|  |  |  |
| --- | --- | --- |
| ITU Logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | FG-AI4H-N-043 |
| **ITU-T Focus Group on AI for Health** |
| **Original: English** |
| **WG(s):** | Plenary | E-meeting, 15-17 February 2022 |
| **DOCUMENT** |
| **Source:** | Editors DEL9.1 |
| **Title:** | DEL9.1 Update: Mobile Applications |
| **Purpose:** | Discussion |
| **Contact:** | Manjeet Singh ChalgaICMR, New DelhiIndia | Tel: +91-9582776792Email: chalgams.hq@icmr.gov.in  |
| **Contact:** | Khondaker A MamunCMED Health Ltd., DhakaBangladesh | Tel: +88017 7653 4220Email: mamun@cmed.com.bd  |
| **Contact:** | Aveek DeCMS – Social Impact Specialists, BangaloreIndia | Tel: Email: aveek@cms-india.org  |
| **Contact:** | Prashant ChughRakesh Singh RawatHimani GandhiSameer RanjanBidisha MandalC-DOT,New Delhi India | E-mail: prashant@cdot.inE-mail: rakeshr@cdot.inE-mail: himani@cdot.inE-mail: sameer@cdot.inE-mail: bidisham@cdot.in |

|  |  |
| --- | --- |
| **Abstract:** | Usage of AI in analysis of health-related problems is a game changer and inevitable. On the other hand, with privacy preservation of personal data and security of communication a major design concerns, any AI tool in the health domain needs to be carefully designed and commissioned. This document proposes a draft of set of provisions an AI tool with the Security concerns, should ensure. These requirements pertain not only to the capabilities of the tool, also to its testing and benchmarking. Globally, privacy regulations have become stringent. Hence, there is a need for enhanced privacy and security in health related mobile applications as well. |

This document also invites Medical & AI researchers to collaborate in development of Mobile Application based Secure AI tools for Health within the International Telecommunication Union (ITU)/World Health Organization (WHO) Focus Group on “Artificial Intelligence for Health” (FG-AI4H).

**Introduction:**

Even after 60 years of rising of artificial intelligence (AI), its use in resource-poor countries is relatively less as compared to developed countries [1]. The use of AI in Mobile Applications is growing rapidly [2]. It was estimated in the beginning of 2019, that more than 5 billion people have mobile devices worldwide, and more than half of these devices were smartphones [3]. The healthcare mobile apps have a significant positive impact on health and health care, however, there is a challenge for patients and clinicians to find a confirmed product among infinite choice of unproven mobile applications [4]. Apart from this, breach in privacy of the patient’s data also prevents such application from becoming a widely acceptable product in the healthcare domain [13][14]. Thus, there is a wide scope for development of reliable and Secure AI based Mobile Applications for healthcare within the sphere of International Telecommunication Union (ITU)/World Health Organization (WHO) Focus Group on “Artificial Intelligence for Health” (FG-AI4H).

**Objectives:**

The objectives of the topic groups are:

1. to prepare the rules for development of Secure AI tool for Health using Mobile Applications
2. to discuss the privacy preservation concerns for the data management within the Mobile Application
3. to discuss the schemes for secure communication within the mobile application framework
4. to discuss the regulatory/ethical rules for Mobile Apps with AI for Healthcare
5. to provide a forum for open communication among various stakeholders,
6. to develop benchmarking for the Apps,
7. to coordinate the complete process in collaboration with the Focus Group management

and working groups.

**Basic rules for development of Secure AI tool for Health using Mobile Application:**

The desired key features for development of an AI tool using mobile application are that it should attract the attention of the user, serve the desires of the user and develop the faith of the user with the tool. Giving due importance to Privacy Preservation, the application shall also ensure that the privacy of the users’ data is maintained. Some desirable features/ rules may be followed as detailed below:

1. Simple Registration [5]:

Registration may be kept as simple as possible. Login may be allowed with user’s existing Facebook/ Google ID/ similar system.

1. Minimal Introduction [5]:

The introduction should not be imposed on the user. However, complete introduction may be provided on demand of the user.

1. Training/ Instructions [5]:

The user should be informed about the importance of the data required for the working of the AI tool before collection of data. The user must be explained why permission to access the camera, geolocation or similar features of mobiles are being asked.

1. Privacy Preservation [6]:

The data sent for inference should be encrypted so as to protect the privacy of the user, and the inference on the model should be done using the same encrypted data which can be achieved by using homomorphic encryption based Privacy Enhancing Technology (PET)

1. Simplified user interface [5]:

All the features which are available in the desktop website version of an AI tool should be intelligently made simpler and key functions of the tool.

1. Functionality [7]:

The mobile applications should be developed keeping in view the desired features of application, target audience and the distribution channel such as Google Play, Apple App store etc. Some key points are as follows:

* Verify accessibility in respect of compatibility with mobile platforms, user friendly language, easy to use and affordability
* Confirm that mandatory fields are being collected, format of data and display of data is correct
* Proper error handling and relevant error messages
* User-friendly console of the App, appropriate size of the buttons and user manual for users
* Collection of text information should be minimized and use of checkboxes/ radio buttons should be increased.
* The font size should be clear enough to read and to select the desired option
1. Performance [7]:

Some key points for validation of the performance of mobile applications are as follows:

* The client server communication should work properly at peak, average and minimum user levels
* Identify the bottlenecks which prevent the application to perform at the required acceptability levels.
* Identify optimum response time of the app
* Identify the optimum mobile device requirement for the app
* Identify optimum performance of resources such as GPS, Camera, Battery etc in various situations
1. Security Validation:

The security of mobile applications should be validated. Some key points are as follows:

* Enforce secure communication by applying signature-based permissions, disallow access to your app's content, ask for credentials before showing sensitive information etc. [8]
* Apply network security measures by using SSL communication, applying network security configuration and creating your own trust manager [8].
* Use privacy preservation methods which provides additional security to the clients’ data [6].
* Use the best Cryptography Tools and Techniques [8].
* Get security audit of Mobile App
* Design App for handling data overflow
* Privacy policy should not be copied
* SDK may be used in place of NDK
* Encryption Key of at least 128 bits may be used
1. Positive Discontinuation [5]:

If a user wishes to discontinue the use of AI tool, he/she may be allowed with clear guidelines on how to discontinue and with a simple feedback procedure.

**Regulations for Secure Mobile Apps with AI for Healthcare**

A product that meets the definition of a medical device falls within the purview of the FDA and is then subject to regulation before and after it is marketed [8]. Section 201(h) of the Federal Food Drug & Cosmetic (FD&C) Act defines a device as “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals.. ..”. If the App is a medical device, then it must be evaluated whether the developer meets applicable regulations in offering the product to the public.

When an App draws data from a medical device, it is considered as accessory to that medical device, thus, are regulated according to regulations of parent device. If the app creates a new property or function that the parent device does not have, such apps might fall into Class-III classification and regulated accordingly.

**Ethical issues [11]**

There are 17 principles mentioned in the “ICMR - National Ethical Guidelines for Biomedical and Health Research Involving Human Participants”. According to Principle of essentiality, the use of human participants should be duly vetted by an ethics committee (EC) independent of the proposed research. According to Principle of professional competence, the app must be developed in consultation with medical experts and contain accurate medical information.

The researcher should not have conflict of interest, such as participant’s welfare or financial interest etc. Efforts should be made to communicate the findings of the research study to the individuals/communities wherever relevant. All members of a research team are expected to maintain high standards and to uphold the fundamental values of research. Unethical behaviour in scientific research can destroy the public’s trust in science and have a negative impact on the research team. The researcher must ensure that the patient records is secured and will not be shared with third parties, such as medical institutions, insurance companies, advertisers etc. An ethical framework based on equality and equity is required for international collaboration, due to different levels of development in terms of infrastructure, expertise, social and cultural perceptions, laws relating to IPR, ethical review procedures, etc. There is a need to follow all the guidelines related to Ethics issues before designing a research study.

**Call for Topic Group Participation in AI4H applications and platforms: Mobile Applications**

The International Telecommunication Union (ITU)/World Health Organization (WHO) Focus Group on “Artificial Intelligence for Health” (FG-AI4H; https://www.itu.int/go/fgai4h) seeks engagement from members of the medical and artificial intelligence (AI) communities to collaborate in development of Secure Mobile Application based AI tools for Health.

**References**

1. “Artificial Intelligence in Healthcare”. Wikipedia. <https://en.wikipedia.org/wiki/Artificial_intelligence_in_healthcare>
2. Hasnain Haider K Niazi . “Artificial Intelligence (AI) Impact on Mobile Apps”. Becoming Human: Artificial Intelligence Magazine. <https://becominghuman.ai/artificial-intelligence-ai-impact-on-mobile-apps-7a2c44a77bc8>
3. Laura Silver. “Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally”. Pew Research Centre. <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/>
4. Larson R. S. (2018). A Path to Better-Quality mHealth Apps. JMIR mHealth and uHealth, 6(7), e10414. doi:10.2196/10414
5. “Mobile App UX Design Principles” <https://www.altexsoft.com/blog/mobile/mobile-app-ux-design-principles-15-rules-for-creating-apps-that-stick/>
6. “Homomorphic Encryption”. Wikipedia. https://en.wikipedia.org/wiki/Homomorphic\_encryption
7. “Mobile Apps Testing: Sample Test Cases & Test Scenarios”.Guru99. <https://www.guru99.com/testing-mobile-apps.html>
8. “Apply network security measures”. Android Developer Documentation. <https://developer.android.com/topic/security/best-practices>
9. Roth V. North Carolina Journal of Law and Technology. [2018-03-13]. “The mHealth Conundrum: Smartphones & Mobile Medical Apps - How Much FDA Medical Device Regulation Is Required” <http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1245&context=ncjolt>.
10. “Is the product a Medical Device”. U.S. Food & Drug Administration. [https://wayback.archive-it.org/7993/20190911151538/https://www.fda.gov/medical-devices/classify-your-medical-device/product-medical-device](https://wayback.archive-it.org/7993/20190911151538/https%3A//www.fda.gov/medical-devices/classify-your-medical-device/product-medical-device)
11. Accessory Regulation in mHealth, EPSTEIN BECKER & GREEN, P.C., (May 10,2011), <http://mhealthregulatorycoalition.org/wp-content/uploads/2010/06/mrcaccessguiddraft.pdf>
12. “National Ethical Guidelines For Biomedical And Health Research Involving Human Participants” developed by Indian Council of Medical Research, New Delhi, India. https://www.icmr.nic.in/sites/default/files/guidelines/ICMR\_Ethical\_Guidelines\_2017.pdf
13. Kocabaş, Övünç & Soyata, Tolga. (2015). “Medical Data Analytics in the Cloud Using Homomorphic Encryption”. 10.4018/978-1-4666-8756-1.ch038.
14. M. A. Sahi et al., "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," in IEEE Access, vol. 6, pp. 464-478, 2018, doi: 10.1109/ACCESS.2017.2767561.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_