, sauf exception prévue par un texte législatif ou réglementaire.	
► Met en œuvre des mesures organisationnelles, juridiques et techniques adaptées à la criticité des données traitées par le professionnel de santé ;	
► S'engage à respecter la plus stricte confidentialité concernant l'ensemble des informations auxquelles il aurait accès dans le cadre de la mise en œuvre de la prestation de service ;	
► S'engage à ce que toute personne intervenant pour son compte dans le cadre de la prestation de service signe un engagement de confidentialité.	

Le fournisseur a établi une charte de sécurité ou un document équivalent, opposable à son personnel participant aux prestations de service fournies, et fixant les bonnes pratiques, interdictions et obligations auxquels ce personnel est soumis.	

Raison sociale du fournisseur :

Désignation du service fourni :

Je, soussigné ….. atteste l'exactitude des informations de conformité portées sur ce questionnaires.

Fait le ..../…./20…. à …..

Signature :

Questionnaire 2 : Installation et/ou de maintenance informatique

Ce questionnaire doit être renseigné pour toute fourniture de service d'installation ou de maintenance informatique sur place ou à distance, en plus du questionnaire 1.

Le fournisseur doit indiquer dans la colonne Conformité : « OUI » si la prestation de service considérée est conforme à la formulation du point d'attention, « NON » si ce n'est pas le cas, ou le cas échéant « N/A » si le sujet du point d'attention sort du cadre de la prestation de service considérée (exemple : les points d'attention relatifs au réseau local si le fournisseur n'a pas en charge ce réseau local).

Règles générales d'hygiène informatique

Point d'attention	Conformité
Le fournisseur a pris connaissance des guides publiés par l'ANSSI : ► Guide d'hygiène informatique Pour en savoir plus… ► Recommandations relatives à l'administration sécurisée de systèmes d'information Pour en savoir plus…	
Le fournisseur a pris connaissance des guides pratiques spécifiques disponibles dans l'espace de publication PGSSI-S. Pour en savoir plus…	
Le fournisseur s'engage à appliquer ces guides autant que possible dans le cadre de sa prestation de service.	

Architecture informatique

Point d'attention	Conformité
Réseau local	
Le réseau local mis en place dans les locaux du professionnel de santé est un réseau physique autonome qui accueille exclusivement des équipements destinés au professionnel de santé et aux collaborateurs qu'il désigne. Des mesures techniques sont prises pour restreindre les possibilités de connexion d'équipements non autorisés.	
Dans le cas d'un réseau local sans fil (Wifi), les protocoles et clés utilisés sont conformes aux préconisations des guides publiés par l'ANSSI : ► Fiche n°20 du Guide d'hygiène informatique Pour en savoir plus… ► Recommandations de sécurité relatives aux réseaux Wifi Pour en savoir plus…	
Le fournisseur s'assure que les fonctions Wifi et Bluetooth des différents équipements sont désactivées s'il n'est pas prévu de les utiliser.	
Accès Internet	
L'accès Internet est conçu et paramétré pour n'autoriser que les connexions sortantes ou, si une télémaintenance informatique est prévue ou si un accès en mobilité est prévu, les connexions entrantes établies exclusivement via un VPN s'appuyant sur des protocoles et des clés conformes aux préconisations de l'ANSSI dans le domaine de la cryptographie. Pour en savoir plus…	

Aucun service fourni par un système hébergé dans les locaux du professionnel de santé n'est rendu accessible depuis Internet *(comme, par exemple, un service qui permettrait d'accéder depuis Internet aux dossiers patients conservés sur un serveur situé dans le cabinet médical)*. Si de tels services partagés sont nécessaires, ils sont fournis et hébergés par des fournisseurs de service informatique disposant des certifications ou agréments éventuellement requis par la loi, sur leurs propres infrastructures techniques.	
Postes de travail et serveurs locaux	
Tout poste de travail ou serveur est équipé au moins d'un antivirus. L'antivirus est mis à jour automatiquement (signatures de virus, moteur) au minimum une fois par jour.	
Autant que possible, tout poste de travail ou serveur est équipé d'un pare-feu, activé et paramétré pour limiter les connexions réseau, entrantes comme sortantes, aux seules applications qui le nécessitent.	
Autant que possible, les supports de stockage des postes de travail et des serveurs qui stockent des données de santé à caractère personnel sont chiffrés en respectant les préconisations de l'ANSSI dans le domaine de la cryptographie mentionnées plus haut.	
Les supports de stockage de tout poste de travail mobile et de tout autre terminal mobile sont impérativement chiffrés.	
Autant que possible, une solution et la procédure associée sont prévues pour, en cas de perte ou de vol de tout poste de travail mobile ou autre terminal mobile, pour permettre l'effacement à distance de l'ensemble des données du terminal.	
Chaque utilisateur dispose d'un compte utilisateur nominatif, avec des droits d'accès correspondant uniquement à ses activités autorisées par le professionnel de santé.	
Les comptes administrateurs sont distincts des comptes utilisateurs. Un compte utilisateur peut toutefois disposer des droits permettant la sauvegarde d'un système si cette tâche est attribuée à cet utilisateur. Le professionnel de santé doit disposer d'au moins un compte administrateur, dont il conserve l'identifiant et le mot de passe de façon sécurisée.	
Une solution de génération et de stockage sécurisé des mots de passe est fournie au professionnel de santé et aux autres utilisateurs du système d'information.	
Les interfaces de changement de mot de passe des systèmes d'exploitation ou des applications sont paramétrées pour imposer un mot de passe sûr au regard des bonnes pratiques en vigueur. Tout mot de passe par défaut d'une application ou d'un équipement est modifié à l'installation, à l'aide d'un mot de passe conforme à ces bonnes pratiques. Le fournisseur signale au professionnel de santé tout usage d'application ou d'équipement ne permettant pas cette conformité des mots de passe aux bonnes pratiques.	

Traces

Point d'attention	Conformité
La génération de traces (« fichiers journaux » ou « logs ») doit être activée au niveau du système d'exploitation des équipements informatiques. Ces traces doivent enregistrer, avec leur date et heure, les évènements suivants au minimum : ► Connexion d'un utilisateur ► Déconnexion d'un utilisateur ► Echec de tentative de connexion ► Toute anomalie de sécurité	
La génération de traces doit être activée au niveau de toute application traitant des données à caractère personnel, de santé ou non. Ces traces doivent enregistrer, avec leur date et heure et l'identité de l'utilisateur les ayant effectuées, toute action de consultation, création, modification ou suppression de données à caractère personnel, et préciser quelles données ont été l'objet de cette action.	
L'accès au paramétrage et à la consultation des traces est restreint aux seules personnes autorisées par le professionnel de santé.	

Les systèmes sont paramétrés pour conserver ces traces sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important), et les supprimer automatiquement à l'issu de cette période.	
Le fournisseur rappelle au professionnel de santé son obligation d'informer les utilisateurs que des traces de leurs actions sont conservées, et que ces traces ne doivent être utilisées exclusivement qu'à des fins de sécurité informatique ou dans le cadre d'une procédure judiciaire ou contentieuse prévue par la loi.	

Sauvegardes

Point d'attention	Conformité
L'architecture installée comporte un système de sauvegarde en mesure d'assurer la restauration des systèmes, des applications et des données. Ce système permet au professionnel de santé de reprendre son activité en cas d'incident informatique (défaillance de support de stockage, incendie, rançongiciel…) en respectant d'une part ses propres exigences de reprises d'activité et d'autre part ses obligations légales en termes de disponibilité des données personnelles et des données de santé dont il a la charge.	
Le fournisseur élabore avec le professionnel de santé un plan de sauvegarde et de restauration du système d'information permettant le respect de ces exigences. Il met à jour le plan de sauvegarde à chaque évolution du système d'information (ajout d'application ou d'équipement, changement du mode de stockage des données d'une application...).	
Le plan de sauvegarde est conçu pour assurer la confidentialité, l'intégrité et la disponibilité des sauvegardes stockées, que ce soit par le(s) lieu(x) choisis pour le stockage de ces sauvegardes et/ou par la mise en œuvre de mécanismes techniques (chiffrement, redondance, …). En tout état de cause, les sauvegardes suffisantes pour respecter les exigences de restauration du système doivent être conservées de manière totalement déconnectée du système sauvegardé, et dans un lieu qui n'est pas susceptible d'être atteint par le même sinistre que celui qui aurait atteint le système sauvegardé.	
Le fournisseur s'assure qu'un jeu de supports de sauvegarde nécessaire à l'exécution du plan de sauvegarde établi est effectivement disponible.	
Le fournisseur effectue un suivi régulier du système de sauvegarde afin de détecter tout dysfonctionnement du système ou tout vieillissement de supports de sauvegarde. Il teste le plan de sauvegarde et de restauration au minimum une fois par an.	

Documentation

Point d'attention	Conformité
Le fournisseur élabore la documentation du système d'information et la maintient à jour avec une fréquence au moins annuelle.	
La documentation inclut au minimum :	
► L'architecture du système d'information ;	
► La liste des équipements et logiciels constitutifs du système d'information, avec leur version et leurs principaux paramétrages techniques (nom, adresse MAC, adresse IP…) ;	
► La liste des licences des logiciels utilisés ;	
► Les procédures de gestion quotidienne du système, qu'il soit prévu que ces opérations soient réalisées par les utilisateurs ou par le fournisseur lui-même (sauvegarde, restauration, création ou suppression d'utilisateur, mise au rebut de matériel, retour en arrière après mise à jour entrainant des dysfonctionnements…).	

Le fournisseur communique au professionnel de santé, conjointement à chaque application installée qui traite des données à caractère personnel, un document précisant l'ensemble des informations requises par le RGPD[1] pour permettre au professionnel de santé de renseigner le registre des activités de traitement de données à caractère personnel qu'il doit tenir conformément à l'article 30 du RGPD.	

Maintenance

Point d'attention	Conformité
Le fournisseur s'assure de l'application la plus rapide possible des mises à jour de sécurité disponibles des différents composants du système d'information (systèmes d''exploitation, applications, outils, équipements…). Il privilégie l'activation des mises à jour automatiques au moins en ce qui concerne les mises à jour de sécurité. Il prévoit une procédure de retour en arrière en cas de constatation de dysfonctionnement bloquant consécutif à une mise à jour.	
Le fournisseur assure une surveillance préventive des composants matériels du système d'information afin de préparer leur remplacement.	
Le fournisseur assure le suivi des dates de fin de support constructeur des différents composants logiciels et matériels du système d'information, et en informe le professionnel de santé suffisamment en avance pour qu'une migration puisse être discutée et planifiée. Il veille à ce qu'aucun de ces composants ne continue à être utilisé après sa date de fin de support, et alerte formellement le professionnel de santé des risques encourus chaque fois qu'une telle situation n'est pas traitée.	
Le fournisseur documente et applique systématiquement une procédure de mise au rebut des actifs du système d'information. Pour les supports de stockage, cette procédure doit au minimum inclure une procédure d'effacement sécurisé ou de destruction physique par incinération ou déchiquetage (le cas échéant selon la nature du support de stockage) et donner lieu à un procès-verbal formel d'effacement ou de destruction établi par la personne qu'il a chargée de l'opération.	
Le fournisseur tient un journal de ses interventions menées sur le système d'information du professionnel de santé, dans lequel il consigne systématique la date d'intervention, l'identité des intervenants, la nature des interventions effectuées et l'issue de l'intervention (succès ou problèmes rencontrés).	

Raison sociale du fournisseur :

Désignation du service fourni :

Je, soussigné …..
sur ce questionnaire.

atteste l'exactitude des informations de conformité portées

Fait le ..../…./20…. à …..

Signature :

[1] RGPD : Règlement général sur la protection des données (RGPD) et loi n°78-17 du 6 janvier 1978 modifiée

Questionnaire 3 : Maintenance informatique à distance

Ce questionnaire doit être renseigné pour toute fourniture de service de maintenance informatique à distance (« télémaintenance »), en plus des questionnaires 1 et 2.

Le fournisseur doit indiquer dans la colonne Conformité : « OUI » si la prestation de service considérée est conforme à la formulation du point d'attention, et « NON » dans les autres cas.

Sécurité du système d'information du fournisseur

Point d'attention	Conformité
Le fournisseur confirme que les points d'attentions du questionnaire 2 sont bien vérifiés au sein de ses propres systèmes d'information.	
Le système d'information utilisé pour les prestations de maintenance à distance est réservé à cet usage et cloisonné vis-à-vis de tout autre système d'information.	
Le fournisseur a établi un Plan d'Assurance Sécurité (PAS) qui décrit, sans entrer dans les détails techniques, les différentes mesures mises en œuvre pour assurer la sécurité de son système d'information et des interventions de maintenance à distance qu'il réalise. Ce document est consultable sur demande par le professionnel de santé.	

Outils de maintenance à distance

Point d'attention	Conformité
Les communications entre le système de maintenance à distance du fournisseur et le système d'information maintenu sont réalisées via un VPN établi entre ces deux systèmes d'information et s'appuyant sur des protocoles et des clés conformes aux préconisations de l'ANSSI dans le domaine de la cryptographie mentionnées à la section « Architecture informatique - Accès Internet » du questionnaire 2.	
Les outils utilisés pour la maintenance à distance établissent des connexions directes entre le système de maintenance à distance du fournisseur et le système d'information maintenu, sécurisées en conformité avec les mêmes préconisations.	
Il n'est fait usage d'aucun outil de communication à distance s'appuyant sur un système intermédiaire tiers qui ne serait contrôlé ni par le fournisseur de service de maintenance, ni par le professionnel de santé.	
Chaque intervention à distance requiert techniquement qu'elle soit autorisée de manière active par le professionnel de santé ou un de ses collaborateurs autorisés, depuis un équipement informatique présent au sein du système d'information maintenu. Cette autorisation est accordée pour une durée limitée, et doit être renouvelée de la même manière si besoin.	

Modalités de maintenance à distance

Point d'attention	Conformité
Le fournisseur assure une traçabilité nominative des accès de maintenance à distance aux systèmes du professionnel de santé.	
Le fournisseur dispose des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation de service.	
Le fournisseur informe le professionnel de santé préalablement à la signature du contrat, de manière claire et explicite, lorsqu'il effectue un traitement de données personnelles depuis un pays tiers à l'Union-Européenne dans le cadre de la fourniture de son service de maintenance à distance (exploitation, administration, hébergement, etc.).	
En cas de traitement de données depuis un pays tiers à l'Union-Européenne, le fournisseur communique au professionnel de santé un document présentant les mesures juridiques, organisationnelles et techniques[2] prises par le fournisseur, en conformité avec le RGPD, afin de garantir la sécurité du transfert (clauses contractuelles, règles d'entreprise contraignantes…).	

Raison sociale du fournisseur :

Désignation du service fourni :

Je, soussigné …..
atteste l'exactitude des informations de conformité portées sur ce questionnaire.

Fait le ..../…./20…. à …..

Signature :

[2] Voir RGPD chapitre V « Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales »

Questionnaire 4 : Stockage de données à distance ou téléservice

Ce questionnaire doit être renseigné pour toute fourniture de service de stockage de données à distance (fichiers, bases de données, sauvegardes, archivage…) ou de fourniture de téléservice ou d'hébergement d'application (gestion de cabinet ou d'officine, prise de rendez-vous, téléconsultation…), en plus du questionnaire 1.

Le fournisseur doit indiquer dans la colonne Conformité : « OUI » si la prestation de service considérée est conforme à la formulation du point d'attention, « NON » si ce n'est pas le cas, ou le cas échéant « N/A » si le point d'attention porte sur un type de prestation ne correspondant pas à la prestation de service considérée.

Point d'attention	Conformité
Le fournisseur qui fournit un service d'archivage électronique au professionnel de santé est titulaire de l'agrément délivré par le ministre chargé de la culture pour la conservation de données de santé à caractère personnel sur support papier ou sur support numérique dans le cadre d'un service d'archivage électronique.	
Le fournisseur qui héberge des données de santé à caractère personnel autre que d'archivage électronique, recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social pour le compte du professionnel de santé est titulaire d'un certificat de conformité d'hébergeur de données de santé « hébergeur d'infrastructure physique » et/ou « hébergeur infogéreur » selon le cas, délivré par un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen).	
Le fournisseur qui traite, pour le compte du professionnel de santé, des données à caractère personnel et/ou des données de santé se conforme notamment aux dispositions du RGPD, de la loi Informatique et Libertés modifiée et du code de la santé publique, que ce soit en sa qualité de sous-traitant ou de responsable de traitement, selon le cas.	
Le fournisseur informe le professionnel de santé de tout risque d'expiration ou de perte d'agrément ou de certificat, ou de tout risque de sanction, qui lui interdirait de continuer à héberger des données de santé à caractère personnel.	
Le fournisseur informe le professionnel de santé préalablement à la signature du contrat, de manière claire et explicite, lorsqu'il effectue un traitement de données personnelles depuis un pays tiers à l'Union-Européenne dans le cadre de la fourniture de son service de stockage de données à distance, de téléservice ou d'hébergement d'application (exploitation, administration, hébergement, etc.).	
En cas de traitement de données depuis un pays tiers à l'Union-Européenne, le fournisseur communique au professionnel de santé un document présentant les mesures juridiques, organisationnelles et techniques [1] prises par le fournisseur, en conformité avec le RGPD, afin de garantir la sécurité du transfert (clauses contractuelles, règles d'entreprise contraignantes…).	
Le fournisseur s'engage à restituer au professionnel de santé, à la fin de la prestation de service, l'ensemble des données qu'il héberge pour son compte sans en conserver de copie. Le support sur lequel seront restituées les données devra permettre au professionnel de santé de poursuivre son activité et, le cas échéant, de recourir à un autre fournisseur pour les héberger.	

Raison sociale du fournisseur :

Désignation du service fourni :

Je, soussigné …..
sur ce questionnaire. atteste l'exactitude des informations de conformité portées

Fait le ..../…./20…. à ….. Signature :