|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2022-2024 | | FG-AI4H-Q-047 | |
| **ITU-T Focus Group on AI for Health** | |
| **Original: English** | |
| **WG(s):** | | Plenary | Douala, 6-9 December 2022 | |
| **DOCUMENT** | | | | |
| **Source:** | | Editor DEL9.1 | | |
| **Title:** | | Updates on DEL9.1 - Mobile Applications | | |
| **Contact:** | | Manjeet Singh Chalga ICMR, New Delhi India | | Tel: +91-9582776792 Email: [chalgams.hq@icmr.gov.in](mailto:chalgams.hq@icmr.gov.in) |
| **Contact:** | | Khondaker A Mamun CMED Health Ltd., Dhaka Bangladesh | | Tel: +88017 7653 4220 Email: [mamun@cmed.com.bd](mailto:mamun@cmed.com.bd) |
| **Contact:** | | Prashant Chugh  Rakesh Singh Rawat  Himani Gandhi  Sameer Ranjan  Bidisha Mandal  C-DOT, New Delhi  India | | E-mail: [prashant@cdot.in](mailto:prashant@cdot.in)  E-mail: [rakeshr@cdot.in](mailto:rakeshr@cdot.in)  E-mail: [himani@cdot.in](mailto:himani@cdot.in)  E-mail: [sameer@cdot.in](mailto:sameer@cdot.in)  E-mail: [bidisham@cdot.in](mailto: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:**

The mobile application based on health concern are increasing globally. In 2018, mobile application market for health is predicted to be valued at US$28.320 billion and is estimated to touch US$102.35 billion by 2023, growing at a compounded annual growth rate of 29.30%[1]. As per Statista, 52,565 healthcare apps were available on the Google play store and 51,320 apps were available at Apple App Store in the first quarter of 2022 [2].

However use of artificial intelligence(AI) in resource-poor countries is relatively less as compared to developed countries [3]. The use of AI in Mobile Applications is growing rapidly [4]. 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 [5]. 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 [6]. 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 [7][8]. 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 understand development of Secured AI tool for Health using Mobile Applications
2. to discuss the regulatory/ethical rules for Mobile Apps with AI for Healthcare
3. to discuss on technology, security and legal issues related to these AI tools,
4. 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 a 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 [9]:

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

1. Minimal Introduction [9]:

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

1. Training/ Instructions [9]:

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 [10]:

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 [9]:

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

1. Functionality [10]:

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 [10]:

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. [11]
* Apply network security measures by using SSL communication, applying network security configuration and creating your own trust manager [11].
* Use privacy preservation methods which provides additional security to the clients data[12].
* Use the best Cryptography Tools and Techniques [11].
* 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 [9] :

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.

**Classification of Mobile Applications:**

Mobile Applications can be classified as Native App, Web App and Hybrid App depending upon the measures used for development of the Mobile Application.

1. **Native apps**

The Mobile Applications developed for one specific platform or operating system may be classified as Native Apps[13]

Advantages of Native Apps[13]

* Native Apps are Faster and perform better
* It has Native UI
* Native Apps can access device features like camera, Bluetooth, etc.

Disadvantages of Native Apps[13]

* Its maintenance is costly
* It utilizes the space in Device
* Updates are need to be installed time to time.

1. **Web Apps**

Websites delivered using a mobile browser are known as Web Apps. Web apps are responsive versions of websites that can work on any mobile device or OS [13].

Advantages of Web Apps [13]

* Web-based apps can perform on all mobile devices and operating systems
* As these apps are responded by web server, their maintenance is easy
* It don’t consumes space of device

Disadvantages of Web Apps [13]

* It is dependent on browser
* It cannot work offline, internet connection is required to run these Apps
* It cannot be integrated with device hardware

1. **Hybrid Apps**

Hybrid apps are combinations of both native and web apps, but wrapped within a native app. Thus, it gives the ability to be downloaded from an app store with its own icon [13].

Advantages of Hybrid Apps [13]

* Can be built quickly and less costly
* Its loads quickly on devices
* It requires less code for maintenance

Disadvantages of Hybrid Apps [13]

* It has less powers as compared to Native Apps
* Sometimes it slows down as it has to download each element
* Certain features may not be usable on devices

**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 [11]. 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 a 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.

**Mobile App Security:**

1. Security Measures:

When creating a medical mobile app, publishers (and developers) need to be aware of whether or not their app requires compliance with specific regulations differ from region to region [14].

1. Analyzing Security:

Despite being better aligned with security best practices than non-mHealth apps, mHealth apps are still far from ensuring robust security guarantees [15].

Like all mobile applications, medical apps face serious threats from cyber criminals and data hackers who target devices / users in the telehealth, medical device, health commerce, and COVID-tracking segments. Data theft groups are targeting Patient-generated health data (PGHD) with code injections / SQL injections, errors and cross-site scripting [16].

1. Cryptographic Test:

91% of medical apps have weak encryption that puts them at risk for data exposure and IP theft. This means the encryption used in these medical apps can be easily broken by cybercriminals, potentially exposing confidential PGHD, and enabling attackers to tamper with reported data, send illegitimate commands to connected medical devices, or otherwise use the application for malicious purposes. [16].

* 71% of tested medical apps have at least one high-level security vulnerability.
* 34% of Android Apps and 28% of iOS Apps Are Vulnerable to Encryption Key Extraction.

1. Patient Information Security

Mobile health (mHealth) apps must make sure the data they are collecting is secure from hackers, malware and other external threats and they must maintain the integrity, availability, confidentiality and resilience of the data [17]. In December 2016, HIMSS co-founded the Xcertia initiative with the \*\*\*American Medical Association (AMA), American Heart Association (AHA), and DHX Group. Xcertia aimed to develop a framework of guidelines to promote safe and effective mobile health apps for healthcare [18].

1. Other areas key to app security [17]:

• Vulnerability management

• Systems and communication protection

• Compliance

• Access control and authentication

• Asset management

• Physical and environmental security

• Incident response

• Disaster recovery and business continuity

**Ethical issues [19][20][21][22]**

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. Mobile Health (mHealth) App Market 2017-2023 (<https://www.globenewswire.com/news-release/2017/12/15/1262662/0/en/Mobile-Health-mHealth-App-Market-2017-2023-by-App-Type-Service-Connected-Medical-Device-Geography.html>)
2. Statistica (https://www.statista.com/)
3. “Artificial Intelligence in Healthcare”. Wikipedia. (<https://en.wikipedia.org/wiki/Artificial_intelligence_in_healthcare>)
4. 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>)
5. 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/>)
6. Larson R. S. (2018). A Path to Better-Quality mHealth Apps. JMIR mHealth and uHealth, 6(7), e10414. doi:10.2196/10414
7. Kocabaş, Övünç & Soyata, Tolga. (2015). “Medical Data Analytics in the Cloud Using Homomorphic Encryption”. 10.4018/978-1-4666-8756-1.ch038.
8. 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.
9. “Mobile App UX Design Principles” (<https://www.altexsoft.com/blog/mobile/mobile-app-ux-design-principles-15-rules-for-creating-apps-that-stick/>)
10. “Mobile Apps Testing: Sample Test Cases & Test Scenarios”.Guru99. (<https://www.guru99.com/testing-mobile-apps.html>)
11. “Apply network security measures”. Android Developer Documentation. (<https://developer.android.com/topic/security/best-practices>)
12. “Homomorphic Encryption”. Wikipedia. (https://en.wikipedia.org/wiki/Homomorphic\_encryption)
13. CleverTop : What Are the Different Types of Mobile Apps? And How Do You Choose? (<https://clevertap.com/blog/types-of-mobile-apps/>)
14. SteelKiwi : How to Build a Secure Medical Mobile App in Six Steps (<https://steelkiwi.com/blog/how-to-build-secure-medical-mobile-app-six-steps/>)
15. Tangari G, Ikram M, Sentana IWB, Ijaz K, Kaafar MA, Berkovsky S. Analyzing security issues of android mobile health and medical applications. J Am Med Inform Assoc. 2021 Sep 18;28(10):2074-2084. doi: 10.1093/jamia/ocab131. PMID: 34338763; PMCID: PMC8449631. (<https://pubmed.ncbi.nlm.nih.gov/34338763/>)
16. AIThority : 71% of Healthcare Medical Apps Have a Serious Vulnerability; 91% Fail Crypto Tests (<https://aithority.com/ait-featured-posts/71-of-healthcare-medical-apps-have-a-serious-vulnerability-91-fail-crypto-tests/>)
17. AMA : How to keep patient information secure in mHealth apps (<https://www.ama-assn.org/practice-management/digital/how-keep-patient-information-secure-mhealth-apps>)
18. ANI : Xcertia Transitions to Health App Guidelines Work Group (<https://www.allianceni.org/initiatives/xcertia>)
19. 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>.)
20. “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>)
21. Accessory Regulation in mHealth, EPSTEIN BECKER & GREEN, P.C., (May 10,2011), (<http://mhealthregulatorycoalition.org/wp-content/uploads/2010/06/mrcaccessguiddraft.pdf>)
22. “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)

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