RÉPUBLIQUE FRANÇAISE

Ministère de la santé et de l’accès aux soins

Arrêté du XX modifiant l'arrêté du 20 novembre 2023 modifiant l'arrêté du 23 octobre 2023 modifiant l'arrêté du 23 juin 2022 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé

NOR : SPRD2310767A

Le ministre de la santé et de l’accès aux soins,

Vu la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015, prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, et notamment la notification n° 2022/083/F ;

Vu le code de la santé publique, notamment ses articles L. 1470-5, R. 1111-37 et R. 1111-39 ;

Vu l’arrêté du 23 juin 2022 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé modifié ;

Vu l’arrêté du 23 octobre 2023 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé modifié ;

Vu l’arrêté du 20 novembre 2023 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé modifié ;

Arrête :

Article 2

L'annexe de l'arrêté du 20 novembre 2023 susvisé, intitulée « Référentiel V2 relatif aux critères de référencement d'un outil ou service numérique dans “Mon espace santé” », est remplacée par le document annexé au présent arrêté, intitulé « Référentiel V3 relatif aux critères de référencement d’un outil ou service numérique dans « Mon espace santé ».

Article 3

La déléguée du numérique en santé est chargée de l'exécution du présent arrêté, qui sera publié au *Journal Officiel* de la République française.

Fait le XX 2025,

Pour le ministre et par délégation :

La déléguée du numérique en santé

H. Ghariani

ANNEXE – Référentiel V3 relatif aux critères de référencement d'un outil ou service numérique dans « Mon espace santé »

Les critères sont répartis dans sept questionnaires thématiques selon la nature des applications candidates au référencement : deux questionnaires spécifiques pour les applications disposant déjà d'un certificat de conformité l'Agence du numérique en santé, quatre questionnaires génériques (« urbanisation », « interopérabilité », « maturité sécurité » et « éthique ») et un questionnaire complémentaire spécifique au référencement avec échange de données (« sécurité pour le référencement avec échange de données »). Les questionnaires sont à compléter sur la plateforme « Convergence » mise à disposition par l'Agence du numérique en santé.

Pour les questionnaires génériques « urbanisation », « interopérabilité », « maturité sécurité », les critères dont les réponses sont graduées et peuvent comporter entre deux et quatre niveaux numérotés de 0 à 3. La liste des critères détaillée ci-après ne comporte que les niveaux définis et accessibles sur la plateforme « Convergence ».

Pour le questionnaire « éthique », les réponses apportées pour les critères sont : « non conforme » ou « conforme » Dans le cas où il est indiqué que le critère obligatoire « éthique » est conforme, une ou des pièces justificatives doivent être fournies pour justifier l'atteinte du critère.

Pour le questionnaire « sécurité pour le référencement avec échange de données », l'éditeur doit, sur la plateforme « Convergence », télécharger un formulaire dédié, et après l'avoir complété le déposer ainsi que les preuves associées.

Par ailleurs, pour justifier l'atteinte de certains critères optionnels, des pièces justificatives doivent être constituées et tenues à disposition par l'éditeur dans la perspective de l'évaluation continue du service numérique, elles ne sont pas à fournir lors de la demande initiale.

Les réponses aux questionnaires sont exigées ou non en fonction du type d'outil ou du service numérique et du type de référencement souhaité (sans / avec échange de données avec « Mon espace santé »). Ce conditionnement est réalisé sur la plateforme « Convergence » par un questionnaire d'orientation caractérisant l'outil ou le service numérique et la demande de son propriétaire. L'obtention d'un certificat de conformité aux référentiels sectoriels adoptés par l'ANS (dispositifs médicaux numériques ou société de

téléconsultation) permet de remplir les conditions prévues à l'article R1111-37 du code de la santé publique pour permettre le référencement d'un outil au catalogue de service.

Sommaire

1. Parcours dédié aux dispositifs médicaux numérique....2
2. Parcours dédié aux sociétés de téléconsultation....3
3. Parcours générique de référencement....3
   a. Urbanisation....3
   b. Interopérabilité....4
   c. Maturité sécurité....7
   d. Qualité du contenu....19
   e. Ethique....23
4. Sécurité pour le référencement avec échange de données....34
5. Finalités....42

Légende
gatoire en fonction de la typologie du service et de la demande de référencement
Niveaux acceptés pour les critères obligatoires
Critère optionnel

1. Parcours dédié aux dispositifs médicaux numérique

DMN 1.1 – Possession d'un certificat DMN valide

L'industriel DOIT avoir un certificat définitif de conformité au référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques (DMN) en cours de validité, prévu à l'article L. 1470-5 du code de la santé publique établis par le groupement d'intérêt public mentionné à l'article L. 1111-24 du code de la santé publique (ANS) et l'application candidate au référencement DOIT être inclue dans le périmètre du certificat de conformité.

a. Pièces justificatives : le certificat définitif de conformité au référentiel d'interopérabilité et de sécurité des DMN

2. Parcours dédié aux sociétés de téléconsultation

TLC 1.1 – Possession d'un certificat TLC valide

L'industriel DOIT avoir un certificat définitif de conformité au référentiel d'interopérabilité, de sécurité et d'éthique des SI de téléconsultation en cours de validité, prévu à l'article L. 1470-5 du code de la santé publique établi par le groupement d'intérêt public mentionné à l'article L. 1111-24 du code de la santé publique (ANS) et l'application candidate au référencement DOIT être inclue dans le périmètre du certificat de conformité.

a. Pièces justificatives : le certificat de conformité définitif au référentiel d'interopérabilité, de sécurité et d'éthique des SI de téléconsultation

3. Parcours générique de référencement

a. Urbanisation

A06. Identification électronique des patients, usagers ou personnes

❗ A06.1 Mise en œuvre 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 apparait.
- 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 est autorisé CNDA à faire appel au téléservice INSi.
- ✓ Niveau 2 : Le produit est autorisé CNDA à faire appel au téléservice INSi et a intégré l'ensemble des exigences applicables au produit du guide d'implémentation de l'INS.

❗ 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 apparait.
- 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.

b. Interopérabilité

A08.1 Référentiel d'interopérabilité (généralités)

ℹ A08.1.1 Utilisation et enrichissement du CI-SIS

- Niveau non applicable : Toujours applicable si le critère apparait.
- 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)

ℹ A08.3.1 Connexion synchrone avec d'autres SI

- Niveau non applicable : Toujours applicable si le critère apparait.
- Niveau 0 : La connexion avec d'autres SI se fait via des normes autres que celles identifiées dans le CI-SIS (ex. VPN et MLLP pour des connexions WAN, FTP, CFT...).
- Niveau 1 : La connexion avec d'autres SI se fait via les normes identifiées dans le CI-SIS sans respecter exactement l'ensemble des spécifications d'un des volets de la couche transport du CI-SIS (transport synchrone pour client lourd ou transport synchrone pour applications mobiles ou web).
- Niveau 2 : La connexion avec d'autres SI se fait en suivant les spécifications d'un des volets de la couche transport du CI-SIS (transport synchrone pour client lourd ou transport synchrone pour applications mobiles ou web).
- Niveau 3 : La connexion avec d'autres SI se fait en suivant les spécifications d'un des volets de la couche transport du CI-SIS (transport synchrone pour client lourd ou transport synchrone pour applications mobiles ou web) et les éléments fournis dans le VIHF contribuent à la mise en œuvre de la politique de sécurité (droit d'accès, traçabilité...).

A08.4 Référentiel d'interopérabilité (service)

ℹ 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).

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

- Niveau non applicable : Toujours applicable si 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).

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

- Niveau non applicable : Toujours applicable si 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)

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).

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

A10.2 Utilisation des nomenclatures de l'ANS

- Niveau non applicable : Toujours applicable si le critère apparait.
- 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.

c. Maturité sécurité

01. Gouvernance SSI

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, les responsables de la sécurité sont identifiés. Leurs responsabilités couvrent les activités de conception, de développement, d'installation, d'exploitation, d'administration et de maintenance (selon le périmètre dont l'industriel a la responsabilité vis à vis de la structure utilisatrice).
- ✓ 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.

❗ 01.04.01 - Sensibilisation des équipes en charge (pour les services n'échangeant pas de données avec Mes et/ou contenant des données personnelles)

- 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).

❗ 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 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).

03. Conception sécurisée

❗ 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.

❗ 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.

❗ 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.

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.

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 de 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.

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

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.

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.

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.

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.

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.

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

❗ 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 par les scanners de vulnérabilité ou au cours d'un test d'intrusion 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

❗ 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.

❗ 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 environnement 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 environnement de fonctionnement sont effectués au moins 1 an avant la fin de support annoncée pour ces éléments.

09. Continuité d'activité

❗ 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 et d'améliorer son efficacité

❗ 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 informations nécessaires. Cependant, ce plan ainsi que l’ensemble des documents le 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.

❗ 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/appliance 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

- 11.01 - Hébergement de 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).

d. Qualité du contenu

QUA Qualité du contenu

- ❗ 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.
  - Pièces justificatives : Noms, qualifications et liens d'intérêts des experts impliqués dans la sélection, validation et/ou rédaction du contenu médical/de santé, preuve de l'accessibilité des informations (copies d'écran des pages livrant l'information et les indications de navigation permettant d'y accéder).
  - Détail des pièces dans Convergence
    - 1. Liste des contributeurs
      Dresser la liste ou rediriger vers la liste des experts ayant sélectionné, validé ou rédigé chaque contenu médical avec leur nom et leurs qualifications. Faire la différence entre les personnes ayant participé à la construction du contenu médical publié dans le service et les personnes ayant validé ce contenu médical.
    - 2. Déclaration des liens d'intérêts
      Indiquer ou rediriger vers la déclaration des liens d'intérêts des experts
    - 3. Accessibilité de l'information
      Fournir les pages/ endroits consultables en ligne qui fournissent les informations des 1. et 2. (copies d'écran avec parcours d'accès, liens vers les URL du site web...), si possible en distinguant ceux produits et ceux repris d'une organisation externe.

- ❗ 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.

  - Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment la liste des sources et références scientifiques, de même que les copies d'écran des pages livrant l'information et les indications de navigation permettant d'y accéder.

  1. Détails des pièces dans convergence
     - 1. Liste des sources et références scientifiques

       Indiquer ou rediriger vers – la liste des organisations à l'origine du contenu et URL actualisée des sites internet associés (intra-App, site web ressources, documentation externe, référence en fin de contenu…).
       Indiquer la liste des références scientifiques utilisées.
     - 2. Accessibilité de l'information

       Fournir les endroits consultables en ligne qui fournissent les informations (copies d'écran, liens vers les URL du site web…).

- ❗ 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.

  1. Pièces justificatives : synthèse de la stratégie de veille et de mise à jour du contenu, ainsi que les copies d'écran des pages livrant l'information et les indications de navigation permettant d'y accéder.
  2. Détails des pièces dans convergence
     - 1. Stratégie de veille et de mise à jour

       Décrire la stratégie de veille et de mise à jour des sources clés et des références scientifiques (notamment la fréquence) ainsi que les principaux experts en charge de la veille avec leur nom et leurs qualifications.
     - 2. Accessibilité de l'information

       Fournir les endroits où la date de mise à jour de l'information est publiée et la manière dont l'actualisation est mise en avant auprès de l'utilisateur (copies d'écran, liens vers les URL du site web, parcours de navigation, lisibilité de l'information, résultats d'enquêtes de satisfaction/groupes utilisateurs, etc.). En cas de transmission des résultats d'une enquête utilisateurs, préciser quelle question évalue la facilité d'accès de l'information concernant le processus de veille.

- ❗ QUA.1.4 Evaluation clinique et éléments 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.

  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tout document décrivant l'évaluation clinique du service et justifiant de l'accessibilité de l'information. En l'absence d'évaluation clinique, tout document prouvant l'accessibilité de cette information.
  2. Détails des pièces dans convergence

- 1. Evaluation du service

Lorsqu'elle existe, décrire l'évaluation clinique réalisée (description du design de l'étude clinique, des résultats obtenus et de leur niveau de preuve)

- 2. Accessibilité de l'information

Fournir les preuves de l'accessibilité des informations mises à disposition des utilisateurs (copies d'écran, liens vers les URL du site web…). Ces informations peuvent être :

  - des publications dans des revues scientifiques à comité de lecture, protocoles, rapports d'études ;
  - des informations publiques issues de bases de données d'essais sur les études en cours, à venir ou les études dont les résultats n'auraient pas été publiés ;
  - une mention indiquant l'absence de données cliniques disponibles pour documenter l'intérêt, qu'il soit clinique ou organisationnel ;
  - le ou les avis de la CNEDiMTS dans le cas où la solution aurait fait l'objet d'une évaluation dans le cadre d'une demande de remboursement par la solidarité nationale (le plus récent s'il correspond à l'ensemble des indications pour lesquelles le remboursement a été revendiqué ou l'ensemble des avis les plus récents correspondant à chacune des indications pour lesquelles le remboursement a été revendiqué).

- ❗ 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.

1. Pièces justificatives : une synthèse de la procédure d'interprétation détaillant notamment la liste des personnes qualifiées pour cette interprétation, leurs qualifications, et les contenus de santé dépendant de leur champ d'expertise.
2. Détails des pièces dans convergence
   - 1. Liste des professionnels de santé qualifiés pour l'interprétation

     Décrire qui sont les professionnels de santé (avec leur nom et leurs qualifications) en rappelant l'ensemble des contenus de santé et en attribuant à chaque contenu de santé au moins une personne qualifiée pour les interpréter.
   - 2. Processus d'interprétation

     Décrire quand (en première ligne, en deuxième ligne…) et comment est mise en place l'interprétation.

- ℹ QUA.1.6 Implication des utilisateurs (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)

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

1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tous les documents de la stratégie de sollicitation des utilisateurs dans le développement du contenu du service numérique.
2. Détails des pièces dans convergence
   - 1. Décrire la stratégie de sollicitation des utilisateurs dans le développement du contenu du service numérique (grille d'analyse, Living Lab, etc.), nombre d'utilisateurs et/ou liste des organisations d'utilisateurs impliquées.

e. Ethique

ACC Accessibilité - Conditions d'accès au service

- ❗ 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.).

  1. Pièces justificatives :
     - tout document de nature à attester de la mise en œuvre d'une méthode d'évaluation de l'intuitivité
     - tout document de nature à attester de la mise en oeuvre d'une méthode d'évaluation de l'accessibilité
  2. Détails des pièces dans convergence
     - 1. Par exemple transmettre le certificat RG2A, les documents multilingues.
     - 2. Indiquer les travaux en cours pour augmenter l'accessibilité et l'intuitivité du service. Par exemple préciser si le service existe en plusieurs langues, notamment en créole.
     - 3. Si des tests utilisateurs ont été réalisés Décrire la méthodologie - notamment les utilisateurs impliqués en insistant sur la diversité du groupe (en termes par exemple d'âge, de sexe, de handicap, de niveau de littératie, de CSP...) - et les résultats des tests. Exemple de tests : groupes utilisateurs, sondages, enquêtes de satisfaction...
     - 4. S'il n'y a pas eu de tests utilisateurs Décrire le format ou la méthode utilisé(e) pour évaluer la capacité du service à n'exclure aucun public et être intuitif (grille d'analyse, écritoire, living lab, etc.).

- ❗ 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 les utilisateurs à utiliser la solution numérique

  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment un descriptif du service d'assistance, un document attestant de l'accessibilité de l'information sur son existence, un descriptif du parcours de navigation permettant d'y accéder.
  2. Détails des pièces dans convergence
     - 1. Documentation du service d'assistance et de support Fournir la documentation du service d'assistance et de support avec une interaction humaine (incluant notamment les modalités d'assistance telles que mail avec délai de réponse, téléphone avec heures d'ouverture...).
     - 2. Accessibilité de l'information
       Fournir les endroits où ces informations sont publiées, ainsi que le parcours de navigation pour y parvenir (copies d'écran, URL du site web, etc.).

- ℹ ACC.1.4 Aides en ligne (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)

  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

  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tous les documents d'orientation vers l'aide en ligne (copies d'écran).

2. Détails des pièces dans convergence
    - 1. Décrire la stratégie dans ce domaine et les éléments mis à disposition de l'utilisateur pour faciliter l'utilisation du service (aide contextuelle, aide en ligne, manuel utilisateur, tutoriel, didacticiel, e-learning, etc.).

- ℹ ACC.1.6 Alerte sur décision critique (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  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.
  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment l'analyse des risques, le système d'alerte et ses éventuels prérequis.
  2. Détails des pièces dans convergence
     - 1. Fournir une analyse des risques en fonction du niveau de gravité des conséquences en cas de mauvaise interprétation de l'information ciblée par l'application.
     - 2. Décrire le système d'alerte mis en place et le calibrage de son déclenchement.
       S'il y a des prérequis pour que le système d'alerte fonctionne, les préciser (numéro de téléphone de l'utilisateur connu, adresse mail de l'utilisateur connue, etc.).

- ℹ ACC.1.7 Réponses aux questions (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  Le système documente, actualise et rend accessible aux utilisateurs les réponses aux questions fréquemment posées
  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tout document attestant l'accessibilité de l'information concernant les questions fréquemment posées, et le parcours de navigation pour y accéder.
  2. Détails des pièces dans convergence
     - 1. Fournir les endroits où cette information est publiée
     - 2. Fournir le parcours de navigation pour y parvenir (copies d'écran, liens vers les URL du site web...).

ETH Ethique de la transparence

- ℹ ETH.1.1 Compréhension RGPD (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)
  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.
  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment la méthode mise en œuvre pour évaluer la compréhension de l'utilisateur sur le périmètre de son consentement à la ré-utilisation de ses données, de l'éventuelle valorisation commerciale de ses données, de leur éventuel partage avec d'autres acteurs et la limitation de ses droits RGPD.

2. Détails des pièces dans convergence

    - 1. Décrire les moyens utilisés pour évaluer la bonne compréhension par l'utilisateur du périmètre de son consentement à la ré-utilisation de ses données, de leur éventuel partage avec d'autres acteurs et la limitation de ses droits RGPD ainsi que les résultats obtenus (par exemple groupes de travail, enquêtes utilisateurs, etc.)
    - 2. Si des tests utilisateurs ont été réalisés, décrire la méthodologie - notamment les utilisateurs impliqués en insistant sur la diversité du groupe (en termes par exemple d'âge, de sexe, de handicap, de niveau de littératie, de CSP...) - et les résultats des tests (par exemple, groupes utilisateurs, sondages, enquêtes utilisateurs, etc.)

- ❗ ETH.1.2 Consentement

  Pour les finalités dont la base légale est le 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.

  1. Pièces justificatives : Tout élément de nature à prouver que l'utilisateur a la possibilité de consentir à une partie seulement du traitement de ses données.
  2. Détails des pièces dans convergence
     - 1. Décrire les mécanismes de consentement « à la carte » : le service doit proposer un consentement distinct pour chacune des finalités. Capture d'écran montrant qu'il n'existe pas de case pré-cochée. En cas de transmission des Conditions Générales d'Utilisation, veuillez fournir une copie d'écran de l'endroit où se trouvent les informations concernées (page / paragraphe).
- ❗ ETH.1.3 Service identique

  Le système DOIT proposer un service identique quels que soient les choix opérés par l'utilisateur concernant le traitement de ses données personnelles
  - Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment une description des moyens utilisés pour évaluer le caractère identique du service dans différents scenarios d'utilisation et les résultats obtenus.
  - Détails des pièces dans convergence
    - 1. Donner accès à un compte de démonstration sur le service numérique, permettant de tester les scenariois d'utilisation quel que soit le consentement de l'utilisateur
    - 2. En cas d'impossibilité à tester ces scenarios via le compte de démonstration , décrire les moyens utilisés pour évaluer le caractère identique de la solution dans différents scenarios d'utilisation quel que soit le consentement de l'utilisateur :

- ❗ 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)
  1. Pièces justificatives : description du paramétrage des interactions
  2. Détails des pièces dans convergence

        - 1. Décrire les mécanismes permettant de moduler / paramétrer l'intensité des interactions avec la solution numérique (par exemple, ne pas recevoir de sms le soir et le weekend) et les modalités d'activation de ces mécanismes par l'utilisateur (ex. copie d'écran et parcours de navigation pour arriver à obtenir les explications pour faire le paramétrage).

- ℹ ETH.1.6 Effacement des données (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)
  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'utilisateur décide finalement de ne pas aller au bout et de renoncer à l'utilisation du service.
  1. Pièces justificatives : Document décrivant le processus d'effacement des données.
  2. Détails des pièces dans convergence
     - 1. Décrire les mécanismes permettant l'effacement total des données saisies au cours des premières étapes de l'utilisation du service si l'utilisateur décide de ne pas aller au bout (par exemple les données recueillies lors de la création d'un compte) et renonce à l'utilisation du service, ainsi que la façon pour les utilisateurs de les mettre en œuvre.

- ℹ ETH.1.9 Données sensibles (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  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

  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tout document attestant de l'accessibilité de l'information, tout document décrivant la méthode mise en œuvre pour évaluer la compréhension des motifs justifiant cette collecte.
  2. Détails des pièces dans convergence

     - 1. Accessibilité de l'information
       Fournir les endroits où l'information sur les raisons du recueil de données susceptibles de donner lieu à des discriminations est publiée.
     - 2. Compréhension par l'utilisateur
       Décrire les moyens utilisés pour évaluer la bonne compréhension par l'utilisateur de ces raisons.

2. ℹ ETH.1.10 Bénéfices et limites (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
   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

   1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tout document attestant de l'accessibilité de l'information, tout document décrivant la méthode mise en œuvre pour évaluer la compréhension des bénéfices et limites
   2. Détails des pièces dans convergence

      - 1. Accessibilité de l'information
        Fournir les endroits où l'information sur les bénéfices et les limites du service

est publiée. Nb : Les bénéfices (avantages) sont souvent listés dans les CGU de la solution, sur sa home page, au sein d'une brochure commerciale… Les limites (inconvénients) apparaissent souvent dans les CGU, la FAQ, ou des pop-ups contextuelles à l'utilisation. Par exemple, une limite peut être un résultat d'écoscore faible, une performance partielle ou encore des fonctionnalités non-couvertes par la solution. Elles indiquent généralement que la solution ne se substitue pas à un service d'urgence et qu'en cas de doute l'utilisateur doit contacter le SAMU ou consulter un professionnel de santé.

- 2. Compréhension par l'usager
  Décrire les moyens utilisés pour évaluer la bonne compréhension par l'usager de ces bénéfices et limites afin qu'il réalise un choix éclairé.

INT Intelligence artificielle et éthique

On appelle système d'intelligence artificielle (SIA) un logiciel, développé à l'aide d'une ou de plusieurs des techniques et approches énumérées ci-dessous, capable de calculer à partir d'éléments reçus en entrée des résultats représentant des prédictions, des recommandations ou des propositions de décisions susceptibles d'influencer des environnements, physiques ou virtuels, avec lesquels le SIA interagit. Les différents systèmes d'IA varient en fonction de leur niveau d'autonomie et de leur capacité d'adaptation après leur déploiement.

Les techniques et approches considérées pour ce questionnaire sont les suivantes :

- Les approches d'apprentissage automatique (AAA) encore appelées apprentissage machine, notamment les apprentissages supervisé, non supervisé ou par renforcement, pouvant utiliser une grande variété de techniques, y compris l'apprentissage profond. Les systèmes d'IA générative utilisant ce type d'approche et s'appuient sur des réseaux neuronaux numériques profonds pour générer leurs résultats. Les AAA permettent aux SIA d'identifier des motifs, des structures, ou des relations dans les données puis de les utiliser pour produire un résultat.
- Les approches logiques et fondées sur les connaissances, intégrant le raisonnement (symbolique), les bases de connaissances, les moteurs d'inférence notamment déductifs, la programmation inductive (logique) et les systèmes experts.
- Les approches statistiques, l'estimation bayésienne, les méthodes de recherche et d'optimisation.

- 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.
  - Pièces justificatives : Document attestant de l'accessibilité de l'information.
  - Détails des pièces dans convergence
    1. 1. Fournir les endroits où l'utilisateur est informé qu'il interagit avec une solution d'IA (copies d'écran, liens vers le site web…)

- 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
  - Pièces justificatives : Document attestant de l'accessibilité de l'information.
  - Détails des pièces dans convergence
    1. 1. Fournir les endroits où le niveau de performance et les biais algorithmiques de la solution d'IA est publié (copies d'écran, liens vers le site web…).

- ℹ INT.1.4 Détection dérive (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  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

    1. Pièces justificatives : Document décrivant les mécanismes de détection précoce de dérive.
    2. Détails des pièces dans convergence

        - 1. Décrire les mécanismes permettant de détecter précocement si le système d'IA a « dérivé » et nécessite une nouvelle évaluation.

- ℹ INT.1.5 Explicabilité (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  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
    - Pièces justificatives : Document décrivant l'explicabilité.
    - Détails des pièces dans convergence
        - 1. Décrire les mécanismes permettant d'expliquer les propositions du système d'IA ou de mettre en place d'autres mesures d'explicabilité.

- ℹ INT.1.6 Eviter les biais (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  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
    1. Pièces justificatives : Document décrivant les mécanismes permettant d'éviter les biais discriminatoires.
    2. Détails des pièces dans convergence
        - 1. Décrire les mécanismes permettant d'éviter de créer ou de renforcer les biais discriminatoires tout au long du cycle de vie de la solution d'IA.

DEV Développement durable

- ❗ 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
    1. Pièces justificatives : valeur d'éco-score correspondant au service et code GDSL du script ayant été utilisé pour la mesure finale.
    2. Détails des pièces dans convergence
        - 1. Fournir la copie d'écran du site écoscore avec votre résultat publié https ://ecoscore-appli.esante.gouv.fr.

- ℹ DEV.1.2B Ecoconception (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  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

1. Pièces justificatives : tout document de nature à attester de la mise en œuvre des principes d'écoconception
2. Détails des pièces dans convergence
    - 1. Par exemple transmettre le score d'Ecoconception en utilisant NumEcoDiag proposé par la MiNumEco (https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/numecodiag/)
    - 2. Indiquer le taux des collaborateurs de l'entreprise qui sont sensibilisés / formés à l'éc-conception, aux analyses en cycle de vie de l'impact environnemental du numérique, etc.
    - 3. Fournir tout élément de nature à démontrer l'engagement de l'éditeur dans une démarche de développement durable (écolabel attribué par des organismes indépendants, politique GreenIT, rapport annuel RSE, etc.)

- ℹ DEV.1.4 Faible débit et équipements anciens (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  Le système est accessible en faible débit et à partir d'équipements ne nécessitant pas d'être de dernière génération.
  1. Pièces justificatives : tout document de nature à démontrer que le service est accessible en faible débit et utilisable avec des équipements anciens
  2. Détails des pièces dans convergence :
     - 1. Faible débit :
       - Concernant une application web : copies écrans de l'application avec un navigateur bridé en 3G
       - Concernant une application mobile : activation du mode 3G et enregistrement du fonctionnement dans un film vidéo
     - 2. Equipements anciens : Le service doit pouvoir fonctionner correctement sur tout produit/plateforme qui fait toujours l'objet d'un support par son fabriquant/éditeur/fournisseur, c'est à dire jusqu'à sa date de fin de support officiellement communiquée par ce fabriquant.
       - Fournir la liste des versions de système d'exploitation supportées par l'éditeur

- ℹ DEV.1.5 Réduire consommation datacenters (ce critère étant optionnel, aucune évaluation ne sera faite en évaluation initiale)
  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. Pièces justificatives : Document actions de réduction consommation.
  2. Détails des pièces dans convergence
     - 1. Fournir tout élément de nature à démontrer les actions mises en œuvre pour réduire la consommation de ressources et d'énergie liée à l'hébergement (par exemple mesures de sobriété énergétique telles que valorisation de la chaleur fatale, limitation d'utilisation de ressources en eau à des fins de refroidissement, limitation du renouvellement des terminaux, réduction des espaces de stockage (source : loi REEN, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044327272).

4. Sécurité pour le référencement avec échange de données

Règle 01

- ❗ R01 - Politique de Sécurité des Systèmes d'Information (PSSI)

L'industriel DOIT élaborer, tenir à jour et mettre en œuvre une politique de sécurité des réseaux et systèmes d'information (PSSI).

La PSSI DOIT couvrir l'application soumise au référencement Mon espace santé et l'ensemble des environnements liés à l'application (production et hors-production).

- Pièces justificatives : la Politique de Sécurité des Système d'Information – PSSI

Règle 02

- R02 - Analyse de risques

L'industriel DOIT effectuer et tenir à jour une analyse de risques. Le périmètre de l'analyse de risques DOIT couvrir l'application soumise au référencement Mon espace santé et le système d'information de production sous-jacent. En résultat de l'analyse de risques, l'industriel DOIT identifier les biens sensibles et les risques associés, les mesures de sécurité identifiées à mettre en œuvre et les risques résiduels.

- Pièces justificatives : Analyse de risques présentant notamment le plan de traitement des risques et les risques résiduels (le plan de traitement des risques doit être mis à jour à la date du référencement sur Mon espace santé).

Règle 03

- R03 - Audits de sécurité

L'industriel DOIT définir et mettre en œuvre un programme d'audit qui permette d'évaluer au cours du temps le niveau de sécurité de l'application soumise au référencement Mon espace santé et de l'environnement de production sous-jacent au regard des menaces et des vulnérabilités connues.

Le programme d'audit DOIT notamment prévoir un audit au minimum trisannuel (aligné avec le processus d'homologation, cf. règle R04), réalisé obligatoirement par un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié. Cet audit DOIT notamment comprendre :

- L'audit de la configuration des serveurs et équipements réseau inclus dans le périmètre du service. Cet audit est réalisé par échantillonnage et doit inclure tous types d'équipements et de serveurs présents dans le système d'information du service, y compris ceux participants à l'exploitation et à l'administration du service ;

- Le test d'intrusion des accès externes au service ;

- Si le service bénéficie de développements internes, l'audit de code source portant sur les fonctionnalités de sécurité implémentées.

- Pièces justificatives :
  1. Programme d'audit (types d'audit, fréquence, périmètre…) ;
  2. Derniers rapports d'audit :
     - Tests d'intrusion applicatif pour vérifier l'implémentation des fonctions de sécurité ;
     - Tests d'intrusion sur le SI lié à l'environnement de production de l'application ;
     - Tests d'intrusion sur le SI d'administration ;
     - Audit de code de l'application pour vérifier l'implémentation des fonctions de sécurité ;

        - Audit de configuration pour vérifier l'implémentation des règles de sécurité et durcissement (hardening) sur les équipements (serveurs, matériels réseau & sécurité).
    3. Si les rapports d'audits contiennent des anomalies majeures, il sera nécessaire de présenter :
        - Le plan d'action associé à l'audit ;
        - Des preuves permettant de constater que les mesures correctives ont été implémentées

Règle 04

- ❗ R04 - Homologation interne de sécurité

L'industriel DOIT procéder à l'homologation interne de sécurité de l'application soumise au référencement Mon espace santé.

- Pièces justificatives :
    1. Dossier d'homologation.
    2. Décision d'homologation (dernière en date) comportant la signature de l'autorité d'homologation interne de l'industriel.

Règle 05

- ❗ R05 - Conception et développement sécurisés de l'application

L'industriel DOIT respecter les bonnes pratiques de sécurité lors de la conception et du développement de l'application soumise au référencement Mon espace santé.

L'industriel DOIT mettre en place des mesures de sécurité adaptées dans l'environnement de production mais aussi du côté du terminal de l'utilisateur.

- Pièces justificatives :
    1. Rapport d'audit :
        - Tests d'intrusion applicatif pour vérifier l'implémentation des fonctions de sécurité.

Règle 06

- ❗ R06 - Configuration sécurisée des systèmes d'information liés à l'application

L'industriel DOIT respecter les bonnes pratiques de configuration sécurisée lorsqu'il installe des services et des équipements sur les systèmes d'information de l'application soumise au référencement Mon espace santé.

Les règles de configuration visent le renforcement du niveau de sécurité des SI par un durcissement (hardening) et incluent :

- La limitation et une configuration adaptée des fonctions présentes sur les SI ;
- La maîtrise des éléments matériels des SI ;
- La maîtrise et sécurisation des vecteurs d'intégration de données vers les SI (tels que les supports amovibles).

- Pièces justificatives :
    - Rapport d'audit :
    - Rapports d'audit :

        - Tests d'intrusion sur le SI lié à l'environnement de production de l'application.
        - Audit de configuration pour vérifier l'implémentation des règles de sécurité et durcissement (hardening) sur les équipements (serveurs, matériels réseau & sécurité).
    - Description des mesures de durcissement employées.
        - Pour la partie 'maitrise des vecteurs d'intégration de données', la description de la politique antivirale (périmètre technique sur lequel la couverture antivirale est appliquée / non appliquée ; procédure de surveillance des alertes antivirales).
        - Dernier rapport d'audit de configuration pour vérifier l'implémentation des règles de sécurité et durcissement (hardening) sur les équipements (serveurs, matériels réseau & sécurité).
        - Dernier rapport des tests d'intrusion sur le SI lié à l'environnement de production de l'application.

Règle 07

- R07 - Cryptographie

L'intégrité et la confidentialité des données sensibles de l'application soumise au référencement Mon espace santé et du SI de production sous-jacent DOIVENT être garanties et contrôlées à l'aide de mécanismes cryptographiques conformes au Référentiel Général de Sécurité (RGS) et aux dernières recommandations de l'ANSSI en vigueur.

- Pièces justificatives :
    - Description des protocoles et algorithmes de protection d'intégrité et confidentialité des données au repos et lors du transport (Ces éléments peuvent apparaître lors des analyses de risques).

Règle 08

- R08 - Cloisonnement et filtrage

L'industriel DOIT réaliser le cloisonnement de ses systèmes d'information afin de limiter la propagation des incidents de sécurité au sein de ses systèmes ou ses sous-systèmes.

L'industriel DOIT mettre en place des mécanismes de filtrage des flux de données circulant dans ses systèmes d'information afin de n'autoriser que les seuls flux de données nécessaires au fonctionnement et à la sécurité des SI.

L'industriel DOIT mettre en place une revue régulière des mesures de cloisonnement et de filtrage.

- Pièces justificatives :
    - Description des protocoles et algorithmes de protection d'intégrité et confidentialité des - Compte-rendu de la revue (contrôle interne ou externe) de l'application des mesures de cloisonnement et filtrage.
    - Des éléments qui prouvent que les revues des mesures de cloisonnement et filtrage sont réalisées régulièrement. Cela inclut :
        - Formalisation de la fréquence adoptée par l'industriel pour la réalisation de ces revues ;
        - Compte rendu des revues précédentes prouvant la réalisation des revues avec la fréquence définie par l'industriel.

Règle 09

- R09 - Protection des accès distants au SI

L'industriel DOIT mettre en place des mesures de sécurité pour protéger le système d'information de production des accès réalisés à travers des systèmes d'information tiers.

  - Pièces justificatives :
    - Description de l'architecture et des mécanismes de protection des accès distants des postes de travail se connectant au SI associé à l'application soumise au référencement Mon espace santé.

Règle 10

- R10 - Sécurité de l'administration des systèmes d'information

L'industriel DOIT créer des comptes (appelés « comptes d'administration ») destinés aux seules personnes (appelées « administrateurs ») chargées d'effectuer les opérations d'administration (installation, configuration, gestion, maintenance, supervision, etc.) des ressources (infrastructures et applications) du SI de production sous-jacent à l'application soumise au référencement Mon espace santé.

Les ressources matérielles et logicielles des SI d'administration DOIVENT être utilisées exclusivement pour réaliser des opérations d'administration.

L'industriel DOIT effectuer une revue régulière des comptes d'administration.

  - Pièces justificatives :
    - Descriptif des mesures de séparation des privilèges, de séparation du SI d'administration et des ressources utilisées pour l'administration, accompagné d'un schéma d'architecture du SI d'administration.
    - Rapport de la revue des comptes d'administration.
    - Rapports des tests d'intrusion sur le périmètre du SI d'administration approuvé par l'industriel.

Règle 11

- R11 - Gestion des identités et des accès

L'industriel DOIT créer des comptes individuels pour tous les utilisateurs et pour tous les processus automatiques accédant aux ressources de ses systèmes d'information.

L'industriel DOIT protéger les accès aux ressources de l'application et des systèmes d'information sous-jacents, que ce soit par un utilisateur ou par un processus automatique, au moyen d'un mécanisme d'authentification impliquant un élément secret.

L'industriel DOIT définir, conformément à sa politique de sécurité des réseaux et systèmes d'information, les règles de gestion et d'attribution des droits d'accès aux ressources de l'application et des systèmes d'information sous-jacents.

Les mécanismes d'identification et d'authentification des usagers de l'application DOIVENT respecter les exigences du Référentiel d'Identification Electronique des Usagers ou du Référentiel d'Identification Electronique des acteurs de santé publiés par l'Agence du Numérique en Santé.

- Pièces justificatives :
    - Descriptif des règles d'identification, authentification et droits d'accès, formalisées dans un document de communication interne (PSSI, politique de mots de passe, procédure d'identification, procédures d'authentification, procédure de gestion des droits, rapport de revue des comptes et des accès…).
    - Description de l'architecture associée aux moyens d'identification électronique.

Règle 12

- R12 - Maintien en condition de sécurité

L'industriel DOIT élaborer, tenir à jour et mettre en œuvre un processus de maintien en condition de sécurité des ressources matérielles et logicielles de l'application soumise au référencement Mon espace santé.

- Pièces justificatives :
    - Description des processus de maintien en condition de sécurité.

Règle 13

- R13 - Systèmes de journalisation, corrélation, analyse et détection des évènements

L'industriel DOIT mettre en œuvre des mesures organisationnelles et techniques de journalisation, détection, corrélation et analyse d'évènements de sécurité de l'application soumise au référencement Mon espace santé et du SI de production sous-jacent.

- Pièces justificatives :
    - Description du système de journalisation.
    - Description du système de corrélation et d'analyse de journaux.
    - Description des processus de détection des incidents de sécurité.

Règle 14

- R14 - Réponse aux incidents de sécurité et gestion de crise

L'industriel DOIT mettre en place un processus spécifique pour traiter les incidents de sécurité et un processus de gestion de crises en cas d'incidents de sécurité ayant un impact majeur sur l'application et/ou les SI sous-jacents, en conformité avec la convention de référencement à Mon espace santé.

Le processus DOIT comprendre un annuaire ou une procédure incluant un annuaire des correspondant à alerter en cas de crise.

- Pièces justificatives :
    - Procédure de réponse aux incidents.
    - Procédure de gestion de crises.

Règle 15

- R15 - Certification des Hébergeurs de Données de Santé

Les hébergeurs des applications soumises à l'article L. 1111-8 du Code de la Santé Publique DOIVENT être certifiés Hébergeur de Données de Santé (HDS).

Une justification doit être fournie lorsque la certification HDS n'est pas applicable à l'industriel.

- Pièces justificatives :
  - Certification HDS à jour couvrant le SI de production sous-jacent à l'application soumise au référencement Mon espace santé ou une justification de non-applicabilité.

5. Finalités

- **Case à cocher impérativement par l'éditeur afin de poursuivre son référencement**

« L'outil ou le service numérique ne peut accéder (en lecture et/ou en écriture) aux données de Mon espace santé, avec l'accord exprès du titulaire, qu'à la condition que cet accès poursuive l'une des finalités suivantes : prévention, diagnostic, soins, suivi social et médico-social (art. L.1111-13-1 III du code de la santé publique). Les données de Mon espace santé auxquelles l'outil ou le service numérique aura ainsi accédé ne peuvent pas être réutilisées pour une quelconque autre finalité. »