Questionnaires de la démarche « Référencement guidé » Parcours Mon espace santé

Industriels – 30/10/2024

Sommaire

Types de critères

Obligation — Critères avec un niveau de maturité minimum attendu

Option — Critères sans niveau de maturité minimum attendu

Légende des réponses

✓ Niveaux acceptés pour les critères de type « Obligation »

NA possible — Niveau non applicable possible pour un critère du questionnaire « Ethique Mon santé »

○ Une seule réponse est acceptée

☐ Plusieurs réponses sont acceptées

1. Questionnaires de la démarche

1.1 Questionnaire d'orientation

Généralités

Obligation 1. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical ?

- Oui
- Non

Obligation 2. Le service, pour lequel vous candidatez au référencement Mes, inclut-il un dispositif médical connecté ?

- Oui
- Non

Obligation 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ?

- Mesures de santé
- Documents
- Agenda
- Aucune réponse correspondante

Obligation 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ?

- Oui
- Non

Obligation 4. Pour quelle architecture du service sollicitez-vous un référencement à Mon Espace Santé ?

- Web
- Android
- iOS
- Aucune réponse correspondante

Obligation 4. bis. Autres architectures à indiquer – Champ texte libre

Obligation 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ?

- Oui
- Non

Obligation 6. Fournir un compte de démonstration (url, identifiant et mot de passe) – Champ texte libre

Obligation 7. Le service fait-il appel à un hébergement de données (y compris en cas d'hébergeur interne/cloud ou en cas de sous-traitance de l'hébergement) ?

- Oui
- Non

Métier

Obligation 8. Quelles sont les activités auxquelles concourt votre service ?

- Thérapeutique
- Prévention
- Diagnostic
- Soin
- Soulagement de la douleur
- Compensation du handicap ou prévention de la perte d'autonomie
- Suivi social ou médico-social
- Interventions nécessaires à la coordination de plusieurs de ces actes
- Aucune réponse correspondante

Obligation 8.bis. Autres activités à indiquer – Champ texte libre

Obligation 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ?

- Oui
- Non

Interopérabilité

Obligation 10. Le service échange-t-il des données avec d'autres applications ou SI que Mes ?

- Oui
- Non

Obligation 11. Le service partage-t-il des données avec d'autres applications ou SI que Mes ?

- Oui
- Non

Obligation 12. Le service produit ou consomme-t-il ce type de document ?

- Gestion d'agendas partagés
- Mesures de santé
- Structuration minimale - Production
- Structuration minimale – Consommation
- Aucune réponse correspondante

Urbanisation

Obligation 13. Le service gère-t-il un référentiel d'identité ?

- Oui
- Non

Obligation 14. Le service reçoit-il des données de santé à caractère personnel provenant d'un autre domaine d'identification ?

- Oui
- Non

Obligation 15. Le service reçoit-il des données de santé à caractère personnel provenant d'un autre service appartenant au même domaine d'identification ?

- Oui
- Non

Obligation 16. Le service est-il une application de télésanté ?

- Oui
- Non

Sécurité

Obligation 17. Le service permet-t-il l'import par un utilisateur (administrateurs compris) de fichiers susceptibles de constituer ou de contenir un logiciel malveillant (malware, virus ou autre) ?

- Oui
- Non

Obligation 18. Le service comporte-t-il une partie centralisée (serveurs, etc.) accédée via Internet ?

- Oui
- Non

Obligation 19. Le service est-t-il susceptible, dans certains cas de mise en œuvre autorisés par le contrat de fourniture, d'être accessible depuis des réseaux publics (Internet...) ? OU L'analyse de risques a-t-elle identifié le besoin d'une architecture n-tiers pour le service ?

- Oui
- Non

Obligation 20. Le service comporte-t-il la fourniture à la fois de logiciel et de matériel à l'utilisateur, tout ou partie de ce logiciel s'exécutant sur le matériel fourni, et l'ensemble étant destiné à être directement utilisé par l'utilisateur ?

- Oui
- Non

Obligation 21. Le service comporte-t-il un ou plusieurs composants qui peuvent être connectés à un système de communication informatique, qu'il s'agisse d'un réseau local, d'Internet ou d'un réseau sans fil (Wifi, Bluetooth, réseaux de téléphonie mobile, réseau pour IoT…) ?

- Oui
- Non

Obligation 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ?

- Oui
- Non

Obligation 23. Le service comporte-t-il un ou plusieurs équipements fournis par l'industriel pouvant être utilisés en mobilité par l'utilisateur ?

- Oui
- Non

Obligation 24. Les équipements mobiles fournis par l'industriel ont-ils la capacité d'utiliser le wifi ?

- Oui
- Non

Obligation 25. Le service fournit-il un accès dédié à des acteurs de santé personnes physiques ?

- Oui
- Non

Obligation 26. Le service gère-t-il l'identité d'acteurs de santé personnes physiques dans les données qu'il traite (stockage, affichage, utilisation de données d'identité de professionnel de santé) ?

- Oui
- Non

Obligation 27. Le service fournit-il un accès dédié à des acteurs de santé personnes morales ?

- Oui
- Non

Obligation 28. Le service gère-t-il l'identité d'acteurs de santé personnes morales dans les données qu'il traite (stockage, affichage, utilisation de données d'identité de professionnel de santé) ?

- Oui
- Non

Obligation 29. Le service fournit-il un accès à des données à caractère personnel à des utilisateurs ou patients ?

- Oui
- Non

Obligation 30. Le service est-il multi-utilisateurs (utilisateurs finaux, administrateurs, etc.) ?

- Oui
- Non

Obligation 31. L'offre comporte-t-elle une prestation de télémaintenance de l'application, conjointement à la fourniture de l'application qui est exploitée sous la responsabilité de son utilisateur ?

- Oui
- Non

Obligation 32. Existe-t-il des remontées d'informations issues des dispositifs maintenus vers le SI du prestataire dans le cadre de la prestation de télémaintenance ?

- Oui
- Non

Ethique

Obligation 33. Le service, pour lequel vous candidatez au référencement Mon Espace Santé, est-il un DM de classe 2A et supérieures ou un DM DIV classe B et supérieures (fournir le certificat de marquage CE délivré par un organisme notifié et le certificat ISO 13485) ?

- Oui
- Non

Obligation 34. En répondant "Oui" à la question précédente, vous devez déposer le certificat de marquage CE et le certificat ISO – Preuve à déposer

Obligation 35. Le service comporte-il un ou plusieurs contenus médicaux/de santé ?

- Oui
- Non

Obligation 36. Le service a-t-il fait l'objet d'une évaluation clinique ?

- Oui
- Non

Obligation 37. Le service repose-t-il sur une interprétation de données de santé par des experts ?

- Oui
- Non

Obligation 38. Le service permet-il de réaliser des démarches essentielles de santé ou de vie courante ?

- Oui
- Non

Obligation 39. Le service produit-il des décisions critiques ?

- Oui
- Non

Obligation 40. Le service permet-il la création de compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ?

- Oui
- Non

Obligation 41. Si l'utilisateur ne finalise pas la création de son compte, le service enregistre-t-il les données saisies ?

- Oui
- Non

Obligation 42. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires ?

- Oui
- Non

Obligation 43. Le service valorise-t-il les données collectées (anonymisées ou non, monétisées ou non) sous forme de statistiques, recherches, amélioration du service, marketing etc. ?

- Oui
- Non

Obligation 44. A l'exception de Mon Espace Santé, le service partage-t-il des données recueillies avec d'autres acteurs (ex. partenaires, destinataires, sous-traitants notamment hébergeur...) ?

- Oui
- Non

Obligation 45. Le service limite-t-il des droits RGPD de l'utilisateur ?

- Oui
- Non

Obligation 46. Le service manipule-t-il des données sensibles discriminatoires ?

- Oui
- Non

Obligation 47. Le service intègre-t-il un traitement algorithmique produit par une intelligence artificielle ??

- Oui
- Non

1.2 Questionnaire Interopérabilité

A08.1 Référentiel d'interopérabilité (généralités)

Option A08.1.1 Utilisation et enrichissement du CI-SIS

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Aucun principe d'interopérabilité n'est intégré à la conception du produit.
- Niveau 1 : La conception du produit est faite sans recours systématique aux normes d'interopérabilité proposées par le CI-SIS.
- Niveau 2 : La conception du produit est faite avec le recours systématique aux normes d'interopérabilité proposées par le CI-SIS. Les usages non couverts par le CI-SIS ne sont pas portés à la connaissance de l'ANS et sont mis en œuvre par des développements propriétaires.
- Niveau 3 : La conception du produit est faite avec le recours systématique aux normes d'interopérabilité proposées par le CI-SIS. Les usages non couverts sont systématiquement portés à la connaissance de l'ANS pour améliorer de manière continue le Cadre d'Interopérabilité des SI de santé. Ces usages sont mis en œuvre par développements basés sur les normes d'interopérabilité sur lesquelles s'appuie le CI-SIS.

A08.2 Référentiel d'interopérabilité (modélisation)

Option A08.2.1 Formalisation des usages

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Le produit n'a pas fait l'objet d'une formalisation des usages.
- Niveau 1 : Le produit a fait l'objet d'une formalisation des usages.
- Niveau 2 : Le produit a fait l'objet d'une formalisation des usages et d'une modélisation des processus métier mais sans recherche de mutualisation des concepts avec les autres projets du secteur.
- Niveau 3 : Le produit a fait l'objet d'une formalisation des usages et d'une modélisation des processus métier fondées sur un catalogue de concepts commun au secteur (ex. le MOS pour les concepts non médicaux, OMOP ou HL7 DAM pour les concepts médicaux).

A08.3 Référentiel d'interopérabilité (transport)

Option A08.3.1 Connexion synchrone avec d'autres SI

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Aucun principe d'interopérabilité n'est intégré à la conception du produit.
- Niveau 1 : La conception du produit est faite sans recours systématique aux normes d'interopérabilité proposées par le CI-SIS.
- Niveau 2 : La conception du produit est faite avec le recours systématique aux normes d'interopérabilité proposées par le CI-SIS. Les usages non couverts par le CI-SIS ne sont pas portés à la connaissance de l'ANS et sont mis en œuvre par des développements propriétaires.
- Niveau 3 : La conception du produit est faite avec le recours systématique aux normes d'interopérabilité proposées par le CI-SIS. Les usages non couverts sont systématiquement

portés à la connaissance de l'ANS pour améliorer de manière continue le Cadre d'Interopérabilité des SI de santé. Ces usages sont mis en œuvre par développements basés sur les normes d'interopérabilité sur lesquelles s'appuie le CI-SIS.

A08.4 Référentiel d'interopérabilité (service)

Option A08.4.1 Mise en œuvre interopérable du service Partage de Documents de Santé

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Les usages du produit correspondants au volet Partage de Documents de Santé sont mis en œuvre de manière propriétaire sans rapport avec les spécifications du CI-SIS.
- Niveau 1 : Les usages du produit correspondants au volet Partage de Documents de Santé sont mis en œuvre en utilisant les orientations normatives du CI-SIS sans les suivre rigoureusement.
- Niveau 2 : Les usages du produit correspondants au volet Partage de Documents de Santé sont mis en œuvre avec quelques modifications majeures (ex. extensions spécifiques, nomenclatures propriétaires...) qui font l'objet de demandes d'évolution du CI-SIS.
- Niveau 3 : Les usages du produit correspondants au volet Partage de Documents de Santé sont mis en œuvre sans modification majeure (i.e. sans extension des spécifications).

Option A08.4.6 Mise en œuvre interopérable du service Gestion d'agendas partagés

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Les usages du produit correspondants au volet Gestion d'agendas partagés sont mis en œuvre de manière propriétaire sans rapport avec les spécifications du CI-SIS.
- Niveau 1 : Les usages du produit correspondants au volet Gestion d'agendas partagés sont mis en œuvre en utilisant les orientations normatives du CI-SIS sans les suivre rigoureusement.
- Niveau 2 : Les usages du produit correspondants au volet Gestion d'agendas partagés sont mis en œuvre avec quelques modifications majeures (ex. extensions spécifiques, nomenclatures propriétaires...) qui font l'objet de demandes d'évolution du CI-SIS.
- Niveau 3 : Les usages du produit correspondants au volet Gestion d'agendas partagés sont mis en œuvre sans modification majeure (i.e. sans extension des spécifications).

Option A08.4.8 Mise en œuvre interopérable du service Mesures de santé

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Les usages du produit correspondants au volet Mesures de santé sont mis en œuvre de manière propriétaire sans rapport avec les spécifications du CI-SIS.
- Niveau 1 : Les usages du produit correspondants au volet Mesures de santé sont mis en œuvre en utilisant les orientations normatives du CI-SIS sans les suivre rigoureusement.
- Niveau 2 : Les usages du produit correspondants au volet Mesures de santé sont mis en œuvre avec quelques modifications majeures (ex. extensions spécifiques, nomenclatures propriétaires...) qui font l'objet de demandes d'évolution du CI-SIS.
- Niveau 3 : Les usages du produit correspondants au volet Mesures de santé sont mis en œuvre sans modification majeure (i.e. sans extension des spécifications).

A08.5 Référentiel d'interopérabilité (contenu métier)

Obligation A08.5.01 Partage et/ou échange de documents (producteur de documents CDA) - document structuration minimale

- ✓ Niveau non applicable : Le produit ne crée pas de documents de santé.
- Niveau 0 : Le produit crée des documents santé mais ne peut pas produire de documents CDA (production restreinte aux formats types PDF, Word, TxT ...).
- ✓ Niveau 2 : Le produit crée des documents santé et dispose de capacités de production de documents CDA sans suivre totalement le volet structuration minimale des documents de santé (quel que soit le niveau de structuration du corps du CDA).
- ✓ Niveau 3 : Le produit crée des documents santé et dispose de capacités de production de documents CDA en mettant totalement en œuvre le volet structuration minimale des documents de santé (quel que soit le niveau de structuration du corps du CDA).

Obligation A08.5.23 Partage et/ou échange de documents (consommateur de documents CDA) - structuration minimale

- ✓ Niveau non applicable : Le produit ne consomme aucun document CDA.
- Niveau 0 : Le produit ne dispose pas de capacités d'affichage de documents CDA.
- Niveau 1 : Le produit dispose de capacités d'affichage des corps non structurés des documents CDA, sans capacité de restitution de l'entête ni du corps des documents CDA à corps structuré.
- ✓ Niveau 2 : Le produit dispose de capacités d'affichage des documents CDA (quel que soit le niveau de structuration de leur corps) sans interprétation de leur contenu. Le produit permet également l'enregistrement manuel par l'utilisateur.
- ✓ Niveau 3 : Le produit dispose de capacités d'affichage des documents CDA (quel que soit le niveau de structuration de leur corps) avec interprétation de l'entête CDA pour traitement automatique ou semi-automatique (ex. enregistrement dans le dossier du patient).

A08.6 Référentiel d'interopérabilité (test)

Option A08.6.1 Test des interfaces

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Les interfaces du produit ne sont jamais testées avant mise en ligne.
- Niveau 1 : Les interfaces du produit sont testées manuellement ou avec des outils internes avant mise en ligne.
- Niveau 2 : Les interfaces du produit sont systématiquement testées par des outils de tests externes (ex. Gazelle) avant leur mise en ligne.
- Niveau 3 : Les interfaces du produit sont systématiquement testées par les outils de tests nationaux avant leur mise en ligne.

A10. Terminologies de santé

Option

A10.1 Récupération des nomenclatures sur une source d'autorité et intégration automatique, gestion des mises à jour

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Les listes des codes utilisables sont codées en dur.
- Niveau 1 : Les listes de codes sont gérées comme des paramètres modifiables avec une alimentation manuelle sous un format propriétaire.
- Niveau 2 : Les listes de codes sont gérées comme des paramètres modifiables avec alimentation manuelle via un format standard.
- Niveau 3 : Les listes de codes sont gérées comme des paramètres modifiables avec alimentation via un format standard. Chaque mise à jour est préparée automatiquement et validée humainement avant mise en œuvre.

Option

A10.2 Utilisation des nomenclatures de l'ANS

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Utilisation de nomenclatures locales non mises à disposition par l'ANS.
- Niveau 1 : Utilisation d'une partie des nomenclatures mises à disposition par l'ANS complétées par des codes locaux. Aucune demande de mise à jour n'a été exprimée à l'ANS.
- Niveau 2 : Utilisation des nomenclatures mises à disposition par l'ANS avec définition de JDV si opportun.
- Niveau 3 : Utilisation des nomenclatures mises à disposition par l'ANS avec définition de JDV si opportun. Le cas échéant demande de mise à jour des nomenclatures mises à disposition par l'ANS pour prise en compte des besoins de l'entreprise.

1.3 Questionnaire Urbanisation

A06. Identification électronique des patients, usagers ou personnes

Obligation A06.1 Mise en œuvre de l'INS (référentiel d'identités)

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Le produit n'a pas intégré le téléservice INSi (autorisation CNDA non obtenue, au moins pour la transaction de récupération).
- Niveau 1 : Le produit a intégré le téléservice INSi (autorisation CNDA obtenue, au moins pour la transaction de récupération).
- ✓ Niveau 2 : Le produit a intégré le téléservice INSi (autorisation CNDA obtenue, au moins pour la transaction de récupération) et implémente les identités conformément au guide d'implémentation (a minima, règles de criticité *** du guide) basé sur le référentiel national d'identitovigilance.
- ✓ Niveau 3 : Le produit a intégré le téléservice INSi (autorisation CNDA obtenue, au moins pour la transaction de récupération), implémente les identités conformément au guide d'implémentation (a minima, règles de criticité *** du guide) basé sur le référentiel national d'identitovigilance. Par ailleurs il diffuse les INS qualifiées en aval en respectant les standards d'interopérabilité en vigueur (voir annexe CI-SIS), et notamment dans les documents de santé (CDA, PDF, etc.) éventuellement générés à partir de l'outil.

Obligation A06.2 Mise en œuvre de l'INS (consommation de flux et documents avec l'INS, en provenance d'un domaine d'identification différent)

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Le produit n'est pas en capacité d'intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques.
- ✓ Niveau 1 : Le produit peut intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques.
- ✓ Niveau 2 : Le produit peut intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques et appeler le téléservice INSi pour les vérifier lorsque c'est nécessaire* (autorisation CNDA obtenue, au moins pour la transaction de vérification).
- ✓ Niveau 3 : Le produit peut intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques et appeler le téléservice INSi pour les vérifier lorsque c'est nécessaire* (autorisation CNDA obtenue, au moins pour la transaction de vérification). Par ailleurs le produit sait diffuser les INS qualifiés en aval en respectant les standards d'interopérabilité en vigueur, et notamment dans les documents de santé (CDA, PDF, etc.) éventuellement générés à partir du produit.

Obligation A06.3 Mise en œuvre de l'INS (consommation de flux et documents avec l'INS, en provenance du même domaine d'identification)

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Le produit n'est pas en capacité d'intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques.

- ✓ Niveau 1 : Le produit peut intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques.
- ✓ Niveau 3 : Le produit peut intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques. Par ailleurs le produit sait diffuser les INS qualifiés en aval en respectant les standards d'interopérabilité en vigueur, et notamment dans les documents de santé (CDA, PDF, etc.) éventuellement générés à partir du produit.

A18. Télésanté

Option A18.2 Référentiel télémédecine – Téléexpertise

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : La conception du produit a été faite sans tenir compte du référentiel fonctionnel de téléexpertise.
- Niveau 2 : La conception du produit a tenu compte du référentiel fonctionnel de téléexpertise.
- Niveau 3 : La conception du produit a tenu compte du référentiel fonctionnel de téléexpertise et respecte la totalité des exigences obligatoires du référentiel (exigences de type "DOIT").

1.4 Questionnaire Maturité Sécurité

01. Gouvernance SSI

Obligation 01.01 - Désignation des acteurs responsables du suivi et maintien des mesures de sécurité

- Niveau non applicable : Toujours applicable
- Niveau 0 : Dans l'équipe en charge du produit, les responsables de la sécurité et les personnes responsables de la mise en place et du suivi des mesures de sécurité ne sont pas officiellement définis et nommés.
- ✓ Niveau 1 : Dans l'équipe en charge du produit, des responsables de la sécurité sont identifiés et leurs responsabilités couvrent les activités de conception, de développement, d'installation, d'exploitation, d'administration et de maintenance (selon le périmètre dont le fournisseur du produit a la responsabilité vis à vis de la structure utilisatrice).
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Pour chacun de ces acteurs, un suppléant est identifié pour le remplacer en cas d'absence, et dispose des connaissances et des droits nécessaires afin d'assurer la suppléance.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Pour chaque mesure de sécurité prévue est identifié un responsable qui doit s'assurer de sa bonne mise en place et de son fonctionnement effectif.

Obligation 01.02.01 - Organisation et processus de la sécurité

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Il n'est pas mené de comité de pilotage de la sécurité.
- ✓ Niveau 1 : Des comités de pilotage de la sécurité sont réalisés de façon ad-hoc (ou le sujet est intégré dans la comitologie des différentes activités assurées par l'industriel). Ces comités réunissent des représentants de l'ensemble des acteurs participant aux activités de conception, de développement, d'installation, d'exploitation, d'administration et de maintenance (selon le périmètre dont l'industriel a la responsabilité vis à vis de la structure utilisatrice). À la suite de chaque réunion, un compte-rendu est réalisé et partagé à l'ensemble des acteurs concernés.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les comités de pilotage de la sécurité sont réalisés de manière régulière.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Des tableaux de bord d'indicateurs sont présentés et rassemblent l'ensemble des indicateurs techniques et fonctionnels pour chaque activité assurée.

Obligation 01.02.02 - Organisation et processus de la sécurité

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Il n'est pas mené de comité de pilotage de la sécurité.
- Niveau 1 : Des comités de pilotage de la sécurité sont réalisés de façon ad-hoc (ou le sujet est intégré dans la comitologie des différentes activités assurées par l'industriel). Ces comités réunissent des représentants de l'ensemble des acteurs participant aux activités de conception, de développement, d'installation, d'exploitation, d'administration et de

maintenance (selon le périmètre dont l'industriel a la responsabilité vis à vis de la structure utilisatrice). À la suite de chaque réunion, un compte-rendu est réalisé et partagé à l'ensemble des acteurs concernés.

- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les comités de pilotage de la sécurité sont réalisés de manière régulière.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Des tableaux de bord d'indicateurs sont présentés et rassemblent l'ensemble des indicateurs techniques et fonctionnels pour chaque activité assurée.

Obligation **01.03 - Processus d'amélioration continue**

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun processus d'amélioration continue n'est mis en œuvre.
- Niveau 1 : Un processus d'amélioration continue est mis en œuvre. Cependant, ce processus n'est pas documenté.
- ✓ Niveau 2 : Un processus d'amélioration continue est mis en œuvre lors de tout le cycle de vie du produit. Le processus est documenté (ex : Plan d'Amélioration Continue de la Sécurité) et régulièrement mis à jour. Les actions d'amélioration sont suivies. Cependant, aucun audit organisationnel n'est réalisé afin d'auditer le processus.
- ✓ Niveau 3 : Un processus d'amélioration continue est mis en œuvre sur tout le cycle de vie du produit. Un audit organisationnel est réalisé annuellement afin d'évaluer le processus. Les actions d'amélioration, que ce soit sur l'organisation ou l'efficacité des mesures de sécurité mises en place sont tracées et suivies.

Obligation **01.04.01 - Sensibilisation des équipes en charge**

- Niveau non applicable : Toujours applicable
- Niveau 0 : Aucune sensibilisation n'est mise en place au sein des équipes en charge des activités de conception, de développement, d'installation, d'administration et de maintenance (selon le périmètre dont l'industriel a la responsabilité vis à vis de la structure utilisatrice).
- ✓ Niveau 1 : Une sensibilisation générale aux risques est réalisée pour l'ensemble des équipes (portant sur les enjeux et les risques). Si le produit est destiné à traiter des données à caractère personnel, voire des données de santé, la sensibilisation intègre notamment les obligations et règles de comportement spécifiques à ce sujet.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : La bonne appropriation du sujet par les acteurs est mesurée. La sensibilisation est renouvelée régulièrement. La participation de chaque acteur est tracée.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : La sensibilisation intègre un volet spécifique aux activités de chaque équipe (enjeux/risques/ procédures SSI spécifiques).

Obligation **01.04.02 - Sensibilisation des équipes en charge**

- Niveau non applicable : Toujours applicable
- Niveau 0 : Aucune sensibilisation n'est mise en place au sein des équipes en charge des activités de conception, de développement, d'installation, d'administration et de maintenance (selon le périmètre dont l'industriel a la responsabilité vis à vis de la structure utilisatrice).

- Niveau 1 : Une sensibilisation générale aux risques est réalisée pour l'ensemble des équipes (portant sur les enjeux et les risques). Si le produit est destiné à traiter des données à caractère personnel, voire des données de santé, la sensibilisation notamment intègre les obligations et règles de comportement spécifiques à ce sujet.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : La bonne appropriation du sujet par les acteurs est mesurée. La sensibilisation est renouvelée régulièrement. La participation de chaque acteur est tracée.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : La sensibilisation intègre un volet spécifique aux activités de chaque équipe (enjeux/risques/ procédures SSI spécifiques).

Option 01.05 - Certification ISO 27001 si le critère apparaît

- Niveau non applicable : Toujours applicable
- Niveau 0 : L'industriel n'applique pas, ou de manière accessoire, les standards de la série ISO 2700x au périmètre incluant les SI utilisés pour ses différentes activités liées au produit (selon le cas : développement, distribution, gestion des mises à jour, tests, hébergement et exploitation, administration système, applicative et sécurité, maintenance ou administration à distance, ...).
- Niveau 1 : L'industriel ne s'est pas engagé dans le processus de certification ISO 27001, mais se conforme autant que possible à la norme ISO 27001 sur un périmètre incluant les SI utilisés pour ses différentes activités liées au produit (selon le cas : développement, distribution, gestion des mises à jour, tests, hébergement et exploitation, administration système, applicative et sécurité, maintenance ou administration à distance, ...).
- Niveau 2 : L'industriel s'est engagé dans le processus de certification ISO 27001 sur un périmètre incluant les SI utilisés pour ses différentes activités liées au produit.
- Niveau 3 : L'industriel dispose de la certification ISO 27001 sur un périmètre incluant les SI utilisés pour ses différentes activités liées au produit.

02. Dossier sécurité

Obligation 02.02.01 - Analyse de risques et certification de sécurité

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune analyse de risques formelle n'a été réalisée pour le produit.
- ✓ Niveau 1 : Une analyse des risques a été réalisée. Cependant, la couverture des risques par des mesures n'a pas été évaluée et les risques résiduels n'ont pas été identifiés.
- ✓ Niveau 2 : Une analyse des risques a été réalisée avec une méthode conforme à l'ISO 27005. Des mesures de maîtrise des risques sont définies et mises en œuvre dans le produit. Le niveau de risque résiduel est évalué. La documentation de ces risques résiduels est mise à disposition de la structure utilisatrice. Des préconisations de mesures de maîtrise des risques complémentaires sont définies à l'attention de la structure utilisatrice. La revue de l'analyse de risques en cas de changement majeur est systématique.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Le produit a fait l'objet d'une certification de sécurité délivrée sous le contrôle d'une autorité étatique (ex : CSPN délivrée par l'ANSSI), et cette certification fait l'objet d'un renouvellement à chaque évolution majeure du produit.

Obligation 02.02.02 - Analyse de risques et certification de sécurité

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune analyse de risques formelle n'a été réalisée pour le produit.
- Niveau 1 : Une analyse des risques a été réalisée. Cependant, la couverture des risques par des mesures n'a pas été évaluée et les risques résiduels n'ont pas été identifiés.
- ✓ Niveau 2 : Une analyse des risques a été réalisée avec une méthode conforme à l'ISO 27005. Des mesures de maîtrise des risques sont définies et mises en œuvre dans le produit. Le niveau de risque résiduel est évalué. La documentation de ces risques résiduels est mise à disposition de la structure utilisatrice. Des préconisations de mesures de maîtrise des risques complémentaires sont définies à l'attention de la structure utilisatrice. La revue de l'analyse de risques en cas de changement majeur est systématique.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Le produit a fait l'objet d'une certification de sécurité délivrée sous le contrôle d'une autorité étatique (ex : CSPN délivrée par l'ANSSI), et cette certification fait l'objet d'un renouvellement à chaque évolution majeure du produit.

Obligation 02.03.01 - Plan d'Assurance Sécurité

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune exigence de sécurité n'a été définie pour le produit ni pour son environnement de mise en œuvre.
- ✓ Niveau 1 : Des exigences de sécurité ont été définies pour le produit mais les mesures découlant de ces exigences n'ont pas toutes été implémentées.
- ✓ Niveau 2 : Des exigences de sécurité ont été définies et documentées pour le produit. Les mesures découlant de ces exigences ont été mises en œuvre. Cependant, les exigences ne sont pas mises à jour ou les mesures remises en question (pas de mise à jour du Plan d'Assurance Sécurité du produit). Des exigences de sécurité et des propositions de mesures de sécurité correspondantes ont également été définies, à l'attention de la structure utilisatrice, pour l'environnement de mise en œuvre du produit, aussi bien au niveau logique que physique.
- ✓ Niveau 3 : Des exigences de sécurité ont été définies et documentées pour le produit. Les mesures découlant de ces exigences ont été mises en œuvre. Des exigences de sécurité et des propositions de mesures de sécurité correspondantes ont également été définies, à l'attention de la structure utilisatrice, pour l'environnement de mise en œuvre du produit. Une revue est réalisée lors de toute évolution majeure du produit et au moins annuellement : les exigences sont mises à jour (notamment en fonction de l'évolution de l'analyse de risques) et les mesures de sécurité corrigées (en fonction des résultats d'audit ou des retours d'expérience d'incident).

Obligation 02.03.02 - Plan d'Assurance Sécurité

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune exigence de sécurité n'a été définie pour le produit ni pour son environnement de mise en œuvre.
- Niveau 1 : Des exigences de sécurité ont été définies pour le produit mais les mesures découlant de ces exigences n'ont pas toutes été implémentées.
- ✓ Niveau 2 : Des exigences de sécurité ont été définies et documentées pour le produit. Les mesures découlant de ces exigences ont été mises en œuvre. Cependant, les exigences ne

sont pas mises à jour ou les mesures remises en question (pas de mise à jour du Plan d'Assurance Sécurité du produit). Des exigences de sécurité et des propositions de mesures de sécurité correspondantes ont également été définies, à l'attention de la structure utilisatrice, pour l'environnement de mise en œuvre du produit, aussi bien au niveau logique que physique.

- ✓ Niveau 3 : Des exigences de sécurité ont été définies et documentées pour le produit. Les mesures découlant de ces exigences ont été mises en œuvre. Des exigences de sécurité et des propositions de mesures de sécurité correspondantes ont également été définies, à l'attention de la structure utilisatrice, pour l'environnement de mise en œuvre du produit. Une revue est réalisée lors de toute évolution majeure du produit et au moins annuellement : les exigences sont mises à jour (notamment en fonction de l'évolution de l'analyse de risques) et les mesures de sécurité corrigées (en fonction des résultats d'audit ou des retours d'expérience d'incident).

03. Conception sécurisée

Obligation 03.01 - Configuration sécurisée des composants du produit

- Niveau non applicable : Toujours applicable
- Niveau 0 : Aucun durcissement des paramètres ni des configurations des composants (ex : librairies logicielles, système d'exploitation, applications, middleware applicatifs, SGBD, frameworks, équipements réseau...) n'a été réalisé (utilisation majoritaire de configuration par défaut).
- ✓ Niveau 1 : Les paramètres et configurations par défaut (dont les mots de passe par défaut) des composants ont été modifiés. Tous les services non indispensables au produit sont désactivés. Les composants non utilisés dans la mise en œuvre documentée du produit sont supprimés quand c'est possible, ou à défaut désactivés.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Une revue sécurité exhaustive des paramètres et configurations par défaut a été menée. L'ensemble des composants du produit a bénéficié de ce durcissement. Cependant, le durcissement n'est pas revu régulièrement.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Le durcissement est revu régulièrement, notamment à l'occasion des montées de version des composants.

Obligation 03.02 - Antivirus

- Niveau non applicable : Toujours applicable si le critère applicable.
- Niveau 0 : Aucun antivirus n'est intégré, ni prévu d'être intégrable, dans le produit.
- ✓ Niveau 1 : Un antivirus est intégré dans le produit, ou intégrable (par exemple via le protocole ICAP "Internet Content Adaptation Protocol - RFC3507" ou CVP "Content Vectoring Protocol", ou par appel d'exécutable local), afin de contrôler tout fichier reçu au niveau de tout composant permettant l'import de fichier (par téléversement ou autre) susceptible de constituer ou de contenir un malware (virus ou autre). A défaut, dans le cas où les composants recevant les fichiers téléchargés sont fournis sous forme uniquement logicielle, ces composants réagissent de manière appropriée, et sans dysfonctionner, au blocage d'un fichier par l'antivirus présent sur la plateforme qui héberge ces composants. La documentation identifie explicitement les éventuels fichiers faisant légitimement partie du produit mais devant être exclus de toute analyse par antivirus (en cas de risque élevé de faux

positif). Si un antivirus fait partie du produit, les procédures d'exploitation et de mise à jour de l'antivirus sont documentées. Si le produit est fourni sous forme de service, il intègre effectivement la fonction antivirus.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : Si le produit est fourni sous forme de plateforme/appliance, un antivirus contrôle tout fichier présent sur tout équipement informatique constitutif de cette plateforme/appliance et les signatures de virus sont maintenues à jour. La nature de l'antivirus est indiquée dans la description du produit. Si le produit est fourni sous forme de service, le moteur antivirus et les signatures de virus sont maintenues à jour.

Obligation 03.04 - Contrôle des flux réseaux et applicatifs

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le produit (en incluant son environnement d'hébergement) n'intègre pas de dispositif de filtrage au niveau réseau (pare-feu). OU Le produit (en incluant son environnement d'hébergement) n'intègre pas de dispositif de filtrage ni de rupture de protocole au niveau applicatif (proxy).
- ✓ Niveau 1 : Le produit (en incluant son environnement d'hébergement) intègre un dispositif de filtrage au niveau réseau (pare-feu) et un dispositif de filtrage (WAF) et/ou de rupture de protocole (reverse proxy) au niveau des flux applicatifs entrants. Certains services (métier ou techniques) du produit ne sont toutefois pas protégés par l'ensemble de ces dispositifs (quand ils sont applicables). Les bonnes pratiques de configuration standard de ces dispositifs sont appliquées.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Le produit intègre un dispositif de rupture de protocole (proxy) au niveau des flux applicatifs sortants. Tous les services (métier et techniques) du produit sont protégés par l'ensemble de ces dispositifs (quand ils sont applicables). La configuration de ces dispositifs est spécifiquement adaptée au produit.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : L'architecture de filtrage réseau s'appuie sur deux couches de filtrage qui utilisent des solutions de pare-feu différentes : une première couche protège les serveurs frontaux et une deuxième le reste de l'infrastructure. Les règles des différents dispositifs de sécurité sont mises à jour régulièrement et font l'objet d'une revue au moins annuelle.

Obligation 03.05 - Développement sécurisé

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun standard de développement et de configuration sécurisés ou guide de bonnes pratiques n'a été défini ou suivi.
- ✓ Niveau 1 : Un standard ou guide de bonnes pratiques est défini et suivi lors de la réalisation du produit.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Des outils sont mis en œuvre pour vérifier le respect des règles (outils de qualimétrie, vérification de l'obsolescence des librairies, outils de vérification de la sécurisation de la plateforme système…). Les résultats de ces vérifications concernant la sécurité donnent lieu à un plan d'actions en vue de leur correction. Le plan d'action est pris en compte par les développeurs, et cette prise en compte fait l'objet d'un suivi. Les composants utilisés et issus de tiers sont sélectionnés en tenant compte du respect de bonnes pratiques similaires par ces tiers.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : Une revue de code par les pairs est intégrée dans le processus de développement et de maintenance, de sorte que chaque modification de code est vérifiée par au moins un second développeur afin de garantir sa qualité.

Obligation 03.06 - Protection des développements

- Niveau non applicable : Toujours applicable si le critère est applicable
- Niveau 0 : Aucune mesure visant spécifiquement à empêcher ou à détecter toute introduction de code malveillant dans le produit n'est mise en place.
- ✓ Niveau 1 : Au sein de l'organisation qui assure le développement du produit, seules les personnes en charge de produire ou modifier le logiciel sont effectivement autorisées à modifier le code du produit au sein du SI de développement.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Le processus de revue de tout code modifié est incontournable, par exemple par la mise en œuvre d'un dépôt de code où tout code modifié est automatiquement identifié comme tel, et ne peut être intégré à une nouvelle version du produit destinée à être diffusée qu'après une validation explicite par une personne spécifiquement autorisée à accomplir cette tâche. La mise à disposition du produit à de la structure utilisatrice est effectué dans un cadre fixé, documenté et sécurisé
- ✓ Niveau 3 : Conforme au niveau précédent, plus : L'intégrité des logiciels utilisés dans la chaîne de développement et les droits d'accès aux exécutables de ces logiciels font l'objet de vérification avant tout assemblage final du produit. L'intégrité des versions mises à disposition est assurée dès leur production par des mécanismes de signature cryptographique, ou à défaut de prise d'empreinte numérique par des mécanismes cryptographiquement valides. Ces informations qui permettent la vérification d'intégrité du produit sont mis à disposition de la structure utilisatrice.

Obligation 03.07 - Architecture sécurisée

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Aucun mécanisme de sécurité réseau n'a été implémenté. L'architecture du produit est du type 1-tier (la base de données, le serveur applicatif, le frontal… sont sur le même serveur).
- ✓ Niveau 1 : L'architecture du produit est de type 3-tiers (un serveur frontal, un middle, et une base de données répartis sur des systèmes distincts). Cependant, toutes ces parties se situent au sein du même sous-réseau et peuvent librement communiquer entre elles.
- ✓ Niveau 2 : Les différents tiers du produit sont séparés (base de données, middle, frontal…). Ils se situent au sein de différents sous-réseaux. Seuls les flux requis sont ouverts afin que les tiers puissent communiquer entre eux.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Un réseau d'administration séparé est mis en œuvre afin d'exploiter et superviser le service.

Obligation 03.08 - Contrôle d'accès au réseau

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun composant du produit connecté au réseau ne dispose de fonction standard d'authentification réseau.
- ✓ Niveau 1 : La majorité des composants du produit connectés au réseau disposent de fonctions standard d'authentification réseau, par exemple par l'utilisation du protocole 802.1X.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les composants utilisés qui ne supportent pas le protocole 802.1X sont affectés à des réseau physiques ou virtuels (VLAN…) dédiés, en fonction de la nature de ces composants et des exigences de sécurité qui leur sont attachées.
- ✓ Niveau 3 : Tous les composants du produit connectés au réseau disposent de fonctions standard d'authentification réseau, par exemple par l'utilisation du protocole 802.1X.

Obligation 03.09 - Environnements

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le produit fourni sous forme de service dispose d'un seul environnement, utilisé pour la production (Prod).
- ✓ Niveau 1 : Le produit fourni sous forme de service dispose de plusieurs environnements (Prod, Préprod, Dev …). Cependant les personnes en charge du produit pour le compte de l'industriel disposent des mêmes droits sur chaque environnement.
- ✓ Niveau 2 : Le produit fourni sous forme de service dispose au minimum de 3 environnements (Prod, Préprod, Dev …). Les personnes en charge du produit pour le compte de l'industriel disposent de droits différents sur chaque environnement. L'environnement de Préprod n'est pas totalement identique à l'environnement de Prod.
- ✓ Niveau 3 : Le produit fourni sous forme de service dispose au minimum de 3 environnements (Prod, Préprod, Dev …). Les personnes en charge du produit pour le compte de l'industriel disposent de droits différents selon les environnements. Ces personnes ne disposent pas de droits sur tous les environnements. Des processus et outils permettent de garantir que les configurations techniques sont identiques sur l'ensemble des environnements. L'environnement de Préprod est identique à l'environnement de Prod. L'environnement de Préprod est utilisé systématiquement pour valider en amont toutes les opérations réalisées sur la production.

Obligation 03.10 - Procédures opérationnelles

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune documentation opérationnelle spécifique au produit n'est fournie à la structure utilisatrice.
- ✓ Niveau 1 : Une documentation de la gestion opérationnelle du produit est formalisée et fournie à la structure utilisatrice.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : la documentation opérationnelle fournie porte au minimum sur les opérations de configuration, d'administration, de sauvegarde/restauration et sur la gestion des incidents.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : la documentation opérationnelle fournie fait l'objet de mises à jour régulières (pour tenir compte des évolutions de la plateforme, en fonction des incidents…).

Obligation 03.11 - Inventaire des composants et des flux

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Il n'est pas établi d'inventaire des composants qui constituent le produit et d'inventaire des flux de données entre les équipements qui constituent le produit et d'inventaire des flux de données qu'il établit entre les équipements qui le constituent et avec d'autres systèmes.
- ✓ Niveau 1 : Il est établi un inventaire des composants qui constituent le produit et un inventaire des flux de données entre les équipements qui constituent le produit et entre ces composants et d'autres systèmes. Toutefois ces inventaires ne sont pas mis à jour à chaque évolution du produit et sont potentiellement inexacts.
- ✓ Niveau 2 : Il est établi un inventaire des composants qui constituent le produit (comprenant les numéros de version et les dates de fin de support pour les composants fournis par des tiers) et un inventaire des flux de données (précisant les protocoles, ports réseau, ... utilisés) entre les équipements qui constituent le produit et entre ces composants et d'autres systèmes. Ces inventaires sont mis à jour à chaque évolution du produit.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : La sensibilité métier (par exemple sur les critères DICT) de chaque composant et de chaque flux est qualifiée.

Obligation 03.12 - Intégrité du produit

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Il n'est pas prévu de mécanisme permettant de vérifier que les composants logiciels installés et la configuration du produit n'ont pas été altérés.
- ✓ Niveau 1 : Il est prévu un mécanisme qui permet de vérifier que les composants logiciels installés et la configuration du produit n'ont pas été altérés de manière accidentelle. Ces mécanismes peuvent être spécifiques au produit ou s'appuyer sur des fonctionnalités de l'environnement requis pour le produit (système d'exploitation...).
- ✓ Niveau 2 : Il est prévu une solution qui permet de vérifier que les composants logiciels installés du produit n'ont pas été altérés de manière accidentelle ou volontaire et non autorisée (altération potentiellement plus élaborée et complexe qu'une altération accidentelle).
- ✓ Niveau 3 : Conforme au niveau précédent, plus : la solution utilisée permet également de vérifier que la configuration du produit n'a pas été altérée de manière accidentelle ou volontaire et non autorisée.

Obligation 03.13.01 - Protection des informations (Cryptographie)

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Certains échanges d'informations sensibles (mot de passe, jeton d'authentification, données à caractère personnel…) ne sont pas chiffrés, ne sont pas soumis à une vérification de leur intégrité ou leur destinataire n'est pas authentifié.
- ✓ Niveau 1 : Les informations sensibles sont toujours protégées pendant les communications sur les canaux publics (Internet) ou externes à la structure utilisatrice : leur

destinataire est authentifié préalablement à l'échange, les données sont chiffrées et leur intégrité est vérifiée.

- ✓ Niveau 2 : Les informations sensibles sont toujours protégées pendant les communications sous tout type de canal interne ou externe : leur destinataire est authentifié préalablement à l'échange, les données sont chiffrées et leur intégrité est vérifiée. A titre d'exception, le chiffrement des données sensibles n'est pas requis dans les cas de communication : avec des périphériques en proximité immédiate des postes de travail où est installé le produit ; avec des dispositifs médicaux communicants ; à condition que les moyens de communication utilisés soient dédiés à cet usage et cheminent et s'étendent exclusivement dans des locaux à accès contrôlé par des moyens physiques (fermeture à clé, par digicode...). Seule une raison majeure peut justifier une exception à ces exigences, et toute exception doit être clairement documentée et justifiée dans la documentation du produit. La documentation du produit explicite ces exigences de sécurité pour la mise en œuvre du produit, à l'attention des structures utilisatrices.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Des mécanismes de protection adaptés aux risques et justifiés sont mis en œuvre, notamment en matière de chiffrement des informations sensibles transmises ou stockées. Les algorithmes de chiffrement, de vérification d'intégrité, et d'authenticité, et plus généralement les mécanismes cryptographiques utilisés et les tailles de clés correspondantes sont à l'état de l'art, conformes aux règles énoncées par le RGS, par les Recommandations de sécurité relatives à TLS (v1.2+) et par le guide des mécanismes cryptographiques (v2.0.4+), publiés par l'ANSSI. Les mécanismes utilisés par le produit sont revus régulièrement pour rester conformes à ces recommandations.

Obligation 03.13.02 - Protection des informations (Cryptographie)

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Certains échanges d'informations sensibles (mot de passe, jeton d'authentification, données à caractère personnel…) ne sont pas chiffrés, ne sont pas soumis à une vérification de leur intégrité ou leur destinataire n'est pas authentifié.
- Niveau 1 : Les informations sensibles sont toujours protégées pendant les communications sur les canaux publics (Internet) ou externes à la structure utilisatrice : leur destinataire est authentifié préalablement à l'échange, les données sont chiffrées et leur intégrité est vérifiée.
- Niveau 2 : Les informations sensibles sont toujours protégées pendant les communications sous tout type de canal interne ou externe : leur destinataire est authentifié préalablement à l'échange, les données sont chiffrées et leur intégrité est vérifiée. A titre d'exception, le chiffrement des données sensibles n'est pas requis dans les cas de communication : avec des périphériques en proximité immédiate des postes de travail où est installé le produit ; avec des dispositifs médicaux communicants ; à condition que les moyens de communication utilisés soient dédiés à cet usage et cheminent et s'étendent exclusivement dans des locaux à accès contrôlé par des moyens physiques (fermeture à clé, par digicode...). Seule une raison majeure peut justifier une exception à ces exigences, et toute exception doit être clairement documentée et justifiée dans la documentation du produit. La documentation du produit explicite ces exigences de sécurité pour la mise en œuvre du produit, à l'attention des structures utilisatrices.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Des mécanismes de protection adaptés aux risques et justifiés sont mis en œuvre, notamment en matière de chiffrement des

informations sensibles transmises ou stockées. Les algorithmes de chiffrement, de vérification d'intégrité, et d'authenticité, et plus généralement les mécanismes cryptographiques utilisés et les tailles de clés correspondantes sont à l'état de l'art, conformes aux règles énoncées par le RGS, par les Recommandations de sécurité relatives à TLS (v1.2+) et par le guide des mécanismes cryptographiques (v2.0.4+), publiés par l'ANSSI. Les mécanismes utilisés par le produit sont revus régulièrement pour rester conformes à ces recommandations.

Obligation 03.14 - Gestions des secrets (clés privées et mots de passe)

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Il n'est pas défini de principe explicite de gestion des secrets pour le produit.
- Niveau 1 : Des principes de gestion des secrets sont explicitement définis pour le produit. Certains secrets utilisés par le produit (clés symétriques, clés privées, mots de passe...) sont conservés en clair dans les fichiers de configuration.
- ✓ Niveau 2 : Des principes de gestion des secrets sont explicitement définis pour le produit. Les clés symétriques et clés privées des certificats sont accessibles uniquement par un compte restreint et privilégié (ex : "root") et uniquement en lecture seule en dehors des opérations de changement de ces secrets. Si des mots de passe sont gérés au sein du produit, ils sont stockés sous une forme qui interdit définitivement d'accéder à leur valeur en clair.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Si des accès sont prévus depuis l'extérieur de la structure qui héberge le produit (Internet, autres tiers), alors : soit un système bastion est mis en place afin de centraliser ces accès par connexions sécurisées depuis l'extérieur et de protéger les secrets utilisés pour les connexions effectives au produit ; soit les clés symétriques et les clés privées utilisées pour ces connexions sont confinées dans un composant sécurisé qui réalise l'ensemble des fonctions cryptographiques mobilisant ces clés et utilisées pour les connexions effectives au produit et dont elles ne peuvent pas être extraites.

Obligation 03.15 - Chiffrement des supports de stockage

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Les supports de stockage données internes à l'équipement mobile ne sont pas tous chiffrés.
- ✓ Niveau 1 : Tous les supports de stockage données internes à l'équipement mobile sont chiffrés.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les clefs de chiffrement sont sous le contrôle exclusif de la structure utilisatrice, soit directement, soit via un logiciel de gestion des équipements mobiles.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Des mécanismes conformes au RGS et au guide des mécanismes cryptographiques (v2.0.4+), publié par l'ANSSI sont mis en œuvre à cette fin. Les mécanismes utilisés par le produit sont revus régulièrement pour rester conformes à ces recommandations.

Obligation 03.16 - Connectivité Wifi

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : La documentation du produit ne précise pas les modalités techniques de connectivité sans fil par Wifi.
- Niveau 1 : Les équipements mobiles du produit ne disposent pas de protocole sécurisé Wifi à l'état de l'art pour communiquer. Une description des niveaux de sécurité supportés et des compléments de sécurisation possibles est toutefois fournie à la structure utilisatrice pour permettre l'évaluation d'un mode de prise en charge acceptable de la sécurité.
- ✓ Niveau 2 : L'authentification des utilisateurs, l'intégrité et la confidentialité des données échangées par Wifi avec les équipements mobiles du produit sont assurées par la mise en œuvre de mécanismes s'appuyant sur le mode WPA2-PSK (WPA2-Personnel) avec utilisation de l'algorithme de chiffrement AES-CCMP. La clé de sécurité pour WPA2 est conforme aux règles d'élaboration de mots de passe non triviaux et changée dès l'installation puis régulièrement. Si un point d'accès Wifi fait partie du produit, il est conforme au Guide pratique technique pour la mise en place d'un accès Wifi de la PGSSI-S. NB : le mode WPA2-PSK n'est acceptable que dans la mesure où les flux applicatifs sensibles sont chiffrés, conformément à l'objectif fixé sur ce point dans le critère relatif à la protection des informations.
- ✓ Niveau 3 : L'authentification des utilisateurs, l'intégrité et la confidentialité des données échangées par Wifi avec les équipements mobiles du produit sont assurées par la mise en œuvre de mécanismes s'appuyant sur la norme WPA2-entreprise (standard 802.1X et protocole EAP, idéalement EAP-TLS) ou ultérieurs garantissant le plus haut niveau de sécurité (version de la norme IEEE 802.11i certifiée par la Wifi Alliance), avec utilisation de l'algorithme de chiffrement AES-CCMP.

Obligation 03.17 - Application de la réglementation relative aux dispositifs médicaux

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Les exigences de sécurité et les exigences d'évaluation de la conformité du produit fixées par les Règlements (UE) 2017/745 et 2017/746 (selon la nature du dispositif) n'ont pas été prises en compte.
- ✓ Niveau 2 : Les exigences de sécurité fixées par les Règlements (UE) 2017/745 et 2017/746 (selon la nature du dispositif) ont été prise en comptes pour le produit. Le processus d'évaluation de la conformité du produit aux exigences fixées par les Règlements (UE) 2017/745 et 2017/746 (selon la nature du dispositif) est en cours, dans le respect des exigences d'évaluation fixées par ce même règlement.
- ✓ Niveau 3 : Les exigences de sécurité fixées par les Règlements (UE) 2017/745 et 2017/746 (selon la nature du dispositif) ont été prises en compte pour le produit. Le processus d'évaluation de la conformité du produit aux exigences fixées par les Règlements (UE) 2017/745 et 2017/746 (selon la nature du dispositif) a été mené à son terme dans le respect des exigences d'évaluation fixées par ce même règlement. L'industriel dispose pour le produit de la déclaration de conformité UE et/ou des certificats de conformités établis comme requis par les Règlements (UE) 2017/745 et 2017/746 (selon la nature du dispositif) et en cours de validité.

04. Identification, authentification et autorisations

Obligation 04.01 - Utilisation et mise à jour des identités nationales des acteurs de santé personnes physiques

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le service n'a pas la capacité d'identifier les acteurs de santé à l'aide de l'identité nationale (RPPS, et ADELI en transitoire) ou d'une identité locale (matricule RH, etc.).
- Niveau 1 : Le service peut identifier les acteurs de santé à l'aide de l'identité nationale (RPPS, et ADELI en transitoire) ou d'une identité locale (matricule RH, etc.). Ces identités sont modifiables avec un processus de gestion documenté.
- ✓ Niveau 2 : Le service identifie les acteurs de santé au moins à l'aide de l'identité nationale (RPPS, et ADELI en transitoire), lorsque l'acteur en dispose. Ces identités sont modifiables avec un processus de gestion documenté.
- ✓ Niveau 3 : Le service identifie les acteurs de santé au moins à l'aide de l'identité nationale (RPPS, et ADELI en transitoire), lorsque l'acteur en dispose. Ces identités sont modifiables avec un processus de gestion documenté, systématisant les recherches/vérifications au répertoire de référence (RPPS) et limitant les modifications à des attributs absents de l'identité nationale telle que visible sur l'annuaire santé et les autres couches d'exposition du RPPS. Les vérifications sur les couches d'exposition du RPPS (import de fichiers plats, interfaces de programmation, etc.) sont effectuées à échéance régulière ou à l'occasion de transactions effectuées par les utilisateurs concernés (identification électronique, etc.), dans le respect des exigences réglementaires.

Obligation 04.02 - Niveau de garantie de l'identification électronique des acteurs de santé personnes physiques

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le service n'a pas mis en œuvre une identification électronique basée sur un moyen d'identification électronique de transition (toléré jusqu'au 1.1.2026) tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des acteurs de santé personnes physiques.
- ✓ Niveau 1 : Le service a mis en œuvre une identification électronique basée sur un moyen d'identification électronique de transition (toléré jusqu'au 1.1.2026) tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des acteurs de santé personnes physiques.
- ✓ Niveau 3 : Le service a mis en œuvre exclusivement Pro Santé Connect (Web et/ou CIBA) et/ou une identification électronique basée sur une carte de la famille CPx et/ou une identification électronique au moins conforme au niveau eIDAS substantiel tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des acteurs de santé personnes physiques, avec une certification ANSSI permettant de l'attester et/ou une identification électronique basée sur un moyen d'identification électronique homologué conformément à ce qui est défini dans le référentiel de la PGSSI-S sur l'identification électronique des acteurs de santé personnes physiques.

Obligation 04.03 - Niveau de garantie de l'identification électronique des patients ou usagers

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le service a mis en œuvre une identification électronique non conforme au minimum requis (moyens d'identification électronique de transition tolérés jusqu'au 1.1.2026 et/ou de niveau eIDAS substantiel à élevé) tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des patients.
- ✓ Niveau 1 : Le service a mis en œuvre une identification électronique basée a minima sur un moyen d'identification électronique de transition (toléré jusqu'au 1.1.2026) tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des patients.
- ✓ Niveau 3 : Le service a mis en œuvre une identification électronique au moins conforme au niveau eIDAS substantiel tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des patients, avec une certification ANSSI permettant de l'attester.

Obligation 04.04 - Documentation de la procédure d'autorisation (ajout, modification, suppression)

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune procédure de gestion des autorisations des utilisateurs du produit n'est documentée.
- Niveau 1 : Les procédures de gestion des autorisations des utilisateurs du produit sont documentées.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Ces procédures incluent une procédure d'extraction de la liste des utilisateurs et des autorisations qui leurs ont été attribuées, afin d'en permettre la revue régulière.

Obligation 04.05 - Gestion et séparation des droits

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune séparation des droits n'est implémentée dans le produit.
- Niveau 1 : Une séparation des droits est assurée dans le produit. En particulier, les autorisations d'administration technique du produit sont distinctes des autorisations métier (i.e. un administrateur technique n'a pas automatiquement accès aux fonctions et informations métier)
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les autorisations peuvent être gérées par profils, et les utilisateurs par groupes.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Les autorisations contrôlant la gestion des autorisations et celles contrôlant la gestion des traces constituent chacune des autorisations distinctes de toutes les autres. Une séparation entre des autorisations potentiellement incompatibles entre elles (ex : "demandeur" et "validateur") est mise en place pour les processus métier qui le justifient, ou il a été vérifié qu'il n'existait pas de telles autorisations potentiellement incompatibles entre elles.

Obligation 04.06 - Comptes génériques

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Des comptes génériques existent (comptes prédéfinis lors de la conception du produit, nécessaires au fonctionnement, à l'exploitation ou au dépannage du produit et disposant d'autorisations fixes prédéfinies). Ces comptes peuvent être utilisés directement par des utilisateurs (au sens large) pour se connecter à la solution.
- ✓ Niveau 1 : Conforme au niveau précédent, plus : Tous les comptes génériques sont répertoriés et documentés. Chaque compte générique peut être désactivé et son mot de passe modifié par configuration du produit. Le produit permet que des mots de passe "complexes" soient configurés pour ces comptes génériques, et à ce titre permet des mots de passe composés d'au moins 20 caractères alphanumériques et spéciaux.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les comptes génériques ne servent qu'à attribuer temporairement des privilèges spécifiques, que ce soit pour des processus internes à la solution ou pour des opérations à accès restreint réalisées ponctuellement par certains utilisateurs. Ces comptes ne peuvent pas être utilisés directement pour se connecter au produit (pas de "login" possible) et ne peuvent être "endossés" (ex: "RUNAS", "sudo"...) que de manière temporaire, à la demande, par les seuls utilisateurs autorisés.
- ✓ Niveau 3 : Le produit ne possède pas de compte générique.

Obligation 04.08 - Utilisation et mise à jour des identités nationales des acteurs de santé personnes morales

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le produit n'a pas la capacité d'identifier les acteurs de santé personnes morale à l'aide d'une identité nationale (FINESS juridique, FINESS géographique, SIREN ou SIRET).
- Niveau 2 : Le produit identifie les acteurs de santé personnes morales à l'aide d'une identité nationale conforme au référentiel d'identification électronique des acteurs de santé personnes morales de la PGSSI-S. Ces identités sont modifiables via un processus de gestion documenté.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Le processus de gestion documenté systématise les recherches/vérifications au répertoires de référence et limite les modifications à des attributs absents de l'identité nationale telle que visible sur l'annuaire santé et les autres couches d'exposition des répertoires FINESS et SIREN. Les vérifications sur ces couches d'exposition sont effectuées à échéance régulière ou à l'occasion de transactions effectuées par les utilisateurs concernés (identification électronique, etc.), dans le respect des exigences réglementaires applicables.

Obligation 04.09 - Niveau de garantie de l'identification électronique des acteurs de santé personnes morales

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le produit ne met pas en œuvre d'identification électronique de ses utilisateurs acteurs de santé personnes morales.
- Niveau 1 : Le produit assure l'identification électronique de ses utilisateurs acteurs de santé personnes morales, mais il ne permet pas à la structure utilisatrice d'être conforme aux exigences du référentiel d'identification électronique des acteurs de santé personnes morales de la PGSSI-S.
- ✓ Niveau 2 : Le produit assure l'identification électronique de ses utilisateurs acteurs de santé personnes morales, et il permet à la structure utilisatrice d'être conforme aux

exigences du référentiel d'identification électronique des acteurs de santé personnes morales de la PGSSI-S. Notamment, si le produit est susceptible d'être mise en œuvre dans le cadre de services numériques partagés, il permet l'authentification des acteurs de santé personnes morales par des certificats émis par l'IGC Santé. Dans le cas où le produit comporte un service SaaS, il est mis en œuvre de façon conforme au référentiel d'identification électronique des acteurs de santé personnes morales de la PGSSI-S, notamment en ce qui concerne le type de moyen d'identification électronique utilisé.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : Dans le cas où le produit comporte un service SaaS qui entre dans le cadre de services numériques partagés, l'identification électronique est exclusivement basée sur des certificats d'authentification de personne morale émis par l'IGC Santé.

06. Sécurité physique

Obligation 06.01 - Contrôle d'accès physique aux équipements informatiques

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun contrôle d'accès physique aux équipements informatiques n'est mis en œuvre.
- Niveau 1 : Un contrôle d'accès physique aux locaux informatiques est mis en œuvre. L'accès en est réservé aux personnes habilitées.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Des moyens sont mis en œuvre afin d'interdire aux personnes non autorisées d'accéder aux locaux hébergeant des équipements informatiques, en fonction de la nature des équipements hébergés (équipements utilisateurs, serveurs, infrastructure réseau...). Les équipements sensibles (serveurs, infrastructure...) sont eux-mêmes hébergés dans des racks fermés à clé. Le contrôle d'accès est nominatif et fait l'objet d'une journalisation. Les autorisations d'accès font l'objet d'une revue régulière, et au moins tous les 2 ans.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Un système de vidéosurveillance permet de surveiller l'accès aux équipements informatiques.

07. Audit

Obligation 07.01 - Réalisation d'audits de code

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun audit de code n'est réalisé sur le produit.
- Niveau 1 : Un audit de code est réalisé avant la validation de la version initiale du produit. Le périmètre de cet audit doit au minimum inclure le code qui assure : le traitement des données en entrée, le traitement de données en sorties, les fonctions de sécurité, telles qu'authentification, gestion de session, contrôle d'accès, fonctions cryptographiques, gestion des clés et aux secrets... Les vulnérabilités, erreurs et non-conformités aux règles de développement en vigueur identifiées donnent lieu à un plan d'actions en vue de leur correction.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Un audit de code est réalisé sur le produit de manière au minimum annuelle. Au sein du périmètre défini au niveau précédent, cet audit porte au minimum sur les parties du code modifiées depuis le dernier audit et sur celles susceptibles d'être impactées par ces modifications.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : Un audit de code est réalisé avant toute validation de changement majeur dans le produit. Au sein du périmètre défini aux niveaux précédents, cet audit porte au minimum sur les parties du code modifiées depuis le dernier audit et sur celles susceptibles d'être impactées par ces modifications.

Obligation 07.02 - Recherche de vulnérabilités

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun test d'intrusion ni test de vulnérabilité n'a été réalisé sur le produit.
- Niveau 1 : Des scanners de vulnérabilité auditent l'ensemble des composants du produit avant tout mise à disposition d'une nouvelle version. Les vulnérabilités identifiées donnent lieu à un plan d'actions en vue de leur correction.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Un test d'intrusion est également réalisé sur le produit de manière au minimum annuelle. La présence de vulnérabilité majeure, identifiée par un scanner ou par test d'intrusion, bloque la mise à disposition de la nouvelle version et déclenche un nouveau cycle de développement à fin de correction. La liste des vulnérabilités résiduelles et de leurs impacts est mise à disposition des RSSI des structures utilisatrices. En cas de détection de vulnérabilité majeure sur une version existante du produit, les RSSI des structures utilisatrices sont immédiatement alertés et des mesures palliatives à appliquer dans l'attente d'un correctif leur sont communiquées dans les meilleurs délais.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Un test d'intrusion est également réalisé sur le produit avant toute mise à disposition de nouvelle version comportant des évolutions majeures.

Obligation 07.04 - Plan d'actions

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Il n'est pas systématiquement établi de plan d'actions particulier suite à l'identification de failles de sécurité dans le produit.
- Niveau 1 : Un plan d'actions est défini et appliqué pour toute faille de sécurité affectant le produit, quelle que soit l'origine de l'identification de cette faille (test d'intrusion, audit ou revue de code, audit ou revue de configuration, outil de vérification automatisée, notification de faille de sécurité dans un composant utilisé...). Ce plan d'actions comporte au minimum les éléments suivants : Date initiale de l'action, Nom du responsable de l'action, Description de l'action, Date de correction. En cas d'identification de faille de sécurité grave dans le produit, la structure utilisatrice en est notifiée dans les plus bref délais, et des mesures palliatives lui sont communiquées dès que possible, dans l'attente de la mise à jour du produit.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Pour la correction de failles de sécurité qui concernent une version en production du produit (i.e. utilisée par des structures utilisatrices), le plan d'actions respecte les délais maxima de correction suivants :
  Score CVSS supérieur à 8 : 48h
  Score CVSS à 6 ou 7 : 2 semaines
  Score CVSS inférieur à 6 : 1 mois
- ✓ Niveau 3 : Conforme au niveau précédent, plus : À la suite des corrections, une procédure de vérification est appliquée afin de confirmer l'effectivité et l'efficacité de la correction.

08. Maintien en condition de sécurité

Obligation 08.02 - Veille et patch management

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Ni veille, ni processus de patch management n'est défini et mis en œuvre concernant les composants du produit fournis à l'industriel par des tiers, les plateformes avec lesquelles le produit est réputé compatible, ou les vulnérabilités génériques susceptibles d'affecter le produit.
- ✓ Niveau 1 : Un processus de veille sur les vulnérabilités des composants du produit fournis à l'industriel par des tiers, et d'application des patchs ou des mises à jour de ces composants est défini et appliqué. Dans le cas de produits de type logiciel ou plateforme, ces mises à jour donnent lieu à la mise à disposition d'une nouvelle version du produit, et la structure utilisatrice en est notifiée. En cas de vulnérabilité grave, la structure utilisatrice en est notifiée dans les plus bref délais, et des mesures palliatives lui sont communiquées dès que possible, dans l'attente de la mise à jour du produit.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Si le produit requiert pour son fonctionnement un environnement technique particulier qui ne fait pas partie de ses composants (ex : un système d'exploitation, un système de gestion de base de données...), un processus de veille sur les mises à jour de cet environnement est défini et appliqué. Le produit est testé avec toute mise à jour standard de cet environnement. Dans le cas de produits de type logiciel ou plateforme, en cas de dysfonctionnement du produit lié à une mise à jour de cet environnement, la structure utilisatrice en est informée, et des mesures palliatives lui sont communiquées si elles existent. Une nouvelle version du produit compatible avec la mise à jour de l'environnement est mise à disposition dans les meilleurs délais.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Un processus d'industrialisation du patch management est mis en œuvre. Il permet de patcher et de tester le produit afin de s'assurer de son bon fonctionnement avec toutes les évolutions appliquées. Dans le cas de produits de type logiciel ou plateforme, le produit requiert pour son fonctionnement un environnement technique particulier, un tableau de bord accessible à la structure utilisatrice lui permet de consulter la compatibilité explicite du produit avec les différents patchs ou versions de l'environnement de fonctionnement du produit.

Obligation 08.03 - Gestion de l'obsolescence

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun processus de gestion de l'obsolescence n'est défini et appliqué concernant les composants du produit fournis à l'industriel par des tiers et les plateformes avec lesquelles le produit est réputé compatible (dans le cas de produits de type logiciel ou plateforme/appliance) ou sur lesquelles le produit est effectivement exploité (dans le cas de produits de type service).
- ✓ Niveau 1 : Les composants fournis à l'industriel par des tiers sont remplacés dans le produit quand ils ont atteint leur fin de support par leur éditeur/fabriquant. Le produit est adapté à une version de son environnement (ex: système d'exploitation, base de données...) supportée par son éditeur/fabriquant quand la version actuelle atteint sa fin de support.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Le remplacement des composants et l'adaptation du produit à une version supportée de son environnent de fonctionnement sont

effectués au moins 6 mois avant la fin de support annoncée pour ces éléments. Dans le cas de produits de type logiciel ou plateforme, la structure utilisatrice est informée dans le même délai de cette évolution, ainsi que de la procédure spécifique de migration associée en ce qui concerne le produit s'il y a lieu.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : Le remplacement des composants et l'adaptation du produit à une version supportée de son environnent de fonctionnement sont effectués au moins 1 an avant la fin de support annoncée pour ces éléments.

Obligation 08.04 - Mécanismes de supervision du fonctionnement et de la sécurité (Nagios, SIEM...)

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun mécanisme (ou ensemble de mécanismes) de supervision du produit, couvrant la supervision du fonctionnement et la supervision de la sécurité, n'a été implémenté.
- Niveau 1 : Des mécanismes de supervision du fonctionnement et de supervision de la sécurité sont mis en œuvre au sein du produit et couvrent l'intégralité du produit.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Une procédure de traitement des alertes est mise en place. Suite à ce traitement d'alerte, la procédure de gestion des incidents peut être activée afin de réagir à l'alerte.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Un responsable de la supervision et son suppléant sont identifiés et garants du traitement des alertes.

Obligation 08.05.01 - Politique de gestion des changements

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune politique de gestion des changements n'est définie et mise en œuvre.
- ✓ Niveau 1 : Une politique de gestion des changements est définie et mise en œuvre mais elle ne couvre pas l'intégralité des points suivants :
  La politique de gestion des changements doit faire partie de la documentation opérationnelle ;
  La procédure à suivre doit être définie et un comité d'approbation des changements doit être nommé ;
  Le suivi des changements doit être assuré dans un fichier qui peut être un simple tableur. Ce fichier devra être revu de façon régulière (lors des comités de pilotage du produit et/ou lors des comités dédiés à la sécurité par exemple).
- ✓ Niveau 2 : Une politique de gestion des changements est définie, mise en œuvre et couvre l'intégralité des points. Cependant, aucune mise jour de la documentation opérationnelle n'est réalisée.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : La documentation opérationnelle est mise à jour périodiquement et en cas de changement majeur de l'organisation.

Obligation 08.05.02 - Politique de gestion des changements

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune politique de gestion des changements n'est définie et mise en œuvre.
- Niveau 1 : Une politique de gestion des changements est définie et mise en œuvre mais elle ne couvre pas l'intégralité des points suivants :
  La politique de gestion des changements doit faire partie de la documentation opérationnelle ;
  La procédure à suivre doit être définie et un comité d'approbation des changements doit être nommé ;
  Le suivi des changements doit être assuré dans un fichier qui peut être un simple tableur. Ce fichier devra être revu de façon régulière (lors des comités de pilotage du produit et/ou lors des comités dédiés à la sécurité par exemple).
- ✓ Niveau 2 : Une politique de gestion des changements est définie, mise en œuvre et couvre l'intégralité des points. Cependant, aucune mise jour de la documentation opérationnelle n'est réalisée.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : La documentation opérationnelle est mise à jour périodiquement et en cas de changement majeur de l'organisation.

09. Continuité d'activité

Obligation 09.01 - Gestion de crise

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune procédure de gestion de crise n'est mise en place.
- Niveau 1 : Une procédure de gestion de crise est définie et connue des acteurs concernés. Cependant, aucune fiche réflexe n'a été établie. La liste des personnes à mobiliser ou à contacter en cas de crise, avec leurs coordonnées, n'est pas rédigée ou pas maintenue à jour. Les situations de crise considérées sont celles qui surviennent dans l'environnement du fournisseur du produit (environnement de développement/intégration, environnement d'exploitation pour un produit SaaS...) ou au sein de la structure utilisatrice (pour un produit logiciel, Appliance...) quand le produit est impacté par la situation de crise, ou qu'il semble en être une des causes.
- ✓ Niveau 2 : Une procédure de gestion de crise est définie et connue des acteurs concernés. La liste des personnes à mobiliser ou à contacter en cas de crise est rédigée et maintenue à jour, avec leurs coordonnées. Des fiches réflexes (par typologie de scénario) sont disponibles afin de réagir efficacement.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : La gestion de crise est testée régulièrement afin d'évaluer son efficacité.

Obligation 09.02 - Plan de continuité d'activité

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun Plan de continuité d'activité (PCA) n'est mis en place.
- ✓ Niveau 1 : Les responsables du produit connaissent les conditions de lancement du PCA et les différentes tâches à réaliser quand le PCA doit être lancé. Cependant, aucun document n'est rédigé sur ce sujet. Les processus sont connus mais pas tous formalisés par écrit.

- ✓ Niveau 2 : Un plan de continuité d'activité existe et comprend toutes les données nécessaires. Cependant, ce plan ainsi que l'ensemble des documents la constituant ne sont pas testés régulièrement.
- ✓ Niveau 3 : Un plan de continuité d'activité existe et comprend toutes les informations nécessaires. Il est révisé périodiquement et en cas de changement du produit ou de l'organisation. Le PCA est testé au moins annuellement afin d'évaluer son efficacité.

Obligation 09.04 - Réalisation des sauvegardes

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun processus spécifique de sauvegarde hors ligne du produit n'est prévu.
- ✓ Niveau 1 : Les procédures de sauvegarde hors ligne et de restauration de la configuration et des données du produit sont documentées. Dans le cas de produits de type service hébergé ou Saas, la procédure de sauvegarde est effectivement mise en œuvre comme documentée. En outre, dans le cas de produits de type plateforme/applicance intégrant la solution de sauvegarde, ou de service hébergé ou Saas, les sauvegardes sont effectuées sur des supports conservés totalement hors ligne.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les procédures documentées incluent une procédure de vérification de la bonne sauvegarde et couvrent également les composants logiciels du produit. Il est fourni une méthode permettant de calculer l'espace de stockage nécessaire aux sauvegardes en fonction de l'usage prévu du produit et de la durée de conservation souhaitée. Dans le cas de produits de type service hébergé ou Saas, la sauvegarde est au moins journalière et le test de sauvegarde et des procédures de restauration est réalisé de façon régulière.
- ✓ Niveau 3 : Conforme au niveau précédent, plus :
  - Le produit est de type de service hébergé ou Saas ;
  - Ou les procédures et mécanismes liés à la sauvegarde sont conçus pour permettre la réalisation des sauvegardes/restauration à l'aide d'outils de sauvegarde polyvalents tiers tout en garantissant un état cohérent de la sauvegarde, et ne contraignent pas à l'usage d'un produit de sauvegarde spécifique intégrée ou non au produit.

10. Télémaintenance

Option 10.01 - Remontées d'informations

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : La documentation (contrat ou autre) de la prestation ne précise pas si des remontées d'informations issues des dispositifs maintenus ont lieu vers le SI du prestataire.
- Niveau 1 : La documentation (contrat ou autre) de la prestation précise que des remontées d'informations issues des dispositifs maintenus ont lieu vers le SI du prestataire. La nature des informations remontées est décrite précisément et exhaustivement, ainsi que les modalités techniques de ces communications.
- Niveau 2 : Conforme au niveau précédent, plus : Ces remontées d'information sont effectuées exclusivement à des fins de surveillance du maintien en condition opérationnelle et en condition de sécurité. Ces remontées d'information utilisent des protocoles sécurisés, sont tracées et peuvent passer par les passerelles de contrôle d'accès à internet éventuellement mises en place par la structure utilisatrice ou par un VPN IPSEC site à site établi avec le site de télémaintenance.

- Niveau 3 : Conforme au niveau précédent, plus : L'absence de données à caractère personnel directement ou indirectement liées aux patients (ou autres personnes liées aux traitements) est garantie.

Option

10.02 - Architecture de télémaintenance et de téléassistance

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le système de télémaintenance ou de téléassistance s'appuie sur un outil ou un prestataire tiers intermédiaire entre le prestataire de télémaintenance ou de téléassistance et des composants installés sur chaque équipement télémaintenu ou téléassisté du SI de la structure utilisatrice.
- Niveau 1 : Les systèmes de télémaintenance et de téléassistance s'appuient sur des connexions directes (i.e. sans intermédiation par un service contrôlé par un tiers) entre le prestataire de télémaintenance et de téléassistance et des composants installés sur les équipements télémaintenus ou téléassistés du SI de la structure utilisatrice, sauf intermédiation éventuelle par un système bastion sous contrôle de la structure utilisatrice. Les communications de télémaintenance sont sécurisées par usage de protocoles sécurisés, et peuvent être filtrées et contrôlées par les équipements de sécurité de la structure utilisatrice.
- Niveau 2 : Conforme au niveau précédent, plus : Si la structure utilisatrice ne dispose pas d'un bastion d'administration, l'industriel est en mesure de fournir un système bastion qui peut être intégré à l'architecture de sécurité de la structure utilisatrice et qui apporte les mêmes garanties de protection, de traçabilité, de preuve opposable et d'accès à la demande aux traces avec possibilité d'audit. Selon les besoins d'intervention, l'accès aux systèmes à maintenir, à exploiter ou à téléassister peut être ouvert et fermé par le personnel habilité de la structure utilisatrice quand nécessaire à l'intervention du prestataire.
- Niveau 3 : Conforme au niveau précédent, plus : Si la structure utilisatrice dispose d'un bastion d'administration ou le met en place ultérieurement, le prestataire est en mesure de l'utiliser pour accéder aux systèmes qu'il doit maintenir, exploiter, ou téléassister, sans pénalité pour la structure utilisatrice ni sur la qualité des prestations réalisées.

Option

10.03 - Traçabilité des interventions

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le prestataire n'effectue pas de suivi particulier des personnes qui réalisent les opérations d'installation, de maintenance ou de téléassistance sur le SI de la structure utilisatrice, et/ou n'effectue pas de suivi détaillé des actions réalisées par ces personnes.
- Niveau 1 : Le prestataire assure un contrôle d'accès physique et logique aux postes de travail utilisés pour la réalisation de la prestation de télémaintenance ou de téléassistance, en en restreignant l'accès aux seules personnes autorisées à l'aide de mesures physiques et/ou logiques.
- Niveau 2 : Conforme au niveau précédent, plus : Le prestataire assure la traçabilité de chaque intervention, et enregistre notamment l'identité des intervenants, authentifiés avec des comptes nominatifs, ayant participé à la réalisation de l'intervention.
- Niveau 3 : Conforme au niveau précédent, plus : Une procédure est en place et mise en œuvre afin de garantir que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées. Un rapport détaillé de chaque intervention est fourni à la structure utilisatrice.

1.5 Questionnaire Ethique Mon espace santé

SF_CON Contenu médical éditorial ou lié aux données de santé de l'utilisateur
QUA Qualité du contenu

- QUA.1 Ethique
  - Obligation QUA.1.1 Expertise des contributeurs

    Le système DOIT mentionner et documenter que l'expertise des personnes qui sélectionnent, valident ou rédigent les contenus médicaux/de santé publiés dans le service est adaptée à la thématique couverte par le service. Cette information, ainsi que les liens d'intérêts des personnes, est mise à disposition des utilisateurs du service numérique et facilement accessible à tous. Lorsque les contenus médicaux sont directement repris du site internet d'une organisation, notamment d'une agence nationale ou d'une société savante, dont l'information est réputée comme fiable, le nom de l'organisation et l'URL du site devront être indiqués.

  - Obligation QUA.1.2 Références scientifiques

    Le système DOIT permettre la consultation par tous des sources et des références scientifiques clé qui ont été utilisées pour l'élaboration du contenu médical/de santé du service.

  - Obligation QUA.1.3 Processus de veille

    Le système DOIT documenter que le processus de veille et de mise à jour des sources et des références scientifiques qui ont été utilisées pour l'élaboration du contenu médical/de santé du service est adapté à la thématique couverte par le service. Cette information est mise à disposition des utilisateurs du service numérique et facilement accessible à tous.

  - Obligation QUA.1.4 Evaluation clinique et niveaux de preuve

    SI la solution a fait l'objet d'une évaluation clinique et que des niveaux de preuves ont été produits ALORS cette information est mise à disposition des utilisateurs de la solution numérique et facilement accessible à tous.

  - Obligation QUA.1.5 Interprétation par professionnels de santé

    Si le service nécessite une interprétation des contenus à visée de santé (données de santé, contenu scientifique, etc.), ALORS le système DOIT garantir que celle-ci est assurée par des professionnels de santé dont l'expertise est adaptée à la thématique couverte par le service ou par des personnes compétentes spécifiquement formées.

SF_ACC Accessibilité
ACC Accessibilité - Conditions d'accès au service

- ACC.1 Ethique
  - Obligation ACC.1.1 Inclusion de tous les publics

    Le système DOIT être développé dans l'intention de n'exclure aucun public (diversité culturelle, handicap, littératie, etc.).

  - Obligation ACC.1.2 Intuitif et compréhensible

    Le système DOIT être intuitif, c'est-à-dire simple d'usage pour tous les publics, facilement compréhensible et ne demandant aucune formation particulière.

  - Obligation ACC.1.3 Support humain

    Le système DOIT mettre à disposition un service d'assistance et de support avec une interaction humaine permettant d'aider l'utilisateur à utiliser la solution numérique.

  - Option ACC.1.4 Aides en ligne

    Le système peut mettre à disposition des utilisateurs un service d'aide à l'utilisation du système (aide contextuelle, aide en ligne, manuel utilisateur, tutoriel, didacticiel, e-learning, etc.) afin de développer leurs capacités d'apprentissage.

  - Option ACC.1.5 Guichet

    Si le service permet de réaliser des démarches essentielles de santé ou de vie courante ALORS le système DOIT proposer des modes d'accès humain alternatifs et une assistance en présentiel (par exemple, un guichet).

  - Option ACC.1.6 Alerte sur décision critique

    Si une décision critique est produite par le système ALORS le système doit remonter une alerte directement auprès du professionnel de santé ou du 15 pour éviter tout risque d'erreur de compréhension par l'utilisateur.

  - Option ACC.1.7 Réponses aux questions

    Le système documente, actualise et rend accessible aux utilisateurs les réponses aux questions fréquemment posées.

SF_TRA Transparence sur le traitement des données
ETH Ethique de la transparence

- ETH.1 Ethique
  - Option ETH.1.1 Finalités

    Le système DOIT mettre en œuvre des mécanismes afin de garantir la bonne compréhension de l'utilisateur sur le périmètre de son consentement au traitement de ses données personnelles, en faisant la différence entre les traitements servant la production du service (la ou les finalité(s) principale(s)) et ceux servant des finalités secondaires/accessoires.

  - Option ETH.1.2 Consentement

    Le système DOIT mettre en œuvre des mécanismes afin de permettre un consentement « à la carte » au traitement des données, permettant notamment de consentir au traitement servant la ou les finalité(s) principale(s) et de ne pas consentir aux traitements servant les finalités secondaires/accessoires.

  - Obligation ETH.1.3 Service identique

    Le système DOIT proposer un service identique quels que soient les choix opérés par l'usager concernant le traitement de ses données personnelles.

  - Obligation ETH.1.4 Valorisation

    Si une valorisation des données propres à l'application (non issues ou dérivées de Mon Espace Santé) fait partie des finalités secondaires/accessoires du traitement (commercialisation, recherche, valorisation, etc.) ALORS le système DOIT mettre en œuvre des mécanismes pour en garantir la bonne compréhension par l'utilisateur au moment du recueil de son consentement.

  - Obligation ETH.1.5 Paramétrage

    Le système DOIT mettre en œuvre des mécanismes afin que les utilisateurs soient en capacité de paramétrer l'intensité de leurs interactions avec la solution numérique (ex. paramétrage des notifications).

  - Option ETH.1.5 Effacement des données

    Le système met en œuvre des mécanismes afin de permettre l'effacement total des données saisies au cours des premières étapes de l'utilisation du service si l'usager décide de ne pas aller au bout et renonce à l'utilisation du service.

- Option ETH.1.7 Destinataires/Sous-traitants

  Si les données recueillies sont partagées avec d'autres acteurs, notamment des sous-traitants, ALORS le système met en œuvre des mécanismes afin de garantir la bonne compréhension par l'utilisateur de l'existence de ce partage et de sa finalité.

- Option ETH.1.8 Limitation des droits RGPD

  Dans les cas où certains droits RGPD ne s'appliquent pas, le système DOIT mettre en œuvre des mécanismes afin de garantir la bonne compréhension par l'utilisateur que certains de ses droits (notamment le droit à l'effacement de ses données, le droit à la portabilité) peuvent être limités en fonction de la base légale du traitement de ses données dans le cadre du service.

- Option ETH.1.9 Données sensibles

  SI des données susceptibles de donner lieu à des discriminations (comme la religion, les mœurs, l'orientation ou la vie sexuelle de la personne) sont collectées parce qu'elles sont nécessaires à la production du service ALORS le système met en œuvre des mécanismes afin de garantir la bonne compréhension par l'utilisateur que l'objectif du recueil n'est pas discriminatoire.

- Option ETH.1.10 Bénéfices et limites

  Le système met en œuvre des mécanismes afin que l'utilisateur soit en capacité de comprendre les bénéfices et les limites du service et de choisir de l'utiliser de façon éclairée.

SF_INT Intelligence artificielle
INT Intelligence artificielle et éthique

- INT.1 Ethique
  - Obligation INT.1.1 Interaction avec IA

    SI le service intègre un traitement algorithmique produit par une IA ALORS le système DOIT informer l'utilisateur qu'il interagit avec une solution d'IA.

  - Obligation INT.1.2 Documentation biais

    SI le service intègre un traitement algorithmique produit par une IA ALORS le système DOIT documenter et rendre consultable par tous le niveau de performance et les biais algorithmiques de la solution d'IA.

  - Obligation INT.1.3 Détection dépendance

    SI le service intègre un traitement algorithmique produit par une IA ALORS le système DOIT mettre en œuvre des mécanismes permettant de détecter

précocement si le système d'IA crée une dépendance des utilisateurs ou manipule leur comportement.

- Option INT.1.4 Détection dérive

  SI le service intègre un traitement algorithmique produit par une IA ALORS le système met en œuvre des mécanismes afin de détecter si le système d'IA a « dérivé » et nécessite une nouvelle évaluation.

- Option INT.1.5 Explicabilité

  SI le service intègre un traitement algorithmique produit par une IA ALORS le système met en œuvre des mécanismes permettant d'expliquer les propositions du système d'IA. Dans le cas des systèmes "boîtes noires", d'autres mesures d'explicabilité (traçabilité, auditabilité, etc.) sont mises en place.

- Option INT.1.6 Eviter les biais

  SI le service intègre un traitement algorithmique produit par une IA ALORS le système met en œuvre des mécanismes permettant d'éviter de créer ou de renforcer les biais discriminatoires tout au long du cycle de vie de la solution d'IA.

SF_DEV Développement durable
DEV Développement durable

- DEV.1 Ethique
  - Obligation DEV.1.1 Ecoscore

    Le système DOIT être évalué à l'aune de l'impact environnemental de son utilisation au moyen de la méthode d'eco-score fournie par la DNS et l'ANS.

  - Option DEV.1.2 Cycle de vie

    Le système s'intègre, dans son cycle de vie, dans une démarche plus globale de développement durable.

  - Option DEV.1.3 Ecoconception

    Le système met en œuvre des pratiques de conception responsable afin de réduire l'impact environnemental du service.

  - Option DEV.1.4 Faible débit et équipements anciens

    Le système est accessible en faible débit et à partir d'équipements ne nécessitant pas d'être de dernière génération.

- Option DEV.1.5 Réduire consommation datacenters

  Le système retient des choix d'architecture pour l'hébergement de la solution numérique visant à réduire la consommation de ressources et d'énergie.

1.6 Questionnaire RGPD Mon espace santé

Obligation 01. Questionnaire RGPD

- Télécharger le questionnaire RGPD, le compléter puis le déposer dans l'espace de dépôt du questionnaire RGPD dédié.

Obligation 02. CGU et Mentions d'information RGPD

- Déposer les CGU ;
- Déposer les mentions d'information RGPD/Politique de protection des données ou de confidentialité contenant les mentions d'information RGPD.

Obligation 03. Analyse d'Impact relative à la Protection des Données – AIPD

- Ajouter la preuve AIPD au conteneur ZED et le déposer dans l'espace de dépôt dédié.

1.7 Questionnaire Sécurité Mon espace santé pour les échanges de données

Obligation 01. Questionnaire et preuves Sécurité

- Télécharger le questionnaire Sécurité, le compléter puis l'ajouter au conteneur ZED à déposer ;
- Ajouter les preuves ci-dessous dans les dossiers respectifs du conteneur ZED à déposer :
  - R01 Politique de Sécurité des Systèmes d'Information (PSSI),
  - R02 Analyse de risque,
  - R03 Audits de sécurité,
  - R04 Homologation interne de sécurité,
  - R05 Conception et développement sécurises de l'application,
  - R06 Configuration sécurisée des systèmes d'information lies à l'application,
  - R07 Cryptographie,
  - R08 Cloisonnement et filtrage,
  - R09 Protection des accès distants au SI,
  - R10 Sécurité de l'administration des systèmes d'information,
  - R11 Gestion des identités et des accès,
  - R12 Maintien en condition de sécurité,
  - R13 Systèmes de journalisation corrélation analyse et détection des évènements,
  - R14 Réponse aux incidents de sécurité et gestion de crise,
  - R15 Certification des Hébergeurs de Données de Sante ;
- Déposer le conteneur ZED complété avec toutes les preuves dans la zone de dépôt du dédiée.

2. Annexe - Profilage des questionnaires

2.1 Questionnaire d'orientation

Question d'orientation	Condition d'apparition
3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ?	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
4.bis. Autres architectures à indiquer	Répondre « Autres » à la question « 4. Pour quelle architecture du service sollicitez-vous un référencement à Mon Espace Santé ? »
5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ?	Répondre « Aucune réponse correspondante » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
8.bis. Autres activités à indiquer	Répondre « Autres » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
13. Le service gère-t-il un référentiel d'identité ?	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? » **OU** Répondre « Thérapeutique », « Prévention », « Diagnostic », « Soulagement de la douleur », « Compensation du handicap ou prévention de la perte d'autonomie » ou « Interventions nécessaires à la coordination de plusieurs de ces actes » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
14. Le service reçoit-il des données de santé à caractère personnel provenant d'un autre domaine d'identification ?	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? » **OU** Répondre « Thérapeutique », « Prévention », « Diagnostic », « Soulagement de la douleur », « Compensation du handicap ou prévention de la perte d'autonomie » ou « Interventions nécessaires à la coordination de plusieurs de ces actes » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
15. Le service reçoit-il des données de santé à caractère personnel provenant d'un autre service appartenant au même domaine d'identification ?	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? » **OU** Répondre « Thérapeutique », « Prévention », « Diagnostic », « Soulagement de la douleur », « Compensation du handicap ou prévention de la perte d'autonomie » ou « Interventions nécessaires à la coordination de plusieurs de ces actes » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
17. Le service permet-t-il l'import par un utilisateur (administrateurs compris) de fichiers susceptibles de constituer ou de contenir un logiciel malveillant (malware, virus ou autre) ?	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
18. Le service comporte-t-il une partie centralisée (serveurs, etc.) accédée via Internet ?	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus

	accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
19. Le service est-t-il susceptible, dans certains cas de mise en œuvre autorisés par le contrat de fourniture, d'être accessible depuis des réseaux publics (Internet...) ? OU L'analyse de risques a-t-elle identifié le besoin d'une architecture n-tiers pour le service ?	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
20. Le service comporte-t-il la fourniture à la fois de logiciel et de matériel à l'utilisateur, tout ou partie de ce logiciel s'exécutant sur le matériel fourni, et l'ensemble étant destiné à être directement utilisé par l'utilisateur ?	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
21. Le service comporte-t-il un ou plusieurs composants qui peuvent être connectés à un système de communication informatique, qu'il s'agisse d'un réseau local, d'Internet ou d'un réseau sans fil (Wifi, Bluetooth, réseaux de téléphonie mobile, réseau pour IoT…) ?	Répondre « Oui » à la question « 20. Le service comporte-t-il la fourniture à la fois de logiciel et de matériel à l'utilisateur, tout ou partie de ce logiciel s'exécutant sur le matériel fourni, et l'ensemble étant destiné à être directement utilisé par l'utilisateur ? »
22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ?	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
23. Le service comporte-t-il un ou plusieurs équipements fournis par l'industriel pouvant être utilisés en mobilité par l'utilisateur ?	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
24. Les équipements mobiles fournis par l'industriel ont-ils la capacité d'utiliser le wifi ?	Répondre « Oui » à la question « 23. Le service comporte-t-il un ou plusieurs équipements fournis par l'industriel pouvant être utilisés en mobilité par l'utilisateur ? »
25. Le service fournit-il un accès dédié à des acteurs de santé personnes physiques ?	Répondre « Prévention », « Diagnostic », « Soin » ou « Suivi social ou médico-social » ou « Interventions nécessaires à la coordination de plusieurs de ces actes » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
26. Le service gère-t-il l'identité d'acteurs de santé personnes physiques dans les données qu'il traite (stockage, affichage, utilisation de données d'identité de professionnel de santé) ?	Répondre « Non » à la question « 25. Le service fournit-il un accès dédié à des acteurs de santé personnes physiques ? »
27. Le service fournit-il un accès dédié à des acteurs de santé personnes morales ?	Répondre « Prévention », « Diagnostic », « Soin » ou « Suivi social ou médico-social » ou « Interventions nécessaires à la coordination de plusieurs de ces actes » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
28. Le service gère-t-il l'identité d'acteurs de santé personnes morales dans les données qu'il traite (stockage, affichage, utilisation de données d'identité de professionnel de santé) ?	Répondre « Non » à la question « 27. Le service fournit-il un accès dédié à des acteurs de santé personnes morales ? »

29. Le service fournit-il un accès à des données à caractère personnel à des utilisateurs ou patients ?	Répondre « Prévention », « Diagnostic », « Soin » ou « Suivi social ou médico-social » ou « Interventions nécessaires à la coordination de plusieurs de ces actes » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? » **ET** Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
31. L'offre comporte-t-elle une prestation de télémaintenance de l'application, conjointement à la fourniture de l'application qui est exploitée sous la responsabilité de son utilisateur ?	Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »
32. Existe-t-il des remontées d'informations issues des dispositifs maintenus vers le SI du prestataire dans le cadre de la prestation de télémaintenance ?	Répondre « Oui » à la question « 20. Le service comporte-t-il la fourniture à la fois de logiciel et de matériel à l'utilisateur, tout ou partie de ce logiciel s'exécutant sur le matériel fourni, et l'ensemble étant destiné à être directement utilisé par l'utilisateur ? »
33. Le service, pour lequel vous candidatez au référencement Mon Espace Santé, est-il un DM de classe 2A et supérieures ou un DM DIV classe B et supérieures (fournir le certificat de marquage CE délivré par un organisme notifié et le certificat ISO 13485) ?	Répondre « Oui » à la question « 1. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical ? »
34. En répondant "Oui" à la question précédente, vous devez déposer le certificat de marquage CE et le certificat ISO	Répondre « Oui » à la question « 33. Le service, pour lequel vous candidatez au référencement Mon Espace Santé, est-il un DM de classe 2A et supérieures ou un DM DIV classe B et supérieures (fournir le certificat de marquage CE délivré par un organisme notifié et le certificat ISO 13485) ? »
35. Le service comporte-il un ou plusieurs contenus médicaux/de santé ?	Répondre « Non » à la question « 1. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical ? » **OU** Répondre « Non » à la question « 33. Le service, pour lequel vous candidatez au référencement Mon Espace Santé, est-il un DM de classe 2A et supérieures ou un DM DIV classe B et supérieures (fournir le certificat de marquage CE délivré par un organisme notifié et le certificat ISO 13485) ? »
36. Le service a-t-il fait l'objet d'une évaluation clinique ?	Répondre « Non » à la question « 1. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical ? » **OU** Répondre « Non » à la question « 33. Le service, pour lequel vous candidatez au référencement Mon Espace Santé, est-il un DM de classe 2A et supérieures ou un DM DIV classe B et supérieures (fournir le certificat de marquage CE délivré par un organisme notifié et le certificat ISO 13485) ? »
37. Le service repose-t-il sur une interprétation de données de santé par des experts ?	Répondre « Non » à la question « 1. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical ? » **OU** Répondre « Non » à la question « 33. Le service, pour lequel vous candidatez au référencement Mon Espace Santé, est-il un DM de classe 2A et supérieures ou un DM DIV classe B et supérieures (fournir le certificat de marquage CE délivré par un organisme notifié et le certificat ISO 13485) ? »

41. Si l'utilisateur ne finalise pas la création de son compte, le service enregistre-t-il les données saisies ?	Répondre « Oui » à la question « 40. Le service permet-il la création de compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ? »
42. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires ?	Répondre « Oui » à la question « 40. Le service permet-il la création de compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ? »

2.2 Questionnaire Interopérabilité

Critères du questionnaire d'Interopérabilité	Condition d'apparition
A08.1.1 Utilisation et enrichissement du CI-SIS	Répondre « Oui » à la question « 10. Le service échange-t-il des données avec d'autres applications ou SI que Mes ? »
	OU Répondre « Oui » à la question « 11. Le service partage-t-il des données avec d'autres applications ou SI que Mes ? »
A08.2.1 Formalisation des usages	Répondre « Oui » à la question « 10. Le service échange-t-il des données avec d'autres applications ou SI que Mes ? »
	OU Répondre « Oui » à la question « 11. Le service partage-t-il des données avec d'autres applications ou SI que Mes ? »
A08.3.1 Connexion synchrone avec d'autres SI	Répondre « Oui » à la question « 10. Le service échange-t-il des données avec d'autres applications ou SI que Mes ? »
	OU Répondre « Oui » à la question « 11. Le service partage-t-il des données avec d'autres applications ou SI que Mes ? »
A08.4.1 Mise en œuvre interopérable du service Partage de Documents de Santé	Répondre « Oui » à la question « 11. Le service partage-t-il des données avec d'autres applications ou SI que Mes ? »
A08.4.6 Mise en œuvre interopérable du service Gestion d'agendas partagés	Répondre « Gestion d'agendas partagés » à la question « 12. Le service produit ou consomme-t-il ce type de document ? »
A08.4.8 Mise en œuvre interopérable du service Mesures de santé	Répondre « Mesures de santé » à la question « 12. Le service produit ou consomme-t-il ce type de document ? »
A08.5.01 Partage et/ou échange de documents (producteur de documents CDA) - document structuration minimale	Répondre « Structuration minimale – Production » à la question « 12. Le service produit ou consomme-t-il ce type de document ? »
A08.5.23 Partage et/ou échange de documents (consommateur de documents CDA) - structuration minimale	Répondre « Structuration minimale – Consommation » à la question « 12. Le service produit ou consomme-t-il ce type de document ? »
A08.6.1 Test des interfaces	Répondre « Oui » à la question « 10. Le service échange-t-il des données avec d'autres applications ou SI que Mes ? »
A10.1 Récupération des nomenclatures sur une source d'autorité et intégration automatique, gestion des mises à jour	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
A10.2 Utilisation des nomenclatures de l'ANS	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »

2.3 Questionnaire Urbanisation

Critères du questionnaire d'Urbanisation	Condition d'apparition
A06.1 Mise en œuvre de l'INS (référentiel d'identités)	Répondre « Oui » à la question « 13. Le service gère-t-il un référentiel d'identité ? »
A06.2 Mise en œuvre de l'INS (consommation de flux et documents avec l'INS, en provenance d'un domaine d'identification différent)	Répondre « Oui » à la question « 14. Le service reçoit-il des données de santé à caractère personnel provenant d'un autre domaine d'identification ? »
A06.3 Mise en œuvre de l'INS (consommation de flux et documents avec l'INS, en provenance du même domaine d'identification)	Répondre « Oui » à la question « 15. Le service reçoit-il des données de santé à caractère personnel provenant d'un autre service appartenant au même domaine d'identification ? »
A18.2 Référentiel télémédecine - Téléexpertise	Répondre « Oui » à la question « 16. Le service est-il une application de télésanté ? »

2.4 Questionnaire Maturité Sécurité

Critères du questionnaire de Maturité Sécurité	Condition d'apparition
01.02.01 - Organisation et processus de la sécurité	Répondre « Aucune réponse correspondante » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
	ET Répondre « Non » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
01.02.02 - Organisation et processus de la sécurité	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
01.03 - Processus d'amélioration continue	Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	OU Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
01.04.01 - Sensibilisation des équipes en charge	Répondre « Aucune réponse correspondante » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? » **ET** Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	OU répondre « Non » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
01.04.02 - Sensibilisation des équipes en charge	Répondre « Oui » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
01.05 - Certification ISO 27001	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »

02.02.01 - Analyse de risques et certification de sécurité	Répondre « Aucune réponse correspondante » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? » **ET** Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? » **ET** Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
	OU répondre « Non » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
02.02.02 - Analyse de risques et certification de sécurité	Répondre « Oui » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
02.03.01 - Plan d'Assurance Sécurité	Répondre « Aucune réponse correspondante » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **ET** Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
	OU répondre « Non » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
02.03.02 - Plan d'Assurance Sécurité	Répondre « Oui » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
03.01 - Configuration sécurisée des composants du produit	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
	OU Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
03.02 - Antivirus	Répondre « Oui » à la question « 17. Le service permet-t-il l'import par un utilisateur (administrateurs compris) de fichiers susceptibles de constituer ou de contenir un logiciel malveillant (malware, virus ou autre) ? »
03.04 - Contrôle des flux réseaux et applicatifs	Répondre « Oui » à la question « 18. Le service comporte-t-il une partie centralisée (serveurs, etc.) accédée via Internet ? »
03.05 - Développement sécurisé	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
03.06 - Protection des développements	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »

03.07 - Architecture sécurisée	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Oui » à la question « 19. Le service est-t-il susceptible, dans certains cas de mise en œuvre autorisés par le contrat de fourniture, d'être accessible depuis des réseaux publics (Internet...) ? ou L'analyse de risques a-t-elle identifié le besoin d'une architecture n-tiers pour le service ? »
	ET Répondre « Oui » à la question « 21. Le service comporte-t-il un ou plusieurs composants qui peuvent être connectés à un système de communication informatique, qu'il s'agisse d'un réseau local, d'Internet ou d'un réseau sans fil (Wifi, Bluetooth, réseaux de téléphonie mobile, réseau pour IoT…) ? », **OU** répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »
03.08 - Contrôle d'accès au réseau	Répondre « Oui » à la question « 21. Le service comporte-t-il un ou plusieurs composants qui peuvent être connectés à un système de communication informatique, qu'il s'agisse d'un réseau local, d'Internet ou d'un réseau sans fil (Wifi, Bluetooth, réseaux de téléphonie mobile, réseau pour IoT…) ? »
03.09 - Environnements	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »
03.10 - Procédures opérationnelles	Votre solution est une solution en marque blanche d'un éditeur distributeur ou d'un éditeur producteur
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
03.11 - Inventaire des composants et des flux	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
03.12 - Intégrité du produit	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Oui » à la question « 18. Le service comporte-t-il une partie centralisée (serveurs, etc.) accédée via Internet ? »

03.13.01 - Protection des informations (Cryptographie)	Répondre « Aucune réponse correspondante » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **ET** Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? », **ET** Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
	OU répondre « Non » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
03.13.02 - Protection des informations (Cryptographie)	Répondre « Oui » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
03.14 - Gestions des secrets (clés privées et mots de passe)	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
03.15 - Chiffrement des supports de stockage	Répondre « Oui » à la question « 23. Le service comporte-t-il un ou plusieurs équipements fournis par l'industriel pouvant être utilisés en mobilité par l'utilisateur ? »
03.16 - Connectivité Wifi	Répondre « Oui » à la question « 24. Les équipements mobiles fournis par l'industriel ont-ils la capacité d'utiliser le wifi ? »
03.17 - Application de la réglementation relative aux dispositifs médicaux	Répondre « Oui » à la question « 2. Le service, pour lequel vous candidatez au référencement Mes, inclut-il un dispositif médical connecté ? »
	ET Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
04.01 - Utilisation et mise à jour des identités nationales des acteurs de santé personnes physiques	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **ET** répondre « Oui » à la question « 25. Le service fournit-il un accès dédié à des acteurs de santé personnes physiques ? »
	OU Répondre « Oui » à la question « 26. Le service gère-t-il l'identité d'acteurs de santé personnes physiques dans les données qu'il traite (stockage, affichage, utilisation de données d'identité de professionnel de santé) ? »
04.02 - Niveau de garantie de l'identification électronique des acteurs de santé personnes physiques	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
	ET Répondre « Oui » à la question « 25. Le service fournit-il un accès dédié à des acteurs de santé personnes physiques ? »
04.03 - Niveau de garantie de l'identification électronique des patients ou usagers	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
	ET Répondre « Oui » à la question « 29. Le service fournit-il un accès à des données à caractère personnel à des utilisateurs ou patients ? »

04.04 - Documentation de la procédure d'autorisation (ajout, modification, suppression)	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Oui » à la question « 30. Le service est-il multi-utilisateurs (utilisateurs finaux, administrateurs, etc.) ? »
04.05 - Gestion et séparation des droits	Répondre « Oui » à la question « 30. Le service est-il multi-utilisateurs (utilisateurs finaux, administrateurs, etc.) ? »
04.06 - Comptes génériques	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
04.08 - Utilisation et mise à jour des identités nationales des acteurs de santé personnes morales	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? » **ET** répondre « Oui » à la question « 27. Le service fournit-il un accès dédié à des acteurs de santé personnes morales ? »
	OU Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **ET** répondre « Oui » à la question « 28. Le service gère-t-il l'identité d'acteurs de santé personnes morales dans les données qu'il traite (stockage, affichage, utilisation de données d'identité de professionnel de santé) ? »
04.09 - Niveau de garantie de l'identification électronique des acteurs de santé personnes morales	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
	ET Répondre « Oui » à la question « 27. Le service fournit-il un accès dédié à des acteurs de santé personnes morales ? »
06.01 - Contrôle d'accès physique aux équipements informatiques	Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »
07.01 - Réalisation d'audits de code	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
07.02 - Recherche de vulnérabilités	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »

07.04 - Plan d'actions	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
08.02 - Veille et patch management	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
08.03 - Gestion de l'obsolescence	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
08.04 - Mécanismes de supervision du fonctionnement et de la sécurité (Nagios, SIEM...)	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »
08.05.01 - Politique de gestion des changements	Répondre « Aucune réponse correspondante » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **ET** Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? », **ET** Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »
	OU répondre « Non » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
08.05.02 - Politique de gestion des changements	Répondre « Oui » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
	ET Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »
09.01 - Gestion de crise	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
09.02 - Plan de continuité d'activité	Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? »

09.04 - Réalisation des sauvegardes	Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il des données personnelles ? »
	ET Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? »
10.01 - Remontées d'informations	Répondre « Non » à la question « 9. Le service consiste-t-il en la seule publication de contenus informatifs (textes, images, graphismes, vidéos, sons…) via des plateformes Internet standard de diffusion de contenu, ces contenus étant ainsi rendus accessibles de façon exclusivement anonyme (i.e. sans authentification ni usage d'identifiant) à tout utilisateur d'Internet ? » **ET** votre solution est une solution en marque blanche d'un éditeur producteur
	OU Répondre « Oui » à la question « 32. Existe-t-il des remontées d'informations issues des dispositifs maintenus vers le SI du prestataire dans le cadre de la prestation de télémaintenance ? »
10.02 - Architecture de télémaintenance et de téléassistance	Répondre « Oui » à la question « 31. L'offre comporte-t-elle une prestation de télémaintenance de l'application, conjointement à la fourniture de l'application qui est exploitée sous la responsabilité de son utilisateur ? »
10.03 - Traçabilité des interventions	**OU** Répondre « Oui » à la question « 22. Tout ou partie des composants du service est-elle hébergée par l'industriel ou par un tiers sous sa responsabilité ? » **ET** votre solution est une solution en marque blanche d'un éditeur distributeur ou d'un éditeur producteur
	Répondre « Oui » à la question « 31. L'offre comporte-t-elle une prestation de télémaintenance de l'application, conjointement à la fourniture de l'application qui est exploitée sous la responsabilité de son utilisateur ? »

2.5 Questionnaire Ethique Mon espace santé

Critères du questionnaire Ethique Mon espace santé	Condition d'apparition
QUA.1.1 Expertise des contributeurs	Répondre « Oui » à la question « 35. Le service comporte-il un ou plusieurs contenus médicaux/de santé ? »
QUA.1.2 Références scientifiques	Répondre « Oui » à la question « 35. Le service comporte-il un ou plusieurs contenus médicaux/de santé ? »
QUA.1.3 Processus de veille	Répondre « Oui » à la question « 35. Le service comporte-il un ou plusieurs contenus médicaux/de santé ? »
QUA.1.4 Evaluation clinique et niveaux de preuve	Répondre « Oui » à la question « 36. Le service a-t-il fait l'objet d'une évaluation clinique ?»
QUA.1.5 Interprétation par professionnels de santé	Répondre « Oui » à la question « 37. Le service repose-t-il sur une interprétation de données de santé par des experts ? »
ACC.1.5 Guichet	Répondre « Oui » à la question « 38. Le service permet-il de réaliser des démarches essentielles de santé ou de vie courante ? »
ACC.1.6 Alerte sur décision critique	Répondre « Oui » à la question « 39. Le service produit-il des décisions critiques ? »
ETH.1.1 Finalités	Répondre « Oui » à la question « 42. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires ? »
ETH.1.2 Consentement	Répondre « Oui » à la question « 42. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires ? »
ETH.1.3 Service identique	Répondre « Oui » à la question « 42. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires ? »
ETH.1.4 Valorisation	Répondre « Oui » à la question « 43. Le service valorise-t-il les données collectées (anonymisées ou non, monétisées ou non) sous forme de statistiques, recherches, amélioration du service, marketing etc. ? »
ETH.1.6 Effacement des données	Répondre « Oui » à la question « 41. Si l'utilisateur ne finalise pas la création de son compte, le service enregistre-t-il les données saisies ? »
ETH.1.7 Destinataires/Sous-traitants	Répondre « Oui » à la question « 44. A l'exception de Mon Espace Santé, le service partage-t-il des données recueillies avec d'autres acteurs (ex. partenaires, destinataires, sous-traitants notamment hébergeur...) ? »
ETH.1.8 Limitation des droits RGPD	Répondre « Oui » à la question « 45. Le service limite-t-il des droits RGPD de l'utilisateur ? »
ETH.1.9 Données sensibles	Répondre « Oui » à la question « 46. Le service manipule-t-il des données sensibles discriminatoires ? »
INT.1.1 Interaction avec IA	Répondre « Oui » à la question « 47. Le service intègre-t-il un traitement algorithmique produit par une intelligence artificielle ? »
INT.1.2 Documentation biais	Répondre « Oui » à la question « 47. Le service intègre-t-il un traitement algorithmique produit par une intelligence artificielle ? »

INT.1.3 Détection dépendance	Répondre « Oui » à la question « 47. Le service intègre-t-il un traitement algorithmique produit par une intelligence artificielle ? »
INT.1.4 Détection dérive	Répondre « Oui » à la question « 47. Le service intègre-t-il un traitement algorithmique produit par une intelligence artificielle ? »
INT.1.5 Explicabilité	Répondre « Oui » à la question « 47. Le service intègre-t-il un traitement algorithmique produit par une intelligence artificielle ? »
INT.1.6 Eviter les biais	Répondre « Oui » à la question « 47. Le service intègre-t-il un traitement algorithmique produit par une intelligence artificielle ? »
DEV.1.5 Réduire consommation datacenters	Répondre « Oui » à la question « 7. Le service fait-il appel à un hébergement de données (y compris en cas d'hébergeur interne/cloud ou en cas de sous-traitance de l'hébergement) ? »

2.6 Questionnaire Sécurité Mon espace santé pour les échanges de données

Ce questionnaire s'applique à votre produit si pour la question 3 du questionnaire d'orientation « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il les données suivantes ? », vous sélectionnez l'une des options suivantes :

- Mesures de santé
- Documents
- Agenda