# DIRECTIVES DE CERTIFICATION DES APP MHONCODE

Ce document a pour but de vous aider à mettre votre application mobile en conformité avec les 8 principes du mHONcode et les tests de sécurité réalisés par notre équipe.

## 1 - AUTORITÉ

**Les détails concernant l'équipe éditoriale et l'équipe de l'application sont clairement mentionnés.**

Les noms et qualifications des membres de l'équipe responsables du développement de l'application sont indiqués.

Si l'application présente du contenu médical, les noms et qualifications des auteurs sont indiqués.

Si l'application propose un service avec un algorithme médical, les responsables (et leurs qualifications) de celui-ci sont indiqués.

Si l'auteur n'est pas un professionnel de santé, cela doit être clairement mentionné.

## 2 - COMPLEMENTARITÉ

**Mention claire des limites de l'application qui ne remplace pas la relation médecin-patient.**

L'information diffusée sur l'application doit être destinée à encourager, et non à remplacer, les relations directes entre le patient et les professionnels de santé.

Cela doit être indiqué par une mention claire et visible du type :
*« Les informations fournies sur l'app sont destinées à améliorer et non à remplacer, la relation directe entre le patient (ou utilisateur de l'app) et les professionnels de santé. »*

Il en est de même si l'application propose un service avec un algorithme médical, il doit être indiqué que les résultats de celui-ci ne se substituent pas à l'avis d'un professionnel de santé.

## 3 -CONFIDENTIALITÉ

**Déclaration expliquant toutes les exigences légales concernant la confidentialité des données personnelles.**

L'application doit respecter le nouveau Règlement Général de Protection des Données : https://www.hon.ch/fr/certification/rgpd.html

La politique de confidentialité doit être spécifique à l'application et facilement accessible, idéalement au sein de celle-ci.

Le traitement des données confidentielles de l'utilisateur de l'application doit être détaillé, notamment :

- Le consentement à la collecte des données est-il demandé au premier lancement de l'application ?
- Où sont stockées les données (sur l'application, sur la carte SD, etc)
- Les données sont-elles transmises à des tiers ?
- A quels tiers sont-elles transmises ?

## 4 - VALIDITÉ

**L'application et tous les contenus santé et légaux ont une date de dernière mise à jour.**

L'application possède une date de dernière mise à jour générale.
Les contenus légaux (Mentions légales; CGU; Confidentialité) possèdent une date de dernière mise à jour.

Dans les domaines scientifiques et médicaux, l'évolution des connaissances est très rapide, il est donc nécessaire d'indiquer la date de création du contenu ainsi que sa date de dernière mise à jour. Ainsi, si l'application possède du contenu médical, celui-ci possède une date de dernière mise à jour.
L'utilisateur doit pouvoir savoir aisément de quand datent les informations de santé qu'il consulte.

## 5 - JUSTIFIABILITÉ OBJECTIVITÉ

**L'information de santé comporte des références, elle est complète et fournie de façon objective.**

Si l'application possède du contenu médical, les références et sources des informations scientifiques et médicales sont indiquées, notamment des données statistiques sont données, même si l'auteur est un professionnel de santé.
Cela peut être indiqué sous la forme suivante, et à chaque fois que nécessaire *Auteur1, Auteur2, Auteur3, Titre, Nom du journal/article/Livre/Conférence, Année de référence, numéro de la page*
L'information est présentée de manière objective et pondérée.

Si l'application présente des traitements, médicaments et/ou chirurgies, toutes les informations concernant les contre-indications, effets indésirables, interactions, précautions d'emploi... sont présentées.

Si la recommandation d'une marque unique est donnée, le professionnel doit expliquer qu'il s'agit de sa pratique médicale et doit mentionner qu'il existe d'autres produits.
Tous les noms de marque doivent être identifiés, avec ® par exemple.

Si l'application propose un service avec un algorithme médical, l'implémentation de l'algorithme a été vérifiée, et ses références sont données.

Si l'application possède des photographies avant/après, une déclaration à ce sujet est présente : "*Les photos illustrant nos cas cliniques avant/après présentent des personnes consentantes et les mêmes patients y figurent, respectivement, pour le résultat avant/après. Ces photos n'ont pas été retouchées. Nous attirons expressément votre attention sur le fait que le résultat observé est propre à la personne concernée et qu'un résultat identique ne peut être attendu pour une autre personne, en raison de la propre individualité de chacun.*" Plus d'informations: *https://www.hon.ch/fr/paa.html*

## 6 -PROFESSIONALISME

**L'application est facile à utiliser, sa mission est claire, et l'équipe est aisément joignable.**

La mission de l'application est clairement énoncée et respectée.
L'audience de l'application est clairement énoncée (professionnels de santé ou non professionnels de santé) et respectée.
Si l'application est interdite d'usage aux mineurs, cela doit être clairement indiqué et l'application doit être conçue de telle manière que son usage par des mineurs soit impossible.

Un moyen de contact (adresse e-mail, formulaire de contact) est accessible au sein de l'application.

Des instructions pour l'utilisation sont accessibles au sein de l'application.
L'application est facilement utilisable et ne présente pas de bugs particuliers.

## 7 - FINANCEMENT

**Toutes les sources de financement et les services payants sont identifiés et transparents.**

Les sources de financement de l'application sont indiquées et détaillés.

Si l'application propose des achats intégrés, la politique à ce sujet est accessible et claire, et ces achats intégrés représentent une réelle plus-value pour l'application.

Une déclaration des liens d'intérêts est accessible si des professionnels de santé ont participé à la création du contenu de l'application. Ainsi, il doit être mentionné si les auteurs du contenu, professionnels de santé, ont des liens d'intérêts avec des entreprises de produits de santé et de cosmétiques.
Plus d'informations sur cette directive concernant les liens d'intérêts disponible ici:
*https://www.hon.ch/fr/liens.html*

## 8 - POLITIQUE PUBLICITAIRE

**Toutes les publicités sont identifiées et différenciées du contenu.**

Si l'application diffuse de la publicité :
- Celle-ci est identifiée comme telle, avec le terme "Publicité" par exemple.
- Celle-ci est clairement différenciée du contenu d'information de l'application
- Une politique publicitaire est accessible au sein de l'application,
- Les publicités type armes, pornographie, religion, dating, sont interdites.

Retrouvez en images comment identifier clairement la publicité sur votre application ici:
*https://www.hon.ch/fr/pub.html*

Si l'application ne diffuse pas de publicité, une déclaration en ce sens l'indique, par exemple *"L'application n'affiche aucune forme de publicité"*.

## TESTS SÉCURITÉ

**Détection des faiblesses et vulnérabilité.**

L'application mobile devrait minimiser les mésusages suivants
- **Utilisation incorrecte de la plate-forme** : éviter l'utilisation abusive d'une fonctionnalité de la plate-forme ou l'impossibilité d'utiliser les contrôles de sécurité de la plate-forme.
- **Stockage de données non sécurisé** : éviter le stockage de données non sécurisé et les fuites de données involontaires.
- **Communication non sécurisée** : éviter les mauvaises transmissions, les versions SSL incorrectes.
- **Authentification non sécurisée** : assurer l'authentification de l'utilisateur final en cas de besoin ou éviter une mauvaise gestion de session.
- **Cryptographie insuffisante** : s'assurer que la cryptographie est effectuée correctement.
- **Autorisation non sécurisée** : éviter les échecs d'autorisation
- **Qualité du code client** : identifier les problèmes d'implémentation au niveau du codechez le client .
- **Falsification de code** : éviter la modification de la mémoire dynamique
- **Rétro-ingénierie** : éviter de comprendre le fonctionnement interne de l'application
- **Fonctionnalité externe** : éviter d'introduire des fonctionnalités créant une porte d'entrée cachée dans le code

*Source : https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10*

## TESTS SÉCURITÉ

### Analyse du réseau d'applications. Confidentialité et cryptage.

- Les requêtes de l'application doivent être cryptées avec le protocole SSL.
- Seules les données requises doivent être transférées et utilisées. Cela empêche l'utilisation excessive de la bande passante et les fuites de données.
- L'authentification (login / mot de passe) doit être cryptée.
- Seules les autorisations requises (caméra, géolocalisation, accès Internet) doivent être demandées.
- La transmission des données de l'utilisateur (y compris l'adresse IP) à des tiers doit se faire après accord explicite de l'utilisateur.

## TESTS SÉCURITÉ

### Auto-évaluation RGPD.

L'application mobile doit respecter le nouveau Règlement Général sur la Protection des Données:

- Les données recueillies (par vous ou par un tiers) doivent l'être avec le consentement explicite de l'utilisateur.

- Utilisez l'auto-évaluation RGPD pour identifier les améliorations à apporter à vos services afin d'être conforme au RGPD : *https://www.hon.ch/fr/certification/rgpd.html#autoevaluation*

Notre équipe se tient à votre entière disposition pour vous accompagner dans la mise en conformité mHONcode de votre application.

N'hésitez pas à nous contacter par email updateNF@healthonnet.org