mHealth Use in Healthcare Facilities: Raising Awareness in Data Protection, Privacy and Safety

Lilian G. Motti Ader[1,2][a], Bróna MacEntee[1], Kristina Rutkauskaite[1], Nutsa Chichilidze[1], Dylan Kearney[1], Sean A. Lynch[1], Katie Crowley[1,2][b] and Ita Richardson[1,2][c]

[1]*Dept. Computer Science and Information Systems, University of Limerick, Limerick, Ireland*

[2]*Lero Research Centre, University of Limerick, Limerick, Ireland*

Keywords: Mobile Devices, Healthcare, mHealth, Medical Device, Cyber Security, Privacy, Data Protection.

Abstract: During the COVID-19 pandemic, many patients and healthcare professionals embraced the possibility of using available mobile devices and applications, exploring the opportunities to reduce the burden on strained services. However, despite strict surveillance under the European GDPR or Medical Device (MD) regulations, users are considered to be primarily responsible for verifying that their application of choice is approved and certified. We searched academic and grey literature and discuss some of the challenges related to the use of personal devices and mobile applications for health and medical purposes. Our position is that policies and technologies should be more considerate of users' behaviour, which includes use of non-medical software for medical purposes, and situations where users seem to choose usability over safety.

1 INTRODUCTION

As the COVID-19 pandemic increased the burden in healthcare, staff, patients and the public turned to mobile technologies to improve efficiency in resources, patient care, information and communication. This raised questions and challenges relating to the use of personal devices, mainstream applications and even regulated mobile applications for health in healthcare facilities.

In Europe, existing regulations for medical devices and software (MDR, EU Regulation 2017/745), as well as for Data Protection (GDPR, EU Regulation 2016/679) have been recently reviewed (2017, 2018, 2020 and 2021) and their extended applications provide a reassuring framework to protect personal data and privacy of users. However, recent news in Ireland, regarding a cyber-attack on the national health service and a major fine for WhatsApp (discussed in Section 2), drew public attention to the issues related to the use of technologies for health or medical purposes. The risks of using smartphones in hospital settings may extend way beyond the control of regulatory agencies and institutions' policies.

We searched the literature on the use of mobile devices and applications in hospital and healthcare facilities to identify risks associated with data protection, privacy, and safety, for both patients and healthcare staff, that might have been overlooked and need further attention. In this position paper, we highlight some challenges related to the use of personal devices and mobile applications for health and medical purposes. We present our findings following the People Policy Technology model (PPT) proposed by Schlarman (Schlarman, 2001), aligning social and technical dimensions of cybersecurity. Then, we discuss our proposal on possible solutions to address risks related to users' behaviour (e.g. contamination, misuse, lack of awareness), use of non-regulated health-related apps (e.g. wellness and fitness apps, websites), and poor design (e.g. lack of transparency, difficulties in running user tests or clinical trials, access to specialized databases).

[a] https://orcid.org/0000-0003-2952-7765
[b] https://orcid.org/0000-0003-3596-4363
[c] https://orcid.org/0000-0002-5493-2837

Ader, L., MacEntee, B., Rutkauskaite, K., Chichilidze, N., Kearney, D., Lynch, S., Crowley, K. and Richardson, I.
mHealth Use in Healthcare Facilities: Raising Awareness in Data Protection, Privacy and Safety.
DOI: 10.5220/0010854100003123
In *Proceedings of the 15th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2022) - Volume 5: HEALTHINF*, pages 565-572
ISBN: 978-989-758-552-4; ISSN: 2184-4305

2 MOTIVATION AND GOALS

Europe has strong legislation for data protection and privacy, with additional reinforcement when it concerns medical information. For example, in Ireland, the Heath Products Regulatory Authority – HPRA, is implementing the new EU MDR/IVDR regulation – which is now a legal requirement rather than a directive. Having been postponed due to the COVID-19 pandemic and its implications, the new regulations have become fully applicable since the 26th May 2021[1]. This results in 'clearer requirements for clinical data on medical devices' and 'more specific product requirements', including technical standards.

However, users are considered primarily responsible for verifying that the apps of their choice are approved and certified. There is some evidence that more actions are needed to protect users. We outline below two events in Ireland that recently featured in worldwide news.

In December 2018 the Data Protection Commission (DPC) initiated an investigation into the social media and instant messaging application WhatsApp. In September 2021, the investigation was concluded showing lack of compliancy with the GDPR transparency obligations. WhatsApp was imposed a fine of €225 million[2]. We highlight this example as it raises concerns on the use of applications not compliant with MDR (non-MD apps) in healthcare settings. Because of the convenience of using general publicly available applications, the Ireland Health Service Executive (HSE) had approved, as an 'exceptional provision', the use of WhatsApp for messaging and video calls in 2020[3].

In May 2021, the HSE had data stolen in a cyber security incident[4]. Criminal ransomware groups look for organisations with highly sensitive data and insufficient information security, generating big disruptions on services relying on computers. As a result of the cyberattack, there were major disruptions on access to medical records and services which lasted over five months.

Following this attack, measures and law enforcements were undertaken to improve the infrastructure and prevent future cyberattacks. However, it is unclear whether an improvement in awareness and training could help users understand how their actions could prevent future security and data breaches.

Mobile Health (mHealth) is medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices (Kay et al., 2011). While there is a trend of increasing opportunities for design, development and adoption of mHealth, solutions for enhancing services and patient care are not restricted to MD regulated software. When users choose mainstream apps, or non-MD apps, to support their practices or treatment, they should pay attention to how personal and health data is processed, stored and shared. For convenience, medical staff and patients may be using mHealth solutions on their own devices, and raises additional concern (Wani et al., 2020).

The goal of this position paper is to present an overview of some of the factors related to the use of personal devices and mobile applications, in hospital or healthcare facilities, that raise challenges in data protection, privacy and safety for patients and staff.

3 METHODS

The PPT model (Schlarman, 2001) has been used in previous studies to evaluate risks of use of mobile devices in healthcare facilities (Wani et al., 2020). In the present paper, we define three categories for exploring the literature research, inspired by the PPT model (Table 1), or as follows:

- User behaviour: in the PPT model, Schlarman focuses on people responsible for the security process. We extend this approach to include general users, from healthcare staff having access to patient data, to data controllers and processors, as well as patients and family members. We do this for two reasons: (1) because there is a trend in technologies designed to support healthcare to consider a holistic approach and facilitate continuous monitoring and communication between care provider and patients and (2) because patients, as well as family members and caregivers, are also interested in safeguarding their personal and medical data. We argue that raising awareness for all groups of users could help them to adopt responsible behaviour.
- Policies and regulations: we refer to the existing regulations in Europe applied to the commercialization of medical devices and

[1] https://www.hpra.ie/homepage/medical-devices/regulatory-information/new-eu-device-regulations

[2] https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

[3] https://healthservice.hse.ie/staff/coronavirus/working-from-home/virtual-health/guide-to-whatsapp-for-hse-staff.html

[4] https://www2.hse.ie/services/cyber-attack/how-it-may-affect-you.html

software, as well as general data protection regulations (GDPR). Following the examples from the literature, we included relevant examples of grey literature such as codes of conduct and hospital policies (Garousi et al., 2016; Wani et al., 2020).

- Mobile devices and applications: while the PPT model refers to all the products, tools and materials supporting security, we decided to highlight the challenges of detecting or controlling the use of personal devices, such as smartphones, due to their availability, ease of access and ubiquity. As mobile devices are not often designed for medical purposes, we decided to focus on software running on mobile devices, also referred as mobile applications.

Our literature search is limited to publications from 2010 up to 2021. We believe this data limit is sufficient to include literature considered representative of the recent advances and dynamic turnaround on mobile devices, network infrastructure, software availability and users' practices.

Table 1: Overview of the focus of the present paper after PPT model.

PPT model	Aspect highlighted or extended in the discussion of the present study
People	Users' behaviour, including all user groups having access and therefore responsibilities for the use of personal data for medical purposes, including medical staff and patients
Policy	EU Medical Device Regulations (MDR), EU General Data Protection Regulations (GDPR), Hospital Policies and Codes of conduct
Technology	Mobile devices such as smartphones, regulated MD software, including mobile applications, and general public software and applications, non- MD apps, having access to personal information

4 USERS' BEHAVIOUR

Users are at the centre of our analysis. Data protection regulations and policies are designed to protect people's data: personal information, medical records, and history of communication between patients and staff. Users are also the main operators of technologies, in charge of choices, decisions and interactions with systems and devices. It is important to consider factors driving their behaviour, from acceptance of technology to inappropriate use of systems. Table 2 presents the main group of users of mobile devices in healthcare facilities, from our analysis of existing policies.

Table 2: Groups of users of mobile devices in healthcare facilities in the context of the present study.

Group of users	Actions or behaviours related to data protection in healthcare facilities
Patients, visitors, and informal carers	Usually responsible for their decisions in following prescriptions and recommendations
Medical staff, interns, students, and social workers	Usually responsible for making decisions, monitoring outcomes and supporting patients during treatment
Contractors, administration, and third-parties	Responsible for providing general infrastructure and resources

In the context of this paper, we also consider factors related to the users' behaviour actions such as selecting a device or software, installing, initiating interaction, learning how to use the app, becoming familiar with a system, usages related to the system's initial intended purpose, appropriation of the system for different purposes, and the choice to maintain use or stop.

Human errors are often related to security issues. Also, we consider whether users' actions relating to data protection and safety could be intentional or unintended.

We would like to highlight the following behaviours that present risks for data protection, privacy and safety:

- *Use of personal devices:* There is evidence of medical staff using their own devices for work (Wani et al., 2020), for communication (Bautista & Lin, 2016; Wu et al., 2010), education (Cho & Lee, 2016) or clinical practice (Koehler, 2013). Attention is called to issues related to distraction (Gill et al., 2012), risk of infection (de Jong et al., 2020) and patient safety (D. McBride et al., 2015).
- *Inappropriate use of devices or apps*: It is necessary that users keep their devices safe, password protected, with operating systems and software up to date. Reasons for inappropriate use include lack of education, lack of awareness, and issues related to accessibility and availability of affordable options.
- *Use of non-MD apps:* The use of general apps during work could be considered inappropriate and generate negative attitudes from managers (D. L. McBride et al., 2015) or patients (Koehler,

2013). Recently, patients and staff acceptance of mobile applications and devices has improved, since it has been perceived as useful, facilitating communication or organisation (Benedictis et al., 2019; de Jong et al., 2020; Lee Ventola, 2014; Wyatt et al., 2020). However, general applications such as calendar, internet browser, and instant messaging can present risks as there is no guarantee that users will not disclose or store personal data (Benedictis et al., 2019; Dexheimer & Borycki, 2015)

- *Disclosure of personal or medical data inadvertently:* Users may disclose personal information when seeking health information online, or posting reviews for apps and services. Many are unaware of the fact that their pictures, full name and contact details may be publicly displayed. Additionally, some users may not understand what characterises personal and medical data, how technologies process and store them and the risks associated with use of non-MD apps for health-related purposes.
- *Lack of awareness and accessibility on policies and regulations:* As with “Terms and Conditions”, many users only have access to existing policies and regulations if actively looking for them. Often the language used can be a barrier for the users to comply with safety and security guidelines. Furthermore, users tend not to read the ‘small print’, and therefore may not be aware of breaches of specific policies and regulations which their use of an app may cause.

In summary, many difficulties in misuse of medical software are not caused by the software itself, but rather, by the inappropriate use of the software. Users may not have enough understanding on what characterises personal and medical data, how technologies process and store them and the risks associated with use of non-MD apps for medical purposes. Additionally, users do not necessarily understand the importance of MDR, and may not be on a position to verify compliancy or appropriate use of them.

5 POLICIES AND REGULATIONS

Given the issues pertaining to Users’ Behaviour as discussed in the previous section, it is important that we present and discuss the current regulations and policies concerning the use of mobile devices and apps in healthcare settings.

5.1 GDPR and MDD Devices and Software

By definition, Medical Devices (MD) include a wide range of products used in healthcare and are subjected to strict regulations[5], which vary depending on the class of device. In Europe, MDs are reviewed by notified bodies (e.g. National Standards Authority of Ireland – NSAI, Health Products Regulatory Authority HPRA) and, once certified compliant, they are distinguished by a CE mark (European Conformity), which indicates, amongst other criteria, that the product has been adequately tested, that medical claims are supported by clinical data and that users are correctly informed about safety of use[6].

Software, such as mobile applications, once intended for medical purposes are also considered a medical device[7]. After a transition period of three years, the new MDRs are applicable, and include reinforcement of risk assessment, post-market surveillance and investigations of clinical evidence.

The collection and processing of personal information is a sensitive issue, not limited to medical devices and software. In Europe, the General Data Protection Regulation (GDPR) was put into effect on May 25, 2018. Data protection and processing policies include limitations on data storage, third party transfers, data anonymisation and pseudonymisation and disclosure[8].

We outline some of the issues currently faced by the users of MDs that seem uncovered by existing regulations:

- *Users’ responsibilities* It is the responsibility of the manufacturer, or in the case of software, the developer, to follow MD regulations. Compliancy is required before products are placed in EU markets. However, it is responsibility of the user to verify that devices and software used for medical purposes are appropriately CE marked. It seems to us that users may not be aware of their responsibilities in ensuring that regulations are applied, apps are compliant and that their use is fair and appropriate.
- *Distinction between MD and non-MD apps:* For mobile apps and software, it is difficult for the users to distinguish regulated and non-regulated options in applications stores. Many MD apps might remain unknown or inaccessible.

[5] https://ec.europa.eu/health/md_newregulations/overview_en

[6] https://www.hpra.ie/docs/default-source/Safety-Notices/in201703_mobileappinhealthcare_140917.pdf?sfvrsn=0

[7] http://www.hpra.ie/homepage/medical-devices/special-topics/standalone-software-and-applications

[8] https://www.hse.ie/eng/gdpr/hse-data-protection-policy/hse-data-protection-policy.pdf

Additionally, non-MD apps may seem an easy option to users who are often unaware of the implications of use on data protection and privacy.

- *Assessment of compliancy*: mHealth apps for use in the Irish public healthcare system must complete a Privacy Impact Assessment (PIA) to ensure compliance with privacy and GDPR. This process is detailed and can be lengthy (MacEntee, 2021).
- *PIA not suitable for small systems*: An examination of research has indicated that PIAs are designed for large scale systems but do not identify privacy issues when applied to a variety of smaller scale mHealth apps. This research also suggests that one size does not fit all with respect to PIAs and mHealth apps
- *Transparency of selection and compliancy over time:* As with many apps, mHealth solutions should be constantly updated and improved, as they might be dependent on the configurations of operative systems and devices. Major updates should be complying with the regulations. However, the current offer can quickly become obsolete and present risks of safety and security for the users.
- *The gap between designers, practitioners, and regulatory authorities*: From conception to launch in the market, users' needs must be identified and met. The challenges in accessing patients for user tests and clinical trials are barriers to improving design, reliability and possibly effectiveness of digital solutions.

5.2 Policies and Codes of Conduct

Other regulations exist and try to cover aspects related to the use and application of MDR and GDPR. With regards to healthcare, hospital and institutions usually define and circulate their policies, and members of staff should respect existing codes of conduct. Examples are the HSE Data Protection Policy[9] targeting people who may have access to patients and their data including 'staff, students, interns and work experience candidates, contractors, sub-contractors, agency staff, medical colleges and authorised third party commercial service providers'. According to the literature (Bautista & Lin, 2016; de Jong et al., 2020; Johnston et al., 2015), some issues around policies and codes of conduct can relate to

- *Target groups not inclusive:* Policies and codes of conduct are provided to staff, students, interns, and contractors, who are informed and obligated to comply. Patients are usually not included as target groups.
- *Non-generalisable:* Policies and procedures are local, and can apply from institutions, groups, and localities to national bodies. It is difficult for users to be aware of these variations, as well as for developers to adapt the systems to current guidelines and updates.
- *Lack of implementation plans and training*: Policies usually do not define how training is going to be provided.

Finally, there is often a lack of communication, accessibility and availability. Some users might be unaware of their responsibilities and general codes of conduct.

6 MOBILE DEVICES AND APPLICATIONS

As presented in the introduction, the focus of this paper is to discuss the use of personal mobile devices in healthcare settings, and to discuss issues related to the use of mobile applications having access to personal data in these settings, potentially with medical or health information.

Because of the regulations in place, it is important to distinguish the risks associated with the use of regulated MD software, which includes MD mobile apps, to risks of using mainstream non-regulated mobile apps that can also be used for medical or health-related purposes.

6.1 MD Mobile Apps

MD software designed for monitoring patients, facilitating diagnosis or self-management of care is subject to regulations according to the clinical category and risk assessment defined by MDR. Some issues include:

- *Customisation of MD apps:* Some institutions would support the development of private solutions, e.g. specially designed communication platform for staff-staff or staff-patients. This can be costly, and users might prefer interfaces that are familiar.
- *Some mHealth solutions are excluded from MDR*: mHealth apps are currently being developed to support many medical fields, including dermatology, paediatrics, cardiology,

[9] https://www.hse.ie/eng/gdpr/hse-data-protection-policy/hse-data-protection-policy.pdf (June 2019)

oncology, and a variety of chronic conditions such as diabetes. They may also support assistive devices. Other areas such as falls, frailty and clinical trials also are covered under MD regulations However, some health conditions such as mental well-being, pregnancy or menstruation can benefit from mHealth solutions. If not covered by MDR, users are at risk of losing control of very sensitive data.

- *Intentional use of non-MD apps:* Users may intentionally choose apps with which they are familiar, prioritising usability over safety. Intentional use may include instant messaging between staff, teleconsultations, search of prescriptions or medication details, and booking appointments.
- Networks and communications: As conventional server–client applications in PCs, mobile applications communicate with many cloud services and share information connecting to many networks and platforms. The use of private or public networks present risks to secure transfer of data and many users do not know how to keep their connections safe.

6.2 mHealth non-MD

Some apps, such as those developed to support wellness, fitness, period trackers, pregnancy, smoke cessation, diet, and nutrition, can collect a large amount of sensitive data from users, and most are not transparent on how this data is managed. We highlight the following issues:

- *Lack of transparency:* as for MD apps, it is the responsibility of designers and developers to provide users with information on the transparency of data collection, control of data capture, storage, and processing such as anonymisation, pseudonymisation, removal, time limits, and sharing. Lack of regulation makes non-MD apps less clear about how data is managed.
- *Third parties and shared data:* As apps are selected for available countries, the use of data by third-party in different countries is not always clearly indicated. From target advertisements to data breaches, and risks of safety and privacy to the users, existing regulations provide a reassuring framework. However, users do not always verify if apps developers are ethically responsible for the management and control of their sensitive data.
- *App permission:* Upon installation, use or updates, the users can grant permission, often unknowingly, as they do not check or read detailed terms and conditions, to mobile applications to capture, store, process or even share the users' location, camera or audio recordings, media content or textual information. Recent mobile devices are equipped with many sensors enabling data collection: connectivity such as Wi-Fi and Bluetooth, contactless NFC, motion sensors as gyroscope, accelerometers are user to recognise levels of activity, localisation from GPS as well as Wi-Fi, biometric sensors, microphones, and others. If GDPR preconises fair use of data, users are not always attentive when enabling permissions to the apps installed in their devices. Apps do not generally give options to the users to select when and how to turn data access in or off.

7 CONCLUSION

We reviewed challenges related to the use of mobile devices and apps for health and medical purposes. As discussed in the literature, users might prefer to use their personal devices and familiar interfaces to improve the effectiveness of their practices, sometimes without understanding the implications or risks for data protection, privacy and safety. We argue that policies and regulations, as well as designers and developers, should be more considerate of users' behaviour.

When the purpose of the system and its use of data is not transparent, there is a risk for data protection and privacy with unintended data breaches or security faults. Therefore, there is an onus on the software engineer or developer to ensure that the MD software such as MD apps, as well as general apps supporting mHealth are fit-for-purpose. It is responsibility of designers and developers to provide users with information transparency on data collection, control for data capture, storage, and processing such as anonymisation, pseudonymisation, removal, time limits, sharing.

References for this position paper were selected to enable an initial discussion on the issues raised by the use of mobile applications and devices in healthcare facilities, such as hospital and clinics. By referring to the PPT model, we have provided a holistic view of the issues related to use of smartphones in hospital observed in the past 10 years. Future work should further study the aspects highlighted in the present paper in the scope of security and privacy threats for conventional information systems. It would be important to take this step, as mobile applications create an additional layer to collect, store and share health and medical data that are not restricted to MD software. Further studies could benefit from a historical perspective or to analyse the trends based on recent advances related to the adoption of mHealth solutions after the COVID-19 pandemic (Storni et al., 2021; Webb et al., 2020).

7.1 Future Work

We argue that the challenges outlined in this paper could be addressed by policies and regulations reinforcing the need for public training, education and awareness, and these could be two-fold:

- for users, about their choices and risks,
- for designers and developers, about transparency, ethics and their responsibilities.

It is necessary to provide users with information regarding their responsibilities in ensuring that regulations are applied, apps are compliant and that their use is fair and appropriate. Some suggestions are:

- *Supporting users to choose safe mHealth:* A possible solution would be a filter in digital stores, such as Google Play Store or Apple Store, to differentiate MD from general apps. Apps available in these stores must already comply with software development guidelines.
- *Involving users in the design process:* In Ireland, the digital transformation includes initiatives such as training and support to healthcare staff in identifying opportunities to design and develop technological solutions[10], offering unique insight to solving real-world problems.
- *A database of regulated mHealth:* This could help users, both patients and healthcare staff, to find the support they need from MD. This solution has been suggested in the literature as a mean to address general public and patients' needs (Olivero et al., 2019). Recently, initiatives such as the NHSX[11] in UK have been created to support the transition to the digital healthcare. As part of their services, manufacturers can apply to be listed in a selection of existing MD apps, and centralize their review and offer to healthcare staff.
- *Awareness and means to action:* Users also might be informed and provided with easier means to contact regulatory bodies for verification, information or indicate possible issues.
- *Improving user experience*: It is important that the design of mHealth solutions support users in making good choices, being aware of policies and processes, reflecting on transparency, reporting inappropriate use or system.

Regarding the responsibility of designers and developers, we highlight the following suggestions:

- *Education*: Guidelines should be presented early and regularly in educational settings to systems developers. These would cover best practices so that they would understand the factors involved in launching in the MD market and the issues with the use of non-regulated apps in healthcare. They should also be familiar with sanctions for security breaches or threats.
- *Improved design:* MD software should automatically prompt users with options for encryption or better management of security options. For example, public websites or search engines could detect use of personal data, such as fields labelled "first name", "last name", "date of birth" when classifying information and alert users.

ACKNOWLEDGEMENTS

This research has been partially supported by the Science Foundation Ireland Grant number 13/RC/2094_P2 to Lero - the Science Foundation Ireland Research Centre for Software (www.lero.ie).

REFERENCES

Bautista, J. R., & Lin, T. T. C. (2016). Sociotechnical analysis of nurses' use of personal mobile phones at work. *International Journal of Medical Informatics*, *95*, 71–80. https://doi.org/10.1016/j.ijmedinf.2016.09.002

Benedictis, A. De, Lettieri, E., Masella, C., Gastaldi, L., Macchini, G., Santu, C., & Tartaglini, D. (2019). WhatsApp in hospital? An empirical investigation of individual and organizational determinants to use. *PLoS ONE*, *14*(1), 1–12. https://doi.org/10.1371/journal.pone.0209873

Cho, S., & Lee, E. (2016). Distraction by smartphone use during clinical practice and opinions about smartphone restriction policies: A cross-sectional descriptive study of nursing students. *Nurse Education Today*, *40*, 128–133. https://doi.org/10.1016/j.nedt.2016.02.021

de Jong, A., Donelle, L., & Kerr, M. (2020). Nurses' use of personal smartphone technology in the workplace: Scoping review. *JMIR MHealth and UHealth*, *8*(11), 1–15. https://doi.org/10.2196/18774

[10] https://www.hse.ie/eng/about/who/communications/digital/digital-transformation/

[11] https://www.nhsx.nhs.uk/

Dexheimer, J. W., & Borycki, E. M. (2015). Use of mobile devices in the emergency department: A scoping review. *Health Informatics Journal*, *21*(4), 306–315. https://doi.org/10.1177/1460458214530137

Garousi, V., Felderer, M., & Mäntylä, M. V. (2016). *The need for multivocal literature reviews in software engineering*. 1–6. https://doi.org/10.1145/2915970.2916008

Gill, P. S., Kamath, A., & Gill, T. S. (2012). Distraction: An assessment of smartphone usage in health care work settings. *Risk Management and Healthcare Policy*, *5*, 105–114. https://doi.org/10.2147/RMHP.S34813

Johnston, M. J., King, D., Arora, S., Behar, N., Athanasiou, T., Sevdalis, N., & Darzi, A. (2015). Smartphones let surgeons know WhatsApp: An analysis of communication in emergency surgical teams. *American Journal of Surgery*, *209*(1), 45–51. https://doi.org/10.1016/j.amjsurg.2014.08.030

Kay, M., Santos, J., & Takane, M. (2011). *mHealth - New horizons for health through mobile technologies* (Vol. 3). World Health Organization. https://doi.org/10.1109/CBMI.2010.5529886

Koehler, N. (2013). Healthcare professionals' use of mobile phones and the internet in clinical practice. *Journal of Mobile Technology in Medicine*, *2*(1), 3–13. https://doi.org/10.7309/jmtm.76

Lee Ventola, C. (2014). Mobile devices and apps for health care professionals: Uses and benefits. *P and T*, *39*(5), 356–364.

MacEntee, B. (2021). *Are Privacy Impact Assessments for Mobile Health Applications Fit for Purpose?* (Issue August). University of Limerick.

McBride, D. L., LeVasseur, S. A., & Li, D. (2015). Non-work-related use of personal mobile phones by hospital registered nurses. *JMIR MHealth and UHealth*, *3*(1), 1–5. https://doi.org/10.2196/mhealth.4001

McBride, D., LeVasseur, S. A., & Li, D. (2015). Nursing performance and mobile phone use: Are nurses aware of their performance decrements? *JMIR Human Factors*, *2*(1), 1–6. https://doi.org/10.2196/humanfactors.4070

Olivero, E., Bert, F., Thomas, R., Scarmozzino, A., Raciti, I. M., Gualano, M. R., & Siliquini, R. (2019). E-tools for hospital management: An overview of smartphone applications for health professionals. *International Journal of Medical Informatics*, *124*(January), 58–67. https://doi.org/10.1016/j.ijmedinf.2019.01.010

Schlarman, S. (2001). The people, policy, technology (PPT) model: Core elements of the security process. *Information Systems Security*, *10*(5), 1–6. https://doi.org/10.1201/1086/43315.10.5.20011101/31719.6

Storni, C., Tsvyatkova, D., Richardson, I., Buckley, J., Abbas, M., Beecham, S., Chochlov, M., Fitzgerald, B., Glynn, L., Johnson, K., Laffey, J., Mcnicholas, B., Nuseibeh, B., Connell, J. O., Keeffe, D. O., Keeffe, I. R. O., Callaghan, M. O., Razzaq, A., Rekanar, K., Welsh, T. (2021). *Toward a Compare and Contrast Framework for COVID-19 Contact Tracing Mobile Applications : A Look at Usability*. *5*(Biostec), 557–565. https://doi.org/10.5220/0010307005570565

Wani, T. A., Mendoza, A., & Gray, K. (2020). Hospital Bring-your-own-device security challenges and solutions: Systematic review of gray literature. *JMIR MHealth and UHealth*, *8*(6), 1–13. https://doi.org/10.2196/18175

Webb, H., Parson, M., Hodgson, L. E., & Daswani, K. (2020). Virtual visiting and other technological adaptations for critical care. *Future Healthcare Journal*, *7*(3), e93–e95. https://doi.org/10.7861/fhj.2020-0088

Wu, R. C., Morra, D., Quan, S., Lai, S., Zanjani, S., Abrams, H., & Rossos, P. G. (2010). The use of smartphones for clinical communication on internal medicine wards. *Journal of Hospital Medicine*, *5*(9), 553–559. https://doi.org/10.1002/jhm.775

Wyatt, K. D., Finley, A., Uribe, R., Pallagi, P., Willaert, B., Ommen, S., Yiannias, J., & Hellmich, T. (2020). Patients' experiences and attitudes of using a secure mobile phone app for medical photography: Qualitative survey study. *Journal of Medical Internet Research*, *22*(5), 1–10. https://doi.org/10.2196/14412