RÉPUBLIQUE FRANÇAISE

Ministère de la santé et de la prévention

Arrêté du XX 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 la prévention,

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 les notifications n° 2022/083/F et n° 2023/XXX/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 ;

Arrête :

Article 1

L’arrêté du 23 juin 2022 susvisé est ainsi modifié :

1° A l’article 1er :

Le deuxième alinéa est supprimé.

2° A l’article 4 :

Au premier alinéa, sont supprimés les mots « pour être recevable ».

Au quatrième alinéa, après les mots : « prévoit la production d’une pièce justificative », sont ajoutés les mots : « à fournir en évaluation initiale ».

3° Après l’article 4, il est inséré un article 5 ainsi rédigé : « seule est recevable la demande de référencement au catalogue de service de Mon espace santé qui a été reçue dans les conditions définies aux articles 2,3 et 4. »

Article 2

L'annexe de l'arrêté du 23 juin 2022 susvisé, intitulée « Référentiel V1 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 V2 relatif aux critères de référencement d’un outil ou service numérique dans « Mon espace santé ».

Article 3

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

Fait le XX 2023,

Pour le ministre et par délégation :

La déléguée au numérique en santé

H. Ghariani

ANNEXE – Référentiel V2 relatif aux critères de référencement d'un outil ou service numérique dans « Mon espace santé »

Les critères sont répartis dans cinq questionnaires thématiques : trois questionnaires en lien avec la doctrine du numérique en santé (« urbanisation », « interopérabilité », « maturité sécurité ») et deux questionnaires complémentaires (« éthique » et « sécurité pour le référencement avec échange de données ») à compléter sur la plateforme « Convergence » mise à disposition par l'Agence du numérique en santé en vue d'un dépôt d'une demande de référencement au catalogue de services de Mon espace santé.

Pour les questionnaires thématiques en lien avec la doctrine du numérique en santé (« urbanisation », « interopérabilité », « maturité sécurité »), les critères dont les réponses sont graduées 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 complémentaire « éthique », les réponses apportées **pour les critères sont : «** non conforme », « conforme » ou « non applicable ». 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 complémentaire « 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 pièces justificatives associées.

Par ailleurs, pour justifier l'atteinte de certains critères optionnels, des pièces justificatives doivent être constituées et tenues à disposition par l'éditeur à compter du dépôt de la demande de référencement et pendant toute la durée du référencement, même si elles ne sont pas à fournir lors de la demande initiale.

L'ensemble de ces critères sont exigés ou non en fonction de la typologie de l'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 l'éditeur.

Sommaire

1. Urbanisation.....2
2. Interopérabilité.....4
3. Maturité sécurité.....8
4. Ethique.....34
5. Sécurité pour le référencement avec échange de données.....49
6. Finalités.....57

Légende

oire en fonction de la typologie de l'outil ou du service et de la demande de référencement

Niveaux acceptés pour les critères obligatoires

Critère optionnel

1. Urbanisation

A06. Identification électronique des patients, usagers ou personnes

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

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

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

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

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

- Niveau non applicable : Toujours applicable si le critère apparait.
- Niveau 0 : Le produit n'est pas en capacité d'intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques.
- ✓ Niveau 1 : Le produit peut intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques.
- ✓ Niveau 3 : Le produit peut intégrer des INS (flux, documents, etc.) en provenance d'autres services numériques. Par ailleurs le produit sait diffuser les INS qualifiés en aval en respectant les standards d'interopérabilité en vigueur, et notamment dans les documents de santé (CDA, PDF, etc.) éventuellement générés à partir du produit.

A18. Télésanté

ℹ A18.2 Référentiel télémédecine – Téléexpertise

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

2. 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.

A08.2 Référentiel d'interopérabilité (modélisation)

ℹ A08.2.1 Formalisation des usages

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

A08.3 Référentiel d'interopérabilité (transport)

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).

A08.6 Référentiel d'interopérabilité (test)

ℹ A08.6.1 Test des interfaces

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

A10. Terminologies de santé

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

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

ℹ 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.

3. 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.

01.02.01 - Organisation et processus de la sécurité (pour les services n'échangeant pas de données avec Mes et ne contenant pas de données personnelles)

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

01.02.02 - Organisation et processus de la sécurité (pour les services qui contiennent des données personnelles et/ou échangent des données avec Mes)

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

- ✓ Niveau 3 : Conforme au niveau précédent, plus : Des tableaux de bord d'indicateurs sont présentés et rassemblent l'ensemble des indicateurs techniques et fonctionnels pour chaque activité assurée.

01.03 - Processus d'amélioration continue

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

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 (pour les services qui échangent des données avec Mes)

- 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).

01.05.01 - Certification ISO 27001

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : L'industriel n'applique pas, ou de manière accessoire, les standards de la série ISO 2700x au périmètre incluant les SI utilisés pour ses différentes activités liées au produit (selon le cas :

développement, distribution, gestion des mises à jour, tests, hébergement et exploitation, administration système, applicative et sécurité, maintenance ou administration à distance, ...).

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

02. Dossier sécurité

02.02.01 - Analyse de risques et certification de sécurité (pour les services n'échangeant pas de données avec Mes mais contenant des données personnelles)

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

02.02.02 - Analyse de risques et certification de sécurité (pour les services qui échangent des données avec Mes)

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

02.03.01 - Plan d'Assurance Sécurité (pour les services n'échangeant pas de données avec Mes et ne contenant pas de données personnelles)

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

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

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

❗ 02.03.02 - Plan d'Assurance Sécurité (pour les services qui échangent des données avec Mes)

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

03. Conception sécurisée

❗ 03.01 - Configuration sécurisée des composants du produit (pour les services qui échangent des données avec Mes et/ou contenant des données personnelles)

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

❗ 03.02 – Antivirus

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun antivirus n'est intégré, ni prévu d'être intégrable, dans le produit.
- ✓ Niveau 1 : Un antivirus est intégré dans le produit, ou intégrable (par exemple via le protocole ICAP "Internet Content Adaptation Protocol - RFC3507" ou CVP "Content Vectoring Protocol", ou

par appel d'exécutable local), afin de contrôler tout fichier reçu au niveau de tout composant permettant l'import de fichier (par téléversement ou autre) susceptible de constituer ou de contenir un malware (virus ou autre). A défaut, dans le cas où les composants recevant les fichiers téléchargés sont fournis sous forme uniquement logicielle, ces composants réagissent de manière appropriée, et sans dysfonctionner, au blocage d'un fichier par l'antivirus présent sur la plateforme qui héberge ces composants. La documentation identifie explicitement les éventuels fichiers faisant légitimement partie du produit mais devant être exclus de toute analyse par antivirus (en cas de risque élevé de faux positif). Si un antivirus fait partie du produit, les procédures d'exploitation et de mise à jour de l'antivirus sont documentées. Si le produit est fourni sous forme de service, il intègre effectivement la fonction antivirus.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : Si le produit est fourni sous forme de plateforme/appliance, un antivirus contrôle tout fichier présent sur tout équipement informatique constitutif de cette plateforme/appliance et les signatures de virus sont maintenues à jour. La nature de l'antivirus est indiquée dans la description du produit. Si le produit est fourni sous forme de service, le moteur antivirus et les signatures de virus sont maintenues à jour. Dans les autres cas, le produit peut s'interfacer avec un large choix d'antivirus du marché, dont la liste est communiquée dans la description du produit et au sein de laquelle la structure utilisatrice peut choisir l'antivirus qu'elle souhaite utiliser.

03.04 - Contrôle des flux réseaux et applicatifs

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

03.05 - Développement sécurisé

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

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

03.06 - Protection des développements

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

03.07 - Architecture sécurisée

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

03.08 - Contrôle d'accès au réseau

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

03.09 - Environnements

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Le produit fourni sous forme de service dispose d'un seul environnement, utilisé pour la production (Prod).

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

03.10 - Procédures opérationnelles

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune documentation opérationnelle spécifique au produit n'est fournie à la structure utilisatrice.
- ✓ Niveau 1 : Une documentation de la gestion opérationnelle du produit est formalisée et fournie à la structure utilisatrice.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : la documentation opérationnelle fournie porte au minimum sur : les opérations de configuration, les opérations d'administration, les opérations de sauvegarde/restauration, la gestion des incidents.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : La documentation opérationnelle fournie fait l'objet de mises à jour régulières (pour tenir compte des évolutions de la plateforme, en fonction des incidents...).

03.11 - Inventaire des composants et des flux

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

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 Mon espace santé)

- 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.

03.16 - Connectivité Wifi

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : La documentation du produit ne précise pas les modalités techniques de connectivité sans fil par Wifi.
- Niveau 1 : Les équipements mobiles du produit ne disposent pas de protocole sécurisé Wifi à l'état de l'art pour communiquer. Une description des niveaux de sécurité supportés et des compléments de sécurisation possibles est toutefois fournie à la structure utilisatrice pour permettre l'évaluation d'un mode de prise en charge acceptable de la sécurité.
- ✓ Niveau 2 : L'authentification des utilisateurs, l'intégrité et la confidentialité des données échangées par Wifi avec les équipements mobiles du produit sont assurées par la mise en œuvre de

mécanismes s'appuyant sur le mode WPA2-PSK (WPA2-Personnel) avec utilisation de l'algorithme de chiffrement AES-CCMP. La clé de sécurité pour WPA2 est conforme aux règles d'élaboration de mots de passe non triviaux et changée dès l'installation puis régulièrement. Si un point d'accès Wifi fait partie du produit, il est conforme au Guide pratique technique pour la mise en place d'un accès Wifi de la PGSSI-S. NB : le mode WPA2-PSK n'est acceptable que dans la mesure où les flux applicatifs sensibles sont chiffrés, conformément à l'objectif fixé sur ce point dans le critère relatif à la protection des informations.

- ✓ Niveau 3 : L'authentification des utilisateurs, l'intégrité et la confidentialité des données échangées par Wifi avec les équipements mobiles du produit sont assurées par la mise en œuvre de mécanismes s'appuyant sur la norme WPA2-entreprise (standard 802.1X et protocole EAP, idéalement EAP-TLS) ou ultérieurs garantissant le plus haut niveau de sécurité (version de la norme IEEE 802.11i certifiée par la Wifi Alliance), avec utilisation de l'algorithme de chiffrement AES-CCMP.

❗ 03.17 - Prise en compte du guide Dispositifs connectés

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

04. Identification, authentification et autorisations

❗ 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.

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

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

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.

04.06 - Comptes génériques

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

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.

06. Sécurité physique

❗ 06.01 - Contrôle d'accès physique aux équipements informatiques

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

07. Audit

❗ 07.01 - Réalisation d'audits de code

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun audit de code n'est réalisé sur le produit.
- Niveau 1 : Un audit de code est réalisé avant la validation de la version initiale du produit. Le périmètre de cet audit doit au minimum inclure le code qui assure : le traitement des données en entrée, le traitement de données en sorties, les fonctions de sécurité, telles qu'authentification, gestion de session, contrôle d'accès, fonctions cryptographiques, gestion des clés et aux secrets... Les vulnérabilités, erreurs et non-conformités aux règles de développement en vigueur identifiées donnent lieu à un plan d'actions en vue de leur correction.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Un audit de code est réalisé sur le produit de manière au minimum annuelle. Au sein du périmètre défini au niveau précédent, cet audit porte au minimum sur les parties du code modifiées depuis le dernier audit et sur celles susceptibles d'être impactées par ces modifications.
- ✓ Niveau 3 : Conforme au niveau précédent, plus : Un audit de code est réalisé avant toute validation de changement majeur dans le produit. Au sein du périmètre défini aux niveaux précédents, cet audit porte au minimum sur les parties du code modifiées depuis le dernier audit et sur celles susceptibles d'être impactées par ces modifications.

❗ 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.

❗ 07.04 - Plan d'actions

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

08. Maintien en condition de sécurité

❗ 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.

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

❗ 08.05.01 - Politique de gestion des changements (pour les services n'échangeant pas de données avec Mes mais contenant des données personnelles)
- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucune politique de gestion des changements n'est définie et mise en œuvre.
- ✓ Niveau 1 : Une politique de gestion des changements est définie et mise en œuvre mais elle ne couvre pas l'intégralité des points suivants : la politique de gestion des changements doit faire partie de la documentation opérationnelle ; La procédure à suivre doit être définie et un comité d'approbation des changements doit être nommé ; Le suivi des changements doit être assuré dans un fichier qui peut être un simple tableur. Ce fichier devra être revu de façon régulière (lors des comités de pilotage du produit et/ou lors des comités dédiés à la sécurité par exemple).
- ✓ Niveau 2 : Une politique de gestion des changements est définie, mise en œuvre et couvre l'intégralité des points. Cependant, aucune mise jour de la documentation opérationnelle n'est réalisée.

- ✓ Niveau 3 : Conforme au niveau précédent, plus : La documentation opérationnelle est mise à jour périodiquement et en cas de changement majeur de l'organisation.

08.05.02 - Politique de gestion des changements (pour les services qui échangent des données avec Mes si le critère apparaît)

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

09. Continuité d'activité

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.

10. Télémaintenance

ℹ 10.01 - Remontées d'informations

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : La documentation (contrat ou autre) de la prestation ne précise pas si des remontées d'informations issues des dispositifs maintenus ont lieu vers le SI du prestataire.
- Niveau 1 : La documentation (contrat ou autre) de la prestation précise que des remontées d'informations issues des dispositifs maintenus ont lieu vers le SI du prestataire. La nature des informations remontées est décrite précisément et exhaustivement, ainsi que les modalités techniques de ces communications.
- Niveau 2 : Conforme au niveau précédent, plus : Ces remontées d'information sont effectuées exclusivement à des fins de surveillance du maintien en condition opérationnelle et en condition de sécurité. Ces remontées d'information utilisent des protocoles sécurisés, sont tracées et peuvent passer par les passerelles de contrôle d'accès à internet éventuellement mises en place par la structure utilisatrice ou par un VPN IPSEC site à site établi avec le site de télémaintenance.
- Niveau 3 : Conforme au niveau précédent, plus : L'absence de données à caractère personnel directement ou indirectement liées aux patients (ou autres personnes liées aux traitements) est garantie.

ℹ 10.02 - Architecture de télémaintenance

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

téléassister peut être ouvert et fermé par le personnel habilité de la structure utilisatrice quand nécessaire à l'intervention du prestataire.

- Niveau 3 : Conforme au niveau précédent, plus : Si la structure utilisatrice dispose d'un bastion d'administration ou le met en place ultérieurement, le prestataire est en mesure de l'utiliser pour accéder aux systèmes qu'il doit maintenir, exploiter, ou téléassister sans pénalité pour la structure utilisatrice ni sur la qualité des prestations réalisées.

ℹ 10.03 - Traçabilité des interventions

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

4. Ethique

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

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

    Le système DOIT mentionner et documenter que l'expertise des personnes qui sélectionnent, valident ou rédigent les contenus médicaux/de santé publiés dans le service est adaptée à la thématique couverte par le service. Cette information, ainsi que les liens d'intérêts des personnes, est mise à disposition des utilisateurs du service numérique et facilement accessible à tous. Lorsque les contenus médicaux sont directement repris du site internet d'une organisation, notamment d'une agence nationale ou d'une société savante, dont l'information est réputée comme fiable, le nom de l'organisation et l'URL du site devront être indiqués.
    - Pièces justificatives : liste des contributeurs, tout document mentionnant les liens d'intérêt et leur expertise sur le sujet traité, 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.1.2 Références scientifiques**

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

- 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 sources et références scientifiques clés utilisées pour chaque contenu médical (intra-App, site web ressources, documentation externe, référence en fin de contenu…).
    - 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 système DOIT documenter que le processus de veille et de mise à jour des sources et des références scientifiques qui ont été utilisées pour l'élaboration du contenu médical/de santé du service est adapté à la thématique couverte par le service. Cette information est mise à disposition des utilisateurs du service numérique et facilement accessible à tous.

1. Pièces justificatives : stratégie de veille et de mise à jour, 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 niveaux de preuve**

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

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.
2. Détails des pièces dans convergence
    - 1. Evaluation du service

    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 endroits où l ’évaluation clinique et ses résultats sont publiés (copies d'écran, liens vers les URL du site web…).

- ❗ QUA.1.5 Interprétation par professionnels de santé

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

  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment la liste des personnes qualifiées pour cette interprétation et les contenus de santé dépendant de leur champ d’expertise, et tout document décrivant le processus d'interprétation.
  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.

SF_ACC Accessibilité

ACC Accessibilité - Conditions d'accès au service

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

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

    1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tout document décrivant la méthode d'évaluation de l’accessibilité, Document RG2A, Document multilingue.
    2. Détails des pièces dans convergence
       - 1. 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…
       - 2. 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 (grille d’analyse, écritoire, living lab, etc.). Par exemple transmettre le certificat RG2A.
       - 3. Indiquer les travaux en cours pour augmenter l'accessibilité du service.

       Par exemple préciser si le service existe en plusieurs langues, notamment en créole.

  - ❗ ACC.1.2 Intuitif et compréhensible

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

    1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment la méthode d’évaluation de l’intuitivité.
    2. Détails des pièces dans convergence

        - 1. Si des tests utilisateurs ont été réalisés
          Décrire la méthodologie et les résultats des tests – 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…
        - 2. 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 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 l'utilisateur 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, un descriptif du parcours de navigation.
  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.).

- ACC.1.4 Aides en ligne (ce critère étant optionnel, aucune pièce justificative ne sera exigée 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.).

- ACC.1.5 Guichet (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)
  SI le service permet de réaliser des démarches essentielles de santé ou de vie courante ALORS le système DOIT proposer des modes d'accès humain alternatifs et une assistance en présentiel (par exemple, un guichet)
  1. Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment les documents décrivant les modes d'accès humains, l'accessibilité de l'information, et le parcours de navigation.
  2. Détails des pièces dans convergence
     - 1. Modes d'accès et d'assistance
       Décrire des modes d'accès humains alternatifs et de l'assistance en présentiel
     - 2. Accessibilité de l'information
       Fournir les endroits où ces informations sont publiées

Fournir le parcours de navigation pour y parvenir (copies d'écran, liens vers le site web…).

- ℹ ACC.1.6 Alerte sur décision critique (ce critère étant optionnel, aucune pièce justificative ne sera exigée 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 pièce justificative ne sera exigée 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 ddocument attestant l'accessibilité de l'information, le parcours de navigation
  2. Détails des pièces dans convergence
     - 1. Fournir les endroits où ces informations sont publiées
     - 2. Fournir le parcours de navigation pour y parvenir (copies d'écran, liens vers les URL du site web…).

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

- ETH.1 Ethique
  - ℹ ETH.1.1 Finalités (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)
    Le système DOIT mettre en œuvre des mécanismes afin de garantir la bonne compréhension de l'utilisateur sur le périmètre de son consentement au traitement de ses données personnelles, en faisant la différence entre les traitements servant la production du service (la ou les finalité(s) principale(s)) et ceux servant des finalités secondaires/accessoires.
    - 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 du périmètre du consentement.
    - Détails des pièces dans convergence
      - Compréhension par l'utilisateur

      Décrire les moyens utilisés pour évaluer la bonne compréhension par l'utilisateur du périmètre de son consentement, ainsi que les résultats obtenus (par exemple groupes de travail, enquêtes utilisateurs, etc.).

  - ℹ ETH.1.2 Consentement (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)

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.

- 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.
- Détails des pièces dans convergence
  - Décrire les mécanismes de consentement « à la carte » : le service doit proposer un consentement distinct pour chacune des finalités secondaires. L'ensemble des finalités secondaires/accessoires du service et citées dans les CGU doivent faire l'objet d'un consentement distinct par l'utilisateur (cases à cocher lors de l'inscription, formulaires dédiés au sein de l'application etc.)
    En cas de transmission des Conditions Générales d'Utilisation avec vos réponses au questionnaire RGPD, veuillez nous transmettre ici une copie d'écran de l'endroit où se trouvent les informations concernées (page / paragraphe).

o **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
  - 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 :
    - L'ensemble des traitements de données personnelles est coché
    - Une partie seulement du traitement des données personnelles est cochée
    En cas de transmission des Conditions Générales d'Utilisation, veuillez nous transmettre une copie d'écran de l'endroit où se trouvent les informations concernées (page / paragraphe).

o **ETH.1.4 Valorisation**

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

  - 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, la compréhension de la valorisation secondaire, ainsi que les CGU et la Politique de confidentialité.
- Détails des pièces dans convergence
  - 1. CGU et politique de confidentialité
    Fournir les CGU et la politique de confidentialité et préciser les chapitres (ou pages/articles) où sont listées les finalités des traitements pouvant constituer une valorisation secondaire des données collectées (envoi d'une newsletter, enquêtes de satisfaction, marketing, statistiques etc. y compris après anonymisation de ces données). Ces finalités doivent être les mêmes dans les CGU et dans l'information fournie aux utilisateurs.
  - 2. Compréhension par l'utilisateur

Décrire les moyens utilisés pour évaluer la bonne compréhension de la valorisation secondaire des données, ainsi que les résultats obtenus.

- 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)
  - Pièces justificatives : description du paramétrage des interactions
  - 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).

- 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.
  - Pièces justificatives : Document décrivant le processus d'effacement des données.
  - 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.

- ETH.1.7 Destinataires/Sous-traitants (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)

  SI les données recueillies sont partagées avec d'autres acteurs, notamment des sous-traitants, ALORS le système met en œuvre des mécanismes afin de garantir la bonne compréhension par l'utilisateur de l'existence de ce partage et de sa finalité
  - 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 et tout document décrivant la méthode mise en œuvre pour évaluer la compréhension du partage des données.
  - Détails des pièces dans convergence
    - 1. Accessibilité de l'information

      Fournir les endroits où l'information sur l'existence de sous-traitants et des finalités du partage de données avec chacun d'eux est publiée.
    - 2. Compréhension par l'utilisateur

      Décrire les moyens utilisés pour évaluer la bonne compréhension par l'utilisateur de l'existence de ces partages et de leurs finalités, ainsi que les résultats obtenus.

- ETH.1.8 Limitation des droits RGPD (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)

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

- Pièces justificatives : tout document de nature à attester les mesures mises en œuvre pour atteindre le critère, et notamment tout document décrivant la méthode mise en œuvre pour évaluer la compréhension de la limitation des droits
- Détails des pièces dans convergence
  - Compréhension par l'utilisateur : décrire les moyens utilisés pour évaluer la bonne compréhension par l'utilisateur de cette information sur la limitation de ses droits RGPD.

- ℹ ETH.1.9 Données sensibles (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)
  SI des données susceptibles de donner lieu à des discriminations (comme la religion, 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
  - 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.
  - 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.

- ℹ ETH.1.10 Bénéfices et limites (ce critère étant optionnel, aucune pièce justificative ne sera exigée 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
  - 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
  - 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.1 Ethique
  - 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. 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. 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…).

  - INT.1.3 Détection dépendance

    SI le service intègre un traitement algorithmique produit par une IA ALORS le système DOIT mettre en œuvre des mécanismes permettant de détecter précocement si le système d'IA crée une dépendance des utilisateurs ou manipule leur comportement
    - Pièces justificatives : Document décrivant les mécanismes de détection précoce.
    - Détails des pièces dans convergence
      - 1. Décrire les mécanismes permettant de détecter précocement si le système d'IA crée une dépendance des utilisateurs ou manipule leur comportement.

  - INT.1.4 Détection dérive (ce critère étant optionnel, aucune pièce justificative ne sera exigée 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
    - Pièces justificatives : Document décrivant les mécanismes de détection précoce de dérive.
    - 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.

  - INT.1.5 Explicabilité (ce critère étant optionnel, aucune pièce justificative ne sera exigée 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.

  - INT.1.6 Eviter les biais (ce critère étant optionnel, aucune pièce justificative ne sera exigée 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

- Pièces justificatives : Document décrivant les mécanismes permettant d'éviter les biais discriminatoires.
- 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.

SF_DEV Développement durable
DEV Développement durable

- DEV.1 Ethique
  - 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
    - Pièces justificatives : valeur d'éco-score correspondant au service et rapports de tests.
    - Détails des pièces dans convergence
      - 1. Fournir la copie d'écran du site écoscore avec votre résultat publié https ://ecoscore-appli.esante.gouv.fr.

  - DEV.1.2 Cycle de vie (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)

    Le système s'intègre, dans son cycle de vie, dans une démarche plus globale de développement durable
    - Pièces justificatives : Document engagement développement durable.
    - Détails des pièces dans convergence
      - 1. 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…).

  - DEV.1.3 Ecoconception (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)

    Le système met en œuvre des pratiques de conception responsable afin de réduire l'impact environnemental du service
    - Pièces justificatives : Document engagement écoconception.
    - Détails des pièces dans convergence
      - 1. Fournir tout élément de nature à démontrer l'engagement de l'éditeur (sensibilisation et formation de l'ensemble des parties prenantes aux impacts environnementaux du numérique et à l'éco-conception, prévision d'une revue de conception de la solution orientée vers une solution sobre…)

  - DEV.1.4 Faible débit et équipements anciens (ce critère étant optionnel, aucune pièce justificative ne sera exigée en évaluation initiale)

    Le système est accessible en faible débit et à partir d'équipements ne nécessitant pas d'être de dernière génération.
    - Pièces justificatives : tout document de nature à démontrer que le service est accessible en faible débit et depuis des équipements anciens
    - 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

o ℹ DEV.1.5 Réduire consommation datacenters (ce critère étant optionnel, aucune pièce justificative ne sera exigée 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

- Pièces justificatives : Document actions de réduction consommation.
- 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.

5. 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).

o 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.

o 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 :
        - Programme d'audit (types d'audit, fréquence, périmètre…) ;
        - 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).
        - 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 :
        - Dossier d'homologation.
        - 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 :
  - 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 R06 -

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 :
  - 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 (y compris ceux ayant des comptes privilégiés ou des comptes d'administration) 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.

6. 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. »