Sommaire

1. Questionnaires de la démarche 3
1.1 Questionnaire d'orientation 3
1.2 Questionnaire Interopérabilité 9
1.3 Questionnaire Urbanisation 12
1.4 Questionnaire Maturité Sécurité 13
1.5 Questionnaire Qualité du contenu 23
1.6 Questionnaire Ethique Mon espace santé 25
1.7 Questionnaire RGPD Mon espace santé 29
1.8 Questionnaire Sécurité Mon espace santé pour les échanges de données 30
1.8 Parcours dédié DMN 31
1.9 Parcours dédié TLC 32
2. Annexe - Profilage des questionnaires 33
2.1 Questionnaire d'orientation 33
2.2 Questionnaire Interopérabilité 39
2.3 Questionnaire Urbanisation 40
2.4 Questionnaire Maturité Sécurité 41
2.5 Questionnaire Qualité du contenu 44
2.6 Questionnaire Ethique Mon espace santé 45
2.6 Questionnaire RGPD Mon espace santé 46
2.7 Questionnaire Sécurité Mon espace santé pour les échanges de données 46
2.8 Parcours dédié DMN 46
2.9 Parcours dédié TLC 46

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

Parcours Dédiés

Obligation 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ?

- Dispositif médical numérique
- SI de téléconsultation
- Aucune de ces réponses

Généralités

Obligation 2. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical (sans certificat de conformité délivré par l'ANS) ?

- Oui
- Non

Obligation 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès aux 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
- Autres

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

Obligation 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ?

- Oui
- Non

Obligation 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ?

- Oui
- Non

Obligation 7. Fournir un compte de démonstration (url, identifiant et mot de passe) – Champ texte libre

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
- Autres

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

Sécurité

Obligation 10. Le service comporte-t-il une partie centralisée (serveurs, etc.) accédée via Internet ?

- Oui
- Non

Obligation 11. Le service comporte-t-il un ou plusieurs équipements fournis par l'industriel pouvant être utilisés en mobilité par l'utilisateur ?

- Oui
- Non

Obligation 12. Le service fournit-il un accès dédié à des acteurs de santé (PS ou personnes morales) ?

- Acteurs de santé personnes physiques
- Acteurs de santé personnes morales
- Aucun acteur de santé

Obligation 13. Le service gère-t-il l'identité d'acteurs de santé (PS ou personnes morales) ?

- Acteurs de santé personnes physiques
- Acteurs de santé personnes morales
- Aucun acteur de santé

Obligation 14. Le service fournit-il un accès à des données à caractère personnel à des usagers du service numérique de santé (patient, aidant… hors professionnel de santé) ?

- Oui
- Non

Obligation 15. Le service est-il multi-utilisateurs (utilisateurs finaux, administrateurs, etc.) ?

- Oui
- Non

Obligation 16. Le service assure-t-il ou sous traite-t-il l'hébergement de données de santé au sens des articles L1111-8 et R1111-8-8 du Code de la Santé Publique ?

- Oui
- Non

Urbanisation

Obligation 17. Le service permet-il un accès par un professionnel de santé (PS) aux données de santé personnelles ?

- Oui
- Non

Interopérabilité

Obligation 18. Le service échange-t-il des données avec d'autres applications ou SI que Mes ?

- Oui
- Non

Obligation 19. Le service partage-t-il des données avec d'autres applications ou SI que Mes ?

- Oui
- Non

Obligation 20. 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

Ethique

Obligation 21. 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 21.bis. En répondant "Oui" à la question précédente, vous devez déposer le certificat de marquage CE et le certificat ISO – Preuve à déposer

Obligation 21.ter. Précisez la classe de votre DM – Champ texte libre

Obligation 22. Le service comporte-il un ou plusieurs contenus médicaux/de santé ?

- Oui
- Non

Obligation 23. Le service a-t-il fait l'objet d'une évaluation clinique ?

- Oui
- Non

Obligation 24. Le service repose-t-il sur une interprétation de données de santé par des experts ?

- Oui
- Non

Obligation 25. Le service produit-il des décisions critiques ?

- Oui
- Non

Obligation 26. Le service permet-il la création d'un compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ?

- Oui
- Non

Obligation 27. Si l'utilisateur ne finalise pas la création de son compte, le service enregistre-t-il les données saisies ?

- Oui
- Non

Obligation 28. Le service réutilise-t-il, valorise ou partage-t-il des données personnelles recueillies au cours de l'utilisation du service (valorisation commerciale, partage avec des sous-traitants…) ?

- Oui
- Non

Obligation 29. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires s'appuyant sur la base légale du consentement ?

- Oui
- Non

Obligation 30. Le service manipule-t-il des données sensibles discriminatoires ?

- Oui
- Non

Obligation 31. Le service intègre-t-il une Intelligence Artificielle (IA) ?

- Oui
- Non

Obligation 31.bis. Précisez en quelques mots quel type d'IA est intégrée à votre service – Champ texte libre

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.

A08.3 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).

A10. Terminologies de santé

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 oeuvre de l'INS (pour les services dont les données des utilisateurs sont accessibles par des professionnels de santé)

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Le produit n'est pas autorisé CNDA à faire appel au téléservice INSi et n'a pas intégré les traits de l'INS.
- Niveau 1 : Le produit a intégré le téléservice INSi (autorisation CNDA obtenue, au moins pour la transaction de récupération).
- ✓ Niveau 2 : Le produit est autorisé CNDA à faire appel au téléservice INSi.

Obligation A06.2 Intégration des traits d'identité (pour les services qui concourent à la prévention ou aux soins sans que les données des utilisateurs soient accessibles directement aux professionnels de santé)

- Niveau non applicable : Toujours applicable si le critère apparaît.
- Niveau 0 : Le produit n'a pas intégré l'exhaustivité des traits d'identité suivants : nom de naissance, premier prénom de naissance, date de naissance, libellé de la ville de naissance, département de naissance, sexe, nom utilisé (si différent du nom de naissance), prénom utilisé (si différent du premier prénom de naissance).
- ✓ Niveau 1 : Dans la création et la gestion des identités des utilisateurs, le produit a intégré les traits suivants : nom de naissance, premier prénom de naissance, date de naissance, libellé de la ville de naissance, département de naissance, sexe, nom utilisé (si différent du nom de naissance), prénom utilisé (si différent du premier prénom de naissance).
- ✓ Niveau 2 : Conforme au niveau précédent, plus : le libellé de la ville de naissance est collecté avec le Code officiel géographique de l'INSEE en cohérence avec la date de naissance.

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 01.04.01 - 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).

03. Conception sécurisée

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) (pour les services n'échangeant pas de données avec Mes et/ou contenant des données personnelles)

- 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) (pour les services qui échangent des données avec Mes)

- 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 03.18 – Documentation et bonnes pratiques

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune documentation (un ou plusieurs documents) ne précise les bonnes pratiques et/ou les procédures à respecter pour le développement et la configuration sécurisés
- ✓ Niveau 1 : Une documentation (un ou plusieurs documents) précisant les bonnes pratiques et/ou les procédures à respecter pour le développement et la configuration sécurisés DOIT être disponible et suivie pour la création du système et l'implémentation de nouvelles fonctionnalités. Cette documentation doit adresser à minima les points suivants :
  - Conception sécurisée

- Vérification de la qualité du code
- La gestion de l'obsolescence des composants logiciels
- Tests de sécurité
- Déploiement des correctifs

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 produit 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 préexistante dans la structure utilisatrice (matricule RH, etc.).
- Niveau 1 : Le produit ne correspond pas à un service numérique "sensible" tel que défini dans le référentiel d'identification électronique des acteurs de santé personnes physiques de la PGSSI-S. Il peut identifier les acteurs de santé à l'aide de l'identité nationale (RPPS, et ADELI en transitoire) ou d'une identité locale préexistante dans la structure utilisatrice (matricule RH, etc.). Ces identités sont modifiables via un processus de gestion documenté.
- Niveau 2 : Que le produit corresponde ou non à un service numérique "sensible" tel que défini dans le référentiel d'identification électronique des acteurs de santé personnes physiques de la PGSSI-S, il est conforme à ce même référentiel. En particulier, il identifie les acteurs de santé au moins à l'aide de l'identité nationale (RPPS, et ADELI en transitoire).
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Le processus de gestion documenté systématise les recherches/vérifications au répertoire de référence (RPPS) 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 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 réalisées 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 produit correspond à un service numérique "sensible" tel que défini dans le référentiel d'identification électronique des acteurs de santé personnes physiques de la PGSSI-S, mais il n'est pas conforme à ce même référentiel, ou le produit ne correspond pas à un service numérique "sensible" et n'assure pas l'identification électronique de ses utilisateurs acteurs de santé personnes physiques.
- Niveau 1 : Le produit ne correspond pas à un service numérique "sensible" tel que défini dans le référentiel d'identification électronique des acteurs de santé personnes physiques de la PGSSI-S. Il assure l'identification électronique de ses utilisateurs acteurs de santé personnes physiques, mais il n'est pas conforme aux exigences de ce même référentiel applicables aux services sensibles (qui ne lui sont pas applicables de manière opposable).
- ✓ Niveau 2 : Que le produit corresponde ou non à un service numérique "sensible" tel que défini dans le référentiel d'identification électronique des acteurs de santé personnes physiques de la PGSSI-S, il est conforme aux exigences de ce même référentiel relatives à l'identification électronique. Le produit met notamment en œuvre l'identification

électronique par Pro Santé Connect. Le produit met en œuvre au moins un moyen d'identification électronique entrant dans le cadre des moyens d'identification électronique de transition (de niveau de garantie "eIDAS faible" renforcé) tels que définis par le référentiel susmentionné.

- ✓ Niveau 3 : Conforme au niveau précédent, sauf : Le produit ne met en œuvre aucun moyen d'identification électronique entrant dans le cadre des moyens d'identification électronique de transition défini par le référentiel d'identification électronique des acteurs de santé personnes physiques de la PGSSI-S.

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 produit fournit un accès à des données à caractère personnel à des usagers ou patients, mais il n'est pas conforme au référentiel d'identification électronique des usagers de la PGSSI-S.
- ✓ Niveau 2 : Le produit est conforme au référentiel d'identification électronique des usagers de la PGSSI-S. Le produit met en œuvre au moins un moyen d'identification électronique entrant dans le cadre des moyens d'identification électronique de transition (de niveau de garantie "eIDAS faible" renforcé) tels que définis par le référentiel susmentionné. Le cas échéant, le produit met en œuvre un ou plusieurs moyens d'identification électronique parmi : des moyens d'identification électronique certifiés eIDAS de niveau de garantie substantiel ou élevé ; l'application mobile carte Vitale.
- ✓ Niveau 3 : Conforme au niveau précédent, sauf : Le produit ne met en œuvre aucun moyen d'identification électronique entrant dans le cadre des moyens d'identification électronique de transition défini par le référentiel d'identification électronique des usagers de la PGSSI-S.

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 04.08 - 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.

07. Audit

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.

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.

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.

11. Hébergement

Obligation 11.01 – Hébergement des données de santé

- Niveau 0 : Le candidat ou un tiers sous sa responsabilité assurant l'hébergement de tout ou partie des composants du produit, ou fournissant tout ou partie du service sous forme de service (SaaS) n'a pas obtenu la certification HDS.
- ✓ Niveau 1 : Le candidat ou un tiers sous sa responsabilité assurant l'hébergement de tout ou partie des composants du produit, ou fournissant tout ou partie du service sous forme de service (SaaS) a obtenu la certification HDS auprès d'un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen).

1.5 Questionnaire Qualité du contenu

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

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

    Les contenus médicaux/de santé du service numérique DOIVENT faire l'objet d'une sélection, validation et/ou rédaction par un comité dont l'expertise collective couvre la thématique du service numérique. Les noms, qualifications et liens d'intérêts de ces personnes DOIVENT être mis à disposition des utilisateurs et facilement accessibles.

  - Obligation QUA.1.2B Références scientifiques

    Les contenus médicaux du service numérique DOIVENT être conformes aux recommandations d'organisations dont l'information est réputée fiable. S'ils sont élaborés à partir de références scientifiques, celles-ci sont consultables. L'ensemble des sources utilisées pour la rédaction des contenus médicaux/de santé est facilement accessible par les utilisateurs, par exemple sur une page dédiée du service numérique ou sous forme de références précédant ou suivant le contenu.

  - Obligation QUA.1.3 Processus de veille

    Le service numérique DOIT comporter un processus de veille sur les sources et références scientifiques utiles à l'élaboration des contenus médicaux/de santé afin de refléter l'état actuel des connaissances. Cette information est facilement accessible à tous. L'utilisateur est informé de la date de mise à jour du contenu qu'il consulte.

  - Obligation QUA.1.4 Evaluation clinique et niveaux de preuve

    Les informations documentant la performance, l'intérêt clinique ou organisationnel de l'application, ainsi que les avis émis dans le cadre de demandes de remboursement par la solidarité nationale DOIVENT être facilement accessibles par les utilisateurs. A défaut, l'information relative à l'absence de données documentant l'intérêt clinique ou organisationnel est mise à disposition des utilisateurs du service numérique. Ces informations ainsi que les éléments de preuve sont facilement accessibles par les utilisateurs.

  - Obligation QUA.1.5 Interprétation par professionnels de santé

    L'interprétation de données de santé individualisées, produites ou transmises par l'utilisateur, DOIT être assurée par des professionnels dont l'expertise est adaptée à

la thématique couverte et conformément à la réglementation en vigueur, notamment relative à l'exercice des professions de santé.

- Option QUA.1.6 Implication des utilisateurs

  Les contenus médicaux/de santé du service numérique DOIVENT être élaborés en impliquant des utilisateurs représentatifs de la population cible.

1.6 Questionnaire Ethique Mon espace santé

SF_ACC Accessibilité
ACC Accessibilité - Conditions d'accès au service

- ACC.1 Ethique
  - Obligation ACC.1.1 Intuitivité et inclusion de tous les publics

    Le système DOIT être développé dans l'intention d'être intuitif, de façon à être accessible à tous et à n'exclure aucun public (diversité culturelle, handicap, littératie, etc.).

  - 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.1.6 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 Compréhension RGPD

    Le système DOIT garantir la bonne compréhension par l'utilisateur du sens de son consentement dans le cadre de la réutilisation de ses données personnelles recueillies au cours de l'utilisation de l'application, notamment lorsqu'il y a valorisation commerciale des données ou partage des données avec d'autres acteurs ou sous-traitants. La bonne compréhension de l'utilisateur doit également être garantie en cas de limitations des droits RGPD, par exemple, la limitation des droits à l'effacement de ses données ou à la portabilité.

  - Obligation 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.1.5 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.1.6 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.1.9 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.

  - 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.1.2B Ecoconception

    Le système est développé en conformité avec les principes d'écoconception, mis en œuvre à chaque étape de son cycle de vie, dans une démarche plus globale de développement durable.

  - 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.

1.7 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.

1.8 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.

1.8 Parcours dédié DMN

Obligation DMN 1.1 - Possession d'un certificat DMN valide

- Déposer le certificat définitif de conformité au référentiel d'interopérabilité et de sécurité des DM.

1.9 Parcours dédié TLC

Obligation TLC 1.1 - Possession d'un certificat TLC valide

- Déposer le certificat de conformité définitif au référentiel d'interopérabilité, de sécurité et d'éthique des SI de téléconsultation.

2. Annexe - Profilage des questionnaires

2.1 Questionnaire d'orientation

Question d'orientation	Condition d'apparition
2. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical (sans certificat de conformité délivré par l'ANS) ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
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 ou donne-t-il accès aux données suivantes ? »
4. Pour quelle architecture du service sollicitez-vous un référencement à Mon Espace Santé ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
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 ou donne-t-il accès à des données à caractère personnel ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ?	Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
7. Fournir un compte de démonstration (url, identifiant et mot de passe)	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
8. Quelles sont les activités auxquelles concourt votre service ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
8.bis. Autres activités à indiquer	Répondre « Autres » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
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 ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
10. Le service comporte-t-il une partie centralisée (serveurs, etc.) accédée via Internet ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »

	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 ? »
11. Le service comporte-t-il un ou plusieurs équipements fournis par l'industriel pouvant être utilisés en mobilité par l'utilisateur ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
	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 ? »
12. Le service fournit-il un accès dédié à des acteurs de santé (PS ou personnes morales) ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
	OU Répondre « Prévention », « Diagnostic », « Soin », « 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 ? »
13. Le service gère-t-il l'identité d'acteurs de santé (PS ou personnes morales) ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
	OU Répondre « Prévention », « Diagnostic », « Soin », « 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 ? »
14. Le service fournit-il un accès à des données à caractère personnel à des usagers du service numérique de santé (patient, aidant… hors professionnel de santé) ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »

	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
	OU Répondre « Prévention », « Diagnostic », « Soin », « 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 ? »
15. Le service est-il multi-utilisateurs (utilisateurs finaux, administrateurs, etc.) ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
16. Le service assure-t-il ou sous traite-t-il l'hébergement de données de santé au sens des articles L1111-8 et R1111-8-8 du Code de la Santé Publique ?	Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
	OU Répondre « Prévention », « Diagnostic », « Soin », « Suivi social ou médico-social » à la question « 8. Quelles sont les activités auxquelles concourt votre service ? »
17. Le service permet-il un accès par un professionnel de santé (PS) aux données de santé personnelles ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
	ET (Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès aux données suivantes ? »
	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 ? »
	OU Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
	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 ? »**)**
18. Le service échange-t-il des données avec d'autres applications ou SI que Mes ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
19. Le service partage-t-il des données avec d'autres applications ou SI que Mes ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
20. Le service produit ou consomme-t-il ce type de document ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
21. 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 « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
	ET Répondre « Oui » à la question « 2. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical (sans certificat de conformité délivré par l'ANS) ? »
21.bis. En répondant "Oui" à la question précédente, vous devez déposer le certificat de marquage CE et le certificat ISO	Répondre « Oui » à la question « 21. 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) ? »
21.ter. Précisez la classe de votre DM :	Répondre « Oui » à la question « 21. 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) ? »
22. Le service comporte-il un ou plusieurs contenus médicaux/de santé ?	Répondre « Non » à la question « 21. 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) ? »
	ET Répondre « Non » à la question « 2. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical (sans certificat de conformité délivré par l'ANS) ? »
23. Le service a-t-il fait l'objet d'une évaluation clinique ?	Répondre « Non » à la question « 21. 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) ? »
	ET Répondre « Non » à la question « 2. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical (sans certificat de conformité délivré par l'ANS) ? »

24. Le service repose-t-il sur une interprétation de données de santé par des experts ?	Répondre « Non » à la question « 21. 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) ? » **ET** Répondre « Non » à la question « 2. Le service, pour lequel vous candidatez au référencement Mes, est-il un dispositif médical (sans certificat de conformité délivré par l'ANS) ? »
25. Le service produit-il des décisions critiques ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
26. Le service permet-il la création d'un compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, 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 ? » **OU** Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? » **OU** Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
27. Si l'utilisateur ne finalise pas la création de son compte, le service enregistre-t-il les données saisies ?	Répondre « Oui » à la question « 26. Le service permet-il la création d'un compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ? »
28. Le service réutilise-t-il, valorise ou partage-t-il des données personnelles recueillies au cours de l'utilisation du service (valorisation commerciale, partage avec des sous-traitants…) ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? » **OU** Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
29. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires s'appuyant sur la base légale du consentement ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? » **OU** Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
30. Le service manipule-t-il des données sensibles discriminatoires ?	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 « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	OU Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
31. Le service intègre-t-il une Intelligence Artificielle (IA) ?	Répondre « Aucune de ces réponses » à la question « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? »
31.bis. Précisez en quelques mots quel type d'IA est intégrée à votre service	Répondre « Oui » à la question « 31. Le service intègre-t-il une Intelligence Artificielle (IA) ? »

2.2 Questionnaire Interopérabilité

Ce questionnaire s'applique à votre produit si pour la question 1 du questionnaire d'orientation « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? », vous répondez « Aucune de ces réponses ».

Critères du questionnaire d'Interopérabilité	Condition d'apparition
A08.1.1 Utilisation et enrichissement du CI-SIS	Répondre « Oui » à la question « 18. Le service échange-t-il des données avec d'autres applications ou SI que Mes ? »
	OU Répondre « Oui » à la question « 19. 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 « 18. Le service échange-t-il des données avec d'autres applications ou SI que Mes ? »
	OU Répondre « Oui » à la question « 19. 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 « 19. 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 « 20. 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 « 20. 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 « 20. 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 « 20. Le service produit ou consomme-t-il ce type de document ? »
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

Ce questionnaire s'applique à votre produit si pour la question 1 du questionnaire d'orientation « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? », vous répondez « Aucune de ces réponses ».

Critères du questionnaire d'Urbanisation	Condition d'apparition
A06.1 Mise en œuvre de l'INS	Répondre « Oui » à la question « 26. Le service permet-il la création d'un compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ? »
	ET Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
	ET Répondre « Oui » à la question « 17. Le service permet-il un accès par un professionnel de santé (PS) aux données de santé personnelles ? »
A06.2 Intégration des traits d'identité	Répondre « Oui » à la question « 26. Le service permet-il la création d'un compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ? »
	ET Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
	ET Répondre « Non » à la question « 17. Le service permet-il un accès par un professionnel de santé (PS) aux données de santé personnelles ? »

2.4 Questionnaire Maturité Sécurité

Ce questionnaire s'applique à votre produit si pour la question 1 du questionnaire d'orientation « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? », vous répondez « Aucune de ces réponses ».

Critères du questionnaire de Maturité Sécurité	Condition d'apparition
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 ou donne-t-il accès aux données suivantes ? » **ET** Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
	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 ? »
	ET Répondre « Mesures de santé », « Documents » ou « Agenda » à la question « 3. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès aux données suivantes ? »
03.12 - Intégrité du produit	Répondre « Oui » à la question « 10. Le service comporte-t-il une partie centralisée (serveurs, etc.) accédée via Internet ? »
	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 ? » **OU** répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
03.13.01 - Protection des informations (Cryptographie)	Répondre « Non » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »
	OU 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 ou donne-t-il accès à des données à caractère personnel ? » **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 ? »
03.13.02 - Protection des informations (Cryptographie)	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 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 « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? »

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 « 11. Le service comporte-t-il un ou plusieurs équipements fournis par l'industriel pouvant être utilisés en mobilité par l'utilisateur ? »
03.18 - Documentation et bonnes pratiques	Répondre « Oui » à la question « 5. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données à caractère personnel ? »
04.01 - Utilisation et mise à jour des identités nationales des acteurs de santé personnes physiques	Répondre « Acteurs de santé personnes physiques » à la question « 12. Le service fournit-il un accès dédié à des acteurs de santé (PS ou personnes morales) ? » **OU** Répondre « Acteurs de santé personnes physiques » à la question « 13. Le service gère-t-il l'identité d'acteurs de santé (PS ou personnes morales) ? »
04.02 - Niveau de garantie de l'identification électronique des acteurs de santé personnes physiques	Répondre « Acteurs de santé personnes physiques » à la question « 12. Le service fournit-il un accès dédié à des acteurs de santé (PS ou personnes morales) ? »
04.03 - Niveau de garantie de l'identification électronique des patients ou usagers	Répondre « Oui » à la question « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? » **ET** Répondre « Oui » à la question « 14. Le service fournit-il un accès à des données à caractère personnel à des usagers du service numérique de santé (patient, aidant… hors professionnel de santé) ?» **ET** Répondre « Oui » à la question « 26. Le service permet-il la création d'un compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ? »
04.05 - Gestion et séparation des droits	Répondre « Oui » à la question « 15. Le service est-il multi-utilisateurs (utilisateurs finaux, administrateurs, etc.) ? »
04.08 - Utilisation et mise à jour des identités nationales des acteurs de santé personnes morales	Répondre « Acteurs de santé personnes morales » à la question « 12. Le service fournit-il un accès dédié à des acteurs de santé (PS ou personnes morales) ? » **OU** Répondre « Acteurs de santé personnes morales » à la question « 13. Le service gère-t-il l'identité d'acteurs de santé (PS ou personnes morales) ? »
04.09 - Niveau de garantie de l'identification électronique des acteurs de santé personnes morales	Répondre « Acteurs de santé personnes morales » à la question « 12. Le service fournit-il un accès dédié à des acteurs de santé (PS ou personnes morales) ? »
07.02 - Recherche de vulnérabilités	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** 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 ou donne-t-il accès à des données à caractère personnel ? »
08.02 - Veille et patch management	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 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 ou donne-t-il accès à des données à caractère personnel ? »
08.03 - Gestion de l'obsolescence	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 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 ? »
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 « 6. Le service, pour lequel vous candidatez au référencement Mes, contient-il ou donne-t-il accès à des données de santé personnelles ? »
09.04 - Réalisation des sauvegardes	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 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 ou donne-t-il accès à des données à caractère personnel ? »
11.01 - Hébergement de données de santé	Répondre « Oui » à la question « 16. Le service assure-t-il ou sous traite-t-il l'hébergement de données de santé au sens des articles L1111-8 et R1111-8-8 du Code de la Santé Publique ? »

2.5 Questionnaire Qualité du contenu

Ce questionnaire s'applique à votre produit si pour la question 1 du questionnaire d'orientation « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? », vous répondez « Aucune de ces réponses ».

Critères du questionnaire Qualité du contenu	Condition d'apparition
QUA.1.1B Expertise des contributeurs	Répondre « Oui » à la question « 22. Le service comporte-il un ou plusieurs contenus médicaux/de santé ? »
QUA.1.2B Références scientifiques	Répondre « Oui » à la question « 22. Le service comporte-il un ou plusieurs contenus médicaux/de santé ? »
QUA.1.3 Processus de veille	Répondre « Oui » à la question « 22. 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 « 23. 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 « 24. Le service repose-t-il sur une interprétation de données de santé par des experts ? »
QUA.1.6 Implication des utilisateurs	Répondre « Oui » à la question « 22. Le service comporte-il un ou plusieurs contenus médicaux/de santé ? »

2.6 Questionnaire Ethique Mon espace santé

Ce questionnaire s'applique à votre produit si pour la question 1 du questionnaire d'orientation « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? », vous répondez « Aucune de ces réponses ».

Critères du questionnaire Ethique Mon espace santé	Condition d'apparition
ACC.1.6 Alerte sur décision critique	Répondre « Oui » à la question « 25. Le service produit-il des décisions critiques ? »
ETH.1.1 Finalités	Répondre « Oui » à la question « 28. Le service réutilise-t-il, valorise ou partage-t-il des données personnelles recueillies au cours de l'utilisation du service (valorisation commerciale, partage avec des sous-traitants…) ? »
ETH.1.2 Consentement	Répondre « Oui » à la question « 29. Le service comporte-t-il un traitement des données visant des finalités secondaires / accessoires s'appuyant sur la base légale du consentement ? »
ETH.1.3 Service identique	Répondre « Oui » à la question « 28. Le service réutilise-t-il, valorise ou partage-t-il des données personnelles recueillies au cours de l'utilisation du service (valorisation commerciale, partage avec des sous-traitants…) ? »
ETH.1.5 Paramétrage	Répondre « Oui » à la question « 26. Le service permet-il la création d'un compte par l'utilisateur ou par une tierce personne (proche aidant, professionnel de santé, autre) ? »
ETH.1.6 Effacement des données	Répondre « Oui » à la question « 27. Si l'utilisateur ne finalise pas la création de son compte, le service enregistre-t-il les données saisies ? »
ETH.1.9 Données sensibles	Répondre « Oui » à la question « 30. Le service manipule-t-il des données sensibles discriminatoires ? »
INT.1.1 Interaction avec IA	Répondre « Oui » à la question « 31. Le service intègre-t-il une Intelligence Artificielle (IA) ? »
INT.1.2 Documentation biais	Répondre « Oui » à la question « 31. Le service intègre-t-il une Intelligence Artificielle (IA) ? »
INT.1.4 Détection dérive	Répondre « Oui » à la question « 31. Le service intègre-t-il une Intelligence Artificielle (IA) ? »
INT.1.5 Explicabilité	Répondre « Oui » à la question « 31. Le service intègre-t-il une Intelligence Artificielle (IA) ? »
INT.1.6 Eviter les biais	Répondre « Oui » à la question « 31. Le service intègre-t-il une Intelligence Artificielle (IA) ? »

2.6 Questionnaire RGPD Mon espace santé

Critère du questionnaire RGPD Mon espace santé	Condition d'apparition
AIPD	Répondre « Oui » à la question « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ?»

2.7 Questionnaire Sécurité Mon espace santé pour les échanges de données

Ce questionnaire s'applique à votre produit si pour la question 3.bis. du questionnaire d'orientation « 3.bis. Souhaitez-vous que votre service échange des données avec Mon espace santé ? », vous répondez « Oui ».

2.8 Parcours dédié DMN

Ce questionnaire s'applique à votre produit si pour la question 1 du questionnaire d'orientation « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? », vous répondez « Dispositif médical numérique ».

2.9 Parcours dédié TLC

Ce questionnaire s'applique à votre produit si pour la question 1 du questionnaire d'orientation « 1. Le service a-t-il obtenu un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique pour les dispositifs médicaux numériques ou les SI de téléconsultation ? », vous répondez « SI de téléconsultation ».