REFERENTIEL D'EVALUATION CONTINUE
Catalogue Mon espace santé
Version 2025

Sommaire

L'évaluation continue est la procédure d'évaluation des solutions référencées et est réalisée pour vérifier la conformité du service à la doctrine du numérique en santé et aux exigences spécifiques à Mon espace santé. Elle permet de garantir la conformité dans le temps des éléments déclarés au cours des étapes du référencement.

L'arrêté du 20 novembre 2023 relatif à la procédure d'audit des outils et services numériques référencés au catalogue de service de l'espace numérique de santé, en défini l'organisation et les principales étapes.

L'évaluation porte sur des critères répartis au sein de trois volets et en fonction de la nature du service référencé :

- **Urbanisation** : Les critères sont présentés ci-après. Les exigences applicables à chaque critère et permettant d'évaluer la conformité déclarée, sont décrites pour le volet.

- **Maturité-sécurité** : Les critères sont présentés ci-après. Les exigences et leurs scénarios de conformités applicables à chaque critère et permettant d'évaluer la conformité déclarée, sont également décrits.

- **Ethique** : Les critères éthiques sont qualifiés en deux catégories, P1 et P2. Les critères P1 seront évalués en fonction des conditions d'applicabilité. Si les preuves communiquées ne sont pas suffisantes ou de nombreuses non-conformités détectées, des critères P2 pourront être demandés en complément.

NB : Par ailleurs, pour justifier l'atteinte de certains critères optionnels, des pièces justificatives ont dû être constituées et tenues à disposition dans la perspective de l'évaluation continue du service numérique. Elles pourront également être à soumettre.

Légende éthique

Critère P1 — Critères éthiques P1 (obligatoire)

Critère P2 — Critères éthiques P2 (déclenchés si besoin)

Légende urbanisation & maturité sécurité

Critère — Critère de l'arrêté du référencement initial au catalogue de service de Mon espace santé

Exigence — Exigence applicable au critère

Scénario — Scénario applicable à l'exigence

Légende des réponses

✓ Niveaux acceptés pour les critères

○ Une seule réponse est acceptée

☐ Plusieurs réponses sont acceptées

1. Questionnaires de la démarche

1.1 Questionnaire de qualification

Description du service

Obligation 1. Le service pour lequel vous avez été référencé contient ou donne accès à des données à caractère personnel :

- Oui
- Non

Obligation 1.bis. Le service pour lequel vous avez été référencé contient ou donne accès à des données de santé personnelles :

- Oui
- Non

Hébergement

Obligation 2. Le service référencé assure ou sous traite l'hébergement de données de santé au sens des articles L1111-8 et R1111-8-8 du Code de la Santé Publique :

- Oui
- Non

Description métier du service candidat

Obligation 3. Les activités déclarées auxquelles concourt le service référencé sont :

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

Obligation 3.bis. Autres activités à indiquer – Champ texte libre

Identification, authentification et autorisations

Obligation 4. Le service référencé fournit un accès dédié à des acteurs de santé personnes physique :

- Oui
- Non

Obligation 4.bis. Pour l'identification électronique des PS : Le service met-il en œuvre exclusivement une ou plusieurs identifications électroniques basée sur un moyen d'identification électronique au moins conforme au niveau eIDAS substantiel tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des acteurs de santé personnes physiques ?

- Oui
- Non

Obligation 5. Le service référencé fournit un accès à des données à caractère personnel à des usagers du service numérique en santé (patient, aidant… hors professionnel de santé) :

- Oui
- Non

Obligation 5.bis. Pour l'identification électronique des usagers (patients, aidants, hors PS) : Le service met-il en œuvre exclusivement une ou plusieurs identifications électroniques au moins conformes au niveau eIDAS substantiel tel que défini dans le référentiel de la PGSSI-S sur l'identification électronique des patients ?

- Oui
- Non

Identité Nationale de Santé (INS)

Obligation 6. Le service permet un accès par un professionnel de santé (PS) aux données de santé personnelles :

- Oui
- Non

Obligation 6.bis. Le service référencé créé de l'identité :

- Oui
- Non

1.2 Questionnaire Urbanisation

A06. Identification électronique des patients, usagers ou personnes

Critère A06.1 Mise en œuvre de l'INS (pour les services dont les données des utilisateurs sont accessibles par des professionnels de santé)

- Niveau non applicable : Toujours applicable si le critère apparait.
- Niveau 0 : Le produit n'est pas autorisé CNDA à faire appel au téléservice INSi et n'a pas intégré les traits de l'INS.
- Niveau 1 : Le produit est autorisé CNDA à faire appel au téléservice INSi.
- ✓ Niveau 2 : Le produit est autorisé CNDA à faire appel au téléservice INSi et a intégré l'ensemble des exigences applicables au produit du guide d'implémentation de l'INS.

Exigence INS/va1.01

- Le système DOIT être conforme aux exigences du "Référentiel national d'identito-vigilance (RNIV) - volet 1 à volet 4" [INS8], précisées dans le "Guide d'implémentation INS" [INS9].
- Le système DOIT permettre l'enregistrement de l'ensemble des champs suivants :
    - matricule INS,
    - OID,
    - nom de naissance,
    - prénom(s) de naissance,
    - 1er prénom de naissance,
    - date de naissance,
    - sexe,
    - code lieu de naissance,
    - nom utilisé,
    - prénom utilisé

Exigence INS/va1.21

- Le système DOIT respecter le "Guide d'implémentation INS" [INS9]
- Le système NE DOIT PAS permettre la création d'une identité si les champs suivants ne sont pas alimentés :
    - nom de naissance,
    - 1er prénom de naissance,
    - date de naissance,
    - sexe
    - code lieu de naissance
- A noter : pour rappel, si certaines de ces données ne sont pas connues au moment de la création de l'identité, le "Référentiel national d'identito-vigilance (RNIV) - volet 1 à volet 4" [INS8] précise les valeurs qui peuvent être utilisées pour renseigner ces champs (par exemple : si le code du lieu de naissance n'est pas connu, saisir 99999)

Exigence INS/va1.23

- Le système DOIT gérer les statuts et attributs de l'identité, en respectant le "Guide d'implémentation INS" [INS9]
- Le système DOIT permettre de renseigner la nature du justificatif (pièce justificative ou dispositif à haut niveau de confiance ou son équivalent) ayant permis de créer/vérifier l'identité de l'usager comme mentionné dans le "Référentiel national d'identito-vigilance"[INS8].

Exigence INS/va1.47

- Si le système est référentiel d'identité, alors le système DOIT gérer les statuts et attributs de l'identité, en respectant le "Guide d'implémentation INS" [INS9]
- Le système DOIT mettre en évidence le caractère non modifiable des champs matricule INS, OID, nom de naissance, prénom(s) de naissance, date de naissance, sexe et code lieu de naissance d'une identité au statut « identité récupérée » ou « identité qualifiée ».
- À noter : Le premier prénom de naissance, s'il fait bien partie des traits stricts d'une identité, ne fait pas partie des traits stricts qui composent l'INS.
- A ce titre, ce champ doit rester à la main de l'utilisateur, quel que soit le statut de l'identité, à condition qu'il reste cohérent avec le début de la liste des prénoms de naissance retournés par le téléservice INSi.

Exigence INS/va1.51

- Le système DOIT respecter le "Guide d'implémentation INS" [INS9]
- Le système DOIT s'assurer de la cohérence entre le champ prénom(s) de naissance alimentée par le retour d'INSi et le champ 1er prénom renseigné par l'utilisateur.

Exigence INS/va1.52

- Le système DOIT respecter le "Guide d'implémentation INS" [INS9]
- Le système DOIT alimenter les champs suivants par les données retournées par INSi après attribution du statut "identité qualifiée" ou "identité récupérée" :
    * matricule INS,
    * OID,
    * nom de naissance,
    * prénom(s) de naissance,
    * date de naissance,
    * sexe
    * code lieu de naissance

Exigence INS/va1.54

- Le système DOIT gérer les statuts et attributs de l'identité, en respectant le "Guide d'implémentation INS" [INS9]
- Le système DOIT attribuer par défaut le statut "identité provisoire" à une identité.

- Le système DOIT attribuer le statut "identité validée" à toute identité pour laquelle l'identité de l'usager a été vérifiée sur la base d'un dispositif à haut degré de confiance mais qui n'a pas été créée/mise à jour sur la base du retour d'INSi.
- Le système DOIT attribuer le statut "identité récupérée" à toute identité créée/mise à jour sur la base du retour d'INSi mais pour laquelle l'identité de l'usager n'a pas été vérifiée sur la base d'un dispositif à haut degré de confiance.
- Le système DOIT attribuer le statut "identité qualifiée" à toute identité pour laquelle l'identité de l'usager a été vérifiée sur la base d'un dispositif à haut degré de confiance et a été créée/mise à jour sur la base du retour d'INSi.
- Le système DOIT historiser tout changement de statut (statut antérieur, date de mise à jour du statut et responsable de la mise à jour).

Exigence SC.INS.01

- Le système DOIT permettre l'implémentation des référentiels de l'INSEE portant sur les codes officiels géographiques, y compris la codification des pays et territoires étrangers. Ces référentiels sont disponibles en téléchargement sur le site de l'INSEE (cf. https://www.insee.fr/fr/information/7766585)
- Les fichiers à implémenter et qui doivent faire l'objet d'une mise à jour régulière sont les suivants :
  - Communes
  - Pays
  - Evènements sur les communes
  - Communes depuis 1943
  - Communes des collectivités d'outre-mer
- Le référentiel du logiciel ne DOIT pas comporter de noms de communes abrégés (par exemple, « St » pour « Saint »). Il DOIT, en revanche, comprendre les arrondissements de villes comme Lyon, Paris et Marseille.
- Conformément au "Guide d'implémentation INS" [INS9] - EXI ID14

Exigence SC.INS.02

- LORSQUE le champ « Code lieu de naissance - Code INSEE » n'est pas renseigné à partir du téléservice INSi mais à partir d'une saisie par l'utilisateur, ALORS le système DOIT :
  - au préalable avoir le champ "Date de naissance" renseigné
  - d'une part permettre à l'utilisateur de saisir le nom de la commune / du pays de naissance,
  - et d'autre part lui proposer le code INSEE et le libellé de la commune / du pays adéquats, en tenant compte du code INSEE affecté à la commune / au pays de naissance en vigueur à la date de naissance de l'usager.
- Conformément au "Guide d'implémentation INS" [INS9] - EXI ID15 et à l'implémentation réalisée à l'exigence SC.INS.01

Exigence SC.INS.06

- Le système ne DOIT pas utiliser, en première intention, le code officiel géographique (COG) du lieu de naissance pour interroger le téléservice INSi par saisie des traits. Le COG ne fait pas partie des traits obligatoires pour l'appel au téléservice INSi.
- Le système DOIT permettre de modifier les traits utilisés par l'utilisateur pour l'interrogation du téléservice depuis l'interface affichant la comparaison des traits (ex: suppression du Code Officiel Géographique). (voir SC.INS.19)
- Pour rappel, les traits stricts obligatoires pour l'appel au téléservice INSi sont les suivants :
  - nom de naissance ;
  - premier prénom de naissance ;
  - date de naissance ;
  - sexe.
- Dans le cas de la recherche par traits, les champs renseignés lors de l'appel à INSi peuvent être clairement identifiés (par exemple, étoile à côté du champ, couleur différente, gras, etc.).
- Conformément au "Guide d'implémentation INS" [INS9] - EXI REC 04

Exigence SC.INS.22

- LORSQUE le retour INSi est "00" et LORSQUE le système dispose du NIR de l'usager (stocké et/ou issu de l'interrogation de la carte vitale) ET LORSQU'IL y a correspondance parfaite entre l'ensemble des éléments suivants :
  - le matricule INS et le NIR
  - le nom de naissance local et celui issu de l'INSi
  - la date de naissance local et celle issue de l'INSi
  - le sexe local et celui issu de l'INSi
  - le premier prénom de naissance local et le premier prénom de la liste des prénoms de naissance issu de l'INSi

  alors la récupération DOIT être réalisée automatiquement par le logiciel.
- A l'issue de cette récupération automatique, si l'identité n'est pas déjà validée, le système DOIT permettre à l'utilisateur la qualification en 1 clic de l'identité, sur la base de la pièce d'identité.

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

- Niveau non applicable : Toujours applicable si le critère apparait.
- Niveau 0 : Le produit n'a pas intégré l'exhaustivité des traits d'identité suivants : nom de naissance, premier prénom de naissance, date de naissance, libellé de la ville de naissance, département de naissance, sexe, nom utilisé (si différent du nom de naissance), prénom utilisé (si différent du premier prénom de naissance).
- ✓ Niveau 1 : Dans la création et la gestion des identités des utilisateurs, le produit a intégré les traits suivants : nom de naissance, premier prénom de naissance, date de naissance, libellé de la ville de naissance, département de naissance, sexe, nom utilisé (si différent du nom de naissance), prénom utilisé (si différent du premier prénom de naissance).

- ✓ Niveau 2 : Conforme au niveau précédent, plus : le libellé de la ville de naissance est collecté avec le Code officiel géographique de l'INSEE en cohérence avec la date de naissance.

Exigence INS/va1.01

- Le système DOIT être conforme aux exigences du "Référentiel national d'identito-vigilance (RNIV) - volet 1 à volet 4" [INS8], précisées dans le "Guide d'implémentation INS" [INS9].
- Le système DOIT permettre l'enregistrement de l'ensemble des champs suivants :
    * matricule INS,
    * OID,
    * nom de naissance,
    * prénom(s) de naissance,
    * 1er prénom de naissance,
    * date de naissance,
    * sexe,
    * code lieu de naissance,
    * nom utilisé,
    * prénom utilisé

Exigence INS/va1.21

- Le système DOIT respecter le "Guide d'implémentation INS" [INS9]
- Le système NE DOIT PAS permettre la création d'une identité si les champs suivants ne sont pas alimentés :
    * nom de naissance,
    * 1er prénom de naissance,
    * date de naissance,
    * sexe
    * code lieu de naissance
- A noter : pour rappel, si certaines de ces données ne sont pas connues au moment de la création de l'identité, le "Référentiel national d'identito-vigilance (RNIV) - volet 1 à volet 4" [INS8] précise les valeurs qui peuvent être utilisées pour renseigner ces champs (par exemple : si le code du lieu de naissance n'est pas connu, saisir 99999)

Exigence SC.INS.01

- Le système DOIT permettre l'implémentation des référentiels de l'INSEE portant sur les codes officiels géographiques, y compris la codification des pays et territoires étrangers. Ces référentiels sont disponibles en téléchargement sur le site de l'INSEE (cf. https://www.insee.fr/fr/information/7766585)
- Les fichiers à implémenter et qui doivent faire l'objet d'une mise à jour régulière sont les suivants :
    - Communes
    - Pays
    - Evènements sur les communes
    - Communes depuis 1943

    - Communes des collectivités d'outre-mer
- Le référentiel du logiciel ne DOIT pas comporter de noms de communes abrégés (par exemple, « St » pour « Saint »). Il DOIT, en revanche, comprendre les arrondissements de villes comme Lyon, Paris et Marseille.
- Conformément au "Guide d'implémentation INS" [INS9] - EXI ID14

Exigence SC.INS.02

- LORSQUE le champ « Code lieu de naissance - Code INSEE » n'est pas renseigné à partir du téléservice INSi mais à partir d'une saisie par l'utilisateur, ALORS le système DOIT :
    - au préalable avoir le champ "Date de naissance" renseigné
    - d'une part permettre à l'utilisateur de saisir le nom de la commune / du pays de naissance,
    - et d'autre part lui proposer le code INSEE et le libellé de la commune / du pays adéquats, en tenant compte du code INSEE affecté à la commune / au pays de naissance en vigueur à la date de naissance de l'usager.
- Conformément au "Guide d'implémentation INS" [INS9] - EXI ID15 et à l'implémentation réalisée à l'exigence SC.INS.01

1.3 Questionnaire Maturité Sécurité

01. Gouvernance SSI

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

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

Exigence MES.01.01.01

Dans les équipes en charge du système, les responsables de la sécurité DOIVENT être identifiés.
Leurs responsabilités DOIVENT couvrir les activités de conception, de développement, d'installation, d'exploitation, d'administration et de maintenance (selon le périmètre dont l'industriel a la responsabilité).

Scénario MES.01.01.01.01

- Produire et fournir l'attestation conforme au modèle fourni, complétée en indiquant :
  - pour chaque périmètre de gestion de la sécurité et/ou étapes du cycle de vie applicables au système, depuis sa conception jusqu'à sa maintenance à savoir : la conception, le développement, l'installation, l'exploitation, l'administration et la maintenance
  - la liste des responsables en charge de la sécurité sur chacun de ces périmètres, avec leurs responsabilités respectives.

Critère 01.04.01 - Sensibilisation des équipes en charge

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

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

Exigence MES.01.04.01

Une sensibilisation générale aux enjeux et aux risques liés à la sécurité des systèmes d'information DOIT être menée pour les équipes du système.
Cette sensibilisation DOIT s'effectuer pour l'ensemble des équipes en charge des activités de conception, de développement, d'installation, d'exploitation, d'administration, de maintenance et de support, selon le périmètre dont l'industriel a la responsabilité vis-à-vis de la structure utilisatrice du système.
Dans le cas où le système est destiné à traiter des données à caractère personnel, ALORS la sensibilisation DOIT intégrer des obligations légales ainsi que des réglementations applicables.

Scénario MES.01.04.01.01

- Fournir au minimum :
  - SOIT le document (le cas échéant extrait de la PSSI - Politique de Sécurité des Systèmes d'Information) décrivant le principe de sensibilisation à la sécurité des systèmes d'information des différents groupes de personnel et les obligations et règles relatives à la protection des données à caractère personnel ;
  - SOIT une procédure de sensibilisation à la sécurité des systèmes d'information des différents groupes de personnel et les obligations et règles relatives à la protection des données à caractère personnel, intégrant une évaluation des groupes de personnel spécifiquement concernées par ce dernier sujet.
- Préciser la page et la section correspondant aux exigences de sensibilisation des différentes populations et à la protection des données à caractère personnel.

Identifications, authentifications et autorisations

Critère 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.

Exigence MES.04.02.01

Les moyens d'identification électronique autorisés pour accéder au service DOIVENT être limités :

- Aux moyens d'identification électronique disponibles sous Pro Santé Connect ;
- À la carte CPx ; À des moyens d'identification électronique homologués pour cet usage ;
- À des moyens d'identification électronique certifiés de niveau de garantie eIDAS substantiel ou élevé, et associés à un identifiant conforme aux exigences du référentiel.
- À des moyens d'identification électronique de transition, tels que définis dans le RIE ASPP, sous réserve que les risques résiduels associés à leur utilisation soient considérés comme acceptables par le responsable du service numérique, ces MIE de transition n'étant toutefois autorisés que jusqu'au 31 décembre 2025 au plus tard.

Scénario MES.04.02.01.01

Engagement de sécurisation de l'identification électronique

- Etablir et fournir un engagement de sécurisation de l'identification électronique en respectant le modèle indiqué (attestation partie A uniquement, la partie B n'étant pas requise) et en le complétant intégralement.
- L'engagement doit être signé par un responsable légal du fournisseur des services numériques en santé concernés ou, à défaut, par un délégataire dument habilité.
- Note : cet engagement constitue une seule pièce commune aux scénarios de conformité MES.04.02.01.01, MES.04.02.01.02, MES.04.03.01.01, MES.04.03.01.02 et MES.04.03.06.01.
- Dans le cas de mise en œuvre de MIE entrant dans le cadre prévu par le RIE de "MIE homologués" pour le système, les dossiers d'homologation remis à l'autorité d'homologation, les décisions d'homologation et les dernières décisions de maintien d'homologation établies par cette autorité, doivent être fournis.

Scénario MES.04.02.01.02

- Scénario de connexion de l'utilisateur Acteur de Santé Personne Physique (ASPP) (Professionnel de Santé...)
    - Pour chaque moyen d'identification électronique (MIE) autre que Pro Santé Connect, s'il y en a, accepté par le système pour les utilisateurs ASPP :
        1. Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
        2. Se rendre sur la page de connexion avec un compte utilisateur ASPP ;
        3. Faire apparaître la liste de l'ensemble des moyens d'identification électronique (MIE) acceptés par le système pour ce type d'utilisateurs ;
        4. Sélectionner un MIE autre que Pro Santé Connect, s'il y en a ;
        5. Activer la connexion avec ce MIE ;
        6. Montrer la mire de connexion pour ce MIE ;
        7. Montrer les différentes étapes du processus d'authentification avec ce MIE. Si des étapes ont lieu hors navigateur (ex : clé USB FIDO, générateur d'OTP), intégrer également une capture d'écran, photo ou vidéo de cette étape ;
        8. Accéder au service une fois authentifié ;
        9. Se rendre sur la zone d'interface utilisateur qui permet la déconnexion ;
        10. Activer la déconnexion.
    - Reprendre au départ pour enregistrer une nouvelle séquence avec le MIE suivant.

Exigence MES.04.02.02

Le service DOIT avoir implémenté l'identification électronique par Pro Santé Connect.

Scénario MES.04.02.02.01

Scénario de connexion de l'utilisateur Acteur de Santé Personne Physique (ASPP) par Pro Santé Connect (PSC)

- Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
    - Se rendre sur la page de connexion, et sélectionner l'identification électronique par Pro Santé Connect;
    - Action de lancement de la connexion PSC ;
    - Connexion via mire PSC ;
    - Authentification par eCPS valide ;
    - Retour sur le service ;
    - Se rendre sur la zone d'interface utilisateur qui gère la déconnexion ;
    - Action de lancement de la déconnexion.
- Précision : Les étapes 8 et 9 suivantes ont pour objet de montrer que la déconnexion (étape 7) a bien déconnecté l'utilisateur à la fois du service et de PSC, et donc qu'une nouvelle demande de connexion à PSC (étape 8) entraîne bien une nouvelle authentification (étape 9)
    8. Action de lancement de la connexion PSC
    9. Connexion via mire PSC

Exigence MES.04.02.03

Le système DOIT forcer la déconnexion automatique d'un PS après une durée d'inactivité fixée.

Scénario MES.04.02.03.01

Scénario de déconnexion automatique de l'utilisateur Acteur de Santé Personne Physique (ASPP)

- Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
    1. Se connecter en tant que PS sur le système ;
    2. Attendre la durée d'inactivité prévue ;
    3. Montrer que la session est automatiquement fermée après un certain temps d'inactivité :
- Soit l'interface utilisateur revient automatiquement à la page d'accueil ou de connexion sans aucune action de l'utilisateur,
- Soit l'interface utilisateur revient automatiquement à la page d'accueil ou de connexion dès que l'utilisateur interagit de nouveau avec le système.
- Si le délai est long entre la dernière activité de l'utilisateur et la fermeture automatique de session, la capture peut être scindée en deux fichiers en éliminant une grande partie du temps d'attente intermédiaire, mais en veillant bien à faire apparaître la date et l'heure avant et après la partie supprimée.

Critère 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 1 : 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.

Exigence MES.04.03.01

Les moyens d'identification électronique autorisés pour l'identification électronique des usagers sur le service DOIVENT être limités :

- À des moyens d'identification électronique certifiés eIDAS de niveau de garantie substantiel ou élevé ;

- À l'application mobile carte Vitale (ApCV) ;
- À des moyens d'identification électronique de transition, tels que définis dans le RIE Usagers, sous réserve que les risques résiduels associés à leur utilisation soient considérés comme acceptables par le responsable du service numérique, ces MIE de transition n'étant toutefois autorisés que jusqu'au 31 décembre 2025 au plus tard.

Les moyens d'identification électronique de transition, tels que définis dans le présent référentiel, sont néanmoins autorisés jusqu'au 31 décembre 2025 au plus tard, sous réserve que les risques résiduels associés à leur utilisation soient considérés comme acceptables par le responsable du service numérique.

Scénario MES.04.03.01.01

Engagement de sécurisation de l'identification électronique

- Etablir et fournir un engagement de sécurisation de l'identification électronique en respectant le modèle indiqué et en le complétant intégralement.
- L'engagement doit être signé par un responsable légal du fournisseur des services numériques en santé concernés ou, à défaut, par un délégataire dument habilité.

Scénario MES.04.03.01.02

Scénario de connexion de l'utilisateur Usager (Patient...)

- Pour chaque moyen d'identification électronique (MIE) accepté par le système pour les utilisateurs Usagers :
  - Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
    1. Se rendre sur la page de connexion avec un compte Usager ;
    2. Faire apparaître la liste de l'ensemble des moyens d'identification électronique (MIE) acceptés par le système pour ce type d'utilisateurs ;
    3. Sélectionner un MIE ;
    4. Activer la connexion avec ce MIE ;
    5. Montrer la mire de connexion pour ce MIE ;
    6. Montrer les différentes étapes du processus d'authentification avec ce MIE. Si des étapes ont lieu hors navigateur (ex : clé USB FIDO, générateur d'OTP), intégrer également une capture d'écran, photo ou vidéo de cette étape ;
    7. Accéder au service une fois authentifié ;
    8. Se rendre sur la zone d'interface utilisateur qui permet la déconnexion ;
    9. Activer la déconnexion.
  - Reprendre au départ pour enregistrer une nouvelle séquence avec le MIE suivant.

Exigence MES.04.03.02

Lorsque le système permet à un usager de s'inscrire par lui-même, il DOIT imposer la vérification des attributs d'identité par l'un des moyens suivants :

- FranceConnect ou FranceConnect+ ;
- ApCV ;

A défaut :

- Contrôle (manuel ou automatisé) d'une copie de pièce d'identité déposée sur le site ;
- Service de vérification d'identité à distance (PVID) présentant des garanties objectives de fiabilité (même s'il n'est pas obligatoirement certifié) ;
- Tout autre moyen offrant des garanties équivalentes.

Scénario MES.04.03.02.01

Scénario d'inscription de l'usager par lui-même

- Pour chaque moyen d'identification électronique (MIE) de transition accepté par le système pour les utilisateurs Usagers :
    - Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
        1. Se connecter au système en tant que nouvel usager ;
        2. Montrer que le système impose de vérifier l'identité de l'usager par au moins l'une des méthodes de l'exigence ;
    - Pour chaque méthode proposée :
        - Enregistrer le nouvel usager en suivant la méthode de vérification d'identité,
        - Montrer sur le système que le compte de l'usager est correctement créé.

Exigence MES.04.03.03

SI le système permet la connexion d'un usager ET SI l'adresse de messagerie ou le numéro de téléphone de l'usager sont utilisés dans les mécanismes d'authentification ou de récupération de compte, ALORS le système DOIT vérifier la validité de ces informations lors de la création du compte. Cette vérification peut se faire par l'envoi d'un code ou d'un lien d'activation.

Scénario MES.04.03.03.01

Scénario de vérification des moyens de contact de l'usager lors de son auto-inscription

- Pour chaque moyen d'identification électronique (MIE) de transition accepté par le système pour les utilisateurs Usagers :
    - Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
        1. Se connecter au système pour la création d'un compte usager en tant qu'usager ;
        2. Indiquer un nouveau moyen de contact (adresse de messagerie, numéro de téléphone portable...) ;
        3. Montrer que le moyen de contact n'est pas validé avant sa vérification ;
        4. Montrer qu'un message est envoyé sur le nouveau moyen de contact pour valider celui-ci (avec un lien unique, un code OTP...) ;
        5. Montrer que le nouveau moyen de contact est validé après confirmation par l'usager à l'aide du message reçu.

Exigence MES.04.03.04

Le système DOIT n'autoriser la modification de ses attributs d'identité par un Usager, de même que son adresse de messagerie et son numéro de téléphone, qu'avec des informations obtenues par une vérification d'identité aussi fiable que lors de l'enregistrement initial.
Le système DOIT envoyer une notification de modification à l'usager en utilisant l'ancienne coordonnée et une éventuelle nouvelle coordonnée qui aurait été renseignée.

Scénario MES.04.03.04.01

Scénario de contrôle d'un attribut d'identité modifié par l'usager lui-même

- Pour chaque moyen d'identification électronique (MIE) de transition accepté par le système pour les utilisateurs Usagers :
    1. Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
        - Se connecter au système en tant qu'usager disposant d'un compte ;
        - Demander la modification d'un attribut d'identité, typiquement le nom d'usage ;
        - Montrer que le système contrôle la modification par une vérification d'identité comparable à celle mise en œuvre à l'inscription ;
        - Montrer que le système envoie une notification de modification sur une coordonnée de contact de l'usager.

Scénario MES.04.03.04.02

Scénario de contrôle d'un moyen de contact modifié par l'usager lui-même

- Pour chaque moyen d'identification électronique (MIE) de transition accepté par le système pour les utilisateurs Usagers :
    1. Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
        - Se connecter au système en tant qu'usager disposant d'un compte ;
        - Demander la modification d'un moyen de contact (adresse de messagerie, numéro de téléphone portable) ;
        - Montrer que le moyen de contact n'est pas validé avant vérification ;
        - Montrer qu'une notification de la demande de modification est envoyée au moyen de contact en passe d'être remplacé ;
        - Montrer qu'un message est envoyé sur le nouveau moyen de contact pour valider celui-ci (avec un lien unique, un code OTP...) ;
        - Montrer que le nouveau moyen de contact est validé après confirmation par l'usager à l'aide du message reçu.

Exigence MES.04.03.05

Dans le cadre de l'identification électronique de ses utilisateurs Usagers, le système DOIT enregistrer à minima les attributs suivants de l'Usager :

- Nom de naissance ;
- Premier prénom de naissance ;
- Genre ;
- Date de naissance ;
- Lieu de naissance.

Scénario MES.04.03.05.01

Scénario de vérification des attributs d'un Usager

- Visualiser l'identité d'un utilisateur Usager dans le système (dans l'IHM ou la base de données typiquement) et afficher ses attributs d'identité. L'ensemble des champs suivants doivent être visibles :
    1. Nom de naissance
    2. Premier prénom de naissance
    3. Genre
    4. Date de naissance
    5. Lieu de naissance

Exigence MES.04.03.06

Le système DOIT imposer une méthode d'authentification à 2 facteurs pour les Usagers, pour les MIE de transition, avec au moins 2 facteurs de types différents parmi les trois :

- Connaissance : par exemple d'un mot de passe ;
- Possession : par exemple d'un appareil fixe ou mobile sur lequel s'effectue l'enregistrement ;
- Biométrie : par exemple une empreinte digitale stockée et vérifiée sur un matériel en possession de l'usager.

Scénario MES.04.03.06.01

Scénario d'authentification par un moyen à deux facteurs

- Pas d'élément supplémentaire à produire : les séquences déjà produites pour le scénario MES.04.03.02 sont utilisées ici.

Exigence MES.04.03.07

Si le système s'appuie sur un MIE de transition qui utilise un mot de passe comme l'un des facteurs d'authentifications, le système DOIT implémenter les mesures de restriction d'accès et de vérification de complexité des mots de passe prévues par le Référentiel d'identification électronique des Usagers.

Scénario MES.04.03.07.01

Scénario de vérification de la restriction d'accès par mot de passe

- Pour chaque MIE de transition proposé pour l'authentification de l'Usager utilisant un mot de passe comme facteur d'authentification :
    1. Se rendre en tant qu'usager sur la page de connexion du système ;
    2. Demander l'ouverture d'une session ;
    3. Sélectionner l'authentification basée sur le MIE concerné ;
    4. Entrer un mot de passe incorrect plusieurs fois consécutives ;
    5. Montrer que le système impose des limitations sur les tentatives de connexions erronées, dont au moins une des trois suivantes : temporisations, blocage préventif du compte, demande de captcha.

Scénario MES.04.03.07.02

Scénario de vérification de la restriction de construction de mot de passe

- Pour chaque MIE de transition proposé pour l'authentification de l'Usager utilisant un mot de passe comme facteur d'authentification :
    1. Se connecter en tant qu'usager sur un compte valide
    2. Accéder à l'interface de gestion du MIE concerné ;
    3. Demander la modification du mot de passe ;
    4. Saisir un mot de passe de 7 chiffres et montrer qu'il est refusé ;
    5. Saisir un mot de passe composé uniquement de 6 majuscules ou minuscules et montrer qu'il est refusé.

Exigence MES.04.03.08

Le système DOIT forcer la déconnexion automatique de l'usager après une durée d'inactivité fixée.

Scénario MES.04.03.08.01

Scénario de déconnexion automatique de l'utilisateur Usager

- Enregistrer une nouvelle suite de copies d'écran ou vidéo de la séquence montrant au minimum chaque étape suivante :
    1. Se connecter en tant qu'usager sur le système ;
    2. Attendre la durée d'inactivité prévue ;
    3. Montrer que la session est automatiquement fermée après un certain temps d'inactivité :
        - soit l'interface utilisateur revient automatiquement à la page d'accueil ou de connexion sans aucune action de l'utilisateur,
        - soit l'interface utilisateur revient automatiquement à la page d'accueil ou de connexion dès que l'utilisateur interagit de nouveau avec le système.
- Si le délai est long entre la dernière activité de l'utilisateur et la fermeture automatique de session, la capture peut être scindée en deux fichiers en éliminant une grande partie du temps d'attente intermédiaire, mais en veillant bien à faire apparaître la date et l'heure avant et après la partie supprimée.

08. Maintien en condition de sécurité

Critère 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.

Exigence MES.08.02.01

Un processus de veille (automatisé ou non) sur les vulnérabilités des composants du système (bibliothèques, logiciels, dépendances de l'application, etc.) DOIT être défini et appliqué.
Un processus de patch management DOIT être défini et mis en œuvre (application / distribution des patchs, des mises à jour des composants, etc.)

Scénario MES.08.02.02.01

- Fournir la documentation du processus de veille mis en place sur les vulnérabilités des composants du système.
- Cette documentation DOIT notamment décrire :
  - La méthodologie utilisée : La documentation doit offrir une présentation claire des méthodes employées pour la collecte, l'analyse et la surveillance continue afin de

repérer les vulnérabilités ainsi que les processus de partage et de collaboration avec l'équipe interne ou avec les partenaires externes.
    - Les outils utilisés pour la veille (le cas échéant) : L'inventaire des outils utilisés comme les scanners de vulnérabilités ou les plateformes de surveillance en temps réel, etc.
    - Les sources d'information : La spécification des sources d'information employées, telles que les abonnements à des bulletins de sécurité, les sites web spécialisés dans les vulnérabilités, les forums de sécurité ou les communautés en ligne, etc.
    - Les composants du système surveillés : La nature des composants du système qui font l'objet d'une surveillance pour détecter les vulnérabilités. Ces composants peuvent inclure des logiciels, des matériels, des bibliothèques, des systèmes d'exploitation, etc.
- Si ces informations se trouvent intégrées dans un document plus large, les pages et les sections correspondant à chaque sujet indiqué ci-dessus DOIVENT être précisées.

Scénario MES.08.02.01.02

- Fournir la documentation du processus de patch management/distribution de patchs mis en œuvre pour le système.
- Cette documentation DOIT notamment décrire :
    - Les outils utilisés pour la gestion de l'inventaire du système d'information (SI), en indiquant le périmètre couvert et la granularité de l'inventaire géré.
    - La provenance des mises à jour : Les sources spécifiques des mises à jour et des correctifs telles que les sites web suivis, les serveurs internes ou d'autres canaux utilisés pour obtenir les correctifs nécessaires.
    - La planification et la priorisation des correctifs : Le calendrier de déploiement des correctifs en fonction de leur criticité, le plan de traitement des vulnérabilités établi pour gérer les correctifs par priorité, le nom de l'outil utilisé, le cas échéant, pour faciliter le déploiement des correctifs.
- Si ces informations se trouvent intégrées dans un document plus large, les pages et les sections correspondant à chaque sujet indiqué ci-dessus DOIVENT être précisées.

09. Continuité d'activité

Critère 09.04 - Réalisation des sauvegardes

- Niveau non applicable : Toujours applicable si le critère apparaît
- Niveau 0 : Aucun processus spécifique de sauvegarde hors ligne du produit n'est prévu.
- ✓ Niveau 1 : Les procédures de sauvegarde hors ligne et de restauration de la configuration et des données du produit sont documentées. Dans le cas de produits de type service hébergé ou Saas, la procédure de sauvegarde est effectivement mise en œuvre comme documentée. En outre, dans le cas de produits de type plateforme/applicance intégrant la solution de sauvegarde, ou de service hébergé ou Saas, les sauvegardes sont effectuées sur des supports conservés totalement hors ligne.
- ✓ Niveau 2 : Conforme au niveau précédent, plus : Les procédures documentées incluent une procédure de vérification de la bonne sauvegarde et couvrent également les composants logiciels du produit. Il est fourni une méthode permettant de calculer l'espace de stockage nécessaire aux sauvegardes en fonction de l'usage prévu du produit et de la durée de

conservation souhaitée. Dans le cas de produits de type service hébergé ou Saas, la sauvegarde est au moins journalière et le test de sauvegarde et des procédures de restauration est réalisé de façon régulière.

- ✓ Niveau 3 : Conforme au niveau précédent, plus :
  - Le produit est de type de service hébergé ou Saas ;
  - Ou les procédures et mécanismes liés à la sauvegarde sont conçus pour permettre la réalisation des sauvegardes/restauration à l'aide d'outils de sauvegarde polyvalents tiers tout en garantissant un état cohérent de la sauvegarde, et ne contraignent pas à l'usage d'un produit de sauvegarde spécifique intégrée ou non au produit.

Exigence MES.09.04.01

Le système DOIT disposer :
- d'une procédure de sauvegarde exécutée régulièrement ;
- d'une procédure de restauration testée régulièrement ;
- ainsi que la documentation associée.

Scénario MES.09.04.01.01

- L'industriel DOIT fournir les documentations attendues comme Preuves.
- Ces documents DOIVENT intégrer les informations suivantes :
  - Les acteurs impliqués (ex : administrateurs, supports informatique, responsables de sécurité, etc.) ainsi que leurs rôles selon le modèle RACI.
  - La fréquence de sauvegarde ;
  - Le champ d'application (périmètre de la sauvegarde) ;
  - Le lieu de stockage des sauvegardes (ex : stockage local, Cloud, serveur distant, etc.).
  - Les méthodes de sauvegarde (ex : sauvegardes complètes, incrémentielles ou différentielles)
  - Les règles de sécurité : les mesures de sécurité sont mises en place pour protéger les sauvegardes (ex : chiffrement des données, l'accès restreint aux sauvegardes, etc.) ;
  - Les tests de récupération (périmètre des tests, fréquence, etc.) ;
- Si ces informations se trouvent intégrées dans un document plus large, les pages et les sections correspondant à chaque sujet indiqué ci-dessus DOIVENT être précisées.

11. Hébergement

Critère 11.01 – Hébergement de données de santé

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

Exigence MES.11.01.01

L'industriel, quand il assure l'hébergement de données de santé (HDS) tel que défini par les articles L1111-8 et R1111-8-8 du code de la santé publique, pour tout ou partie du système, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, DOIT disposer d'une certification HDS valide obtenue auprès d'un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen) pour les activités d'hébergement de données de santé sur lesquelles s'appuie le système.
SI l'industriel n'assure aucun hébergement de données de santé (HDS) tel que défini ci-dessus pour le système, ALORS il doit fournir une attestation sur l'honneur de non-hébergement conforme au modèle fourni.

Scénario MES.11.01.01.01

- L'industriel DOIT fournir les documentations attendues comme Preuves :
  - fournir les certificats HDS requis.
- Si l'industriel est lui-même soumis à l'obligation de certification HDS pour le système, il est le seul à devoir fournir les Preuves attendues.
- Si l'industriel n'est pas lui-même soumis à l'obligation de certification HDS pour le système, mais que des tiers sous sa responsabilité le sont, les Preuves attendues doivent être fournies pour chacun de ces tiers hébergeurs.

Scénario MES.11.01.01.02

- L'industriel doit établir et fournir une attestation sur l'honneur de non-hébergement de données de santé conforme au modèle fourni, datée et signée par son représentant légal.

1.4 Questionnaire Ethique Mon espace santé

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

- QUA.1 Ethique
  - Critère P1 QUA.1.1B Expertise des contributeurs

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

  - Critère P2 QUA.1.6 Implication des utilisateurs

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

SF_ACC Accessibilité
ACC Accessibilité - Conditions d'accès au service

- ACC.1 Ethique
  - Critère P1 ACC.1.1 Intuitivité et inclusion de tous les publics

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

  - Critère P1 ACC.1.4 Aides en ligne

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

  - Critère P2 ACC.1.6 Alerte sur décision critique

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

  - Critère P1 ACC.1.7 Réponses aux questions

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

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

- ETH.1 Ethique
  - Critère P2 ETH.1.6 Effacement des données

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

  - Critère P2 ETH.1.9 Données sensibles

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

  - Critère P1 ETH.1.10 Bénéfices et limites

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

SF_INT Intelligence artificielle
INT Intelligence artificielle et éthique

- INT.1 Ethique
  - Critère P2 INT.1.4 Détection dérive

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

  - Critère P2 INT.1.5 Explicabilité

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

  - Critère P2 INT.1.6 Eviter les biais

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

SF_DEV Développement durable
DEV Développement durable

- DEV.1 Ethique
  - Critère P1 DEV.1.2B Ecoconception

    Le système est développé en conformité avec les principes d'écoconception, mis en œuvre à chaque étape de son cycle de vie, dans une démarche plus globale de développement durable.
  - Critère P2 DEV.1.4 Faible débit et équipements anciens

    Le système est accessible en faible débit et à partir d'équipements ne nécessitant pas d'être de dernière génération.
  - Critère P2 DEV.1.5 Réduire consommation datacenters

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