HAUTE AUTORITÉ DE SANTÉ

Évaluation et amélioration des pratiques

Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (*Mobile Health* ou *mHealth*)

Octobre 2016

Ce document et les ressources complémentaires
sont téléchargeables sur : **www.has-sante.fr**

Haute Autorité de Santé
Service communication – information
5, avenue du Stade de France – F 93218 Saint-Denis La Plaine Cedex
Tél. : +33 (0)1 55 93 70 00 – Fax : +33 (0)1 55 93 74 00

Ce document a été validé par le Collège de la Haute Autorité de santé en octobre 2016.

Sommaire

Sommaire 3

Abréviations et acronymes 4

Préambule 5

1. Contexte 7
   1.1 Définitions et concepts : Applications, objets connectés 8
   1.2 Classifications retrouvées dans la littérature 8
   1.3 Évaluation de la santé mobile dans différents pays 9
   1.4 Mesure d'impact et/ou d'efficacité 11
   1.5 Aspects juridiques de l'évaluation des applications et objets connectés en santé 11

2. Le référentiel de bonnes pratiques 14
   2.1 Les domaines à évaluer 14
   2.2 Modulation du périmètre de l'évaluation 14
   2.3 Domaine : informations utilisateurs 16
   2.4 Domaine : contenu de santé 19
   2.5 Domaine : contenant technique 26
   2.6 Domaine : sécurité/fiabilité 28
   2.7 Domaine : utilisation/usage 37

3. Mise en œuvre du référentiel de bonnes pratiques 43

Annexe 1. Le *Mobile App Rating Scale* (MARS) (98, 99) 44
Annexe 2. L'évaluation par les pairs du *Journal of Medical Internet Research* – JMIR – 46
Annexe 3. Recherche documentaire 47
Annexe 4. Liste des tableaux 50
Annexe 5. Glossaire 51
Annexe 6. Méthode de travail 53
Annexe 7. Participants 54
Références 56

Abréviations et acronymes

AFCDP	Association française de normalisation
AFNOR	Association française des correspondants à la protection des données à caractère personnel
ANSM	Agence nationale de sécurité du médicament et des produits de santé
ANSSI	Agence nationale de la sécurité des systèmes d'informations
Apps/OC	Applications mobiles/objet connecté
ASIP-Santé	Agence des systèmes d'information partagés de santé
CE	Marquage CE (conforme aux exigences)
CERT	*Computer Emergency Response Team* - également appelé CSIRT (*Computer security incident response team*)
CERT-FR	*Computer Emergency Response Team* pour la France
CGU	Conditions générales d'utilisation
CNIL	Commission nationale de l'informatique et des libertés
CSRF	*Cross-Site Request Forgery*
DCP	Données à caractère personnelles
DM	Dispositif médical
EBIOS	Expression des besoins et identification des objectifs de sécurité
ECR	Essai contrôlé randomisé
ENISA	*European Union Agency for Network and Information Security*
EU	*European Union*
FAQ	Foire aux questions
GDPR	*General Data Protection Regulation*
HAS	Haute Autorité de Santé
HDS	Hébergeur de données de santé
HON	Health On the Net foundation
IMC	Indice de masse corporelle
IHM	Interface homme machine
ISO	*International Organization for Standardization*
kg	Kilogramme
mHealth	*Mobile health* (santé mobile)
OS	*Operating System*
OWASP	*Open Web Application Security Project*
PAS	*Publically Available Specification*
PDA	*Personal Digital Assistant*
RGI	Référentiel général d'interopérabilité
RGAA	Référentiel général d'accessibilité pour les administrations
RGS	Référentiel général de sécurité
SMS	*Short Message Service*
TIC	Technologies de l'information et de la communication pour l'éducation
TLS	*Transport Layer Security*
XSS	*Cross-Site Scripting* (parfois noté CSS)
W3C	*World Wide Web Consortium*

Préambule

Cette contribution de la HAS vise à **guider, à promouvoir l'usage et à renforcer la confiance** dans les applications et les objets connectés en santé en diffusant pour cela **un référentiel de bonnes pratiques pour les industriels et pour des évaluateurs** (structures d'évaluation, associations de consommateurs ou sociétés savantes médicales) qui pourraient le mettre en œuvre pour conduire leurs propres évaluations.

Ce référentiel porte sur les applications et les objets connectés n'ayant pas de finalité médicale déclarée. Il concerne donc tout particulièrement la zone dite « grise » des applications ou des objets connectés ayant un effet potientiel sur la santé sans être un dispositif médical. Les dispositifs médicaux, au sens de la directive européenne 93/42/CEE qui entraine le marquage CE, en sont donc exclus.

Ce référentiel ne se substitue pas à la loi ou la réglementation concernant les dispositifs médicaux (au sens de la directive européenne 93/42/CEE qui entraine le marquage CE), la protection des données personnelles et la protection des consommateurs. L'application des bonnes pratiques définies dans le présent référentiel s'entend sans préjudice de la réglementation en vigueur.

Ce référentiel de bonnes pratiques de la HAS ne constitue pas un outil d'évaluation en vue de l'admission au remboursement, ni une recommandation professionnelle.

La santé mobile offre de nouvelles possibilités pour améliorer la surveillance des maladies chroniques et permettre au patient d'être plus acteur de sa prise en charge. Elle pourrait également contribuer au développement de la dimension préventive de notre système de santé. La recherche académique autour du big data en santé pourrait également contribuer aux progrès de la médecine.

Dans ce contexte, la HAS a élaboré un référentiel de bonnes pratiques portant sur les applications et les objets connectés (Apps/OC) en santé.

L'évaluation des Apps de santé mobile et des objets connectés fait intervenir de nombreux domaines de bonnes pratiques. La Haute Autorité de Santé (HAS) est légitime pour élaborer un référentiel sur des champs correspondants à ses missions, c'est à dire :

- l'amélioration de la qualité des soins (intérêt thérapeutique, organisation) ;
- la qualité de l'information médicale (exhaustivité, neutralité, exactitude et fraîcheur de l'information médicale) ;
- la sécurité du patient (gradé en niveau et types de risques en fonction de la destination d'usage et du principal utilisateur cible de l'Apps/OC considéré) ;
- l'évaluation en santé (impact sur la santé publique) ;
- la coordination des soins et l'interopérabilité qui en découle (structuration de l'information) ;
- le rapport coût efficacité (efficience économique).

En outre, deux champs complémentaires ne correspondant pas aux enjeux stratégiques de la HAS, mais intrinsèquement liés à la thématique, ont été étudiés ; il s'agit de la protection de la vie privée et de la cybersécurité. Ils sont en partie intégrés dans ce référentiel grâce aux contributions de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la Commission nationale de l'informatique et des libertés[1] (CNIL).

D'autres domaines d'évaluations plus techniques concernent également la santé mobile, et ne sont pas traités par ce guide, par exemple :

- **la télécommunication**[2] sous l'angle technique et sécurité de l'information[3], de sa transmission ou du processus complet lié à l'accès, au stockage et à la transmission de données de santé ;
- **l'hébergement**[4] des données collectées (loi 4 mars 2004) ;
- **la sécurité/fiabilité des données**[5] sous l'angle de **traitement des données ou du signal** et de **la métrologie** ;
- **la fiabilité des algorithmes** et des formules de calcul ;
- etc.

Ce référentiel constitue une première étape dans le processus d'évaluation et de conception des Apps/OC dans le monde de la santé mobile. Il est sujet à évoluer en fonction des évolutions du secteur.

Ce référentiel sera complété de supports à destination des utilisateurs (professionnels de santé et usagers) à paraître ultérieurement.

1. www.cnil.fr/linstitution/actualite/article/article/quantified-self-m-sante-le-corps-est-il-un-nouvel-objet-connecte/
2. www.wi6labs.com/blog/fr/2013/12/13/quelle-technologie-radio-pour-les-objets-connectes-premiere-partie/
3. esante.gouv.fr/sites/default/files/Guide_Pratique_Dispositif_Connecte.pdf
4. esante.gouv.fr/services/referentiels/securite/hebergement-faq
5. internetactu.blog.lemonde.fr/2015/03/07/les-applications-de-sante-en-questions/

À noter qu'au niveau européen, un guide de bonnes pratiques (proposé par un livre vert publié en 2014[6]) est attendu pour 2017[7], il viendra compléter le code de conduite[8] et les processus d'interopérabilité et de standardisation en cours[9] du plan d'actions européen 2012-2020 pour la e-santé.

6. ec.europa.eu/digital-single-market/news/green-paper-mobile-health-mhealth
7. ec.europa.eu/digital-single-market/en/news/new-eu-working-group-aims-draft-guidelines-improve-mhealth-apps-data-quality
8. ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps
9. ec.europa.eu/digital-single-market/en/interoperability-standardisation-connecting-ehealth-services

1. Contexte

Il existe une évolution des réflexions sur l'évaluation des technologies de l'information et de la communication (TIC) dans le monde de la santé. Nous entrons dans une période de mutation en passant d'un modèle d'évaluation de logiciel « généraux » qui pouvaient accomplir plusieurs actions à un modèle « d'Applis » (Apps) qui sont **des petits programmes répondant à des besoins spécifiques ou à des besoins de niches évolutifs très rapidement** (1).

Ce changement de paradigme de l'évaluation ou de la régulation/certification de programmes « généraux » à la notation de petits programmes spécialisés pose la difficulté d'outils d'évaluations adaptés, spécifiques et flexibles dans le temps.

Ces petits programmes répondent mieux aux besoins de terrain et cherchent à être plus pertinents. Ils offrent également de nouvelles perspectives en termes d'actions de promotion/régulation ciblées sur des domaines à forts enjeux de santé publique et/ou médico-économique. C'est une différence notable comparée à la certification des sites Internet dont les enseignements ne sont finalement que très partiellement transposables à la problématique des Apps/OC en santé.

La convergence de différents concepts (TIC, big data, etc.) est liée à **l'évolution rapide** (2) **des technologies** utilisées (miniaturisation, smartphone, flux de données). Les premières utilisations efficaces en « santé mobile auprès du patient » sont l'envoi de SMS pour aider les patients à respecter leur prise médicamenteuse [revue systématique de Park (3)]. En 2014, le développement d'Apps « évoluées » pour remplir la même fonction possède un agenda, un historique, un serveur de données, etc. [revue systématique de Bailey sur les Apps dans le cadre de prise en charge médicamenteuse (4)].

Les questions de fiabilité et de sécurité des Apps/OC se posent avec les développements actuels :

- Apps de **fiche médicale d'urgence** (avec groupe sanguin, allergies, dons d'organe, etc.) accessible sur le smartphone de l'utilisateur en ouverture directe ;
- **conseil/avis** donnés à l'utilisateur par des Apps ou des objets connectés au smartphone (de manière automatisée par algorithme ou auprès d'un professionnel de santé) ;
- utilisation des fonctions de **géolocalisation** des smartphones pour orienter l'utilisateur ;
- collecte de données pour réaliser des **profils de pratique** pour les professionnels de santé ;
- etc.

Dans toutes ces situations, l'utilisateur doit pouvoir bénéficier de **produits qui ne nuisent pas à sa santé** et qui lui apportent **un bénéfice au moins équivalent** par rapport à ce qui existait auparavant.

L'évaluation de la qualité des Apps/OC en santé apparaît nécessaire devant l'hétérogénéité de ce qui est disponible sur un marché en plein essor.

Au niveau utilisateurs, les besoins d'évaluation peuvent se formuler simplement :

- pour le patient ou l'utilisateur bien portant, est-ce que cet Apps/OC peut m'être utile pour ma santé et sur quels points par rapport à ce qui existait auparavant ?
- pour le professionnel de santé, comment répondre aux questions posées par le patient sur les Apps/OC qu'il utilise ? Quels Apps/OC utiliser pour son exercice et à recommander/prescrire à ses patients ?
- pour les associations de patients et les organismes professionnels, que faut-il sélectionner/développer/promouvoir pour sa communauté ?

Au niveau des industriels en charge de la conception et du développement, des questions plus spécifiques se posent :

- comment garantir que les besoins des utilisateurs ont été pris en compte ?
- est-ce que l'Apps/OC a été développé en respectant la transparence, la qualité, la confidentialité et la sécurité des informations ?
- est-ce que les risques ou menaces ont été identifiés, traités et surveillés ?

De 2002 à 2012, l'évaluation de la qualité des Apps/OC en santé mobile a évolué d'une évaluation technologique vers une évaluation de l'impact en Santé Publique. Les pathologies et problèmes de santé les plus étudiés sont : le diabète, l'obésité, la santé mentale, l'usage du tabac, les maladies chroniques, etc. (5).

Même si l'adoption par les patients et les professionnels de santé est variable et des barrières ou des facteurs favorisants ont été identifiés (6), la notion de médecine personnalisée et de mesure de soi (*quantified-self*) est en train de se développer. De la Vega aborde la notion d'évolution de prescription d'Apps/OC pour un patient spécifique ayant un problème spécifique (1).

Pour la *Canadian Advanced Technology Alliance* (7) 5 thématiques sont à développer dans ce secteur :

- sensibilisation et éducation ;
- accès aux informations de santé personnelle ;
- modèles de remboursements pour les cliniciens ;
- certification pour les Apps mobiles en santé ;
- gérer l'écart entre innovation et adoption.

1.1 Définitions et concepts : Applications, objets connectés

L'Organisation mondiale de la santé (8) définit les termes ***Mobile Health (mHealth)*** par : « *pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs de surveillance des patients, les PDA et autres appareils sans fil.* »

Concernant les **objets connectés** (9), aucune définition n'a été identifiée spécifiquement. Ils sont définis dans ce document comme des dispositifs connectés à l'Internet pouvant collecter, stocker, traiter et diffuser des données ou pouvant accomplir des actions spécifiques en fonction des informations reçues.

Aungst (10) définie la typologie des Apps selon 4 types :

- **Application mobile :** logiciel informatique qui fonctionne sur un appareil mobile et qui remplit une/des fonction(s) particulière(s).
- **Application mobile native :** logiciel informatique qui est préinstallé sur un appareil mobile (exemple : logiciel gérant l'utilisation de la caméra de l'appareil mobile).
- **Application mobile téléchargeable :** logiciel informatique qui n'est pas préinstallé sur un appareil mobile et requiert d'être téléchargé au travers d'une source externe (en général un magasin d'Apps mobiles).
- **Application web** (*Web-Based*) : logiciel informatique qui se connecte à un portail web sur Internet et qui adresse le flux sur un appareil mobile. Nécessite une connexion Internet.

L'utilisation du terme « App » est recommandée pour les publications scientifiques en langue anglaise (11). Une check-list spécifique (mERA) pour évaluer les articles du secteur est proposé par Agarwal (12).

La santé mobile (*mHealth*) est comprise dans le domaine de la e-santé et se partage en partie avec les domaines de la télémédecine et du *quantified-self* (13).

1.2 Classifications retrouvées dans la littérature

Différentes classifications sont décrites dans la littérature. Nous en reprenons quelques-unes pour illustrer les orientations de ce secteur.

Classification de Aungst (10)

Aungst propose une classification avec 4 domaines et 4 sous-domaines pour chacun d'eux :

- **Centré patient :** promotion de la santé, communication auprès du patient, suivi de paramètres de santé, rappel de prise médicamenteuse ;
- **Centré praticien :** dossier patient informatisé et prescription électronique, productivité, communication, calcul médical ;
- **Référence :** référence sur la maladie, référence clinique, référence médicament, littérature médicale ;
- **Éducation :** enseignement médical général, enseignement médical spécialisé, enseignement médical continu, enseignement du patient.

Classification de Mosa (14)

Mosa structure les Apps par rapport à l'exercice médical :

- 7 catégories pour les professionnels de santé : diagnostic de maladie, références médicamenteuses, calcul de paramètres médicaux, recherche de littérature scientifique, communication clinique, connexion avec le dossier patient, formation médicale. Une catégorie « générale » pour les autres ;
- Apps de formations pour les étudiants ;
- Apps patients : gestion de pathologies chroniques.

Classification de Yasini (15)

Yasini s'appuie sur une enquête de terrain pour délimiter 31 catégories (évaluées sur 567 Apps « santé » en langue française dont 218 pour les professionnels de santé et 352 pour le grand public).

Les catégories sont les suivantes : recommandation clinique, diffusion scientifique grand public, synthèse de données médicales, informations médicales, recherche dans une base de données (médicament, image, nutrition, etc.), livres, communication publique générale, communication entre professions de santé et institutions, communication entre public et professionnels de santé, communication entre professions de santé, calculer ou interpréter des données, vérification de données du dossier du patient, système d'aide à la décision, gérer à distance ou collecter des données, utiliser l'objet connecté comme un outil diagnostic ou de mesure, calculer les honoraires, soutien comptabilité, gestion d'agenda, recherche d'emplois, soutien à la cotation/codage des actes, gérer le stock de médicaments, localiser un service de santé, interaction avec un établissement de santé/pharmacie/assurance, chercher des informations sur des professionnels de santé/établissement, cas cliniques, serious game, question d'enseignement.

Classification de *Mobile World Capital & Agència de Qualitat i Avaluació Sanitàries de Catalunya* – AquAS (16) :

Mobile World Capital (MWC) et l'agence pour la qualité et l'évaluation sanitaire de Catalogne (*Agència de Qualitat i Avaluació Sanitàries de Catalunya* – AquAS) propose un cadre d'évaluation avec une stratification de 5 niveaux de risque dans une matrice de risque qui catégorise les interventions à risques (de « références/guides » à « suivre/monitoring/alerter ») et les risques spécifiques liés aux personnes et malades.

Autres classifications :

- Labrique (17) structure les Apps par rapport à 12 types de fonctions qui peuvent être gérées par smartphone ;
- Dans le cadre d'Apps dans un domaine spécifique (cancer), Bender (18) décrit 8 catégories d'Apps définies (sensibilisation, information sur la maladie et le traitement, levée de fond, détection précoce, promotion d'une organisation, prise en charge de la maladie, prévention, soutien entre pairs) ;
- Yetisen (19) définit 3 catégories majeures afin d'aider à la régulation (médecine préventive, et promotion de la santé ; instruments portables de diagnostic et de monitoring ; gestion de données, formation médicale, paiement mobile) ;
- Hussain (20) recense les types d'Apps en santé et leurs évaluations et proposent des pistes pour les patients, développeurs, agences, etc. ;
- Cook (21) est un exemple de publication de synthèse sur les Apps censées améliorer le diagnostic de mélanome. Peu de critères sont discriminants, mais il propose de classifier les Apps en fonction des utilisateurs possibles (tous les patients, patients à haut-risque, étudiants).

1.3 Évaluation de la santé mobile dans différents pays

Différents organismes ont proposé ou proposent des services de compilation, de labélisation ou de registre des Apps/OC en santé. Une liste non exhaustive est présentée à titre informatif (tableau 1).

Tableau 1. Compilation non exhaustive des sites évaluant les Apps/OC en santé au niveau de différents pays (présenté par ordre alphabétique)

Pays	Nom	Organisation/Prestataire
Allemagne	AppCheck[10]	*ZTG Zentrum für Telematik und Telemedizin GmbH*
Allemagne	HealthOn[11]	*Sanawork*
Espagne (Andalousie)	AppSaludable : Catálogo de aplicaciones móviles de salud[12]	*Agency of Healthcare Quality of Andalusia*
États-Unis	Zur Institute[13]	*Zur Institute*
États-Unis	Eat right[14]	*Academy of Nutrition and Dietetics*
États-Unis	Happtique[15]	*Greater New York Hospital Association* *NB : Service suspendu*
États-Unis	iMedicalApps[16] iprescribeapps.com[17]	*iMedicalApps*
États-Unis	UF Diabetes Institute[18]	*UF Diabetes Institute*
France	AppScript[19]	*IMS health's*
France	DMD santé[20]	DMD santé
France	GPM e-santé[21]	Groupe Pasteur Mutualité
France	Medappcare[22]	Medappcare
France	Sanofidiabete[23]	SANOFI & DMD santé
Pays-Bas	Royal Dutch Medical Association (KNMG)[24]	*Medical App Checker*
Royaume-Uni	UK's National Health Service (NHS) Apps Library[25]	NHS NB : Service suspendu
Royaume-Uni	myhealthapps.net[26]	*Patient View*

10. www.appcheck.de - 11. www.healthon.de -12. www.calidadappsalud.com/distintivo/catalogo/13. www.zurinstitute.com/mentalhealthapps_resources.html - 14. www.eatright.org/appreviews - 15. www.happtique.com/home - 16. www.imedicalapps.com/about - 17. iprescribeapps.com - 18. diabetes.ufl.edu/my-diabetes/diabetes-resources/diabetes-apps - 19. www.imshealth.com - 20. www.dmd-sante.com - 21. www.gpm.fr/toutes-les-news.html?id=10093 - 22. www.medappcare.com/conseil-scientifique - 23. www.sanofi-diabete.fr/Accueil/Menu/Guide-des-applications-diabete - 24. www.knmg.nl/over-knmg/contact/about-knmg.htm - 25. apps.nhs.uk/review-process/# - 26. myhealthapps.net/about

La plupart des plateformes d'évaluation des Apps/OC utilisent une grille d'analyse recoupant différents domaines et s'appuient sur une expertise de professionnels de santé, d'utilisateurs et d'analyse technique du risque ciblant la cybersécurité, la protection des données personnelles, le respect juridique, etc. Les dispositifs médicaux (DM) ne sont pas du ressort de ces évaluations. Ces systèmes essayent d'évaluer « la zone grise » des Apps/OC n'ayant pas de finalité médicale déclarée.

1.3.1 Système d'évaluation mis en place à un niveau régional ou national

L'Organisation mondiale de la santé (OMS) a rédigé les résultats d'une enquête sur la e-santé en Europe. Concernant la santé mobile, 22 % (10 pays) disent mettre en place un système pour évaluer la qualité, la sécurité et la fiabilité de la santé mobile (22).

Avec AppSaludable, l'agence pour la qualité sanitaire d'Andalousie propose depuis 2013 un catalogue d'Apps qui suivent les 31 recommandations établies par l'agence. En 2015, près de 17 % de la population régionale utilise au moins une de ces Apps.

D'un autre côté, Happtique ou NHS Choice ont soit cessé soit suspendu leur activité de registre après des problèmes de sécurité concernant des Apps référencées sur leurs sites (23).

Au niveau international, il n'a pas été retrouvé d'approches consensuelles sur la manière d'évaluer les Apps mobiles ou les objets connectés qui ne sont pas déclarés comme des dispositifs médicaux (24-29).

Pourtant selon *Canada Health Infoway*, il existe plusieurs situations qui peuvent nécessiter une régulation (2) notamment tout ce qui peut influencer la décision de l'utilisateur ou du professionnel de santé dans le champ de la santé et du bien-être (27, 30-35).

Le hub australien recensant les différentes approches dans différents pays en voie de développement propose des exemples pragmatiques d'intégration d'Apps[27] pour les pays en voie de développement.

Au niveau européen, un groupe de travail de la commission européenne rédige un guide de bonnes pratiques pour garantir la fiabilité et la sécurité des Apps mobiles et des objets connectés. Ce document est attendu pour début 2017[28]. La HAS a participé au groupe de travail et a apporté les éléments présentés dans ce guide.

1.3.2 Échelles et scores d'évaluation

Au niveau individuel, le score d'évaluation retrouvé le plus souvent dans la littérature est le score australien intitulé score de MARS (*Mobile App Rating Scale*). Ce score est utilisé pour les publications évaluant des Apps de santé. Une traduction non validée est publiée en annexe 1 pour information. Une liste non exhaustive des échelles et scores est présentée à titre informatif ci-dessous :

- ABACUS[29] (36) ;
- Gonnermann (37) propose 3 niveaux : évaluation globale (10 critères), contenu (6 critères), niveau étudié (l'évaluation dépend de la méthodologie et suit les recommandations de publication) ;
- McMillan (38) propose 62 questions ;
- Albrecht (39) propose une *checklist* de reporting ;
- Salber (40) propose un guide pour les cliniciens avec 6 critères pragmatiques :
  - évaluer si vos patients ont déjà utilisé des Apps médicales, des dispositifs médicaux sans fils, ou tout autres outils de santé numériques,
  - connaître les types d'informations que vos patients obtiennent de leurs technologies de santé numériques et ce qu'ils en font,
  - comprendre si l'App ou l'objet ou le programme est sûre et s'il fournit des informations précises ;
  - essayer l'Apps/OC vous-même,
  - évaluer si vous et votre patient voyez que l'App ou l'objet connecté sont des moyens d'améliorer la communication et la relation médecin/patient ou pas,
  - déterminer si l'App entre dans votre flux de travail ;
- Murfin (41) propose le modèle KYA (*Know Your Apps*) : aller à la source, sponsors, références, évaluation du protocole, mises à jour ;
- Chan (42) propose une évaluation dans le domaine de la santé mentale :
  - dimension utilité (4 critères),
  - dimension utilisation (5 critères),
  - dimension intégration/infrastructure (5 critères),
  - et catégories ;
- Huckvale (43) propose une évaluation pour les Apps concernant l'asthme. C'est une adaptation des recommandations et des 8 principes de HON ;
- Safavi (44) propose une liste de 10 principes et 9 checklists pour permettre aux développeurs de protéger la confidentialité des données.

27. www.uq.edu.au/hishub/wp25
28. ec.europa.eu/digital-single-market/en/news/new-eu-working-group-aims-draft-guidelines-improve-mhealth-apps-data-quality
29. libguides.library.arizona.edu/c.php?g=122854&p=802639

Pour le grand public ou les patients, l'*American Health Information Management Association* (AHIMA) propose un outil grand public : « *just think APP* »[30]. L'acronyme signifie A pour avis et PP pour les données personnelles et privées. Le document évalue et liste des questions à se poser ou des conseils à réaliser.

1.4 Mesure d'impact et/ou d'efficacité

Le développement des Apps/OC en santé date de moins d'une dizaine d'années ce qui explique que les publications de mesure d'impact ou de mesure de taille d'effet thérapeutique soient encore limitées.

1.4.1 Revue systématique sur la santé mobile

Payne (45) a réalisé une évaluation des principaux domaines où se déploient des Apps dans une revue systématique. Les Apps visant un changement de comportement (alimentaire, addictions, etc.), la promotion de l'activité physique ou le suivi des problèmes dépressifs sont le plus fréquemment étudiés. Au niveau méthodologique, les effectifs sont le plus souvent inférieurs à 100. Des effets sont retrouvés dans tous les domaines étudiés. Des études de plus grande puissance sont attendues.

Free (46) a réalisé une méta-analyse sur l'amélioration des soins avec un même niveau de résultats modestes. Hamine (47) a montré une adhérence élevée pour les maladies chroniques.

La recherche documentaire n'a pas cherché à localiser les études de coûts spécifiquement, car ce n'était pas l'objet du travail demandé. Il existe des publications sur le sujet qui montre une tendance à une réduction des coûts de santé (48-50). Une analyse plus complète serait à mener spécifiquement sur le thème du bénéfice coût/efficacité.

1.4.2 Quelques résultats sur des problèmes de santé

Une sélection non exhaustive de publications ciblant l'efficacité des Apps/OC en santé dans le cadre de différents problèmes de santé est exposée afin de donner un aperçu du type de publications actuelles sur des sujets ciblés. Le type d'Apps/OC figurant dans ces études est hétérogène (certaines sont des dispositifs médicaux, d'autres pas).

▶ Diabètes

Russell-Minda (51) a réalisé une revue systématique sur le diabète et les objets connectés pour mesurer la glycémie et l'activité physique. Les résultats montrent une meilleure gestion de la glycémie et une amélioration de la prise en charge.

Des résultats positifs sont aussi retrouvés dans une méta-analyse chinoise de Liang (meilleur contrôle de la glycémie) (52) et dans une revue systématique de Holtz (53).

Gray (54) dans une revue systématique recommande l'évaluation et la validation externe des risques. Il insiste sur l'effort de pédagogie et d'éducation à la santé spécifique à réaliser dans ce domaine.

▶ Activités physiques et obésité

Liu (55) a réalisé une méta-analyse sur l'impact des Apps sur l'activité physique et la réduction de poids. L'IMC et le poids (–1,44 kg avec un IC95 % : –2,12 à –0,76) sont améliorés.

D'autres études (56, 57) mettent en avant l'intérêt des Apps dans ce domaine ou dans le cadre de recommandation dans le champ de l'obésité pédiatrique (58).

Bort-Roig (59) dans une revue systématique met en avant les Apps/OC qui ont le meilleur impact : définir des profils d'activités physiques, mise en place d'objectifs, feedback en temps réel, réseau de soutien, consultation d'experts en ligne. Ce travail complète une étude antérieure de Fanning (60) sur les critères de qualité des Apps/OC efficaces dans ce domaine.

▶ Asthme

Une revue systématique de la Cochrane de 2013 sur l'asthme (61) n'a pas permis de conclure sur l'intérêt des Apps/OC dans ce domaine car les études sont peu nombreuses et hétérogènes.

Huckvale en 2015 (62) montre une évolution de la qualité des applis dans l'asthme en comparant 2011 à 2013, ce qui tend à démontrer que le secteur évolue sur des cycles courts.

1.5 Aspects juridiques de l'évaluation des applications et objets connectés en santé

La conception et l'exploitation des objets connectés dans le monde de la santé mobile doit se conformer aux cadres juridiques (national et européen) existants notamment en matière de dispositifs médicaux, d'échange d'informations et de traitement des données de santé à caractère personnel.

30. myphr.com/HealthLiteracy/MX7644_myPHRbrochure.final7-3-13.pdf

1.5.1 Respect des dispositions légales et règlementaires relatives aux dispositifs médicaux

Certaines Apps/OC en santé sont susceptibles d'être qualifiés de dispositif médical (DM).

Le DM est défini à l'article L. 5211-1 du code de la santé publique comme « *tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Constitue également un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques* ».

L'agence nationale de sécurité du médicament et des produits de santé (ANSM), autorité compétente en matière de DM notamment pour la surveillance du marché et la « vigilance » de ces produits, propose sur son site Internet[31] des éléments d'appréciation aidant à déterminer si une App en santé relève du statut du DM ou non au regard de sa finalité.

Elle indique notamment les conséquences ainsi que la marche à suivre pour commercialiser les Apps qualifiées de DM (marquage CE, réalisation d'une analyse de risque et constitution de documentation technique, etc.)[32].

1.5.2 Respect des dispositions légales et règlementaires relatives au partage d'informations et aux traitements de données à caractère personnel

Les dispositions relatives à la collecte et au traitement de données s'appliquent dès lors que les données traitées par l'Apps/OC sont relatives à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement[33].

Les principes suivants doivent notamment être respectés en cas de traitements de données à caractère personnel :

- **le principe de finalité :** avant toute collecte et utilisation de données personnelles, le responsable de traitement doit précisément annoncer aux personnes concernées ce à quoi elles vont lui servir ;
- **le principe de la pertinence des données :** seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées. C'est le principe de minimisation de la collecte. Le responsable de traitement ne doit donc pas collecter plus de données que ce dont il a vraiment besoin. Il doit également faire attention au caractère sensible de certaines données ;
- **le principe d'une durée limitée de conservation des informations :** également appelé droit à l'oubli : une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées. Cette durée de conservation doit être définie au préalable par le responsable du traitement, en tenant compte des éventuelles obligations à conserver certaines données ;
- **le principe de sécurité et de confidentialité des données :** le responsable de traitement doit prendre toutes les mesures nécessaires pour garantir la sécurité des données qu'il a collectées mais aussi leur confidentialité, c'est-à-dire s'assurer que seules les personnes autorisées y accèdent. Ces mesures pourront être déterminées en fonction des risques pesant sur ce fichier (sensibilité des données, objectif du traitement, etc.) ;
- **le principe du respect des droits des personnes :** des données concernant des personnes peuvent être collectées à la condition essentielle qu'elles aient été informées de cette opération. Ces personnes disposent également de certains droits qu'elles peuvent exercer auprès de l'organisme qui détient ces données la concernant : un droit d'accéder à ces données, un droit de les rectifier, un droit de s'opposer à leur utilisation ; un droit à l'oubli (effacement des données personnelles), un droit à la portabilité des données qui permet à la personne concernée de transmettre facilement ses données à un autre responsable de traitement, le droit d'être informé en cas de piratage de ses données ;
- les données de santé[34], particulièrement sensibles font l'objet d'un encadrement renforcé.

Par ailleurs, les Apps/OC prévoyant l'échange ou le partage d'informations doivent garantir la sécurité des données.

En outre, le partage ou échange de données de santé d'une personne implique son consentement exprès recueilli préalablement à sa mise en œuvre. Ce consentement doit pouvoir être modifié ou retiré à tout moment.

La CNIL, autorité chargée de veiller à la protection des données personnelles, accompagne les professionnels dans leur mise en conformité avec la loi et propose de nombreux guides quant à la collecte et l'utilisation des données à caractère personnel notamment par les professionnels de santé[35].

31. ansm.sante.fr/Produits-de-sante/Dispositifs-medicaux
32. ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Logiciels-et-applications-mobiles-en-sante/%28offset%29/1
33. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; - Règlement (UE) 2016/679 du Parlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ce règlement s'appliquera à tous les États membres de l'Union européenne à compter du 25 mai 2018 sans qu'il soit nécessaire de le transposer).
34. Les « données concernant la santé » sont définies par le règlement européen du 27 avril 2016 comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».
35. www.cnil.fr

1.5.3 Respect des dispositions relatives à l'hébergement de données de santé à caractère personnel

Les Apps/OC qui nécessitent l'hébergement de données de santé à caractère personnel pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même, doivent respecter l'article L. 1111-8 du Code de la santé publique.

L'Agence des systèmes d'information partagés de santé (ASIP) qui a notamment pour mission de développer une offre de produits et de services qui permettent de structurer la e-santé, publie des guides et informations sur ces questions sur son site Internet[36].

36. esante.gouv.fr

2. Le référentiel de bonnes pratiques

Le référentiel de bonnes pratiques sur les Apps/OC en Santé a été construit en plusieurs étapes : analyse de la littérature, groupe de travail indépendant, groupe de lecture et sollicitation de parties prenantes. Une note de cadrage explicite l'origine et les modalités de réalisation de ce document.

2.1 Les domaines à évaluer

Une revue de littérature importante a été réalisée par Riezebos (63) en 2014. Il cite différents auteurs ayant cherchés à évaluer les Apps/OC en santé. Un système d'évaluation par ses pairs produit par un journal en ligne (annexe 2) a été construit à partir de cette analyse de la littérature[37]. Son tableau de synthèse des différents auteurs a été utilisé pour recenser l'ensemble des critères décrits dans la littérature pour évaluer la santé mobile.

À partir de ce document, le groupe de travail a retenu les critères pertinents et les a structurés par domaines et sous-domaines. Un total de 5 domaines et 14 sous-domaines a été retenu pour le référentiel de bonnes pratiques de ce document.

Liste des 5 domaines et 14 sous-domaines d'évaluation du référentiel de bonnes pratiques :

- **Informations utilisateurs**
  - Description
  - Consentement
- **Contenu de santé**
  - Conception de contenu initial
  - Standardisation
  - Contenu généré
  - Contenu interprété
- **Contenant technique**
  - Conception technique
  - Flux des données
- **Sécurité/Fiabilité**
  - Cybersécurité
  - Fiabilité
  - Confidentialité
- **Utilisation/usage**
  - Utilisation/design
  - Acceptabilité
  - Intégration/import

Pour chacun de ces domaines et sous-domaines des critères d'évaluation ont été assemblés à partir de ceux proposés par Riezebos (63) et ceux suggérés par le groupe de travail ou les experts externes. Ils sont décrits, justifiés et encadrés d'exemples concrets.

2.2 Modulation du périmètre de l'évaluation

Les niveaux de risque des Apps/OC sont différents. Lewis (64) définit différents types de risques pour mieux les évaluer. Cette approche entraîne différents scénarios d'évaluation.

Ce constat implique qu'il ne paraît pas envisageable de produire un seul référentiel qui pourrait répondre à la variété des Apps/OC et leurs différents niveaux de risque.

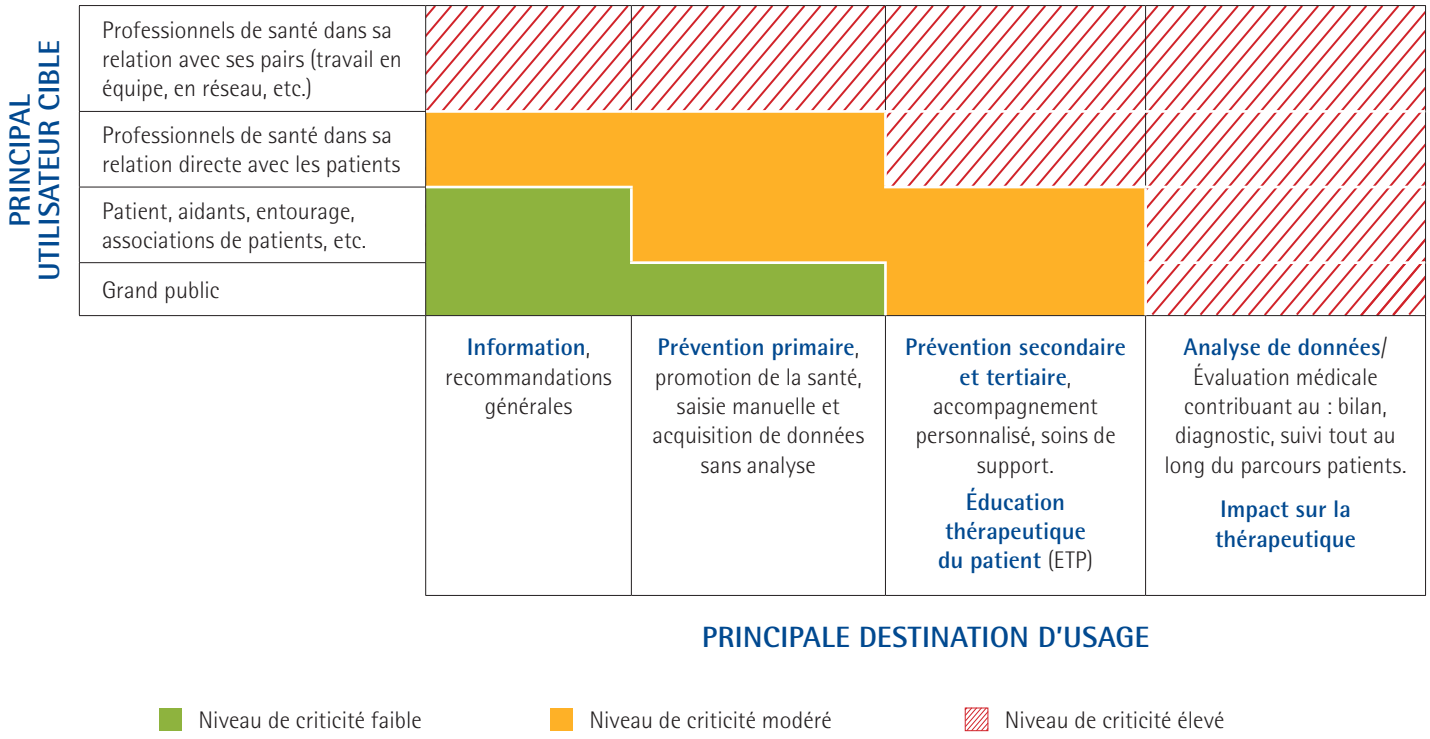
Une solution proposée est de mettre en place une pondération qui permettrait de s'adapter au niveau d'exigence escompté pour l'Apps/OC à évaluer.

Une matrice de risque (Tableau 2) a été construite pour permettre de moduler la liste des critères du référentiel. La pondération est fonction du **principal utilisateur** et de la **principale destination d'usage** déclarée de l'Apps/OC.

Le niveau d'exigence « **vert** » correspond au niveau d'exigence le plus bas et le niveau « **rouge** » correspond au niveau le plus élevé. Le niveau « **jaune** » étant intermédiaire.

37. tinyurl.com/appsform

Tableau 2. Modulation du référentiel par une matrice de risque



Un produit ayant un impact sur la thérapeutique doit systématiquement être sécurisé quelle que soit sa cible. Par ailleurs et même si la matrice ne l'interdit pas, ce type de produit ne devrait a priori pas s'adresser au grand public.

2.2.1 Description des lignes et colonnes de la matrice de risque

L'axe principal utilisateur est divisé en 4 catégories : le grand public, les patients et aidants, le professionnel de santé en relation directe avec le patient et les professionnels de santé entre pairs.

Sur cet axe, le niveau d'exigence le plus élevé cible les professionnels de santé car les décisions sont susceptibles de s'adresser à un grand nombre de patients. Les produits doivent être davantage sécurisés.

L'axe principale destination d'usage est divisé en 4 catégories : informations/recommandations, prévention primaire, prévention secondaire et éducation thérapeutique du patient, enfin, analyse de données et impact sur la thérapeutique.

Sur cet axe, le niveau d'exigence le plus élevé cible l'analyse des données ayant un impact sur le bilan et le diagnostic de l'utilisateur et l'impact sur la thérapeutique par rapport à une information générale.

La pondération ainsi proposée n'a pas pour but de dégrader la qualité de l'évaluation. Elle permet d'aider à sélectionner les critères d'évaluations et le niveau de sureté adaptés à l'utilisation du produit.

▶ Exemple arbitraire A : Appli « monpillulier »

Une App de gestion de prise de médicaments par le patient aurait un niveau d'exigence considéré comme élevé. Tous les critères (sauf ceux qui ne sont pas adaptés) seront à utiliser pour l'évaluation.

▶ Exemple arbitraire B : Appli « monasthme »

Une App d'information aurait un niveau d'exigence considéré comme plus faible. Une sélection restreinte de critères sera effectuée.

À noter que, quel que soit le niveau de pondération, certains critères sont incontournables pour préserver la qualité du produit. Cela concerne tout particulièrement les critères dits « obligatoires », fondés sur la réglementation.

2.2.2 Niveaux des critères

Ce référentiel est un guide de bonnes pratiques. Il est construit dans le but d'améliorer la qualité des Apps/OC disponibles sur le marché. Mis à part, les critères s'appuyant sur les dispositions légales et réglementaires qui sont « obligatoires », les critères retenus dans le référentiel sont considérés comme « souhaités » ou « recommandés » en fonction de la pondération précédente. Ainsi, selon le niveau d'exigence attendu, un même critère d'évaluation, s'il n'est pas obligatoire, pourra être soit « souhaité » soit « recommandé » ce qui permet au référentiel de s'adapter en fonction du type d'Apps/OC à évaluer.

Des exemples concrets permettent d'illustrer les critères de l'ensemble du référentiel.

2.2.3 Mode de sélection et de pondération des critères du référentiel

En pratique, la sélection des critères d'évaluation du référentiel suivrait les étapes suivantes :

- **détermination de l'utilisateur cible principal** (normalement défini par le concepteur ou le fabricant) ;
- **détermination de l'usage principal** de l'Apps/OC (normalement défini par le concepteur ou le fabricant) ;
- **position sur la matrice de risque pour sélectionner le niveau d'exigence** en fonction des 2 réponses précédentes (exemple : site d'informations générales à destination des patients correspond au niveau vert) ;
- **sélection des critères de chaque domaine et sous-domaine** en fonction du niveau d'exigence/de criticité (utilisation du tableur fournit avec ce document ou du tableau récapitulatif de chaque domaine du chapitre suivant) ;
- **exclusion des critères qui ne sont pas adaptés** car ne correspondant pas aux spécificités de l'Apps/OC (exemple : les critères correspondants à la fiabilité de la collecte de mesure ne sont pas utilisables pour évaluer une App d'information en santé) ;
- **évaluation des critères « obligatoires » des 5 domaines d'évaluations**. En cas de non-respect réglementaire ou légal, l'évaluation est arrêtée à ce stade. Il est rappelé que ce référentiel ne se substitue pas à la réglementation relative aux dispositifs médicaux et à la conformité juridique attendue ;
- **évaluation** des critères « recommandés » et « souhaités ». Certains critères nécessitent la mise en place d'une analyse de risque qui ne pourra pas être conduite sans un soutien de personnes compétentes ;
- **compilation des résultats de l'évaluation** des critères et synthèse (éventuellement préconisation spécifique d'amélioration).

Il est rappelé une nouvelle fois que ce référentiel ne se substitue pas au cadre juridique relatif aux dispositifs médicaux et à la conformité juridique attendue. Ce référentiel n'a, par ailleurs, pas vocation à lister de manière exhaustive l'ensemble des dispositions légales et réglementaires applicables aux applications et objets connectés en santé.

La liste des critères est décrite dans les chapitres suivants.

2.3 Domaine : informations utilisateurs

Le domaine de l'information utilisateur (tableau 3) est le premier domaine à évaluer avant de poursuivre l'évaluation.

Tableau 3. Liste des critères se rapportant aux informations utilisateurs

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ Faible / Modérée / Élevée
Description	Dénomination du produit	O O O
	Définition du produit (version et environnement)	R R R
	Prix et facturation éventuelle d'abonnement ou de services intra-App	O O O
	Sources de financement	R R R
	Évaluation	R R R
	Crédits auteurs	O O O
	Contacts (éditeur)	R R R

R Recommandé O Obligatoire

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ
Consentement	Formalités juridiques	Faible – Modérée – Élevée
	Obligation d'information	
	Consentement d'utilisation des données obligatoirement recueilli (indépendant des conditions générales d'utilisation)	
	Consentement révisable et accessible à tout moment	
	Rectification et suppression à tout moment	

2.3.1 *Sous-domaine : description*

▶ Dénomination du produit

La dénomination exacte du produit[38] est-elle décrite précisément sur les supports de promotion et les magasins en ligne ?

Justification : la dénomination doit permettre d'éviter toute confusion avec des noms similaires. Des fausses Apps existent dans différents secteurs et tentent d'imiter une référence connue (recherche d'emplois, faux anti-virus, etc.). L'utilisateur doit prêter attention à des tentatives de phishing par design ou par noms similaires réalisées dans un but malveillant.

Exemple : la sélection dans le magasin en ligne s'effectue sans ambiguïté et l'utilisateur peut re-couper les informations concordantes.

▶ Définition du produit (version et environnement)

La version du produit (indices de version et de révision, date de la version), la liste des modifications majeures (évolutions et corrections) prises en compte dans la version et l'environnement d'utilisation (OS, navigateurs Internet, plateforme, etc.) est-elle accessible ?

Justification : les fonctionnalités des différentes versions peuvent différer. L'utilisateur doit pouvoir identifier la/les version(s) qui correspond(ent) à ses besoins. Il peut également s'agir de correction de sécurité ou autre amélioration qui informent l'utilisateur que certaines anciennes versions ne doivent plus être utilisées pour différentes raisons (conflit inter-Apps, erreur de mesure, etc.). De même, l'environnement d'utilisation doit être adapté au matériel de l'utilisateur.

Exemple : l'utilisateur est informé que des versions antérieures du produit ont posé des problèmes ou des erreurs dans leur fonctionnement afin d'utiliser la version adaptée et fiable correspondant à ses besoins et au matériel à sa disposition.

▶ Prix et facturation éventuelle d'abonnement ou de services intra-App

Le prix, l'abonnement ou les achats éventuels de produits supplémentaires ou intégrés (achat intra-App) sont-ils affichés de manière transparente et explicite pour l'utilisateur ?

Justification : certains produits nécessitent un abonnement pour pouvoir être utilisé. Le modèle économique de certaines Apps s'appuie sur des achats intégrés dans l'App. La ou les fonction(s) de facturation/paiement intégrés sont transparentes, explicites et consultables par tous.

Exemple : l'utilisateur peut se retrouver lié à des contrats de longue durée (après un premier « mois gratuit ») ou des coûts de fonctionnement non spécifié (accès au réseau mobile payant). Le prix « réel » d'utilisation est explicite. L'utilisateur doit être informé de services supplémentaires disponibles dans l'App en surcoût.

38. Dans la suite du document, le terme « produit » est utilisé pour désigner une application de santé mobile seule ou un objet connecté interfacé avec une application.

▶ Sources de financement

Les sources de financement et la provenance des fonds sont-elles documentées[39] et consultables ?

Justification : la provenance du financement peut influer sur la prise des décisions ou impacter la diffusion de contenu biaisé pour maintenir ou promouvoir son activité au dépend de la fiabilité et de l'impartialité exigée par le produit. Les sources de financement ne doivent pas influer sur la neutralité ou crédibilité du produit.

Exemple : une App proposant d'informer/d'éduquer le patient pour une maladie chronique peut orienter les options thérapeutiques dans un sens économiquement favorable au financeur. Les sources de financement doivent être exposées.

▶ Évaluation

Le(s) type(s) et la nature d'évaluation déjà réalisé(s) et à jour est-il/sont-ils documenté(s) ?

Justification : les différents types et nature d'évaluations (évaluation externe, notation en ligne, audit de qualité, marquage CE, etc.) sont disponibles et transparentes.

Exemple : le propriétaire du produit pourrait manipuler les évaluations réalisées de manière à promouvoir celui-ci de manière abusive. Pour prévenir cela, le propriétaire met à disposition l'ensemble des évaluations réalisées en cours de validité de la version à jour de son produit.

▶ Crédits auteurs

Le nom et le rôle des différents contributeurs et éventuellement les droits de copie utilisés (*copyrights*) sont-ils documentés et consultables par tous ?

Justification : les sources des informations doivent être explicites pour connaître la part de chaque contributeur. Les droits de copie[40] (image, vidéos, autres sources) doivent être publiés car un concepteur pourrait reprendre à son compte une partie des informations d'un concurrent ou une iconographie ne lui appartenant pas.

Exemple : l'origine du contenu de l'App est précisée et permet de connaître les auteurs ayant contribués à la conception du produit ainsi que les crédits iconographiques.

▶ Contacts (éditeur)

Les modalités de contacts incluant les délais de réponses entre le demandeur et l'éditeur sont-elles documentées et consultables ?

Justification : l'utilisateur doit pouvoir se référer à un responsable en cas de question(s) liée(s) à l'utilisation du produit en cas d'absence de *hotline*. Une adresse physique et des modalités de contacts téléphonique ou numérique (e-mail, formulaire, etc.) sont à rendre disponible pour tous.

Exemple : une fonctionnalité de l'App n'est pas activée et l'utilisateur a adressé un e-mail au support depuis plusieurs jours sans réponse malgré le fait que le délai de réponse affiché est de moins de 48h. L'éditeur du produit met en place une procédure d'amélioration du suivi des requêtes techniques ou administratives des utilisateurs.

2.3.2 Sous-domaine : consentement

▶ Formalités juridiques

La finalité de traitement est-elle déterminée, explicite et légitime ?

Les formalités ont-elles été réalisées concernant le traitement de données personnelles et l'hébergement de données de santé ?

Justification : les formalités préalables sont des obligations légales.

Exemple : l'App a été déclarée à la CNIL et son hébergeur est agréé hébergeurs agréés données de santé (HDS/HADS) ; une étude des risques sur la vie privée a été réalisée.

▶ Obligation d'information

L'obligation d'information suit-elle les principes de bonnes pratiques suivants ?

Pour les développeurs :

- politique de confidentialité explicite et facilement accessible ;
- avant utilisation, consentement éclairé sur l'accès à des informations sensibles (exemple : géolocalisation, liste de contacts, calendrier, photos, vidéos, etc.) tant que les plateformes et les systèmes d'exploitations n'assurent pas cela systématiquement ;

39. On entend par documenter la présence d'une trace formelle qui peut être consultée sur demande.
40. www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414

- améliorer la communication et la coordination avec les sociétés publicitaires (comme les sociétés d'analyses) éventuellement utilisées par les développeurs, pour harmoniser les informations concernant la collecte de données ;
- se rapprocher des standards qui peuvent être mis en place par différentes organisations.

Cette obligation d'information est-elle mise en œuvre également en cas de modification(s) des conditions générales d'utilisation (CGU) ?

Justification : certains produits peuvent avoir accès au contenu suivant du smartphone : e-mails, messagerie instantanée, liste d'appels téléphoniques, carnet d'adresses, enregistrement des ca-lendriers, réseaux sociaux, historiques de navigations, photographies/films stockés, préférences du système, géolocalisation, accès au microphone, aux caméras, fichiers divers, etc. Pour les développeurs, le principe de « *Privacy by design* » est critique pour l'ensemble des données personnelles de l'utilisateur ; son non-respect peut mettre en cause la loyauté de l'App.

Le concepteur doit informer sur ces éléments de manière explicite.

Exemple : une App demande l'accès à la géolocalisation de l'utilisateur sans préciser les délais d'accès ou l'utilisation simultanée des appareils photographiques. Le concepteur du produit met en place une procédure d'amélioration de son obligation d'information.

▶ Consentement d'utilisation des données obligatoirement recueilli (indépendant des CGU)

Le consentement d'utilisation est-il explicite et en-dehors des conditions générales d'utilisation ?

Avant utilisation, le consentement éclairé est-il recueilli sur l'accès à des informations sensibles (exemple : géolocalisation, liste de contacts, calendrier, photos, vidéos, etc.) tant que les plateformes et les systèmes d'exploitations n'assurent pas cela systématiquement ?

Cette obligation de recueil du consentement est-elle mise en œuvre également en cas de modification(s) des CGU ?

Justification : le consentement d'accès aux données générales doit être recueilli.

Le consentement d'accès aux données spécifiques de son smartphone doit être explicite.

Exemple : l'utilisateur doit approuver une notification ou effectuer un réglage spécifique avant l'utilisation de sa caméra, de sa géolocalisation ou autre contenu de son *smartphone*.

▶ Consentement révisable et accessible à tout moment

L'affichage et la gestion du consentement par l'utilisateur est-il disponible concernant la collecte et le traitement de ses données ?

Justification : l'utilisateur a le droit de changer son consentement à tout moment. Ce qui justifie également une gestion indépendante des conditions générales d'utilisation (qui sont acceptées à la première utilisation uniquement).

Exemple : un élément de réglage est accessible pour modifier le consentement.

▶ Rectification et suppression à tout moment

Le respect du droit des utilisateurs de corriger leurs données et/ou de les effacer est-il mis en œuvre ?

Justification : l'utilisateur a le droit de changer ses données ou de les effacer à tout moment ce qui justifie également que le consentement soit donné indépendamment des conditions générales d'utilisation (qui sont acceptées à la première utilisation uniquement).

Exemple : un élément de réglage est accessible pour modifier ou effacer ses données personnelles.

2.4 Domaine : contenu de santé

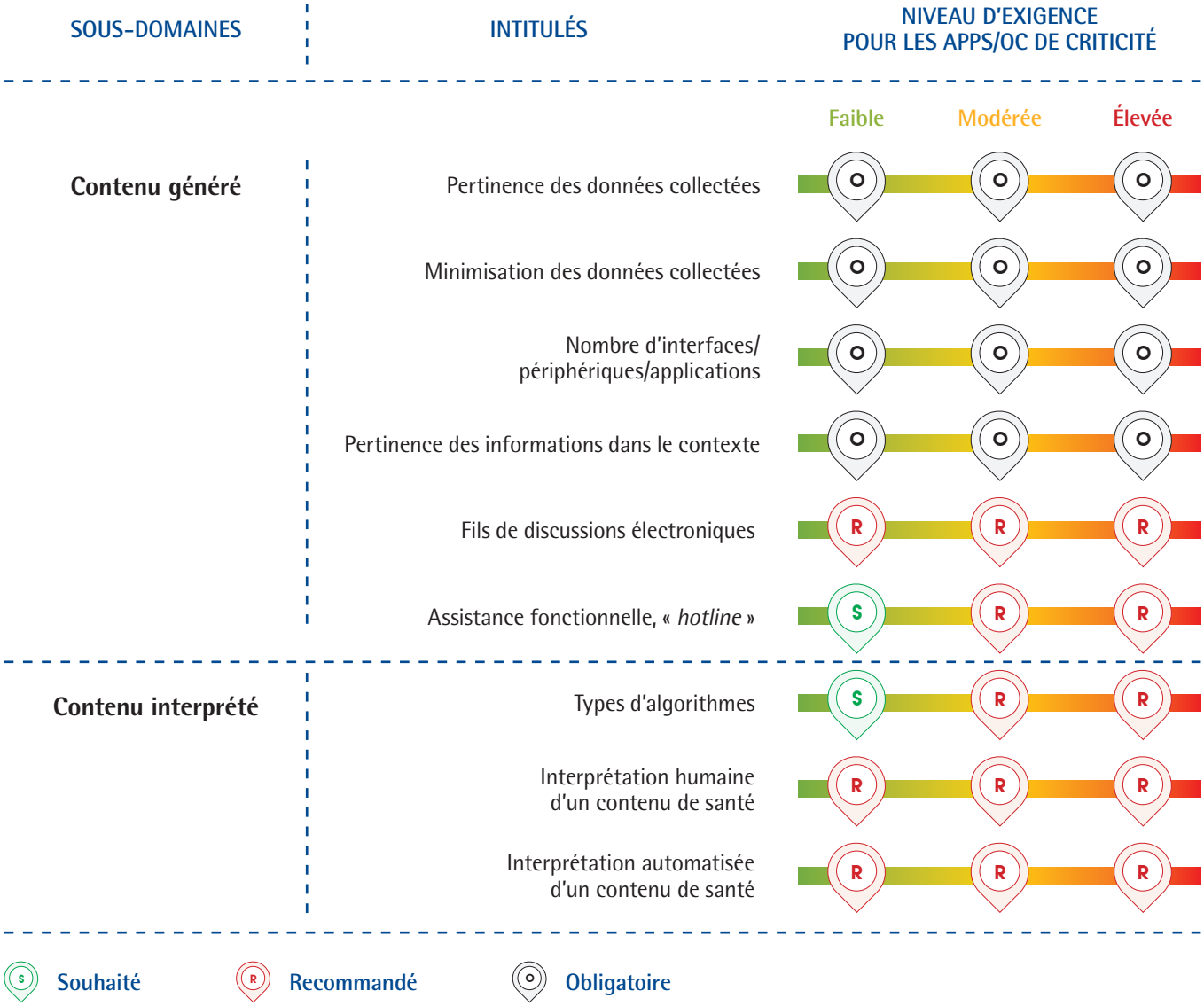
Le domaine contenu de santé (tableau 4) est le domaine qui évalue la fiabilité des informations. Il aborde les notions de contenu généré par le produit ou de contenu interprété lorsqu'un algorithme ou un professionnel du secteur analyse et traite le contenu généré.

BinDhim (65) a publié une enquête montrant que 77 % des utilisateurs ne vérifient pas la crédibilité des informations.

Tableau 4. Liste des critères se rapportant au contenu de santé du produit

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ
		Faible / Modérée / Élevée
Conception du contenu initial	Implication des utilisateurs (patients, professionnels, personne spécifique)	S / R / R
	Méthodologie d'ingénierie des besoins utilisateurs	S / R / R
	Organisation du service de l'information	S / R / R
	Expertise des auteurs du contenu	R / R / R
	Déclarations d'intérêts	R / R / R
	Citation des sources clés et références bibliographiques	R / R / R
	Actualisation des sources clés et références bibliographiques	R / R / R
	Niveau de preuve	R / R / R
	Description de la destination d'usage	O / O / O
	Langue du produit	R / R / R
	Thésaurus-Glossaire	S / S / S
Standardisation	Interopérabilité : standards de sémantique, terminologies de références	S / R / R
	Précision et reproductibilité des données	S / R / R
	Granularité des données	O / O / O
	Perte d'informations (par agrégation, par compression, etc.)	S / R / R
	Performance de la mesure dans le contexte d'utilisation	S / R / R
	Possibilité de synchronisation des données	S / S / S

S Souhaité R Recommandé O Obligatoire



2.4.1 *Sous-domaine : conception du contenu initial*

▶ Implication des utilisateurs (patients, professionnels, personnes spécifiques)

Les principaux utilisateurs sont-ils impliqués dans les phases de spécification, de conception, de recette et de maintenance (ajustements suite à des évolutions ou des corrections) ? Ce critère est-il documenté ?

Justification : la conception avec les différentes parties prenantes spécifiée de manière transparente est un gage de qualité.

Exemple : une App d'apprentissage de lavage des mains est réalisée en collaboration avec des personnes réalisant des formations sur le terrain.

▶ Méthodologie d'ingénierie des besoins utilisateurs

La méthodologie d'ingénierie des besoins utilisateurs (identification, définition, analyse/hiérarchisation des besoins) est-elle documentée ?

Justification : l'évaluation des besoins des utilisateurs permet d'améliorer les objectifs de conception du produit. L'utilisation d'outil ou de méthode de recueil, d'analyse et de structuration des besoins contribue à améliorer la pertinence du produit.

Cette évaluation permet d'identifier l'utilisateur principal du produit. Ce critère est-il documenté ?

Exemples : les évaluateurs externes ont accès à la méthodologie utilisée par le concepteur (grille d'analyse, écritoire, Living Lab, etc.).

Pour en savoir plus :

Hilliard (66) a enquêté pour connaître les besoins utilisateurs dans le cadre de mucoviscidose de l'adulte. Jibb (67) a développé un algorithme pour la douleur liée au cancer. Cela a abouti à la mise en place d'un processus de conception d'une App pour cancer des adolescents. La motivation de l'utilisateur est à développer (68, 69). Silow-Carroll (70) a enquêté sur les besoins des patients. Les réponses dépendent de l'âge et des besoins spécifiques.

▶ Organisation du service de l'information

La présence d'un comité de validation ou d'une organisation gérant la délivrance d'informations est-elle mise en place ? Ce critère est-il documenté ?

Justification : la rédaction et la gestion du contenu disponible dans le produit s'appuie sur un comité de validation qui garantit la qualité de l'information publiée.

Exemple : une App diffusant des synthèses de recommandations de bonnes pratiques à destination des professionnels de santé met en place un comité de lecture pour surveiller que la synthèse respecte bien les recommandations originales.

▶ Expertise des auteurs du contenu

Des experts (professionnels de santé, ingénieurs, organismes professionnels, associations de patients ou consommateurs, etc.) sont-ils impliqués dans l'apport du contenu du produit ? Ce critère est-il documenté ?

Justification : le niveau d'expertise des auteurs du contenu du produit est un gage de qualité. La reconnaissance par ses pairs ou l'adossement à des organismes ou associations professionnelles améliore la crédibilité du contenu produit.

Exemples : des professionnels de santé appuyés par leur association professionnelle scientifique ont mis en place une plateforme d'informations sur la conduite à tenir en cas de crise d'asthme. L'App cite le niveau d'expertise des experts impliqués.

Une association de patients met en place une App d'informations et une FAQ pour les familles et les aidants des patients. Elle fait appel à une association professionnelle en relation avec la pathologie pour donner un avis externe sur le contenu de l'App.

▶ Déclarations d'intérêts

Les déclarations des liens d'intérêts, en rapport avec le produit, des différents contributeurs sont-ils consultables par tous ?

Justification : les déclarations des liens d'intérêts éventuels est un gage de transparence pour les utilisateurs et évaluateurs externes. Les liens d'intérêts peuvent entraîner des biais qui pourraient remettre en cause la fiabilité du produit.

Exemple : les évaluateurs externes réalisent des contrôles par échantillonnage afin de vérifier la véracité de ces déclarations ou les biais éventuels qui proviendraient de ces liens.

▶ Citation des sources clés et références bibliographiques

Les sources clés et références relatives à des publications argumentant le contenu de l'Apps/OC sont-elles documentées et peuvent-elles être consultables par tous[41] ?

Justification : dans le domaine de la santé, la citation des sources bibliographiques et d'une sélection objective des meilleures données disponibles est un gage de qualité requis. L'accès à la liste de références doit être consultable facilement.

Exemple : la citation peut s'effectuer soit en intra-Apps, soit sur un site web ressources, soit par une documentation externe, etc.

▶ Actualisation des sources clés et références bibliographiques

Le processus de veille et de mise à jour des sources clés et des références relatives à des publications sont-ils documentés ?

Justification : la veille bibliographique permet de mettre à jour et d'adapter l'état des connaissances traitées par l'Apps/OC. La date de la mise à jour de l'information est à citer.

Exemple : une alerte liée à des bases de données et un suivi de sommaires de revues spécifiques est mis en place et datée pour une App d'information traitant d'une maladie rare.

▶ Niveau de preuve

S'il existe une évaluation spécifique du produit et des niveaux de preuves, ces références spécifiques sont-elles consultables par tous ?

Justification : la HAS a produit des guides d'analyse critique de la littérature, de gradation de niveaux de preuves ou de méthodologie d'évaluation[42,43,44,45,46].

Certaines Apps/OC ont fait l'objet d'essai contrôlé randomisé (ECR) ou certains types d'Apps ont fait l'objet de revue systématique. Ces références sont majeures et doivent être accessibles pour justifier l'intérêt du produit.

Il y a aussi une réflexion sur des approches d'évaluations « alternatives » pour la santé mobile telles que :

- l'intégration clinique (utilisation du produit) ;
- le changement comportemental lié à l'utilisation du produit ;
- etc.

41. On entend par consultable par tous le fait que l'accès à l'information ne requiert pas ni l'achat, ni l'installation de l'appli.
42. www.has-sante.fr/portail/upload/docs/application/pdf/analiterat.pdf
43. www.has-sante.fr/portail/upload/docs/application/pdf/2013-06/etat_des_lieux_niveau_preuve_gradation.pdf
44. www.has-sante.fr/portail/upload/docs/application/forcedownload/2016-03/guide_methodologique_analyse_critique.pdf
45. www.has-sante.fr/portail/upload/docs/application/pdf/eval_interventions_ameliorer_pratiques_guide.pdf
46. www.has-sante.fr/portail/upload/docs/application/pdf/2011-11/guide_methodo_vf.pdf

Ces approches ne sont pas considérées comme des niveaux de preuve et doivent s'appuyer sur une méthodologie qualitative rigoureuse pour être citée. La recherche académique est en développement sur ce secteur.

Exemple : une Apps/OC est utilisée lors d'un essai contrôlé randomisé (ECR) dans le cadre d'un programme de suivi et de promotion de l'activité physique chez des personnes âgées. Les résultats de l'ECR ont mis en évidence une diminution des chutes pour le groupe intervention. L'Apps/OC cite la publication dans ses références et son rôle comme outil de suivi.

Pour en savoir plus :

À noter que Kumar (71) a proposé d'adapter la méthodologie d'évaluation pour la publication de la fiabilité des mesures ou de l'efficacité thérapeutique. Tomlinson (72) a projeté l'évolution méthodologique de l'évaluation du secteur de la santé mobile pour les prochaines années. Whittaker (36) propose les différentes phases d'évaluation méthodologiques (du *focus group* à l'étude d'impact) pour évaluer la qualité des Apps.

Bull (68) souhaite que les approches psychosociales et psychologiques soient mieux évaluées.

Hussain (20) a exposé les différentes approches actuellement publiées pour évaluer une App.

▶ Description de la destination d'usage

La destination d'usage principal (objectifs ou finalités) du produit fait-elle l'objet d'une description précise et consultable par tous ?

Justification : cette déclaration est un élément important pour définir l'usage qui sera fait du produit.

Si l'usage déclaré par le fabricant est un instrument, appareil, équipement ou encore un logiciel destiné à être utilisé chez l'homme à des fins, notamment, de diagnostic, de prévention, de contrôle, de traitement, d'atténuation d'une maladie ou d'une blessure (*directive 93/42/CEE relative aux dispositifs médicaux*) il est éligible pour être un dispositif médical. Le fabricant devra se rapprocher de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) et se conformer aux dispositions légales et réglementaires applicables[47].

Si l'usage déclaré n'est pas adapté, une requalification de la destination d'usage est envisageable.

À noter que dans certains cas, la destination d'usage déclarée peut masquer l'intention de collecter d'autres types de données pour différentes fins (collecte de données, espionnage, géolocalisation, etc.). Une attention particulière est à porter pour détecter cette mauvaise pratique.

Exemple : une Apps/OC dont la destination d'usage est de mesurer la fréquence cardiaque de repos moyenne de l'utilisateur dans le cadre d'une activité physique régulière n'a pas vocation à servir de référence pour la réhabilitation cardiaque.

Pour en savoir plus :

Wolf (73) a évalué des Apps/OC photographiant des mélanomes. L'utilisation sous supervision médicale est plus efficace.

▶ Langue du produit

L'Apps/OC et sa documentation associée sont-elles disponibles dans la langue de l'utilisateur ?

Justification : la traduction de l'Apps/OC ou le fait d'utiliser une Apps/OC dans une autre langue que sa langue maternelle peut entraîner un risque de mauvaise interprétation des données par incompréhension, « faux-amis » ou une mauvaise traduction des concepteurs dans leur processus de traduction.

Exemple : un concepteur a utilisé un traducteur automatisé pour la traduction du texte de son App. Un test de lecture par un utilisateur montre que la traduction n'est pas fiable. Le concepteur du produit met en place une procédure d'amélioration de la traduction de son App pour ne citer que les langues réellement supportées.

▶ Thésaurus-Glossaire

L'Apps/OC s'appuie-t-elle sur un thésaurus pour les termes présents dans l'App ?

Justification : une liste de termes et leurs définitions permettent d'éviter toute ambiguïté et mauvaise interprétation de la part de l'utilisateur.

Exemple : une App a placé des liens vers un thesaurus pour les mots considérés comme « critiques » pour la compréhension du texte.

2.4.2 Sous-domaine : standardisation

▶ Interopérabilité: standards de sémantique, terminologies de références

La sémantique des flux d'informations est explicitée et les terminologies utilisées entre le professionnel de santé et le patient s'appuient-ils sur des standards (exemples : HL7, SNOMED, etc) ?

Justification : l'interopérabilité est un enjeu important pour le traitement, la diffusion et la conservation des données. L'utilisation de standard est à promouvoir et fait l'objet d'un travail européen[48].

47. ansm.sante.fr/Produits-de-sante/Dispositifs-medicaux
48. ec.europa.eu/digital-single-market/en/interoperability-standardisation-connecting-ehealth-services

Exemple : le concepteur du produit met en place une stratégie d'inter-opérabilité dès la conception du produit.

Pour en savoir plus : Interopérabilité des données (*EU eHealth interoperability framework*) est un des éléments du livre vert de la Commission européenne sur la e-santé (74).

▶ Précision et reproductibilité des données

Le niveau de précision des mesures (fidélité) par rapport à un étalon-or et le niveau de la reproductibilité des données sont-ils documentés et en adéquation de la destination d'usage du produit ?

Justification : si des mesures sont collectées, leurs caractéristiques métrologiques doivent être transparentes pour en connaître leurs niveaux de précision et de fiabilité. Ce niveau de précision est à faire correspondre au niveau d'utilisation attendu du produit.

Ce domaine est critique car la fiabilité des données collectées peut varier entre les produits disponibles sur le marché et les usages attendus. L'utilisateur doit connaître le niveau de précision et de reproductibilité des données mesurées pour l'usage attendu.

Exemple : un produit quantifiant l'activité physique est étalonné par rapport à un étalon-or et son niveau de précision (ou sa marge d'erreur) est cité par le fabricant.

▶ Granularité des données

Le plus petit niveau de données mesuré est-il justifié en regard de la destination d'usage du produit (rafraichissement, fréquence d'échantillonnage, etc.) ?

Justification : le signal brut collecté peut être plus ou moins précis en fonction des réglages et des capacités des capteurs. Dans certaines situations, la perte de données liée à une granularité trop faible peut entraîner une mauvaise interprétation.

Exemple : le réglage de l'accéléromètre du capteur mis en place pour suivre la mobilité d'un utilisateur n'est pas adapté en fonction de la taille de petits sujets. Le concepteur du produit met en place une procédure d'amélioration de la mesure.

▶ Perte d'informations (par agrégation, par compression, etc.)

Les modalités d'agrégation, de lissage des données, de production des courbes, ou autres traitements sont-ils documentés et justifiés en regard de la destination d'usage du produit ?

Justification : il s'agit, ici, d'apprécier le risque éventuel de perte d'informations en relation à son utilisation. Le traitement du signal brut est effectué de manière adaptée en fonction de l'usage attendu du produit. Dans certaines situations, la perte de données liée au lissage des données peut entraîner une mauvaise interprétation.

Exemple : la mesure, par un objet connecté, de la force produite par l'utilisateur donne des résultats de force maximale instable car le lissage des données est trop important. Le concepteur du produit met en place une procédure d'amélioration du traitement de son signal pour améliorer son produit.

▶ Performance de la mesure dans le contexte d'utilisation

La performance de la mesure (robustesse contextuelle) dans le milieu ou le contexte d'utilisation est-elle documentée et justifiée en regard de la destination d'usage du produit ?

Justification : la mesure effectuée en situation réelle peut différer par rapport aux mesures effectuées en laboratoire.

La mesure de données de santé ou de bien-être dans l'environnement de l'utilisateur doit être de qualité.

Exemple : un capteur d'activité placé sur le poignet auprès d'utilisateurs atteints d'un syndrome extrapyramidal peut présenter des données erronées dues aux tremblements de repos liés à la maladie.

▶ Possibilité de synchronisation des données

La possibilité de synchroniser les données sur différents équipements est-elle présente ? Le consentement préalable de l'utilisateur a-t-il été prévu ?

Justification : la santé mobile peut utiliser plusieurs supports : smartphone, tablettes, montres, etc. Les possibilités de synchronisation sur plusieurs supports pour un même utilisateur sont à proposer par le fabricant.

Exemple : l'utilisateur se connecte avec un identifiant et mot de passe sur sa tablette chez lui ou son smartphone en extérieur pour suivre son activité physique.

2.4.3 Sous-domaine : contenu généré

Notez bien que cette partie devrait intégrer également les sous-domaines **standardisation** et **cybersécurité** (authentification des utilisateurs, de l'App, intégrité et authenticité des données, etc.).

▶ Pertinence des données collectées

Le choix des données collectées est-il justifié en regard de la destination d'usage du produit ?

Justification : le fabricant doit pouvoir justifier les éléments utilisés pour son produit et éviter toute dérive de collecte en masse ou d'utilisation malveillante. Certains produits pouvant proposer un service et durant son utilisation collecter des données sans lien avec le service proposé (mais ayant une valeur commerciale par exemple).

Exemple : les évaluateurs externes rechercheront l'adéquation entre l'objectif déclaré et l'utilisation réelle.

▶ Minimisation des données collectées

Le choix des données collectées est-il conforme au principe de minimisation de données qui impose de ne collecter que les données nécessaires à la destination d'usage du produit ?

Pour toutes les données collectées, l'information auprès de l'utilisateur est-elle accessible et transparente ?

Justification : le principe de minimisation est conforme et exposé de manière transparente pour l'utilisateur afin qu'il soit informé de manière objective sur l'utilisation de ses données.

Exemple : une App de recherche prospective sur différents paramètres de qualité de vie de l'utilisateur décrit les données réelles collectées et la période de collecte.

▶ Nombre d'interfaces/périphériques/applications

Le nombre d'interfaces/périphériques/applications avec lesquels dialogue l'Apps/OC est-il adapté aux ressources du terminal et en relation avec la destination d'usage du produit ? Pour toutes les données collectées, l'information auprès de l'utilisateur est-elle accessible et transparente ?

Justification : le nombre d'interfaces/périphériques/applications est exposé de manière transparente pour l'utilisateur afin qu'il soit informé de manière objective sur l'utilisation de ses données. L'Apps/OC utilise ce qui est strictement nécessaire à la destination d'usage déclarée afin d'éviter la collecte ou l'utilisation abusive de données.

Exemple : une App de suivi alimentaire pour les utilisateurs utilise l'appareil photographique du smartphone, une balance de cuisine et un pèse-personne connectée. L'utilisateur est informé des connexions avec les périphériques.

▶ Pertinence des informations dans le contexte

Le contenu correspond-il (utilité, intérêt, etc.) aux besoins de l'utilisateur dans la situation où il se trouve ?

Justification : lorsque du contenu est « généré » lors de son utilisation, il doit être adapté et utile à l'utilisateur.

Exemple : une App de suivi d'activité physique génère des conseils ou des encouragements en fonction de l'activité réalisée par l'utilisateur.

▶ Fil de discussion électronique

Le fil de discussion est-il modéré et régi par une charte d'utilisation définissant notamment les conditions d'utilisation et le comportement à adopter ?

Justification : une charte d'utilisation et une modération sont des moyens d'améliorer la qualité des fils de discussions. Ces moyens permettent d'éviter la diffusion d'informations erronées ou malveillantes. Les éventuels commentaires désobligeants d'utilisateurs ne devront être retirés délibérément par le modérateur, que dans la limite du respect de la charte d'utilisation et de la réglementation.

Exemple : le concepteur met en place un fil de discussion sur l'addiction dans le monde de la santé sur une App d'éducation à la santé. Il met en place le suivi de tous les commentaires par 2 modérateurs qui valident le contenu produit par les utilisateurs.

▶ Assistance fonctionnelle, « *hotline* »

Une « *hotline* » permettant de solliciter une demande d'assistance est-elle mise à la disposition des utilisateurs pour les demandes relatives à l'utilisation du produit (compréhension des contenus et utilisation des fonctionnalités) ? Les questions fréquemment posées sont-elles documentées et peuvent être consultées (FAQ, etc.) ?

Un processus qualité de collecte, d'adressage, de suivi et de restitutions des retours utilisateurs peut être documenté en fonction de l'objet de l'Apps/OC.

Justification : un soutien à l'utilisation du produit permet d'améliorer la qualité d'utilisation. Ce soutien peut prendre différentes formes en fonction des objectifs du produit et de différents facteurs d'utilisation (gestion de données, interface à plusieurs niveaux, etc.).

Exemple : une App pense-bête pour la prise de médicaments propose une FAQ pour le réglage des alertes et notifications.

2.4.4 Sous-domaine : contenu interprété

▶ Types d'algorithmes

Les types d'algorithmes utilisés sont-ils cités afin que l'utilisateur sache si l'Apps/OC utilise des algorithmes « propriétaires » et/ou des algorithmes « ouverts » ou reprenant des calculs ou des scores publiés ?

Justification : le contenu généré peut être interprété par un algorithme propre au fabricant ou reprenant des équations de calculs publiés. Le(s) type(s) d'algorithme utilisé(s) doi(ven)t être transparent(s) pour l'utilisateur.

Exemple : une App de normes de dosage biologiques à destination des médecins calcule les zones thérapeutiques utilisables. Les normes sont liées à une base de données identifiées et les calculs suivent des équations référencées dans l'App.

Pour en savoir plus :

Albrecht (75) propose des éléments de sécurité dans le développement des algorithmes.

Bierbrier (76) liste les Apps de calculs médicaux les plus usuels et a évalué la fiabilité des calculs. Six Apps sur 14 sont précises à 100 %. Les erreurs ne sont pas vitales mais il convient d'évaluer les calculs et les fonctions de ces Apps de calculs.

Concernant la fiabilité des calculs, Chyjek (77) a évalué des Apps mesurant des dates d'accouchements. Plus de la moitié proposaient des dates inexactes.

Huckvale (78) a évalué les erreurs de calcul de glycémie à plus de la moitié (8 en *input* et 5 en *output*).

▶ Interprétation humaine d'un contenu de santé

En cas d'interprétation humaine (non automatisée) de contenus à visée de santé (données de santé, contenu scientifique, etc.), celle-ci est-elle assurée par des professionnels de santé qualifiés ?

Justification : l'interprétation de contenu scientifique ou de données de santé nécessite l'implication de médecins ou de professionnels de santé selon les cas.

Exemples : un cardio-fréquencemètre connecté collecte des données d'activité physique d'un utilisateur. Les informations sont transmises à un médecin/cardiologue pour avis.

Une App d'un journal club propose une revue de presse et une interprétation des données de la littérature. Les évaluateurs externes professionnels de santé du secteur s'assurent de l'interprétation ou de l'absence de biais de sélection des articles.

▶ Interprétation automatisée d'un contenu de santé

Les algorithmes ayant pour objet d'interpréter des contenus à visée de santé (données de santé, contenu scientifique, etc.) sont-ils évalués ? Le plan et les comptes rendus des tests sont-ils documentés ?

Justification : l'interprétation de contenu scientifique ou de données de santé réalisée de manière automatique nécessite d'évaluer la fiabilité de l'interprétation. La crédibilité des tests des algorithmes est un élément critique à évaluer pour garantir cette fiabilité.

Ce critère est amené à évoluer dans les prochaines années car le secteur de la santé mobile et le niveau technologique actuel contribue au développement des algorithmes.

Exemples : un cardio-fréquencemètre connecté collecte des données d'activité physique d'un utilisateur. En fonction des résultats, un programme d'entraînement est proposé de manière automatisée à l'utilisateur. Les évaluateurs externes devraient évaluer le niveau de risque de l'interprétation en consultant la fiabilité des tests utilisés par le(s) concepteur(s).

Un multi-moteur de recherche d'articles se propose de classer les meilleurs articles disponibles. Les évaluateurs externes pourraient effectuer différents tests ciblés pour comparer la pertinence des résultats obtenus ou les plans de test utilisés par le(s) concepteur(s).

Une requête automatisée est lancée sur les bases de données scientifiques pour cibler des articles spécifiques d'un domaine particulier.

2.5 Domaine : contenant technique

Le domaine contenant technique (tableau 5, page suivante) est évalué principalement par des évaluateurs externes.

L'Union européenne souhaite le développement d'Apps/OC dans lesquels l'utilisateur peut avoir confiance (79).

2.5.1 Sous-domaine : conception technique

Le sous-domaine conception technique renvoie également au sous-domaine de **cybersécurité** (utilisation sûre d'un code tiers externe, etc.).

▶ Configuration et performances des équipements[49]

La configuration et les performances des équipements sont-elles documentées et sont-elles en adéquation avec la destination d'usage du produit et de son utilisateur principal ?

Justification : la performance des équipements peut devenir un critère rédhibitoire si elle ne correspond pas aux niveaux de l'usage attendu du produit.

49. La notion d'équipement renvoie à tous les matériels faisant fonctionner l'application (smartphone, ordiphone, tablette, etc.) ou objet connecté.

Tableau 5. Liste des critères se rapportant au contenant technique du produit

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ
		Faible / Modérée / Élevée
Conception technique	Configuration et performances des équipements	R / R / R
	Méthodologie de développement logiciel	S / S / R
	Suivi des mises à jour	R / R / R
Flux des données	Interface avec un dossier patient informatisé[50]	S / S / S
	Rétrocompatibilité	S / R / R
	Import, export et réversibilité des données	O / O / O
	Modèle de données	S / S / S
	Modalités d'hébergement des données	O / O / O
	Hébergement des données et procédure de sauvegarde	O / O / O

S Souhaité R Recommandé O Obligatoire

Le niveau d'équipement peut être :

- la définition et la taille de l'écran dans le cas de lecture d'images/vidéos[51] ;
- la qualité sonore dans le cas d'enregistrement ou de diffusion sonore ;
- les caractéristiques métrologiques en fonction des capteurs et des données à collecter ;
- etc.

Exemple : une App propose de prendre des photos de mélanome pour que le patient les stocke et les présente à son dermatologue. Cela nécessite un appareil photographique adapté et un traitement de l'image fiable.

▶ Méthodologie de développement logiciel

Un contrôle qualité du développement logiciel et l'utilisation des frameworks est-il mis en place ?

Justification : la méthodologie de conception logicielle doit s'appuyer sur des méthodes et une démarche qualité explicites.

Exemple : quelques méthodes de développement logiciel sont cités : agile, Scrum, *Extreme Programming*, UML, etc.

Les évaluateurs externes devraient évaluer la crédibilité de conception.

50. L'interface avec un dossier patient informatisé n'est pas une obligation légale mais sa mise en œuvre implique notamment le respect des dispositions relatives au partage de données et au secret médical.

51. www.knowtex.com/nav/prometee-un-living-lab-pour-faire-rimer-medecine-et-numerique_42225

▶ Suivi des mises à jour

L'historique des versions incluant les modifications apportées (évolutions et corrections) est-il documenté ?

Justification : une liste des versions et des modifications historiques apportées est à maintenir à jour pour tracer le développement du produit. Le niveau de qualité du développement de l'App nécessite une transparence dans la conception et son suivi de mise à jour.

Exemple : les évaluateurs externes pourront demander la liste de cet historique.

2.5.2 Sous-domaine : flux des données

▶ Interface avec le dossier informatisé du patient

L'Apps/OC propose-t-elle une fonctionnalité d'interface avec un dossier patient informatisé? Cette interface respecte-t-elle les conditions légales et réglementaires applicables au partage de données de santé ?

Justification : le dossier informatisé du patient et son interconnexion avec l'environnement du monde de la santé mobile est un enjeu important. Le sujet du dossier du patient informatisé est en développement et sera amené à évoluer, il convient de suivre les obligations réglementaires sur ce sujet.

Exemple : un pèse-personne connecté transmet l'historique du poids de l'utilisateur dans son dossier patient électronique.

▶ Rétrocompatibilité

La compatibilité descendante (compatibilité d'un produit vis-à-vis des anciennes versions) est-elle documentée ?

Justification : si un produit a collecté des données personnelles ou effectué des interactions avec l'utilisateur, la continuité de l'utilisation des données est à garantir au cours des différentes versions de l'Apps/OC.

Exemple : un capteur d'activité physique garantit la continuité des données recueillies entre les versions du produit auprès des utilisateurs.

▶ Import, export et réversibilité des données

Les fonctionnalités d'import, d'export et de conversion des données dans des formats standards (réversibilité) sont-elles documentées ?

Justification : si un produit a collecté des données personnelles ou effectué des interactions avec l'utilisateur, l'import, l'export et la conversion des données est à garantir.

Exemple : un pèse-personne connecté propose un import/export de données dans différents standards compatibles.

▶ Modèle de données

Le modèle de données décrivant la façon dont les données sont représentées et gérées est-il documenté ?

Justification : l'expression « modèle de données » est utilisée pour expliquer comment sont gérées les données (base de données, représentations mathématiques, etc.).

Exemple : les évaluateurs externes pourront demander le type de modèle de données utilisé pour en évaluer la pertinence.

▶ Modalités d'hébergement des données

Les modalités d'hébergement des données sont-elles documentées et conformes aux dispositions légales et réglementaires ?

Justification : les modalités d'hébergement des données suivent des modalités réglementaires (recours à un hébergeur agréé en cas d'externalisation de l'hébergement de données de santé à caractère personnel, sécurité de l'hébergeur, etc.). Pour les autres situations non réglementées, les modalités d'hébergements doivent être transparentes.

Exemple : les évaluateurs externes pourront demander le type d'hébergement et évaluer les risques encourus.

▶ Hébergement des données et procédure de sauvegarde

La procédure de sauvegarde définissant notamment la périodicité, le format, les zones de stockages et les mécanismes de récupération de ces sauvegardes est-elle documentée et conforme aux dispositions légales et réglementaires ?

Justification : la procédure de sauvegarde des données est une garantie de sécurité à maintenir. Pour les autres situations non réglementées, les procédures de sauvegarde doivent être transparentes.

Exemple : le fabricant communique aux utilisateurs les processus de sauvegarde qu'il utilise.

2.6 Domaine : sécurité/fiabilité

Le domaine sécurité/fiabilité (tableau 6, page suivante) porte principalement sur la cybersécurité, la fiabilité des informations et les risques liés aux données personnelles. Les outils d'évaluation de ces domaines peuvent être des approches par « analyse de risque ou de menace ». En fonction de la situation, il sera peut être nécessaire de faire appel à des évaluateurs externes.

Tableau 6. Liste des critères se rapportant à la sécurité et fiabilité du produit

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ
		Faible / Modérée / Élevée
Cybersécurité	Analyse de la menace	
	Sécurité dans le développement	
	Sécurité des fonctions cryptographiques	
	Méthodologie de protection/ vérification du code	
	Utilisation sûre d'un code tiers externe	
	Authentification des utilisateurs/des données	
	Authentification de l'Apps/OC	
	Intégrité et authenticité des données	
	Transfert/échanges des données sécurisées	
	Partage et accès aux données avec d'autres Apps/OC	
	Stockage sécurisé des données sur le terminal	
	Stockage sécurisé des données sur le(s) serveur(s) distant(s)	
	Insécurité et failles des services distants	
	Maintien en condition de sécurité	
	Sensibilisation de l'utilisateur, causes potentielles de brèche de confidentialité	R / R / R
	Évaluation de la sécurité	R / R / R
	Signalement et transparence sur la violation de données ou en cas d'incident de sécurité	

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ
		Faible — Modérée — Élevée
Fiabilité	Fiabilité et maintenabilité hardware (capteurs) et software	S — R — R
	Disponibilité de l'infrastructure	S — S — R
	Assistance technique « *hotline* »	S — R — R
	Qualité des matériaux, innocuité des dispositifs	O — O — O
	Optimisation des fichiers média	S — S — R
	Contre-indications, risques potentiels, limitations d'usage	R — R — R
	Niveau de disponibilité	S — S — R
	Maintenance préventive	S — S — R
	Fonctionnement vis-à-vis des autres Apps/OC	R — R — R
Confidentialité	Destinataire des données collectées, confidentialité des données personnelles, et consentement pour la transmission à des tiers	R — R — R
	Pseudonymisation des données	R — R — R
	Anonymisation des données	O — O — O
	Délais de suppression et temps de mise en œuvre	O — O — O
	Couverture assurance et juridique concernant la perte de données	S — S — S

S Souhaité R Recommandé O Obligatoire

Notez que différents moteurs de recherche[52,53,54] localisent et répertorient les objets connectés disponibles sur le web. Les objets mal protégés peuvent ainsi, être identifiés et utilisés par des personnes malveillantes.

52. censys.io
53. www.shodan.io
54. thingful.net

2.6.1 Sous-domaine : cybersécurité

La satisfaction des exigences de sécurité d'un produit passe en premier lieu par la mise en œuvre de « fonctions de sécurité » (chiffrement, authentification, vérification d'intégrité, etc.) qui sont détaillées dans la suite de ce document.

Elle passe également par le respect de principes de conception et par l'emploi de méthodes visant à limiter le risque d'introduction de failles au cours du cycle de développement et d'exploitation de l'Apps/OC.

Le cadre juridique pour le stockage des données ou les éléments de cybersécurité est sujette à évoluer régulièrement. Il convient de suivre ces évolutions pour rester conforme à la réglementation.

▶ Analyse de la menace

Une analyse de la menace a-t-elle été entreprise sur l'Apps/OC ? La protection des données est-elle prise en compte par construction et par défaut dans la conception de l'Apps/OC?

Justification : une analyse de la menace doit être menée sur l'Apps/OC préalablement à sa mise en œuvre. Cette analyse de la menace doit permettre d'identifier les biens sensibles manipulés par l'Apps/OC, et les fonctions de sécurité permettant de couvrir les menaces susceptibles de porter atteinte à la confidentialité, l'intégrité et la disponibilité des biens sensibles. Cette analyse de la menace doit également permettre d'ajuster le curseur de sécurité au « bon niveau ».

Les notions de *protection by design* et *by default* désignent des mesures de protection qui sont prises en compte dans les spécifications même d'un produit logiciel et visant à contrer une menace identifiée.

Exemple : les évaluateurs externes pourront demander si une analyse de la menace a été effectuée (voir par exemple la méthode EBIOS : Expression des besoins et identification des objectifs de sécurité[55]). Les évaluateurs externes pourront demander si la conception de l'Apps/OC intègre (*built-in*) les fonctions d'authentification/ de pseudonymisation, de transfert et de stockage sécurisé des données.

Pour en savoir plus :

Martinez-Perez (80) propose des recommandations sur la sécurité des données après une analyse de la littérature.

▶ Sécurité dans le développement

Les méthodes et outils utilisés dans les différentes étapes du cycle de développement de l'Apps/OC pour prévenir et détecter des failles de sécurité sont-ils documentés ?

Justification : Les développements sont susceptibles d'introduire des failles involontaires et doivent donc s'appuyer sur des outils et méthodes de conception sécurisés. La sécurité dans le développement logiciel participe aux dispositions prises pour améliorer la qualité globale d'un produit de santé mobile.

Exemple : les évaluateurs externes pourront demander les méthodes et outils de conception employés par les développeurs.

▶ Sécurité des fonctions cryptographiques

Les développeurs ont-ils privilégié l'utilisation de services et de primitives cryptographiques connus et éprouvés (par exemple, ceux proposés par le système d'exploitation de l'appareil mobile) plutôt que le redéveloppement de fonctions analogues ?

Justification : le domaine nécessite de s'appuyer sur des systèmes robustes et reconnus. Le développement de telles fonctionnalités est particulièrement difficile et requiert des compétences expertes.

Exemple : les évaluateurs externes pourront demander le type de service cryptographique.

▶ Méthodologie de protection/vérification du code

L'intégrité du code fait-elle l'objet de procédure de protection et de vérification régulière afin d'éviter que l'Apps/OC ne soit détournée de son utilisation normale et utilisée par exemple comme outil d'espionnage du porteur du terminal ou pour éviter une altération malveillante de l'intégrité du code et/ou des données?

Justification : les mesures de protection en intégrité sont aussi essentielles que celles relatives à la confidentialité des données.

Exemple : les évaluateurs externes pourront demander la méthodologie de protection.

▶ Utilisation sûre d'un code tiers externe

L'Apps/OC utilise-t-elle des codes tiers pour fonctionner ? Ces codes tiers ont-ils fait l'objet d'une évaluation visant à estimer leur sécurité et leur robustesse ?

Justification : le concepteur faisant appel à un code tiers externe assume la responsabilité de son utilisation dans son produit. À charge pour lui de maintenir un niveau de fiabilité, d'absence de collecte de données de marketing à l'insu de l'utilisateur et de sécurité à son utilisation.

Exemple : les évaluateurs externes pourront évaluer le processus de gestion des codes tiers externes. Les évaluateurs pourraient également évaluer la pertinence du modèle économique des Apps/OC tierces externes par rapport aux finalités du produit.

55. www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite

▶ Authentification des utilisateurs/des données

Les mécanismes d'authentification des utilisateurs vis-à-vis de l'Apps/OC ou des services distants sont-ils documentés ? Sont-ils compatibles des exigences d'anonymats des utilisateurs (par exemple, utilisation de pseudonymes de connexion non reliés à l'identité de l'utilisateur) ?

Justification : lorsque des échanges de données ont lieu entre l'Apps/OC et des services distants, les mécanismes d'authentification de l'utilisateur utilisés sont à préciser.

Exemple : les évaluateurs externes évaluent les risques d'authentification des utilisateurs en rapport aux documents fournis par le fabricant.

▶ Authentification de l'Apps/OC

L'Apps/OC authentifie-t-elle les services distants avec lesquels elle échange des données ? Cette authentification est-elle réciproque ? Comment cette authentification est-elle mise en œuvre ? L'impossibilité d'authentifier un serveur conduit-elle à une rupture de la communication et un avertissement de l'utilisateur ? Existe-t-il un mécanisme d'attestation distante ?

Justification : L'authentification de l'Apps/OC vis-à-vis de l'infrastructure devrait être réciproque. Cette fonction d'authentification réciproque doit permettre à l'Apps/OC de s'assurer de l'identité des services distants avec lesquels elle échange des données, d'une part, et à ces services de s'assurer que les données qu'ils reçoivent émanent effectivement d'une Apps/OC légitime.

NB : il convient de distinguer la fonction d'authentification de l'utilisateur vis-à-vis de l'Apps/OC et la fonction d'authentification de l'Apps/OC vis-à-vis de services distants.

Le cas échéant, les services distants peuvent compléter cette authentification des Apps/OC par une procédure dite d'attestation, qui permet d'interdire ou d'autoriser l'accès aux services en fonction de « l'état » des Apps/OC (l'état correspondant à une mesure de l'intégrité de l'Apps/OC).

Exemple : les évaluateurs externes évaluent les risques d'authentification d'un produit en rapport aux documents fournis par le fabricant.

▶ Intégrité et authenticité des données

Les mécanismes de vérification d'intégrité et d'authenticité des données échangées entre l'Apps/OC et les services distants sont-ils documentés ?

Justification : les mécanismes de vérification d'intégrité et d'authenticité des données doivent permettre aux composants de l'Apps/OC (locaux et distants) de détecter toute altération des données échangées et d'apporter une preuve sur leur origine.

Exemple : les évaluateurs externes évaluent les risques liés à l'intégrité des données d'un produit en rapport aux documents fournis par le fabricant.

▶ Transfert/échanges des données sécurisées

La confidentialité et l'intégrité des données transmises sur des serveurs distants est-elle assurée pendant le transit ? Cette protection s'effectue-t-elle à l'aide d'un protocole de chiffrement robuste utilisant des suites cryptographiques à l'état de l'art (par exemple, TLS) ? Ce protocole est-il utilisé indépendamment du réseau support (Wifi, connexion de données cellulaire, etc.) ?

Un chiffrement des données complémentaires du canal confidentiel établi avec les éventuels serveurs distants est-il assuré ?

Justification : la sécurisation des échanges de données est à assurer par le concepteur pour l'utilisateur. De même que le respect des obligations en matière de transfert de données en dehors de l'Union européenne.

Exemple : les évaluateurs externes pourront demander qui dispose des clés et comment celles-ci sont-elles protégées ? Existe-t-il un mécanisme de recouvrement ?

▶ Partage et accès aux données avec d'autres Apps/OC

L' Apps/OC accède-t-elle à des données ou des ressources gérées par des Apps/OC tierces ? L'utilisateur est-il en mesure de contrôler de façon discrétionnaire l'accès à ces données et ces ressources ? L' Apps/OC prévoit-elle de partager les données qu'elle gère avec d'autres Apps/OC? Quels dispositifs de sécurité sont mis en place pour empêcher les accès illégitimes à ces données (par exemple, via une App malveillante) ?

Justification : l'accès aux données et aux ressources externes par une application doit respecter le cadre juridique du partage d'information. L'application doit notamment minimiser autant que possible l'exposition des données qu'elle manipule.

Exemple : une zone de réglage permet à l'utilisateur de diffuser ses données d'activité physique à plusieurs Apps/OC sélectionnables.

▶ Stockage sécurisé des données sur le terminal

Un chiffrement des données stockées sur le terminal, complémentaire du dispositif de chiffrement global proposé par le système d'exploitation est-il assuré ?

Justification : la sécurité des données sur le terminal et sur le serveur est à garantir par le concepteur.

Exemple : les évaluateurs externes pourront demander qui dispose des clés et comment celles-ci sont-elles protégées ? Existe-t-il un mécanisme de recouvrement ?

▶ Stockage sécurisé des données sur le(s) serveur(s) distant(s)

Un chiffrement des données stockées sur le(s) serveur(s) distant(s), complémentaire du dispositif de chiffrement global proposé par le système d'exploitation est-il assuré ?

Justification : la sécurité des données sur le(s) serveur(s) distant(s) et sur le serveur est à garantir par le concepteur.

Exemple : les évaluateurs externes pourront demander qui dispose des clés et comment celles-ci sont-elles protégées ? Existe-t-il un mécanisme de recouvrement ?

NB : Se reporter également aux dispositions réglementaires concernant les hébergeurs agréés données de santé (HDS) lorsque l'Apps/OC le nécessite.

▶ Insécurité et failles des services distants

Les exigences de sécurité, d'intégrité et, le cas échéant, de disponibilité des services distants avec lesquels l'Apps/OC interagit sont-elles satisfaites ? Par quels moyens ?

Justification : Les incidents de sécurité affectant une infrastructure peuvent être potentiellement plus graves qu'un incident isolé sur le terminal d'un patient, notamment en termes de vol de données. La protection des services distants est donc aussi essentielle, sinon plus, que celle des Apps/OC.

Exemple : les évaluateurs externes pourront évaluer les risques de sécurité liés aux services distants.

Pour information concernant les risques liés aux services web distants : le site OWASP recense les 10 plus importantes vulnérabilités (81) :

- faille d'injection ;
- violation de gestion d'authentification et de session ;
- cross-site Scripting (XSS) ;
- références directes non sécurisées à un objet ;
- mauvaise configuration Sécurité (serveurs, etc.) ;
- exposition de données sensibles ;
- manque de contrôle d'accès au niveau fonctionnel ;
- falsification de requête inter-sites (CSRF) ;
- utilisation de composants avec des vulnérabilités connues ;
- redirections et renvois non validés.

NB : la notion de « services distants » ne se limite pas aux seuls services web, même si ces derniers sont prépondérants dans les domaines des Apps/OC. La liste précédente ne saurait être considérée comme étant exhaustive vis-à-vis des menaces liées aux services distants.

▶ Maintien en condition de sécurité

Le développeur/concepteur assure-t-il le suivi et la correction des failles identifiées sur l'Apps/OC?

Ce suivi s'applique-t-il également au logiciel tiers (par exemple, des bibliothèques) utilisées par l'Apps/OC ?

Justification : le maintien en conditions de sécurité de l'Apps/OC et des services distants est à garantir par le concepteur.

Exemple : les évaluateurs externes pourront évaluer les risques liés à la veille de la sécurité du produit.

▶ Sensibilisation de l'utilisateur, causes potentielles de brèche de confidentialité

L'Apps/OC permet-elle de sensibiliser l'utilisateur aux bonnes pratiques de sécurité ?

Justification : le but est de limiter la diffusion de données personnelles lors de la session de son/sa smartphone/tablette (par mauvaise réinitialisation) ou lors d'attaque tentant de se faire passer auprès de l'utilisateur pour l'infrastructure authentique (par exemple attaque par *phishing*).

Des recommandations « génériques » sur la sécurisation de son/sa smartphone/tablette devraient être accessibles (chiffrement du système activé, verrouillage activé, système à jour, etc.).

Exemple : L' App adresse une notification sur le fait d'utiliser un mécanisme de verrouillage de son smartphone pour protéger le contenu de ce dernier contre la perte ou le vol.

Lors de la cession de son/sa smartphone/tablette, l'utilisateur est sensibilisé aux bonnes pratiques pour effacer correctement les données personnelles présentes dans son ancien appareil.

Il est conseillé de lire les **21 recommandations** de l'**ANSSI** pour sécuriser son ordiphone[56], les bonnes pratiques de l'informatique[57], les recommandations de sécurité relatives aux mots de passe[58] ou les recommandations de sécurité relatives aux réseaux Wi-Fi[59].

▶ Évaluation de la sécurité

Une évaluation de la robustesse des fonctions de sécurité et un audit de l'Apps/OC a-t-il été réalisé pour évaluer si le niveau de sécurité est adapté au produit ?

Justification : l'analyse des risques peut être réalisée par différentes approches méthodologiques et permet de déterminer l'exigence de sécurité attendue.

Exemple : les évaluateurs externes pourront demander la façon dont cet audit a été réalisé et s'il était réalisé de manière indépendante.

▶ Signalement et transparence sur la violation de données ou en cas d'incident de sécurité

Un processus de signalement et de transparence est-il prévu en cas d'incident de sécurité ?

Justification : en cas de violation de données et/ou d'incident de sécurité, l'éditeur de l'App ou le concepteur de l'objet connecté s'engage à faire preuve de transparence vis-à-vis d'autorités compétentes (celles en charge de la santé, ANSSI CERT-FR, CNIL, autorités judiciaires le cas échéant) et vis-à-vis de ses utilisateurs.

Exemple : une App a adressé une notification pour mettre à jour l'App suite à une faille de sécurité identifiée.

Pour information

- Sécurité de l'information ISO 27001[60]
- *OWASP IoT Framework Assessment*[61]
- Recommandation ENISA[62] :
  - identifier et protéger les données sensibles sur l'appareil mobile (diminuer les risques de vol ou pertes de données) ;
  - gérer les informations de connexion du compte de manière sécurisée (le risque de *spyware*, surveillance, maliciel financier qui utilisent les mots de passe pour d'autres fonctions) ;
  - s'assurer que les données sensibles sont protégées durant leur transit (risque d'attaque en usurpation de réseau sur les nombreux réseaux utilisées par les smartphones) ;
  - implémenter l'authentification et l'autorisation d'utilisateur correctement ainsi que la gestion des sessions ;
  - maintenir la sécurité des APIs (services) du *back-office* (*backend*) et de la plateforme (serveur) (risques d'attaques sur les systèmes de *back-offices*) ;
  - sécuriser l'intégration de données avec les services de parties tiers et les Apps (risque de fuite de données) ;
  - prêter une attention particulière à la collecte et aux stockages des consentements pour la collecte et l'utilisation des données utilisateurs (risque de divulgation non-intentionnelle d'information personnelle) ;
  - implémenter des contrôles pour prévenir les accès non-autorisés aux ressources de paiements (portefeuille, SMS, appels téléphoniques, etc.) (risque d'abus d'usage/vulnérabilités des ressources de paiements) ;
  - assurer la sécurité dans la distribution/prestation des Apps mobiles (atténuation de tous les risques décrits dans le top 10) ;
  - vérifier avec précaution chaque interprétation de code d'exécution d'erreurs (*runtime interprétation of code errors*).
- TOP10 risques (ENISA)[63] :
  - fuite de données suite à la perte ou le vol de l'appareil (risque haut) ;
  - partage involontaire des données par l'utilisateur (risque haut) ;
  - attaques sur un téléphone mal réinitialisé (risque haut) ;
  - attaques par *phishing* (risque modéré) ;
  - attaques par *spyware* (risque modéré) ;
  - attaques par usurpation de réseau (risque modéré) ;
  - attaques par surveillance (logiciel tiers prenant le contrôle de la caméra, du partage d'écran, etc.) (risque modéré) ;
  - attaques par composition de numéros ou SMS surtaxés (*diallerware attacks*) (risque modéré) ;
  - attaques par maliciels (logiciels malveillants) financiers (interception de transaction bancaire, interposition, etc.) (risque modéré) ;
  - encombrement/congestion de réseau (risque faible).

56. www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-aux-ordiphones
57. www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique
58. www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf
59. www.ssi.gouv.fr/uploads/IMG/pdf/NP_WIFI_NoteTech.pdf
60. www.iso.org/iso/fr/home/standards/management-standards/iso27001.htm
61. www.owasp.org/index.php/IoT_Framework_Assessment
62. www.enisa.europa.eu/media/enisa-en-francais
63. www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks (accédé le 25/02/2016)

2.6.2 Sous-domaine : fiabilité

Concernant la fiabilité du contenu produit, généré ou interprété, il est nécessaire de se reporter au domaine **contenu**.

▶ Fiabilité et maintenabilité hardware (capteurs) et software

Les taux de pannes, d'erreur de mesure, les risques de tous types au niveau hardware sont-ils évalués et documentés ? Les bugs récurrents et de sureté de fonctionnement du software sont-ils documentés ? Les conditions d'utilisations ou les avertissements en fonction de l'utilisation sont-ils consultables par tous ?

Justification : le suivi de la fiabilité du produit est une étape importante à prendre en compte lors de la conception. Les modalités de suivi sont à tracer.

Exemple : les évaluateurs externes pourront demander la façon dont ce suivi est réalisé pour en évaluer la crédibilité et l'efficacité.

▶ Disponibilité de l'infrastructure

Les mesures visant à assurer la disponibilité de l'infrastructure support de l'Apps/OC sont-elles documentées ?

Justification : la fonction support de l'Apps/OC et sa disponibilité sont des éléments de qualité et de crédibilité pour son maintien à jour.

Exemple : les évaluateurs externes pourront demander la façon dont la fonction support est organisée.

▶ Assistance technique, « *hotline* »

Une « *hotline* » permettant de solliciter une demande d'assistance technique (bug informatique, configuration du poste de travail, système d'exploitation, etc.) est-elle mise à la disposition des utilisateurs et des personnes ressources ? Les problèmes fréquemment rencontrés sont-ils documentés et peuvent-ils être consultés (FAQ, etc.) ?

Justification : une assistance technique sous un format adapté est à disposition des utilisateurs pour les aider à résoudre les problèmes rencontrés.

Exemple : les évaluateurs externes pourront demander la façon dont la hotline fonctionne ou la foire aux questions a été conçue et les problèmes usuels rencontrés. Un processus de « Debug » utilisé par les développeurs peut être documenté.

▶ Qualité des matériaux, innocuité des dispositifs

Le processus d'identification des risques liés aux matériaux utilisés (allergie, risques physiques, etc.) et de l'innocuité des dispositifs (exemple : risque de brûlure, etc.) est-il documenté et évalué par des professionnels de santé indépendants et qualifiés ?

Justification : les objets connectés ne doivent pas nuire physiquement à l'utilisateur.

Exemple : les bracelets de maintien d'un objet connecté sont hypoallergéniques.

▶ Optimisation des fichiers média

Le choix des procédés d'optimisation des fichiers média (images et vidéos) est-il documenté et justifié au regard de la destination d'usage du produit ?

Justification : il s'agit de s'assurer que les risques liés à la perte de données par compression, aux délais de connexion, d'affichage, de transmission, etc. sont acceptables. L'optimisation de la définition et du poids des fichiers médias sans augmenter les risques de perte de qualité pour l'utilisateur est réalisé et testé.

Exemple : le temps d'affichage d'une vidéo d'interview est trop long pour une App d'information grand public sur la santé. Le concepteur du produit met en place une procédure d'optimisation des fichiers.

▶ Contre-indications, risques potentiels, limitations d'usage

Les contre-indications, les risques potentiels et les limitations d'usage sont-ils évalués et documentés par un groupe compétent. Ces informations sont-elles accessibles et consultables par les utilisateurs ?

Justification : l'Apps/OC peut présenter des limites d'utilisation ou de fiabilité. L'information auprès de l'utilisateur doit être transparente.

Exemple : un capteur optique d'un cardiofréquencemètre perd sa fiabilité selon la pigmentation de la peau (tatouage, couleur de peau, etc.). L'utilisateur est informé de cette limitation d'usage.

▶ Niveau de disponibilité

Le niveau de disponibilité est-il documenté et adapté à la destination d'usage du produit (par exemple de 7 jours sur 7 et 24 heures sur 24 à des délais moins étendus comme de 9h à 18h les jours ouvrés) ?

Justification : la destination d'usage de certains produits nécessite une connexion permanente avec le réseau Web distant.

Exemple : un moniteur d'activité d'un sportif en cours de reprise du sport après blessure permet de collecter les doses d'efforts réalisés et les phases de repos. Cela nécessite de stocker et/ou de pouvoir transmettre les données collectées en continu.

▶ Maintenance préventive

Des systèmes de détection de panne et d'alertes sont-ils prévus pour prévenir les pannes susceptibles d'entraîner une gêne ou un dommage à l'utilisateur (exemple : alerte batterie faible, etc.) ?

Justification : l'utilisateur doit être informé de l'état de fonctionnement ou de notification de mise à jour ou de renouvellement de batterie lors de collecte de données en continue ou d'utilisation spécifique.

Exemple : un objet connecté adresse un signal sonore ou une vibration pour spécifier que sa batterie est faible.

Pour en savoir plus :

ISO/IEC/IEEE 15288:2015 : Ingénierie des systèmes et du logiciel - Processus du cycle de vie du système.

▶ Fonctionnement vis-à-vis des autres Apps/OC

La compatibilité et les conflits inter-Apps/OC sont-ils évalués et surveillés ?

Justification : le suivi de la compatibilité ou de conflit avec d'autres Apps/OC est mis en place pour collecter les problèmes rencontrés par les utilisateurs et les informer des incompatibilités.

Exemple : un utilisateur rencontre un problème avec une Apps/OC qui entre en conflit avec la caméra de son smartphone. Une alerte d'incompatibilité est reçue par le concepteur de l'Apps/OC. Une information est adressée aux utilisateurs par notification en attendant qu'une correction éventuelle soit apportée.

2.6.3 Sous-domaine : confidentialité

La loi informatique et libertés[64] définit les principes à respecter lors de la collecte, du traitement et de la conservation de données personnelles, notamment pour ce qui concerne la confidentialité.

La CNIL met à disposition des catalogues de bonnes pratiques destinées à traiter les risques que les traitements de données à caractère personnel (DCP) peuvent faire peser sur les libertés et la vie privée des personnes concernées[65].

Le règlement général sur la protection des données (*General Data Protection Regulation* – GDPR) a été adopté en avril 2016[66] et doit être mis en œuvre au niveau national pour le 6 mai 2018[67]. Il convient de suivre ces évolutions.

Sunyaev (82) a réalisé en 2013 une étude montrant que seulement 30,5 % des Apps de santé mobile les plus utilisées possédaient une politique de confidentialité.

L' Association française des correspondants à la protection des données à caractère personnel (AFCDP) a rédigé une synthèse de travaux sur *Quantified Self* connecté et informatique & libertés[68].

▶ Destinataire des données collectées, confidentialité des données personnelles, et consentement pour la transmission à des tiers

La transmission des données collectées (respectant les conditions légales et réglementaires) à des tiers est-elle documentée de manière explicite (destinataires, etc.) ?

Ces informations peuvent-elles être consultées en dehors des conditions générales d'utilisation ?

L'utilisateur peut-il modifier son consentement ?

Justification : toute transmission à des tiers requiert le consentement préalable de l'utilisateur conformément à la loi.

Exemple : un élément de réglage est accessible pour modifier le consentement de transmission à des tiers.

▶ Pseudonymisation des données

Le processus de pseudonymisation est-il documenté et consultable ?

Justification : Le processus de pseudonymisation des données personnelles est un enjeu important pour le domaine de la santé mobile.

Exemple : les évaluateurs externes pourront demander la façon dont la pseudonymisation est réalisée. Les évaluateurs externes pourront demander comment les moyens indirects de lever l'anonymat sont contrôlés. Par exemple, si l'Apps/OC à recours à des identifications uniques de l'appareil sur lequel elle est installée, et si ces identifiants uniques sont liés d'une quelconque façon à l'identité de l'utilisateur (numéro de téléphone ?, etc.).

▶ Anonymisation des données

Les données individuelles, dont notamment les données de santé, transmises à des fins de statistiques sont-elles anonymisées ?

Le processus d'anonymisation est-il documenté et consultable ?

64. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
65. www.cnil.fr/fr/PIA-privacy-impact-assessment
66. eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=EN
67. ec.europa.eu/justice/data-protection
68. esante.gouv.fr/sites/default/files/asset/document/201502_synthese_qs_v10.3_finale.pdf

Justification : l'anonymisation des données est obligatoire avant toute transmission à des tiers en vue d'un traitement statistique.

Exemple : les évaluateurs externes pourront demander la façon dont l'anonymisation est réalisée.

Pour en savoir plus :

Notion de *big data* et de gouvernance abordé dans le livre vert de la Commission européenne (74).

Bonnes pratiques sur les données personnelles pour le Conseil des académies canadiennes (83).

Description du contexte et recommandations pour l'AFNOR (84).

Documentation CNIL (34).

▶ Délais de suppression et temps de mise en œuvre

La durée et les délais de conservation ou de suppression des données sont-ils documentés et consultables par les utilisateurs ?

Justification : la conservation de données de santé sur les serveurs ou tout autre support est à communiquer à l'utilisateur. La durée de conservation nécessaire à l'accomplissement des finalités est à préciser et à ne pas dépasser, à défaut d'une autre obligation légale imposant une conservation plus longue.

Exemple : la page d'information du concepteur décrit la politique de conservation des données. Les évaluateurs externes pourront demander la documentation sur ce sujet.

▶ Couverture assurance et juridique concernant la perte de données

Une couverture assurance et juridique au bénéfice des utilisateurs est-elle prévue pour faire face à une perte éventuelle de données collectées ? Une attestation est-elle consultable ?

Justification : la couverture juridique ou d'assurance permet de protéger la responsabilité du concepteur.

Exemple : les évaluateurs externes pourront demander la documentation sur ce sujet.

2.7 Domaine : utilisation/usage

Le domaine utilisation/usage (tableau 7) porte principalement sur la manière dont l'utilisateur va pouvoir utiliser l'Apps/OC. Ce domaine fait appel à des notions d'évaluation qui peuvent être subjectives ou difficilement évaluables. C'est pourtant un domaine qui contribue à l'utilisation régulière et efficace du produit.

Tableau 7. Liste des critères se rapportant à l'utilisation du produit

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ		
		Faible	Modérée	Élevée
Utilisation/design	Ergonomie	R	R	R
	Processus d'installation et configuration	S	R	R
	Aide à l'utilisation/instructions	R	R	R
	Convivialité et intuitivité	R	R	R
	Lisibilité texte et image	R	R	R
	Niveau d'utilisation	S	R	R
	Accessibilité du contenu pour des personnes en situation de handicap	R	R	R

S Souhaité R Recommandé

SOUS-DOMAINES	INTITULÉS	NIVEAU D'EXIGENCE POUR LES APPS/OC DE CRITICITÉ
		Faible — Modérée — Élevée
Utilisation/design	Facilité d'emploi	R — R — R
	Prévention des erreurs	S — R — R
	Cas d'usages, scénarios métier	S — R — R
	Flexibilité/customisation	S — R — R
	Délais de réponse, temps d'affichage	R — R — R
Acceptabilité	Évaluation par les professionnels de santé externe	R — R — R
	Évaluation par la population cible principale	R — R — R
	Enquête de satisfaction	R — R — R
	Utilisabilité (adhésion des utilisateurs dans le temps, régularité d'utilisation)	S — R — R
	Niveau d'implication utilisateur (acteur de sa prise en charge)	R — R — R
	Posologie et utilisation (mesure de l'observance)	S — R — R
Intégration/import	Infrastructure ouverte	S — S — S
	Capacité de recherche	S — S — R
	Capacité de retrouver un patient	S — S — R
	Possibilité d'imprimer des résumés (sélection)	R — R — R
	Éléments sociaux (vie privée et réseaux sociaux)	S — S — S

S Souhaité R Recommandé

2.7.1 Sous-domaine : utilisation/design

▶ Ergonomie

Le processus de conception de l'interface s'appuie-t-il sur une démarche ergonomique (normes & standard existant ISO, AFNOR, etc.) ? Ce processus est-il documenté ?

Justification : l'ergonomie d'utilisation est un facteur d'implémentation pour l'utilisateur.

Exemple : les évaluateurs externes pourront demander la documentation sur ce sujet.

Pour en savoir plus :

Charte Internet de l'État[69] : la charte ergonomique des sites Internet publics a pour objet de définir un ensemble de règles ergonomiques communes aux interfaces des sites Internet publics. Elle s'inscrit dans le respect des standards du *Word Wide Web Consortium* (W3C) et des principes des référentiels généraux d'interopérabilité (RGI), d'accessibilité (RGAA) et de sécurité (RGS).

Cruz Zapata (85) propose des recommandations pour les développeurs concernant l'interface.

▶ Procédure d'installation et configuration

La procédure d'installation et de configuration a-t-elle été testée sur les principaux OS, navigateurs Internet et plates-formes proposés dans l'environnement d'utilisation ? Cette procédure est-elle documentée ?

Justification : les phases de tests sont à assurer par le concepteur pour garantir une expérience utilisateur de qualité.

Exemple : les évaluateurs externes pourront demander la documentation sur ce sujet.

▶ Aide à l'utilisation/instructions

Un système d'aide à l'utilisation du produit est-il mis à la disposition des utilisateurs (aide contextuelle, aide en ligne, manuel utilisateur, tutoriel, didacticiel, *e-learning*, etc.) ? Ce système favorise-t-il les capacités d'apprentissage de l'utilisateur (apprenabilité) ?

Justification : le niveau de soutien didactique proposé par le concepteur à l'utilisateur permet d'optimiser l'utilisation du produit.

Exemple : lors du lancement de l'Apps/OC, des zones d'aide sont proposées pour aider l'utilisateur lors de sa première utilisation.

▶ Convivialité et intuitivité

La convivialité et l'intuitivité de l'interface et de la navigation ont-elles été testées auprès de différents profils d'utilisateurs ? Le plan et compte-rendu des tests sont-ils documentés ?

Justification : les profils d'utilisateurs différents dans leur manière d'apprendre ou selon des critères spécifiques liés aux utilisateurs cibles sont sollicités par le concepteur pour adapter l'Apps/OC.

Exemple : les évaluateurs externes pourront demander la documentation sur ce sujet.

▶ Lisibilité texte et image

La lisibilité des différents médias utilisés (texte, image, vidéos) a-t-elle été testée ? Le plan et compte-rendu des tests sont-ils documentés ? L'interface ou l'OS permet-il le changement de la lisibilité de l'Apps/OC (modification de la taille/de la police de caractères, etc.) ?

Justification : la lisibilité par des utilisateurs ayant des capacités différentes est un facteur d'accessibilité du produit.

Exemple : l'utilisateur a accès à une zone de réglage pour adapter la taille de la police de caractères et étendre en plein écran la vidéo.

▶ Niveau d'utilisation

Les différents profils utilisateurs sont-ils identifiés en fonction de la destination d'usage du produit et des difficultés possibles pour la lisibilité de l'interface ou de niveau d'utilisations ? Le niveau prérequis pour un utilisateur novice, confirmé ou expert est-il accessible à tous ?

Justification : différents types d'utilisateurs peuvent naviguer différemment dans l'interface du produit.

Exemple : des utilisateurs daltoniens et des personnes âgées ont été identifiés afin de travailler sur l'utilisation des couleurs et des contrastes de l'interface d'une App d'information sur la réhabilitation respiratoire.

Pour en savoir plus :

Arnhold (86) a réalisé une évaluation de l'interface des Apps pour personnes âgées atteintes de diabètes. Watkins (87) a réalisé une revue systématique sur les personnes âgées et le niveau de lecture/compréhension en santé (*health literacy*).

Monkman (88) évalue le risque en fonction de l'interface et du niveau de lecture/compréhension en santé (*health literacy*) de l'utilisateur.

69. references.modernisation.gouv.fr/sites/default/files/Charte_ergonomique_v2.0_2.pdf

▶ Accessibilité du contenu pour des personnes en situation de handicap

Les recommandations d'accessibilité concernant les personnes en situation de handicap sont-elles appliquées ?

Justification : l'accessibilité du produit est à garantir par le concepteur.

Exemple : un test utilisateur spécifique est mis en place par le concepteur pour les utilisateurs en situation de handicap.

Pour en savoir plus :

Charte Internet de l'État[70] : La charte ergonomique des sites Internet publics a pour objet de définir un ensemble de règles ergonomiques communes aux interfaces des sites Internet publics. Elle s'inscrit dans le respect des standards du *Word Wide Web Consortium* (W3C) et des principes des référentiels généraux d'interopérabilité (RGI), d'accessibilité (RGAA) et de sécurité (RGS).

▶ Facilité d'emploi

Un processus de simplification d'utilisation est-il mis en place ? Ce processus est-il documenté ?

Justification : les retours utilisateurs doivent permettre aux concepteurs de faire évoluer vers la simplification leurs produits.

Exemple : des éléments de menu ont été supprimés suite à une mauvaise ou non-utilisation de ces éléments dans une App de bases de données de médicaments à destination des médecins. Le délai d'accès à l'information recherchée a été diminué.

▶ Prévention des erreurs

Un système d'alerte adapté lors de décisions critiques de l'utilisateur est-il mis en place pour prévenir les mésusages éventuels ?

Justification : certaines interactions peuvent entrainer des erreurs de la part de l'utilisateur. Des éléments d'alertes sont à garantir par le concepteur.

Exemple : une App de calcul d'indice de masse corporelle adresse une alerte concernant l'utilisation d'unité de mesure de la taille ou met en place un menu déroulant pour limiter les erreurs de saisie.

▶ Cas d'usages, scénarios métier

Les cas d'usages (ou scénarios métier) couvrent-ils les fonctions principales du produit et permettent-ils de mieux appréhender les différentes utilisations de l'Apps/OC (les scénarios) ? Ces cas d'usage sont-ils documentés et testés ?

Justification : la navigation et le parcours des utilisateurs dans une App peuvent être très différents. De même, que pour le paramétrage d'un objet connecté. L'identification de différents scénarios permet de prévenir les éventuels mésusages ou d'améliorer la navigation dans l'App.

Exemple : une App permettant de gérer la prise de médicaments permet de paramétrer dans l'agenda des prises médicamenteuses à heures fixes de manière itératives durant une période définie. Certains utilisateurs ne connaissant pas cette fonction paramètrent les différents jours un par un une semaine à l'avance. L'identification de ce scénario doit permettre de mettre en place une assistance spécifique.

Pour en savoir plus :

Caburnay (89) effectue une revue du design des Apps portant sur le diabète.

Collins (90) a développé des outils pour évaluer la qualité des questionnaires de santé pour les patients au travers des Apps (*health literacy*[71]).

Différents outils sont proposés pour évaluer la compréhension des patients.

▶ Flexibilité/customisation

L'adaptation en fonction du niveau, des besoins ou des exigences des utilisateurs est-elle envisagée ?

Justification : la santé mobile a permis de développer des Apps/OC réservés à des « niches » de professionnels ou de patients. Il est possible de décliner des versions spécifiques correspondantes aux besoins de l'utilisateur.

Exemples : une plateforme d'échanges de documents entre patients et professionnels permet des niveaux d'accès différents et des niveaux de visualisations des informations différents en fonction des droits des utilisateurs.

Un panneau de réglage spécifique permet d'activer un menu simplifié ou avancé en fonction des besoins de l'utilisateur.

▶ Délais de réponse, temps d'affichage

Les délais de réponse et les temps d'affichages sont-ils testés et adaptés en fonction de la destination d'usage du produit ? Le plan incluant la définition de l'environnement de test et le compte-rendu des tests sont-ils documentés ?

Justification : la fluidité de la navigation est un facteur de fidélité des utilisateurs.

Exemple : les évaluateurs externes pourront tester les temps de réponse lors de banc d'essais.

70. references.modernisation.gouv.fr/sites/default/files/Charte_ergonomique_v2.0_2.pdf
71. health.gov/healthliteracyonline/2010/Web_Guide_Health_Lit_Online.pdf

Pour en savoir plus :

Georgsson (91) a effectué une évaluation des tâches (suivant norme ISO 9241-11). Il montre que les tâches les plus complexes donnent plus d'erreurs. Cinq à 8 utilisateurs trouvent 80-85 % des problèmes d'interface. Les niveaux de réalisation des taches sont gradés en 3 niveaux : sans aide, avec une aide, avec une aide et échec.

2.7.2 Sous-domaine : acceptabilité

▶ Évaluation par les professionnels de santé externe

L'évaluation de l'Apps/OC est-elle réalisée par des professionnels de santé ou des organisations de professionnels de santé indépendantes ?

Justification : dans le cadre de la gestion de qualité, une évaluation externe est un élément à mettre en place.

Exemples : un groupe de professionnels de santé met en place une Apps/OC de recueil de données de patients pour effectuer des statistiques de prise en charge et de suivi de patients. Ils publient un article sur le sujet dans une revue relue par ses pairs.

Une association professionnelle effectue une évaluation d'une dizaine d'Apps/OC concernant un champ spécifique de son secteur d'activité. Elle diffuse les résultats à ses membres et les propriétaires des Apps/OC citent cette évaluation dans leur présentation.

▶ Évaluation par la population cible principale

L'évaluation de l'Apps/OC est-elle réalisée par les utilisateurs ou des groupes d'utilisateurs indépendants ?

Justification : le test en condition réelle auprès des utilisateurs cibles permet d'obtenir des retours sur la qualité du produit.

Exemple : une Apps/OC permettant de mesurer un/des angle(s) sur des captures vidéos ne mémorisent pas les mesures effectuées sur le sujet. Ce retour utilisateur permet une adaptation de la part du concepteur.

▶ Enquête de satisfaction

La satisfaction des utilisateurs est-elle évaluée ? Les résultats de cette évaluation sont-ils documentés et consultables pour tous ?

Justification : la transparence du retour utilisateurs est un niveau d'information. Il peut être manipulé par des « faux » utilisateurs financés pour des donner des avis positifs.

Exemple : les évaluateurs externes pourront analyser les données et évaluer leur niveau de fiabilité.

▶ Utilisabilité (adhésion des utilisateurs dans le temps, régularité d'utilisation)

L'évaluation de l'utilisation régulière de l'Apps/OC est-elle réalisée si cet objectif fait partie de ceux de l'Apps/OC?

Justification : des Apps/OC ont actuellement une durée de vie d'utilisation limitée. Les concepteurs devraient suivre les statistiques d'utilisation/fréquentation.

Exemple : le concepteur diffuse son taux d'utilisation pour mettre en avant la popularité et la fidélité de ses utilisateurs.

▶ Niveau d'implication utilisateur (acteur de sa prise en charge)

Pour une Apps/OC dont l'objectif vise au fait que l'utilisateur devient acteur de sa propre prise en charge, le niveau d'implication de l'utilisateur est-il stimulé et évalué ? Ce processus est-il transparent et documenté ?

Justification : la mesure de soi (*quantified self*) est un objectif spécifique en plein essor dans le milieu de la santé mobile. Le concepteur doit mettre en avant les moyens mis en œuvre pour per-mettre cette autonomie de prise de mesure.

Exemple : un pèse-personne connecté encourage le patient à suivre différents paramètres mesurés sur plusieurs semaines pour adapter son comportement et son hygiène de vie progressivement.

▶ Posologie et utilisation (mesure de l'observance)

L'observance du traitement permise par l'Apps/OC est-elle réalisée si cet objectif fait partie de ceux de l'Apps/OC? Ce processus est-il documenté ?

Justification : les utilisateurs reçoivent différents types de rappels pour améliorer leur observance thérapeutique.

Exemple : les alertes SMS, et les notifications adressées sur le téléphone portable permettent au patient de mieux suivre son traitement.

Pour en savoir plus :

Hall (92) a montré l'impact fort des SMS dans différents secteurs de la santé.

Hamine (47) a montré l'impact réel de la santé mobile sur l'observance pour les malades chroniques.

2.7.3 Sous-domaine : intégration/import

▶ Infrastructure ouverte

L'utilisateur peut-il entrer « manuellement » des données dans l'Apps/OC?

Justification : certains praticiens souhaitent ajouter des commentaires à certaines données recueillies sur le patient ou certaines situations (perte de connexion, déconnexion Internet chez l'utilisateur durant plusieurs jours) nécessitent d'ajouter des données dans l'Apps/OC.

Exemple : le capteur d'activité de l'utilisateur est tombé en panne durant plusieurs jours. L'utilisateur copie les données enregistrées pour des jours similaires en termes d'activité sur les jours manquants de son agenda de suivi.

▶ Capacité de recherche

L'utilisateur a-t-il à sa disposition un moteur de recherche d'informations ou un système de recherche de données lorsque cela est pertinent ?

Justification : les l'Apps/OC portant sur des bases de données d'informations diverses, ou incluant des données collectées devraient permettre d'effectuer des recherches via un moteur de recherche.

Exemple : une Apps/OC recensant les recommandations de bonnes pratiques permet une recherche spécifique.

▶ Capacité de retrouver un patient

Si le patient y consent, le professionnel de santé a-t-il la capacité de retrouver un/des patient(s) ?

Justification : pour certains professionnels stockant de l'information médicale au travers d'App de gestion de cabinet ou autre, un moteur de recherche permet d'accéder plus rapidement au document demandé.

Exemple : les résultats d'examen biologiques d'un patient sont archivés dans une base de données et peuvent être recherchés via une interrogation spécifique.

▶ Possibilité d'imprimer des résumés (sélection)

Une extraction de données partielles permet-elle d'imprimer des résumés ?

Justification : l'extraction de données spécifiques permet à l'utilisateur de conserver auprès de lui un détail concernant un résumé d'article, un résultat d'une mesure effectuée, un état de forme ressenti ou une compilation de données.

Exemple : un praticien collecte des articles spécifiques concernant des méthodes d'évaluation spécifiques au travers d'une App d'informations médicales.

▶ Éléments sociaux (vie privée et réseaux sociaux)

L'envoi de données vers les réseaux sociaux s'appuie-t-il sur un intérêt démontré ? Le transfert de données vers les réseaux sociaux est-t-il conforme à la loi et la réglementation (consentement exprès de l'utilisateur, respect de la vie privée, etc.) ?

Justification : les réseaux sociaux sont utilisés, entre autre, pour renforcer le soutien ou développer des facteurs d'émulation pour suivre les prescriptions d'un praticien ou son comportement. L'implémentation de ce dispositif nécessite un intérêt démontré s'il est proposé.

Exemple : une App de type « agenda de l'humeur » utilisée par des patients dépressifs permet de partager son humeur sur les réseaux sociaux avec un groupe d'amis. Les références cliniques de l'intérêt de cette diffusion sont consultables par tous.

Cette fonctionnalité doit suivre la loi et la réglementation ainsi que l'avis médical éventuel sur l'intérêt de ce partage.

3. Mise en œuvre du référentiel de bonnes pratiques

Différentes théories de l'évaluation et différentes approches en fonction de l'objectif recherché sont publiées sur le sujet. Khoja (93) a décrit les différentes phases du cycle de vie d'une App et les processus d'évaluation qui pourrait en découler pour chacune des phases.

Pour les développeurs, il existe également des travaux de normalisations (par exemple : ISO/IEC 90003, Ingénierie du logiciel - Lignes directrices pour l'App de l'ISO 9001:2008 aux logiciels informatiques ou IEC/FDIS 82304-1, logiciels de santé-Partie 1 : exigences générales pour la sécurité des produits) qui fournissent des standards sur différents champs concernés par le sujet de la santé mobile. Ces éléments permettent aux développeurs de produits d'aller rechercher des certifications.

Par ailleurs, il existe des documents de recommandations comme le PAS 277:2015 (*Health and wellness apps – Quality criteria across the life cycle – Code of practice*) élaboré par le *British Standards Institute* (94) qui se propose de donner des recommandations pour les développeurs.

Lobelo (95) propose également un cadre d'organisation dans ce qu'il qualifie de *Wild Wild West* pour ce qui concerne le domaine de l'activité physique et de la santé et le bien-être mobile.

Les plateformes de magasins en ligne fournissent aussi des recommandations[72] pour aider les développeurs à bien figurer dans leur store[73].

3.1 Les déclinaisons possibles du référentiel de bonnes pratiques de la HAS

Le référentiel de bonnes pratiques de la HAS peut être utilisé et adapté par différents acteurs du secteur :

- les développeurs pourront trouver des éléments à intégrer dans leur(s) projet(s) ;
- les évaluateurs externes pourront cibler la documentation à demander ;
- les organisations professionnelles pourront construire des tableaux de synthèses (*benchmarking*) ou des illustrations synthétiques (graphes en radar) sur des Apps/OC spécifiques en reprenant les critères du référentiel.

Chacun des 5 domaines du référentiel peut ainsi être évalué spécifiquement ou des synthèses peuvent être constituées pour comparer les évaluations de différentes Apps/OC d'un même secteur (objectif principal et utilisateur principal communs).

Les critères « obligatoires » permettent d'effectuer une première analyse de l'App/OC. S'ils ne sont pas présents, l'évaluation n'est pas poursuivie.

Pour certains critères en relation avec des Apps/OC spécifiques (notamment les flux de données), des méthodes d'analyse de risque ou d'analyse de menace sont à mettre en place comme proposé pour certains critères.

Concernant l'interface d'utilisation sous l'angle de l'utilisateur (interface homme-machine-IHM), cette partie peut faire l'objet d'évaluation complémentaire avec des échelles standards comme les 10 questions du *System Usability Scale*[74] (SUS) de Brooke (96) ou les 21 questions de l'approche par *Quality of experience* (QoE) de Martinez-Perez (97).

Le référentiel de bonnes pratiques de la HAS peut servir de référence pour construire différents livrables :

- registre ;
- label ;
- score ;
- évaluation par les pairs ;
- banc d'essai ;
- benchmark.

Ou différentes approches en fonction des objectifs visés par l'évaluateur :

- approche par objectifs/domaines (qualité de l'information, processus de conception, sécurité, etc.) ;
- approche par segmentation (pathologies spécifiques, etc.) ;
- approche par cible (patients, étudiants, professionnels de santé, concepteurs/usage spécifique) ;
- etc.

Un suivi de l'utilisation du référentiel permettrait d'identifier les usages réalisés.

72. developer.apple.com/app-store/review/guidelines/#physical-harm
73. www.fiercehealthcare.com/mobile/apple-debuts-app-review-guidelines-quest-to-boost-quality
74. www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

Annexe 1. Le *Mobile App Rating Scale* (MARS) (98, 99)

Disponible sur le site : mhealth.jmir.org/article/downloadSuppFile/3422/14733

À partir de 349 items regroupés suite à une revue de littérature, le score a été réduit à 23 items et côté de 1 à 5 dans 4 domaines objectifs et 1 domaine subjectif.

Concordance inter-examinateur : CCI=0.79 et Consistance interne : alpha=0.90

Section A – Engageant (amusant, intéressant, personnalisable, interactif (envoie des alertes, messages, reminder, *feedback*, permet le partage), bien ciblé sur l'audience.

Score sur 25 points

1. **Divertissant :** est-ce que l'application est divertissante à utiliser ? Est-ce qu'elle utilise des stratégies pour améliorer l'implication au travers l'aspect divertissant (par exemple : un côté ludique) (5 niveaux de réponses côté de 1 à 5 avec descriptif).
2. **Intérêt :** est-ce que l'application est intéressante à utiliser ? Est-ce qu'elle use de différentes stratégies pour améliorer l'implication au travers d'une présentation intéressante du contenu ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
3. **Personnalisable :** est-ce qu'elle fournit/conserve tous les réglages nécessaires/les réglages de préférences des applis (exemple : son, contenu, notifications, etc.) ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
4. **Interactivité :** est-ce qu'elle permet à l'utilisateur d'entrer des données, fournir un feedback, contenu rapide (*reminders*, options de partage, notifications, etc.) ? Note : ces fonctions ont besoin d'être personnalisables et ne pas s'écraser les unes sur les autres. (5 niveaux de réponses côté de 1 à 5 avec descriptif).
5. **Groupe cible :** est-ce que le contenu de l'application (information visuelle, langage, design) est approprié pour l'audience ciblée ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).

Section B – Fonctionnalité - fonctionnement de l'application, facile à apprendre, navigation, flux/parcours logique, design gestuel de l'application

Score sur 20 points

6. **Performance :** comment fonctionne avec précision/vitesse les éléments de l'application (fonctions) ainsi que ces composantes (boutons/menus) ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
7. **Facilité d'utilisation :** avec quelle facilité est-il possible d'apprendre à utiliser l'application ; quel est le niveau de clarté des icônes/étiquettes de menu et les instructions ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
8. **Navigation :** est-ce que le déplacement entre les écrans est logique/précis/non-interrompu ; est-ce que tous les liens vers les écrans sont présents ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
9. **Design gestuel :** est-ce que les interactions (toucher/glisser/pincer/défiler) sont conformes et intuitifs avec l'ensemble des composantes/écrans ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).

Section C – Esthétique - design des graphismes, attractivité visuelle, cohérence des couleurs, et style uniforme

Score sur 15 points

10. **Mise en page :** est-ce que la disposition et la taille des boutons/icônes/menus/contenu de l'écran est appropriée ou peut-on zoomer si nécessaire ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
11. **Graphisme :** à quel niveau est la qualité de la résolution des graphismes utilisés pour les boutons/icones/menus/contenu ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
12. **Attractivité visuelle :** à quel niveau l'application est-elle visuellement belle ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).

Section D – Information - contenu de haute qualité d'informations (exemple : texte, feedback, mesures, références) provenant de source fiable. Sélectionner non adapté si la composante de l'application ne convient pas.

Score sur 35 points

13. **Précision de la description de l'application (sur le store) :** est-ce que le contenu de l'application est décrit ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
14. **Buts :** est-ce que l'application a des buts spécifiques, mesurables et atteignables ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).

15. **Qualité de l'information :** est-ce que l'application présente un contenu correct, bien écrit, et adapté à l'objectif/au sujet visé par l'application ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
16. **Quantité d'information :** est-ce que l'étendu du domaine couvert est compris dans le cadre de l'application ; et compréhensible en restant concis ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
17. **Information visuelle :** est-ce que l'explication visuelle des concepts – au travers de schéma/graphique/image/vidéos, etc.- est clair, logique, et correct ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
18. **Crédibilité :** est-ce que l'application provient d'une source légitime (spécifiée dans la description sur le store ou dans l'application elle-même) ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).
19. **Fondée sur des preuves :** est-ce que l'application a été testée/évaluée par un essai contrôlé ; a dû être vérifiée par une étude fondée sur les preuves ? (5 niveaux de réponses côté de 1 à 5 avec descriptif).

Score totale de qualité : A + B + C + D

PARTIE SUBJECTIVE

Section E

Score sur 20 points

20. **Est-ce que vous recommanderiez cette application à des personnes qui pourraient en tirer un bénéfice ?** (5 niveaux de réponses côté de 1 à 5 avec descriptif).
21. **Combien de fois pensez-vous que vous pourriez utiliser cette application dans les 12 prochains mois si elle vous était pertinente ?** (5 niveaux de réponses côté de 1 à 5 avec descriptif).
22. **Paieriez-vous pour cette application ?** (5 niveaux de réponses côté de 1 à 5 avec descriptif).
23. **Quel est de manière globale la note que vous attribueriez à cette application ?** (5 niveaux de réponses côté de 1 à 5 avec descriptif).

Annexe 2. L'évaluation par les pairs du *Journal of Medical Internet Research* – JMIR –

Formulaire de Health Apps, 2014
Disponible sur le site : tinyurl.com/appsform

Domaines	Paramètres/critères (compilés par rapport au formulaire du site)
À propos du répondant	Nom, e-mail, fonction, autres personnes répondants aux questionnaires
À propos de l'Appli	Nom, version, MàJ, cycle MàJ, plateforme, pays, URL, accès testeur, URL créateur, URL informations générales et guide utilisateur, URL copies d'écran, copyright, URL tiers, hardware additionnel, prix, nom de la compagnie, type d'entreprise, contact principal, Email contact principal, rôle principal du contact, noms des contributeurs/organisation, lien vers la page contributeur, support utilisateur.
Détails de l'application	Cible audience principale, détaillé les cibles spécifiques, objectif principal de l'application, concurrent similaire et différence, classification (support de livres médicaux, suivi et évaluation de santé, gestion cabinet, aide générique non médicale, dossier de patient informatisé, diagnostic médical, traitement pathologie, prévention, cible une structure ou fonction du corps, accessoire pour un dispositif médical, autre), description des fonctionnalités, auteurs du contenu et cursus et statut, déclaration d'intérêt auteur, déclaration de financement et des sources des fonds, localisation dans l'application de la citation des financements, liens d'intérêt, localisation dans l'application de la citation des conflits d'intérêt, contre-indications, localisation dans l'application de la citation des contre-indications, limitations connues, risques potentiels.
Sécurité et vie privée	Politique de confidentialité des données personnelles, localisation dans l'application de la citation de la politique de confidentialité des données personnelles, réglages utilisateurs des paramètres de confidentialité, transparence des personnes ayant accès aux données utilisateurs par URL ou menu, sécurité des protocoles de transmissions.
Accord de la FDA	Statut de la demande d'accord, détail de la demande ou pas de l'accord.
Développement et processus de test, et EBM	Niveau d'évaluation formative ou développement appuyé sur les retours des utilisateurs, évaluation formative et publications clés, quel est le niveau de preuve de l'application (pas de revue par les pairs ou d'évaluation, revue par les pairs planifiée, revue par les pairs, étude observationnelle en cours, étude observationnelle terminée, essai randomisé en cours (pilote/petit), essai randomisé terminé (pilote/petit), essai randomisé en cours (large effectif), essai randomisé terminé (large effectif), quels sont les critères de jugement principaux et secondaires, registre d'inscription de l'essai, théorie ou preuves justifiant le contenu de l'application, source de EBM/théorie et publications clés, revue par ses pairs et publications clés, revue par un journal externe ou blog, évaluation des résultats des études observationnelles et publications clés, évaluation des résultats des études randomisées et publications clés, évaluation des résultats et données clés des publications probantes, note complémentaire.

MàJ : mise à jour, URL : *uniform resource locator*, EBM : *Evidence-based medicine*, FDA : *Food and drug administration*.

Annexe 3. Recherche documentaire

▶ Bases de données bibliographiques

La recherche documentaire, limitée aux publications en langue anglaise et française, a été réalisée à partir des sources suivantes :

- pour la littérature internationale : la base de données Medline ;
- pour la littérature francophone : la Banque de données en santé publique ;
- la *Cochrane Library* ;
- les sites Internet publiant des recommandations, des rapports d'évaluation technologique ou économique ;
- les sites Internet compétents dans le domaine étudié, y compris des sites d'évaluation d'Apps/OC en santé et des sites d'actualité.

La stratégie d'interrogation des bases de données précise pour chaque question et/ou types d'étude les termes de recherche utilisés, les opérateurs booléens et la période de recherche.

Les termes de recherche utilisés sont soit des termes issus de thésaurus (descripteurs), soit des termes libres (du titre ou du résumé). Ils sont combinés avec les termes décrivant les types d'études.

Le tableau ci-dessous présente de façon synthétique les étapes successives de cette interrogation dans la base de données Medline. Le nombre total de références obtenues par interrogation de cette base de données bibliographiques est 643.

Stratégie de recherche dans la base de données Medline

Type d'étude/sujet	Termes utilisés	Période
Recommandations & conférences de consensus		01/2005 – 12/2015
Étape 1	(Cell Phones OR Mobile Applications)/maj OR (mobile application OR mobile applications OR mobile app OR mobile apps OR smartphone application OR smartphone applications OR Smartphone app OR Smartphone apps OR app stores OR Mobile Medical Application OR Mobile Medical Applications OR medical apps OR medical app OR standalone software OR health apps OR health app OR mhealth OR mobile health)/ti,ab OR (ehealth OR apps OR app)/ti OR ((Medical Informatics Applications/maj OR Software/Maj:NoExp OR (application OR applications OR health OR medical)/ti) AND (mobile OR smartphone OR phone)/ti)	
ET		
Étape 2	(guide OR guidance* OR recommendation* OR guideline* OR statement* OR consensus OR position paper)/ti OR (Guidelines as topic OR health planning guidelines OR Practice Guidelines as topic OR Consensus Development Conferences as topic OR Consensus Development Conferences, NIH as topic)/de OR (practice guideline OR guideline OR Consensus Development Conference OR Consensus Development Conference, NIH OR Government Publications)/pt	
Méta-analyses & revues systématiques		01/2010 – 12/2015
Étape 1		
ET		
Étape 3	(metaanalys* OR meta-analys* OR meta analysis OR systematic review* OR systematic overview* OR systematic literature review* OR systematical review* OR systematical overview* OR systematic literature review* OR systematic literature search)/ti,ab OR meta-analysis as topic/de OR meta-analysis/pt OR cochrane database syst rev/so	

Type d'étude/sujet	Termes utilisés	Période
Évaluation des applications		01/2010 – 12/2015
Étape 1		
ET		
Étape 4	(quality control framework OR regulatory framework OR evaluation framework OR ehealth framework OR Mobile App Rating scale OR MARS OR scoring OR quality assessment)/ti,ab OR (framework OR frameworks OR certificat* OR label* OR standard OR criteria)/ti OR Software Validation/de	
OU		
Étape 5	(mhealth OR mobile health OR apps OR app OR standalone software)/ti AND (evaluat* OR Assessment)/ti	

** : troncature ; de : descriptor ; ti : title ; ab : abstract ; pt : publication type ; so :journal title ;*

▶ Sites consultés

- **Exemples de portails ou sites d'évaluation/classification d'applications en santé**
  - *Agency of Healthcare Quality of Andalusia (appSaludable)* : www.calidadappsalud.com/distintivo/catalogo
  - *AppCheck* : www.appcheck.de
  - dmd Santé (dmdpost) : www.dmd-sante.com
  - *HealthOn* : www.healthon.de
  - *iMedicalApps* (iPrescribeApps) : www.imedicalapps.com
  - *IMS Health* (AppScript) : www.imshealth.com
  - *Medappcare* : www.medappcare.com/conseil-scientifique
  - *myhealthapps.net* : myhealthapps.net/about
  - *UK's National Health Service : NHS choices (Health Apps Library)* : apps.nhs.uk/review-process/#
- **Exemples de sites avec catalogue d'applications en santé (sans évaluation)**
  - *Eat right* : www.eatrightpro.org/resources/media/trends-and-reviews/app-reviews
  - Infirmier.com : www.infirmiers.com/ressources-infirmieres/documentation/tour-horizon-de-quelques-applications-mobiles-bien-utiles.html
  - *National Health Portal : mhealth* : www.nhp.gov.in/mobile-apps
  - *UF Diabetes Institute : mhealth* : diabetes.ufl.edu/my-diabetes/diabetes-resources/diabetes-apps/
  - *US department of Veterans Affairs : VA mobile health (VA App Store)* : mobile.va.gov
  - *Zur Institute : Mental Health Apps* : www.zurinstitute.com/mentalhealthapps_resources.html
- **Sites d'actualités sur la m-santé**
  - Buzz-esanté - le blog du digital santé : linkis.com/buzz-esante.fr/Ab5Ye
  - *Connected doctors* : www.theconnectedmag.fr
  - DSIH e-sante : www.dsih.fr
  - *GeekMedical* : www.geekmedical.fr
  - Le monde de la e-santé : lemondedelaesante.wordpress.com
  - *MedCityNews* : medcitynews.com
  - *mHealth News* : www.mhealthnews.com
  - *Mobihealthnews* : mobihealthnews.com
  - objetconnecte.net : www.objetconnecte.net/category/sante-connectee/
  - Proxima mobile : www.proximamobile.fr/article/france-un-guide-mobile-pour-800-applications-de-sante?cat=none
  - *Smart Phone Healthcare* : www.smartphonehc.com
- **Autres sites consultés**
  - Agence des systèmes d'information partagés de santé - ASIP Santé : www.asipsante.fr
  - Agence fédérale des médicaments et des produits de santé - AFMPS : www.fagg-afmps.be/fr/
  - Agence nationale de sécurité du médicament et des produits de santé - ANSM : ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Logiciels-et-applications-mobiles-en-sante/%28offset%29/1
  - *Agency for Healthcare Research and Quality* - AHRQ : www.ahrq.gov
  - *Alberta Medical Association* : www.topalbertadoctors.org

- *American College of Physicians* – ACP : www.acponline.org/clinical/guidelines/index.html#acg
- *Attorney General* (État de Californie) : www.attorneygeneral.jus.gov.on.ca/french/default.asp
- Bibliothèque médicale Lemanissier : www.bmlweb.org/consensus.html
- Bibliothèque interuniversitaire de médecine - BIUS
- *CATAAlliance* [*CATA Mobile Health Advisory Board* (MHAB)] : www.cata.ca/Communities/MHAB/
- Catalogue et Index des sites médicaux francophones - CISMeF : www.cismef.org
- Centre fédéral d'expertise des soins de santé - KCE : kce.fgov.be/fr
- Commission nationale de l'informatique et des libertés - CNIL : www.cnil.fr
- Conseil de l'Europe : www.coe.int/web/portal/home
- Conseil National de l'Ordre des Médecins - CNOM : www.conseil-national.medecin.fr/e-sante/les-publications-1143
- Contrôleur européen de la protection des données - EDPS/CEPD : secure.edps.europa.eu/EDPSWEB/
- E.sante.gouv : esante.gouv.fr
- *European Commission* : ec.europa.eu/digital-agenda/en/mhealth
- *Euroscan* : www.euroscan.bham.ac.uk
- *Food and Drug Administration* - FDA : www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/default.htm
- *Groupe Speciale Mobile Association* - GSMA : www.gsma.com
- *Guidelines International Network* - GIN : www.g-i-n.net
- *HealthIT.gov* : www.healthit.gov/patients-families/health-conditions
- *Institute for Clinical Systems Improvement* : www.icsi.org
- *International Medical Device Regulators' Forum* - IMDRF : www.imdrf.org
- *International mHealth Standardization Consortium* - IMHSC : www.imhsc.org/legislation_3.html
- *International Network of Agencies for Health Technology Assessment* - INAHTA : www.inahta.org
- *CRD databases* : www.crd.york.ac.uk/crdweb/
- *Medical Technology Association of Australia* - MTAA : www.mtaa.org.au/homepage
- *Medicines or Healthcare products Regulatory Agency* - MHRA : www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency
- *National Guideline Clearinghouse* - NGC : www.guideline.gov
- *National Health and Medical Research Council* - NHMRC : www.nhmrc.gov.au/publications/index.htm
- *National Institute for Health and Clinical Excellence* - NICE : www.nice.org.uk/page.aspx?o=home
- *National Institute of Health* - NIH : obssr.od.nih.gov/scientific_areas/methodology/mhealth/
- *National Telecommunications and Information Agency* - NTIA : www.ntia.doc.gov
- *New Zealand Guidelines Group* - NZGG : www.nzgg.org.nz
- *NHS Evidence* : www.evidence.nhs.uk
- Observatoire de la m-santé : www.ifop.com/?option=com_offer&id=186
- Organisation Mondiale de la Santé - OMS : www.who.int/fr
- *Privacy Rights Clearing House Association* : www.privacyrights.org/content/about-privacy-rights-clearinghouse
- *Scottish Intercollegiate Guidelines Network* - SIGN : www.sign.ac.uk/index.html
- SFT - Société française de télémédecine : www.sft-antel.org/site/accueil.html
- *The Cochrane Library* : www.mrw.interscience.wiley.com/cochrane/cochrane_search_fs.html
- *Therapeutic Goods Administration* - TGA : www.tga.gov.au
- *Tripdatabase* : www.tripdatabase.com/index.html

En complément, une veille a été réalisée sur Twitter avec les mots clés suivants : #mhealth OU « mobile health » OU « m santé » OU #msanté. Des comptes Twitter pertinents dans le domaine ont également été suivis tout au long de l'étude.

Annexe 4. Liste des tableaux

Tableau 1. Compilation non exhaustive des sites évaluant les Apps/OC en santé au niveau de différents pays (présenté par ordre alphabétique)

Tableau 2. Modulation du référentiel par une matrice de risque

Tableau 3. Liste des critères se rapportant aux informations utilisateurs

Tableau 4. Liste des critères se rapportant au contenu de santé du produit

Tableau 5. Liste des critères se rapportant au contenant technique du produit

Tableau 6. Liste des critères se rapportant à la sécurité et fiabilité du produit

Tableau 7. Liste des critères se rapportant à l'utilisation du produit

Annexe 5. Glossaire

Anonymisation
Moyen visant à faire disparaître tout lien avec une personne. Le traitement de données personnelles, qui est normalement interdit par la loi, peut être autorisé par la CNIL si les informations sensibles du traitement font l'objet, à bref délai, d'un procédé d'anonymisation reconnu conforme à la loi.

Big data
On parle depuis quelques années du phénomène de *big data*, que l'on traduit souvent par « données massives ». Avec le développement des nouvelles technologies, d'internet et des réseaux sociaux ces vingt dernières années, la production de données numériques a été de plus en plus nombreuse : textes, photos, vidéos, etc. Le gigantesque volume de données numériques produites combiné aux capacités sans cesse accrues de stockage et à des outils d'analyse en temps réel de plus en plus sophistiqués offre aujourd'hui des possibilités inégalées d'exploitation des informations. Les ensembles de données traités correspondant à la définition du *big data* répondent à trois caractéristiques principales : volume, vélocité et variété.

Cross-Site Request Forgery
Abrégé CSRF (parfois prononcé *sea-surfing* en anglais). L'objet de cette attaque est de transmettre à un utilisateur authentifié une requête HTTP falsifiée qui pointe sur une action interne au site, afin qu'il l'exécute sans en avoir conscience et en utilisant ses propres droits. L'utilisateur devient donc complice d'une attaque sans même s'en rendre compte. L'attaque étant actionnée par l'utilisateur, un grand nombre de systèmes d'authentification sont contournés (source : Wikipedia).

Consentement
Consentement de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Destinataire
La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autori-tés publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

Données à caractère personnel
Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Donnée sensible
Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Empowerment
L'*empowerment*, parfois aussi appelée autonomisation au Québec, est l'octroi de davantage de pouvoir aux individus ou aux groupes pour agir sur les conditions sociales, économiques, politiques ou écologiques qu'ils subissent (source : Wikipedia).

E-santé
Application des technologies de l'information et de la communication à l'ensemble des activités en rapport avec la santé.

Géolocalisation
Technologie permettant de déterminer la localisation d'un objet ou d'une personne avec une certaine précision. La technologie s'appuie généralement sur le système GPS ou sur les interfaces de communication d'un téléphone mobile. Les applications et finalités de la géolocalisation sont multiples : de l'assistance à la navigation, à la mise en relation des personnes, mais aussi à la gestion en temps réel des moyens en personnel et en véhicules des entreprises, etc.

Mobile Health
Pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs de surveillance des patients, les PDA et autres appareils sans fil.

Ordiphone
Téléphone mobile couplé à un assistant numérique personnel.

Phishing
L'hameçonnage, *phishing* ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de nais-sance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques (source : Wikipedia).

Pseudonymisation
Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Quantified-self
Le *quantified-self* désigne la pratique de la « mesure de soi » et fait référence à un mouvement né en Californie qui consiste à mieux se connaître en mesurant des données relatives à son corps et à ses activités.

Smartphone
Un *smartphone* est un téléphone mobile disposant d'un écran tactile et d'un appareil photo numérique, et des fonctions d'un assistant numérique personnel et d'un ordinateur portable (source : Wikipedia).

Tiers
Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

Traitement
Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Violation de données à caractère personnel
Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Annexe 6. Méthode de travail

Ce document a été réalisé de novembre 2015 à septembre 2016. Il a été conduit pour la Haute Autorité de Santé (HAS) dans le Service évaluation de la pertinence des soins et amélioration des pratiques et des parcours (SA3P) par M. Pierre Trudelle, chef de projet, en collaboration avec M. Marc Fumey, Adjoint au chef de service, avec l'aide d'un groupe de travail et de deux experts externes.

Le secrétariat a été effectué par Mme Michèle Le Moigne, assistante de gestion, et avec le soutien de Mme Isabelle Le Puil, assistante de gestion, pour la gestion rationalisée des avis de lecture (GRaAL).

Un appel à candidatures pour participer au groupe de travail a été ouvert en ligne entre le mois de novembre 2015 et le 31 décembre 2015 (note de cadrage 19 novembre 2015). Le bureau de la Commission des parcours et des pratiques (CPP) de la HAS a arrêté la composition finale du groupe de travail et délimité l'attribution vers le groupe de lecture et celui des parties prenantes lors de la réunion 10 février 2016. Les déclarations d'intérêts des membres du groupe de travail sont consultables sur le site de la HAS (www.has-sante.fr).

Les réunions du groupe de travail ont eu lieu les 22 mars 2016, 3 mai 2016 et 6 septembre 2016 toute la journée. Un groupe de lecture, un groupe de parties prenantes et un groupe provenant du comité stratégique de filière (appelé GT28 en référence à la « mesure 28 » du contrat stratégique de filière) a adressé ses cotations en utilisant une échelle de Likert côtée de 1 (désaccord total) à 9 (accord total) sur l'ensemble des critères retenus *via* l'interface GRaAL de la HAS entre la réunion 2 et 3 du groupe de travail de la HAS. Le groupe de lecture était composé de membres sélectionnés lors de la CPP (principalement de personnes non retenues lors de l'appel à participation du groupe de travail) et de personnes suggérées par le groupe de travail.

La recherche documentaire a été effectuée par Mme Marie Georget, documentaliste, et Mme Laurence Frigère assistante-documentaliste, sous la direction de Mme Frédérique Pagès, responsable du service documentation-veille de la HAS.

Le groupe de travail a contribué à la rédaction des parties techniques de ce guide avec le soutien lors de la dernière réunion d'experts de l'ANSSI et de la CNIL. La sélection et l'analyse de la littérature ont été réalisées par M. Pierre Trudelle. La rédaction de recommandations européennes sur le sujet se déroulait en parallèle à la rédaction de ce document. M. Pierre Trudelle a fait partie du groupe de travail (*mHealth assessment guidelines*) pour apporter et traduire les éléments français et synchroniser les informations entre les groupes.

Le service juridique de la HAS a participé à la rédaction du chapitre juridique et la relecture des critères sous la supervision de Mme Ariane Sachs, juriste ; M. Emmanuel Planchet, juriste ; et Mme Christine Vincent, Chef du service juridique de la HAS.

La mise en forme du document a été réalisée par M. Eric Darvoy, maquettiste-infographiste, sous la direction de Mme Annie Chevallier, responsable du pôle édition-diffusion au service communication-information.

Le passage en CPP a été effectué le 27 septembre 2016.

Le passage au Collège de la Haute Autorité de Santé a eu lieu le 26 octobre 2016.

Annexe 7. Participants

Groupe de travail

- Dr Vincent Achard, Maître de conférence universitaire, praticien hospitalier, Université d'Aix-Marseille
- Pr Rachid Bouchakour, Directeur d'institut - CNRS, Université d'Aix-Marseille
- Dr Paul Cattaneo, Chirurgien-Dentiste, Paris
- Dr Pascal Charbonnel, Médecin Généraliste Libéral, Vice-Président du CMG, Les Ulis
- Dr Sébastien Cossin, Médecin de santé publique, CHU de Bordeaux
- M. Mathieu Escot, Responsable des Études, UFC- Que choisir, Paris
- Dr Matthieu Faure, Ingénieur, Nîmes
- M. Marc Fumey, Adjoint au Chef de service, Service évaluation de la pertinence des soins et amélioration des pratiques et des parcours (SA3P), HAS, Saint-Denis
- Dr Leïla Gofti-Laroche, PharmD, PhD, Praticien Hospitalier, CHU Grenoble Alpes
- M.Marin Guy, Kinésithérapeute, Centre Aquitain du Dos, Mérignac
- Dr Philippe Haïk, Docteur Ingénieur ETP/SUPELEC, Responsable du Dept « Énergie & Environnement » à l'ECE, Paris
- Dr Cécile Hubsch, MD-PhD, Neurologue, Fondation Ophtalmologique A. de Rothschild, Paris
- Dr Benjamin Kretz, Chirurgien vasculaire, CH de Colmar
- Dr Pierre Liot, Chef de projet HAS, Service évaluation de la pertinence des soins et amélioration des pratiques et des parcours (SA3P), HAS, Saint-Denis
- Dr Jacques Lucas, Vice-président CNOM, Paris
- Dr Didier Mennecier, Praticien Hospitalier Militaire, Saint Mandé
- M. Loïck Menvielle, EDHEC Business School, Nice
- M. Hervé Nabarette, Conseiller technique auprès du directeur, Direction de l'évaluation médicale, économique et de santé publique, HAS, Saint-Denis
- Dr Grégory Perrard, Cardiologue, membre de la Commission Numérique du Syndicat National des Spécialistes des Maladies du Coeur et des Vaisseaux, BAILLEUL
- M. Vincent Rialle, Maître de conférence-Praticien Hospitalier Émérite, Université Grenoble-Alpes
- M. Valentin Roby, Doctorant en droit public, Université Lille 2
- Dr Philippe Roux, Généraliste, Samatan
- Dr Éric Sermet, Psychiatre, Lyon
- M. Pierre Trudelle, Chef de projet HAS, pilote du projet, Service évaluation de la pertinence des soins et amélioration des pratiques et des parcours (SA3P), HAS, Saint-Denis

Experts externes

- M. Erik Boucher de Crèvecœur, Ingénieur expert, service de l'expertise technologique, CNIL, Paris
- M. Benjamin Morin, Chef adjoint de la division scientifique et technique, Sous-direction Expertise ANSSI, Paris

Groupe de lecture

- Dr Marie-Christine Bene, Professeur des universités-praticiens hospitaliers, Université de Nantes – CHU de Nantes,
- Dr Xavier Billères, Praticien Hospitalier, SAMU 13, CHU de Marseille
- Dr Marie-José Botto Mongaboure, Praticien Hospitalier, Paris
- Dr François Carbonnel, Médecin généraliste, Chef de clinique des Universités, Université de Montpellier
- M. Patrick Corne, Kinésithérapeute, Saint Max – Lorraine
- Dr Didier Cugy, Praticien Attaché – Consultant, CHU de Bordeaux
- M. Stéphane Delliaux, Maître de Conférences des Universités - Praticien Hospitalier, CHU d'Aix-Marseille
- M. Clément Gravereaux, Doctorant-Chercheur, Université Rennes 2 - Responsable de la Stratégie Digitale CHP de Saint-Grégoire
- M. Yoann Guymard, Infirmier référent en soin à domicile (CMS) sur le canton de Vaud, Suisse
- Dr Olivier Heloir, Pharmacien, Nord Pharma, Ligny en Cambrésis
- Dr Bruno Housset, Professeur des Universités-Praticien Hospitalier, Chef de service, CHI de Créteil, Faculté de Créteil
- Dr David Lechaux, Chirurgien, CH de Saint Brieuc
- Mme Blandine Meyrieux-Lefevre, Infirmière - Institut Godinot, Reims
- M. Alexandre Perez, Kinésithérapeute, Bordeaux
- M. Philippe Ruyer, Masseur-Kinésithérapeute, Les Angles

- M. Martin Seyres, Doctorant-Chercheur, Bordeaux
- M. Romain Tavignot, Infirmier Anesthésiste, Centre Antoine Lacassagne,Nice
- M. Yannick Ung, Ergothérapeute, Doctorant-chercheur, Paris Descartes-Sorbonne

▶ Groupe partie prenante

- Pr Francois-André Allaert, Titulaire de la Chaire d'évaluation des allégations de santé ESC Dijon
- Dr Patrick Bacquaert, Médecin Chef IRBMS - Médecin de médecine physique, Villeneuve d Ascq
- M. Jérôme Beranger, Co-fondateur d'ADEL (*Algorithm Data Ethics Label*) et Chercheur (PhD) associé à l'Inserm 1027 - Équipe 4 - Université Paul Sabatier, Toulouse
- Dr Fabrice Denis, Oncologue-Radiothérapeute, Le Mans
- Pr Sébastien Faure, Professeur des universités, UFR santé, département pharmacie, INSERM U1066, Université d'Angers
- M. Frédéric Faurennes, Directeur Associé VIRTUAL CARE, Chantilly
- Dr Sylvia Franc, Praticien Hospitalier en Diabétologie, CH Sud-Francilien, Corbeil Essonne, directeur scientifique du Centre de Recherche CERITD, Evry
- Mme Karine Gueye-Gauchet, Conseillère Médico -Technique, Champigny Sur Marne
- Dr Aurore Guillaume, Endocrinologue, Groupe Elgar, Saint Jean de Luz
- Dr Cécile Monteil, Médecin aux urgences pédiatriques de l'hôpital Robert Debré, Directrice Médicale chez iLumens, Fondatrice d'Eppocrate, Paris
- Mr David Sainati, Président, MEDAPPCARE, Paris
- M. Alain Tassy, Gérant, Virtualtel, Meudon
- Dr Mobin Yasini, Directeur Recherche et Développement, mHealth Quality (dmd Santé), Paris

▶ Groupe de travail 28 (en référence à la « mesure 28 » du contrat de filière) du comité stratégique de filière consultés

- M. Alain Boulanger, Direction générale de la concurrence, de la consommation et de la répression des fraudes, Paris
- Mme Raphaëlle Bove, Direction générale de la concurrence, de la consommation et de la répression des fraudes, Paris
- Mme Hélène Bruyere, ANSM, Saint-Denis
- M. Aymeric Buthion, DGE, Ministère de l'Économie et des Finances, Paris
- M. Emmanuel Clout, Responsable programme labellisation, Agence des Systèmes d'Information Partagés de Santé, Paris
- Dr Thierry Dart, Docteur en médecine, Agence des Systèmes d'Information Partagés de Santé, Paris
- M. Marcelo Dias de Amorim, Direction Générale pour la Recherche et l'Innovation, Paris
- Isabelle Diaz, Direction des Affaires Scientifiques, Les Entreprises du Médicament, Paris
- Mme Florence Éon, Directrice du service juridique, Agence des Systèmes d'Information Partagés de Santé, Paris
- M. Vincent Franchi, DGE, Ministère de l'Économie et des Finances, Paris
- M. Guirec Le Lous, UrgoTech, Paris
- M. Pierre Leurent, Président du Directoire, Voluntis, Paris
- Mme Elinaz Mahdavy, Orange Healthcare – Responsable des Affaires Européennes, Bruxelles
- M. Francis Mambrini, Fédération des Éditeurs d'Informatique Médicale et Paramédicale Ambulatoire, Boulogne Billancourt
- Dr Florence Ollé, Pharmacienne, Syndicat National de l'Industrie des Technologies Médicales, Paris
- M. Stéphane Pasquier, FSSI, Ministères chargés des Affaires Sociales, Paris
- M. Robert Picard, Président Forum Living Labs Santé Autonomie, Paris
- Dr Pierre Simon, Société Française de Télémédecine, Paris
- M. Jean Vannimenus, DGRI / SSRI - Secteur A3, Paris
- M. Dominique Vital, Directeur Recherche et Développement, STAGO, Asnières sur Seine

Références

1. de la Vega R, Miro J. mHealth: a strategic field without a solid scientific soul. a systematic review of pain-related apps. PLoS One 2014;9(7):e101312.

2. Canada Health Infoway. Mobile health computing between clinicians and patient. Montréal: CHI; 2014.

3. Park LG, Howie-Esquivel J, Dracup K. A quantitative systematic review of the efficacy of mobile phone interventions to improve medication adherence. J Adv Nurs 2014;70(9):1932-53.

4. Bailey SC, Belter LT, Pandit AU, Carpenter DM, Carlos E, Wolf MS. The availability, functionality, and quality of mobile applications supporting medication self-management. J Am Med Inform Assoc 2014;21(3):542-6.

5. Fiordelli M, Diviani N, Schulz PJ. Mapping mHealth research: a decade of evolution. J Med Internet Res 2013;15(5):e95.

6. Gagnon MP, Ngangue P, Payne-Gagnon J, Desmartis M. m-Health Adoption by Healthcare Professionals: A Systematic Review. J Am Med Inform Assoc 2015.

7. Canadian Advanced Technology Alliance. Mobile health Canada turn up the volume. Ottawa: CATA; 2014.

8. World Health Organization. mHealth. New horizons for health through mobile technologies : second global survey on eHealth. Geneva: WHO; 2011. www.who.int/goe/publications/goe_mhealth_web.pdf

9. Center for Health + Biosciences, Rice University's Baker Institute for Public Health, Moore Q, Johnson A. U.S. Health care technologies. Houston: BIPP; 2015.

10. Aungst TD, Clauson KA, Misra S, Lewis TL, Husain I. How to identify, assess and utilise mobile medical applications in clinical practice. Int J Clin Pract 2014;68(2):155-62.

11. Lewis TL, Boissaud-Cooke MA, Aungst TD, Eysenbach G. Consensus on use of the term "App" versus "Application" for reporting of mHealth research. J Med Internet Res 2014;16(7):e174; discussion e.

12. Agarwal S, LeFevre AE, Lee J, L'Engle K, Mehl G, Sinha C, et al. Guidelines for reporting of health interventions using mobile phones: mobile health (mHealth) evidence reporting and assessment (mERA) checklist. BMJ 2016;352:i1174.

13. Dumez H, Minvielle E, Marrauld L. Etat des lieux de l'innovation en santé numérique. Paris: Fondation de l'avenir; 2015. www.fondationdelavenir.org/wp-content/uploads/2015/11/Etat-des-lieux-sante-num%C3%A9rique-EditionAug.pdf

14. Mosa AS, Yoo I, Sheets L. A systematic review of healthcare applications for smartphones. BMC Med Inform Decis Mak 2012;12:67.

15. Yasini M, Marchand G. Toward a use case based classification of mobile health applications. Stud Health Technol Inform 2015;210:175-9.

16. Vallespin B, Cornet J, Kotzeva A. Ensuring Evidence-Based Safe and Effective mHealth Applications. Stud Health Technol Inform 2016;222:248-61.

17. Labrique AB, Vasudevan L, Kochi E, Fabricant R, Mehl G. mHealth innovations as health system strengthening tools: 12 common applications and a visual framework. Glob Health Sci Pract 2013;1(2):160-71.

18. Bender JL, Yue RY, To MJ, Deacken L, Jadad AR. A lot of action, but not in the right direction: systematic review and content analysis of smartphone applications for the prevention, detection, and management of cancer. J Med Internet Res 2013;15(12):e287.

19. Yetisen AK, Martinez-Hurtado JL, da Cruz Vasconcellos F, Simsekler MC, Akram MS, Lowe CR. The regulation of mobile medical applications. Lab Chip 2014;14(5):833-40.

20. Hussain M, Al-Haiqi A, Zaidan AA, Zaidan BB, Kiah ML, Anuar NB, et al. The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations. Comput Methods Programs Biomed 2015;122(3):393-408.

21. Cook SE, Palmer LC, Shuler FD. Smartphone mobile applications to enhance diagnosis of skin cancer: A guide for the rural practitioner. W V Med J 2015;111(5):22-8.

22. World Health Organization. From innovation to implementation eHealth in the WHO European Region Copenhagen: WHO; 2016. www.euro.who.int/__data/assets/pdf_file/0012/302331/From-Innovation-to-Implementation-eHealth-Report-EU.pdf?ua=1

23. Huckvale K, Prieto JT, Tilney M, Benghozi PJ, Car J. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Med 2015;13:214.

24. Food and Drug Administration. Mobile medical applications : Guidance for Food and Drug Administration Staff. Silver Spring: FDA; 2015. www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

25. Cortez NG, Cohen IG, Kesselheim AS. FDA regulation of mobile health technologies. N Engl J Med 2014;371(4):372-9.

26. Royal College of Physicians. Using apps in clinical practice [En ligne]. London: RCP; 2015.

27. Medecine & Healthcare producs Regulary Agency. Medical device stand-alone software including apps [En ligne]: MHRA; 2014. www.gov.uk/government/publications/medical-devices-software-applications-apps/medical-device-stand-alone-software-including-apps

28. International Medical Device Regulators Forum. Software as a Medical Device (SaMD): Key definitions : IMDRF; 2013. www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf

29. Quinn P, Habbig AK, Mantovani E, De Hert P. The data protection and medical device frameworks - obstacles to the deployment of mHealth across Europe? Eur J Health Law 2013;20(2):185-204.

30. ITU. Filling the gap: Legal and regulatory challenges of mobile health (mHealth) in Europe : ITU; 2014. www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/ITU%20mHealth%20Regulatory%20gaps%20Discussion%20Paper%20June2014.pdf

31. Charani E, Castro-Sanchez E, Moore LS, Holmes A. Do smartphone applications in healthcare require a governance and legal framework? It depends on the application! BMC Med 2014;12:29.

32. Academy of Medical Sciences, Royal Academy of Engineering. Health apps: regulation and quality control. London: AMS; 2015. www.raeng.org.uk/publications/reports/health-apps-regulation-and-quality-control

33. Conseil national de l'ordre des médecins. Santé connectée. De la e-santé à la santé connecté. Livre blanc. Paris: CNOM; 2015. www.conseil-national.medecin.fr/sites/default/files/medecins-sante-connectee.pdf

34. Commission nationale de l'informatique et des libertés. Étude de benchmark sur les régulations concernant l'utilisation dans le domaine de la santé et du bien-être des capteurs, smartphones et autres objets connectés. Paris: CNIL; 2013.

35. Schulke DF. The regulatory arms race : mobile health applications and agency posturing. Boston University Law Rev 2013;93(1699):1700-52.

36. Whittaker R, Merry S, Dorey E, Maddison R. A development and evaluation process for mHealth interventions: examples from New Zealand. J Health Commun 2012;17 Suppl 1:11-21.

37. Gonnermann A, von Jan U, Albrecht UV. Draft guideline for the development of evidence based medicine-related apps. Stud Health Technol Inform 2015;210:637-41.

38. McMillan B, Hickey E, Patel MG, Mitchell C. Quality assessment of a sample of mobile app-based health behavior change interventions using a tool based on the National Institute of Health and Care Excellence behavior change guidance. Patient Educ Couns 2015.

39. Albrecht UV, Von Jan U, Pramann O. Standard reporting for medical apps. Stud Health Technol Inform 2013;190:201-3.

40. Salber P, Niksch A. A beginner's guide to digital health for ambulatory care clinicians. J Ambul Care Manage 2015;38(1):91-4.

41. Murfin M. Know your apps: an evidence-based approach to evaluation of mobile clinical applications. J Physician Assist Educ 2013;24(3):38-40.

42. Chan S, Torous J, Hinton L, Yellowlees P. Towards a framework for evaluating mobile mental health apps. Telemed J E Health 2015;21(12):1038-41.

43. Huckvale K, Car M, Morrison C, Car J. Apps for asthma self-management: a systematic assessment of content and tools. BMC Med 2012;10:144.

44. Safavi S, Shukur Z. Conceptual privacy framework for health information on wearable device. PLoS One 2014;9(12):e114306.

45. Payne HE, Lister C, West JH, Bernhardt JM. Behavioral functionality of mobile apps in health interventions: a systematic review of the literature. JMIR Mhealth Uhealth 2015;3(1):e20.

46. Free C, Phillips G, Watson L, Galli L, Felix L, Edwards P, et al. The effectiveness of mobile-health technologies to improve health care service delivery processes: a systematic review and meta-analysis. PLoS Med 2013;10(1):e1001363.

47. Hamine S, Gerth-Guyette E, Faulx D, Green BB, Ginsburg AS. Impact of mHealth chronic disease management on treatment adherence and patient outcomes: a systematic review. J Med Internet Res 2015;17(2):e52.

48. Elbert NJ, van Os-Medendorp H, van Renselaar W, Ekeland AG, Hakkaart-van Roijen L, Raat H, et al. Effectiveness and cost-effectiveness of ehealth interventions in somatic diseases: a systematic review of systematic reviews and meta-analyses. J Med Internet Res 2014;16(4):e110.

49. Jones SP, Patel V, Saxena S, Radcliffe N, Ali Al-Marri S, Darzi A. How Google's 'ten Things We Know To Be True' could guide the development of mental health mobile apps. Health Aff (Millwood) 2014;33(9):1603-11.

50. de la Torre-Diez I, Lopez-Coronado M, Vaca C, Aguado JS, de Castro C. Cost-utility and cost-effectiveness studies of telemedicine, electronic, and mobile health systems in the literature: a systematic review. Telemed J E Health 2015;21(2):81-5.

51. Russell-Minda E, Jutai J, Speechley M, Bradley K, Chudyk A, Petrella R. Health technologies for monitoring and managing diabetes: a systematic review. J Diabetes Sci Technol 2009;3(6):1460-71.

52. Liang X, Wang Q, Yang X, Cao J, Chen J, Mo X, et al. Effect of mobile phone intervention for diabetes on glycaemic control: a meta-analysis. Diabet Med 2011;28(4):455-63.

53. Holtz B, Lauckner C. Diabetes management via mobile phones: a systematic review. Telemed J E Health 2012;18(3):175-84.

54. Gray LJ, Leigh T, Davies MJ, Patel N, Stone M, Bonar M, et al. Systematic review of the development, implementation and availability of smart-phone applications for assessing type 2 diabetes risk. Diabet Med 2013;30(6):758-60.

55. Liu F, Kong X, Cao J, Chen S, Li C, Huang J, et al. Mobile phone intervention and weight loss among overweight and obese adults: a meta-analysis of randomized controlled trials. Am J Epidemiol 2015;181(5):337-48.

56. O'Reilly GA, Spruijt-Metz D. Current mHealth technologies for physical activity assessment and promotion. Am J Prev Med 2013;45(4):501-7.

57. Stephens J, Allen J. Mobile phone interventions to increase physical activity and reduce weight: a systematic review. J Cardiovasc Nurs 2013;28(4):320-9.

58. Wearing JR, Nollen N, Befort C, Davis AM, Agemy CK. iPhone app adherence to expert-recommended guidelines for pediatric obesity prevention. Child Obes 2014;10(2):132-44.

59. Bort-Roig J, Gilson ND, Puig-Ribera A, Contreras RS, Trost SG. Measuring and influencing physical activity with smartphone technology: a systematic review. Sports Med 2014;44(5):671-86.

60. Fanning J, Mullen SP, McAuley E. Increasing physical activity with mobile devices: a meta-analysis. J Med Internet Res 2012;14(6):e161.

61. Marcano Belisario JS, Huckvale K, Greenfield G, Car J, Gunn LH. Smartphone and tablet self management apps for asthma (Review). Cochrane Database of Systematic Review 2013;Issue 11:CD010013.

62. Huckvale K, Morrison C, Ouyang J, Ghaghda A, Car J. The evolution of mobile apps for asthma: an updated systematic assessment of content and tools. BMC Med 2015;13:58.

63. Riezebos RJ. Peer-reviewing of mHealth applications. Requirements for peer-reviewing mobile health applications and development of an online peer review tool Amsterdam: University of Amsterdam; 2014. dare.uva.nl/cgi/arno/show.cgi?fid=573074

64. Lewis TL, Wyatt JC. mHealth and mobile medical Apps: a framework to assess risk and promote safer use. J Med Internet Res 2014;16(9):e210.

65. BinDhim NF, Hawkey A, Trevena L. A systematic review of quality assessment methods for smartphone health apps. Telemed J E Health 2015;21(2):97-104.

66. Hilliard ME, Hahn A, Ridge AK, Eakin MN, Riekert KA. User preferences and design recommendations for an mHealth app to promote cystic fibrosis self-management. JMIR Mhealth Uhealth 2014;2(4):e44.

67. Jibb LA, Stevens BJ, Nathan PC, Seto E, Cafazzo JA, Stinson JN. A smartphone-based pain management app for adolescents with cancer: establishing system requirements and a pain care algorithm based on literature review, interviews, and consensus. JMIR Res Protoc 2014;3(1):e15.

68. Bull S, Ezeanochie N. From foucault to freire through facebook: Toward an integrated theory of mHealth. Health Educ Behav 2015.

69. Patel MS, Asch DA, Volpp KG. Wearable devices as facilitators, not drivers, of health behavior change. JAMA 2015;313(5):459-60.

70. Silow-Carroll S, Smith B. Clinical management apps: creating partnerships between providers and patients. Issue Brief (Commonw Fund) 2013;30:1-10.

71. Kumar S, Nilsen WJ, Abernethy A, Atienza A, Patrick K, Pavel M, et al. Mobile health technology evaluation: the mHealth evidence workshop. Am J Prev Med 2013;45(2):228-36.

72. Tomlinson M, Rotheram-Borus MJ, Swartz L, Tsai AC. Scaling up mHealth: where is the evidence? PLoS Med 2013;10(2):e1001382.

73. Wolf JA, Moreau JF, Akilov O, Patton T, English JC, 3rd, Ho J, et al. Diagnostic inaccuracy of smartphone applications for melanoma detection. JAMA Dermatol 2013;149(4):422-6.

74. European Commission. Summary report on the public consultation on the green paper on mobile health [En ligne]. Brussels: EC; 2015. ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-green-paper-mobile-health

75. Albrecht UV, Pramann O, Von Jan U. Medical Apps. the road to trust. Eur J Biomed Info 2015;11(3):en7-en12.

76. Bierbrier R, Lo V, Wu RC. Evaluation of the accuracy of smartphone medical calculation apps. J Med Internet Res 2014;16(2):e32.

77. Chyjek K, Farag S, Chen KT. Rating pregnancy wheel applications using the APPLICATIONS scoring system. Obstet Gynecol 2015;125(6):1478-83.

78. Huckvale K, Adomaviciute S, Prieto JT, Leow MK, Car J. Smartphone apps for calculating insulin dose: a systematic assessment. BMC Med 2015;13:106.

79. European Commission, Joint Research Centre, Gemo M, Lunardi D, Tallacchini M. Wearable sensors and digital platforms in health: empowering citizens through trusted and trustworthy ICT technology. Luxembourg: European Union; 2015.

80. Martinez-Perez B, de la Torre-Diez I, Lopez-Coronado M. Privacy and security in mobile health apps: a review and recommendations. J Med Syst 2015;39(1):181.

81. Open Web Application Security Project. OWAPS TOP 10 2013. Les dix risques de sécurité applications web les plus critiques : OWAPS; 2015.

82. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. J Am Med Inform Assoc 2014;22(e1):e28-33.

83. Conseil des académies canadiennes. L'accès aux données sur la santé et aux données connexes au Canada. Ottawa: CAC; 2015. sciencepourlepublic.ca/uploads/fr/assessments%20and%20publications%20and%20news%20releases/health-data/HealthDataExecSumFr.pdf

84. Association française de normalisation. Le livre blanc données massives - Big Data. Impact et attentes pour la normalisation. Saint-Denis: AFNOR; 2015.

85. Cruz Zapata B, Fernandez-Aleman JL, Idri A, Toval A. Empirical studies on usability of mHealth apps: a systematic literature review. J Med Syst 2015;39(2):1.

86. Arnhold M, Quade M, Kirch W. Mobile applications for diabetics: a systematic review and expert-based usability evaluation considering the special requirements of diabetes patients age 50 years or older. J Med Internet Res 2014;16(4):e104.

87. Watkins I, Xie B. eHealth literacy interventions for older adults: a systematic review of the literature. J Med Internet Res 2014;16(11):e225.

88. Monkman H, Kushniruk A. A health literacy and usability heuristic evaluation of a mobile consumer health application. Stud Health Technol Inform 2013;192:724-8.

89. Caburnay CA, Graff K, Harris JK, McQueen A, Smith M, Fairchild M, et al. Evaluating diabetes mobile applications for health literate designs and functionality, 2014. Prev Chronic Dis 2015;12:E61.

90. Collins SA, Currie LM, Bakken S, Vawdrey DK, Stone PW. Health literacy screening instruments for eHealth applications: a systematic review. J Biomed Inform 2012;45(3):598-607.

91. Georgsson M, Staggers N. Quantifying usability: an evaluation of a diabetes mHealth system on effectiveness, efficiency, and satisfaction metrics with associated user characteristics. J Am Med Inform Assoc 2015.

92. Hall AK, Cole-Lewis H, Bernhardt JM. Mobile text messaging for health: a systematic review of reviews. Annu Rev Public Health 2015;36:393-415.

93. Khoja S, Durrani H, Scott RE, Sajwani A, Piryani U. Conceptual framework for development of comprehensive e-health evaluation tool. Telemed J E Health 2013;19(1):48-53.

94. British Standards Institution. Health and wellness apps. Quality criteria across the life cycle. Code of practice. London: BSI; 2015. shop.bsigroup.com/upload/271432/PAS%20277%20(2015)bookmarked.pdf

95. Lobelo F, Kelli HM, Tejedor SC, Pratt M, McConnell MV, Martin SS, et al. The Wild Wild West: A framework to integrate mHealth software applications and wearables to support physical activity assessment, counseling and interventions for cardiovascular disease risk reduction. Prog Cardiovasc Dis 2016;58(6):584-94.

96. Brooke J. SUS - A quick and dirty usability scale [En ligne]: Usualy. gov; 1996. www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

97. Martinez-Perez B, de la Torre-Diez I, Candelas-Plasencia S, Lopez-Coronado M. Development and evaluation of tools for measuring the quality of experience (QoE) in mHealth applications. J Med Syst 2013;37(5):9976.

98. Queensland University of Technology. Mobile Application Rating Scale (MARS). App Classification. Brisbane: QUT; 2015.

99. Stoyanov SR, Hides L, Kavanagh DJ, Zelenko O, Tjondronegoro D, Mani M. Mobile app rating scale: a new tool for assessing the quality of health mobile apps. JMIR Mhealth Uhealth 2015;3(1):e27.

Toutes les publications de la HAS sont téléchargeables sur
www.has-sante.fr

 N° ISBN 978-2-11-151440-9