**The technological, organizational and environmental determinants of adoption of mobile health applications (m-health) by hospitals in Kenya**

Link: [The technological, organizational... preview & related info | Mendeley](https://www.mendeley.com/catalogue/4f5aa373-114d-3ac0-ab0c-2a6d143f1a12/)

(page 2-3)

WHO defines m-health as the use of any wireless technology or portable device by health providers to enable communication between patients and health services, for consultation between health care professionals, for health monitoring and surveillance, for access to information for health care professionals at point of care.

(page 2-3)

PC m-health applications aim to facilitate communications and data between patients and health providers while FC m-health applications mostly facilitate communications and data between healthcare providers.

(page 4)

This study thus investigated the following 5 constructs as part of environmental determinants of m-health adoption: 1) level of competition and rivalry at country level, effect of global medical tourism 2) government pressure or incentives 3) **patient pressure** 4) **support or resistance from medical professional associations**, and 5) **support or resistance from health insurance companies**.

Positive perceptions of government regulations and incentives will lead to adoption of m-health than negative perceptions**. Perceptions of patients’ readiness and pressure to use m-health will lead to more adoption. Similarly support of m-health by professional associations (doctors, nurses and community health workers) and health insurance companies will lead to m-health adoption.**

**A Mobile App Development Guideline for Hospital Settings: Maximizing the Use of and Minimizing the Security Risks of "Bring Your Own Devices" Policies**

Link: [JMIR mHealth and uHealth - A Mobile App Development Guideline for Hospital Settings: Maximizing the Use of and Minimizing the Security Risks of "Bring Your Own Devices" Policies](https://mhealth.jmir.org/2016/2/e50/)

From our research and subject matter interviews externally and internally to BCH, we created 14 practical recommendations for the BCH BYOD guideline. [Table 1](https://mhealth.jmir.org/2016/2/e50/#table1) describes each recommendation and how it relates to developing a mobile app.

| No. | Risks | Guidelines and Recommendations |
| --- | --- | --- |
| 1 | Unauthorized access to app and decreased productivity | Adopt enterprise-standards but usable authentication |
| Implement RBACa |
| 2 | **Unauthorized access to data** | **Implement at least three layers of security on data transmission (transport layer security, access control, and content security)** |
| **Allow apps to work on internal networks or VPNb only** |
| 3 | **Data transmission to unauthorized parties** | **Protect the mobile app’s notifications** |
| 4 | **Unauthorized access to apps and data** | **Prevent apps from working on jail-broken devices** |
| **Allow apps to only work on encrypted-devices or devices with pass-codes** |
| 5 | Unauthorized access to data | Require apps to use minimal cache |
| 6 | **Unauthorized access to the app** | **Enforce automatic logoff** |
| 7 | **Data transmission to unauthorized parties** | **Limit copy data and print screen functionalities** |
| Limit backup on Cloud services |
| 8 | App distribution to unauthorized parties | Distributing the app: Implement internal over-the-air installation and app updates |
| 9 | **Unauthorized access to app** | Implement remote wipe out functionality |
| **Implement ability to disconnect and block a user anytime** |

**Adopt Enterprise-Standards With Convenient Authentication**

User verification is a crucial component of secured systems, especially for medical-related systems. The verification provides access to valuable information and offers personalized services. Most health care systems require individual and enterprise standard authentication with the ability to time-out a user after a period of inactivity. The enterprise authentication procedure at times requires at least three combinations of keyboards (alphabet, numbers, and special characters) that can be cumbersome to switch between when using a mobile device. Because productivity is impaired by these hassles, this barrier should be minimized for clinicians. Designing an authentication process that complies with the required security standards, while still being usable and convenient, should be built into the app.

**Implement Role-Based Access Control**

Within an organization, are created for various job functions. The permissions and security measures to perform certain operations and access specific features within an app should be assigned based on roles. Employees are assigned particular roles, and through role assignments acquire computer permissions to perform particular computer-system functions. This is widely recognized as role-based access control (RBAC) and has been endorsed by the US government [22,23]. RBAC simplifies security management by providing a role hierarchy structure that eventually reduces a business risk caused by complex user management.

**Prevent Apps From Working on Jail-Broken Devices**

Jail breaking is a process used to modify the operating system running on a device. The process includes removing standard-imposed security and restrictions, allowing unsecured or illegal operations, such as installing malicious code or data sniffing code. The jail-breaking process may also cause a device to function incorrectly or stop working. Therefore, including a requirement that health care apps should not operate or function on jail broken devices is mandatory.

**Allow Apps to Only Work on Encrypted-Devices or Devices With Pass-Codes**

Ideally, in the case where protected medical data has been accessed by unauthorized parties, the data still has one more layer of protection: encryption. The parties will not understand the encrypted data without a proper key to open it. When protected medical data is stolen and not encrypted, the general attorney’s office may get involved. Under certain circumstances, data breaches of unencrypted protected medical data are required to be reported to the general attorney’s office. In 2009, the US Government enacted the Health Information Technology for Clinical Health Act (HITECH) that requires health care organizations to notify patients if their health records have been compromised. Therefore, preventing the apps from being installed on unencrypted devices is of paramount importance.

**Require Apps to Use Minimal Cache**

A cache is a temporal repository for stored data that is used to expedite the process of retrieving data from remote storage. Retrieving data can be quicker because an app will check the cache for previously stored information without having to recompute or refetch the data from its original remote locations (eg, database server). While there are many reasons for using cache in app design, the security threat caching presents is high when handling PHI. Caching increases the risk of unauthorized parties being able to access stored sensitive information. When designing a mobile app within a BYOD environment, it is recommended to use cache in a limited capacity while ensuring quick app performance.

**Patient’s Intention to Use Mobile Health App**

Link: [(PDF) Patient’s Intention to Use Mobile Health App (researchgate.net)](https://www.researchgate.net/publication/333432120_Patient's_Intention_to_Use_Mobile_Health_App)

**(page 16 Conclusion)**

**Perceived Usefulness, perceived ease of use and subjective norms are the factors selected for this study. Based on the analysis of data generated from 300 data via SmartPLS, the statistical results indicate that these three factors have a significant positive relationship with the intention of patients to use the mobile health app.**

**A Research on the Classification and Applicability of the Mobile Health Applications**

**International**

Link: [jpm\_10\_00011\_pdf.pdf (amazonaws.com)](https://com-mendeley-prod-publicsharing-pdfstore.s3.eu-west-1.amazonaws.com/001e-PUBMED/10.3390/jpm10010011/jpm_10_00011_pdf.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEC0aCWV1LXdlc3QtMSJHMEUCIQCEfMUQApMDYcISl9K4m1LAuohVDNK7gMDCNrc%2BB7tvJwIgYFobXzAKAc1ZFzd8qQck%2BurfajLz0l2tg8tBkjyJKHAqgwQIVhADGgwxMDgxNjYxOTQ1MDUiDK3sStVG8XHat2agUyrgA3ZHC7uyLcjYKHtba9sjrRzsePkl4cmtpvd8D4vl9YNxScaCDmBgJ0BP3wCI%2B05u1V5gAjfqo9feCwVXFEiCthhi8w20lJ27iTxOH4eTkqSPFhr5Q0zSmTjDPZrRH0ZUms%2BPj5xxyjav1ZIPe%2BGv3z2sN652fCgoB%2Fb1CmpwC5VJ4zbbJMAZkyX16f6YlwimovZuxHXNSQALQnZGP9mQIznRRia4NidruLK2ru0DkQGirT8zA9sznDbum1gvpsEWAB4L3Vq3gNc8TmjuGygpD7u46An5bHVDANqZNXqE5N9%2BONy%2BypO2GQgs65odIazR2ZW1oJnT0FsMA89B0JIqoCcbml49kFE28yhu7yCuLuWDs9bDncpbNbLI%2FU8Q2ss7pOpeWs8G0KXDwTe4L6baz7iZF63dEltm9E%2FpyVcGhVtFJbgvwSSRkGPQ5B24mF6nXlX%2FO1Fbzt4Z7X54y0fTjVfbFzfyV1k9w62HreEQfwfV%2FsqAn3Cp4RZ0OKpaJqbPyfTE9hL7WJr944lciu5Ze2ed5YZs3GD3UeM%2FhON0tJIdbj73xQVpSRLTEP4h8goBn9F6fQ%2B72yGHz41MCfkwo85lnWw8tc87vSS9Gdd6f9vOwe0AKp0TvLn%2FEBm4gOpo8TCQ0OeIBjqlAR72XhSeJAkcnI65MeUA5Royfw1yc5VIXVnbM%2FtOe4lOjndkK1qSDPgxwk437nuOY9Zce7no25Og7iffWn4QgMQRh%2FjrWxRl9xZHzPAIanZfuyZfAsbbG33PwHIUaRyQdWG8xd5aNq%2F0XEv8hugKMfdqM2QR0%2FUOaZd4WdFJd%2BXxDjKmPwIgXHp%2BY1fudX7HvKvxLZqWw2bjQwNiOejh3mEc9cwJYg%3D%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20210816T071846Z&X-Amz-SignedHeaders=host&X-Amz-Expires=300&X-Amz-Credential=ASIARSLZVEVEZGIIMRFQ%2F20210816%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Signature=bdaa29b09b4f58f6b84616b114aec802aa12fb3259a47193d7878c8e7d59022a)

**(Page 18)**

**Another relevant functionality is the possibility to consult PHR, as presented in Figure 4. These mobile applications can be divided into mobile apps which enable the consulting of symptoms and PHR. The most crucial point of these applications is the security of information accessibility as this information contains relevant patient’s data. Security is a significant challenge related to the lower acceptance of mobile applications in medical communities. Therefore, mobile applications should be validated and tested before their availability in the market.**

**(Page 21)**

**The use of mobile devices will continuously improve healthcare. Therefore, mobile health applications are a vital part of the relation between health and technology.**

**Where should mobile health application providers focus their goals?**

**International**

Link: [Where should mobile health applic... preview & related info | Mendeley](https://www.mendeley.com/catalogue/5246ed9e-b352-312f-a043-82394e2437fd/)

**(Page 10-11)**

**Somewhat surprisingly, user’s value having fewer distractions the most. However, because young people are very averse to being interrupted by useless information, it is reasonable that having fewer distractions is such a high priority for them. Therefore, efforts should be made to ensure that there is no distracting information (advertisements, ambiguous information, etc.) in the content provided. If such information must be added because of commercial interests, we should consider the form of the advertising and try our best to add only a small amount of soft advertising. The second most important indicator is security. Therefore, developers need to take effective measures to protect the privacy of users. Developers should reduce system vulnerabilities, improve security, and prevent the system from being breached by criminals. The third most important indicator is utility, which provides information to solve problems faced by users and provides reliable suggestions to users. Utility is the most basic requirement for mobile health apps. If a mobile health app does not have utility, it does not matter how well the app performs in other respects. Therefore, enterprises need to integrate internal and external high-quality resources to improve service quality. The fourth most important indicator is reliability: the source of content must be authoritative and reliable and must clearly label who is the diagnostician and whether that person has the relevant qualifications. Reliability is the basis for achieving utility. Only information provided from a reliable source can instill in users a sense of security and help them find the right professional in case of an accident. The fifth most important indicator is navigability: the system should have a simple navigation bar or other convenient navigation mode to help users quickly find the information they need.**

**Influencing Factors of Acceptance and Use Behavior of Mobile Health Application Users: Systematic Review**

**International**

Link: [Influencing Factors of Acceptance and Use Behavior of Mobile Health Application Users: Systematic Review (amazonaws.com)](https://com-mendeley-prod-publicsharing-pdfstore.s3.eu-west-1.amazonaws.com/ab3b-PUBMED/10.3390/healthcare9030357/healthcare_09_00357_pdf.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEDAaCWV1LXdlc3QtMSJGMEQCICAXQTaj9xzxLOjx%2FFy4WjV9HN230VkC0z21g31n79SRAiAsiQzihWxRUBf0acFjrKvd2uesPk5I5FyRjfnmOCk1LiqDBAhYEAMaDDEwODE2NjE5NDUwNSIMuLpTt0kvj9c1jS8SKuADXS%2FviGSYNmmlI625p5Sqf1gA21r7uL5doOCDkw%2BSyqhAJaMHDEQxBKwkKmvVwdCOhbxIJcKLNUFgDgQs5RobA%2BqEEjBb0TFz2v51Byife9iOFKDxSlcRW5Ia5CKzC3fMIgqY714F0BLqH%2Bt68elsn90wVbBPna%2BrSLp0NOGMMVMG0P01Sx3%2BS4TLU218DtSwnYS9%2BPUAr7G7zH%2BMJLOoHdNQ6I%2FD1%2BwI6U%2Fd%2BYB6dUlpXjcEpc3yK%2Bj3xliyNKYw78dfbB%2BFKuFqqNRZF7zuXGuSiV8Gu%2Bz7YQpT7rp6t8HTyGk1L3e7FnfD1VFZSYgdoO05QoU1tiRCCoW0Dom%2BPaqKXqF4oQeP%2BeH4622cGjW0DUPXJSDHkt9V%2FFglY2j%2BPpFE%2BYhh8CMQXQfHSQk3nGklDfMK8DKg3peSYTgw%2Ft9iowWm%2BW7sZ%2BzeKykwuYaamKGEEkfGweZ%2BZYrH9lQZwKVoKvgsJ3K9YGJHYPYLvAyWgiXwcmjpAmeO6N%2Bo95pv3eODO1xU%2BvwHEcVsLjMiUOHgxjtNAjy594sjfFr4c%2FBPayXzd3QXPwoWRuDSD0UVHI6IDtN0kcNDEca8f5dtkw4o%2B2BZeTUwlLDsb0xs3Jx6lbaZR0OVqgtmRaKbGbylMLCg6IgGOqYBerMeyT8KDJwZ0pwJgHtwPLa7TC0YLnkwEzR3kPZlzIVbpghPBNRHGR%2Bl8iabeBBBEJeLEkLCDYWBvPitzGMgIVJgkYsVZRyZT%2B6dGAAukmoC7%2BCRgDP6ScyAxd0gJJhpeMSQu7v2n3tcgjnC1CyKEKh%2FVBdO6r%2FPLDAz9FgHITY8ZiwH4l8o%2FZSENvAsQTWABmHUJDwZ6Nbx9aJSfPjDpWT1mAn%2B%2FA%3D%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20210816T080449Z&X-Amz-SignedHeaders=host&X-Amz-Expires=300&X-Amz-Credential=ASIARSLZVEVE7DPOAGVS%2F20210816%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Signature=bb0a49bf062bc34c19fbf96ead3ae1afc749c1901b92349db211b51f06fcc54f)

**(Page 11)**

**As for App design, the research findings are relatively rich, including functionality, perceived ease of use and usefulness, security, and cost. Firstly, the Technology Acceptance Model is widely used in studying the factors that affect users’ behavior, in which perceived ease of use and usefulness are the factors that appear most frequently in the relevant literature. Secondly, functionality is the focus of researchers, in which information quality is an important indicator; however, core functions (e.g., reminders, notifications, incentives, follow-up, and goal setting), personalization, and gamification also attract the attention of researchers. Thirdly, the importance of security cannot be ignored. Finally, research on cost provides a new perspective for application designers**

BAKA

[Untitled (jmir.org)](https://www.jmir.org/2020/12/e23955/PDF)

[Investigating usability of mobile health applications in Bangladesh (springer.com)](https://link.springer.com/content/pdf/10.1186/s12911-020-1033-3.pdf)