# mHONCODE APP CERTIFICATION GUIDELINES

This document is intended to help you bring your mobile application into compliance with the 8 principles of the mHONcode and the security tests performed by our team.

## 1 - AUTHORITY

**Details about the editorial team and the application team are clearly disclosed.**

The names and qualifications of the team members responsible for developing the application are indicated.

If the application contains medical content, the names and qualifications of the authors are indicated.

If the application offers a service with a medical algorithm, the persons responsible (and their qualifications) for it are indicated.

If the author is not a health professional, this must be clearly stated.

## 2 - COMPLEMENTARITY

**Clear mention of the limits of the application which does not replace the doctor-patient relationship.**

The information disseminated on the application should be designed to encourage, and not replace, direct relationships between the patient and health professionals.

This must be indicated by a clear and visible statement such as: "*The information provided on the app is intended to improve, not replace, the direct relationship between the patient (or app user) and healthcare professionals.*"

The same applies if the application offers a service with a medical algorithm, it must be indicated that the results of the algorithm do not replace the opinion of a health professional.

## 3 -CONFIDENTIALITY

Statement explaining all legal requirements regarding the confidentiality of personal data.

The application must comply with the new General Data Protection Regulation: https://www.hon.ch/en/certification/gdpr.html

The privacy policy must be application-specific and easily accessible, ideally within the application.

The treatment of confidential data of the application user must be detailed, including:

- Is consent to data collection required at the first launch of the application?
- Where the data is stored (on the application, on the SD card, etc.)
- Is the data transmitted to third parties?
- To which third parties are they transmitted?

## 4 - VALIDITY

**The application and all health and legal content have a last update date.**

The application has a date of last general update.

The legal content (Legal Notice; Terms and Conditions; Privacy Policy) has dates of last update.

In the scientific and medical fields, the evolution of knowledge is very rapid, and thus, it is necessary to indicate the dates of creation of the content as well as its last update. Thus, if the application has medical content, it has to have a date of last update.

The user must be able to easily know how current the health information is.

## 5 - JUSTIFIABILITY OBJECTIVITY

**Health information has references, is complete and provided in an objective manner.**

If the application has medical content, the references and sources of scientific and medical information should be indicated, including statistical data, even if the author is a health professional.
This can be indicated in the following form, and whenever necessary: *Author1, Author2, Author3, Title, Name of journal/article/Book/Conference, Reference Year, page number.*

The information should be presented in an objective and balanced manner.

If the application contains treatments, drugs and/or surgeries, all information concerning contraindications, adverse reactions, interactions, precautions for use... should be presented.

If the recommendation of a single brand is given, the professional must explain that this is the brand he recommends practice and must mention that there are other products.
All brand names must be identified, for example with ®.

If the application offers a service with a medical algorithm, the implementation of the algorithm should have already been checked and verified, and its references given.

If the application has before/after photographs, a statement on this subject should be provided: "*The images displayed have been published following full consent from all persons in these photographs. Before and After photos show the same person in both instances. These photos have not been retouched in any way. We expressly draw your attention to the fact that the observed result is specific to the person concerned and that an identical result cannot be expected for another person, because of the individuality of each person.*"

## 6 -USER'S PRACTICE

**The application is user friendly, its mission is clear, and the team is easily reachable.**

The mission of the application should be clearly stated and respected.

The application's audience should be clearly stated (health professionals or non-professionals) and respected.
If the application is prohibited for use by minors, this must be clearly indicated and the application must be designed in such a way that its use by minors is impossible.

A contact method (e-mail address, contact form) should be easily visible and available within the application.

Instructions for use should also be provided within the application and the application should be easy to use without any bugs.

## 7 - FINANCIAL DISCLOSURE

All funding sources and paid services are identified and transparent.

The sources of funding for the application should be indicated and detailed.

If the application offers integrated purchasing, the policy on this subject should be accessible and clear, and these integrated purchases should represent a real added value for the application.

A declaration of links of interest must be available if health professionals have been involved in creating the content of the application. Thus, it must be mentioned whether the authors of the content, health professionals, have links of interest with health products and cosmetics companies.

More information on this directive on interest links is available here:
*https://www.hon.ch/en/links.html*

## 8 - ADVERTISING POLICY

All ads are identified and clearly separated from content.

If the application spreads advertising:

- This is identified as such, with the term "Advertising" for example.
- This is clearly differentiated from the application's information content
- An advertising policy is accessible within the application,
- Advertisements such as weapons, pornography, religion, dating, are prohibited.

See below for images on how to clearly identify the advertising on your application here:
*https://www.hon.ch/en/ai.html*

If the application does not advertise, a statement to that effect should indicate this. For example "*The application does not display any form of advertising*".

## SECURITY TESTS

Detection of weaknesses and vulnerabilities.

The mobile app should minimize the following misuse:

- **Improper Platform Usage**: avoid misuse of a platform feature or failure to use platform security controls.
- **Insecure Data Storage**: avoid insecure data storage and unintended data leakage.
- **Insecure communication**: avoid poor handshaking, incorrect SSL versions
- **Insecure authentication**: ensure authenticating the end user when needed or avoid bad session management.
- **Insufficient Cryptography**: ensure that cryptography is done correctly.
- **Insecure Authorization**: avoid any failures in authorization
- **Client Code Quality**: catch-all for code-level implementation problems in the mobile client.
- **Code tampering**: avoid dynamic memory modification
- **Reverse engineering**: avoid insight the inner workings of the application
- **Extraneous Functionality**: avoid hidden backdoor functionality

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

SECURITY TESTS

## Analysis of the application network. Privacy & Encryption.

- Application requests/queries must be encrypted with SSL protocol.
- Only required data must be transferred and used. It prevents excessive bandwidth usage and data leaks.
- Authentication (login /password) should be encrypted
- Only required permissions (camera, location, internet access) must be asked.
- Transmission of user data (including IP address) to third party should be done after explicit consent of the user

SECURITY TESTS

## GDPR checklist

The mobile application must comply with the new General Data Protection Regulations:

- Gathered Data (by you or a tier) must be done with explicit consent of the User.

- Use the GDPR check list to identify the improvement necessary to your services in order to be compliant with the GDPR : https://www.hon.ch/en/certification/gdpr.html#selfassessment

Our team is at your entire disposal to assist you in bringing your health mobile app into mHONcode compliance.

Feel free to contact us by email updateNF@healthonnet.org