Privacy and security analysis – Assessing harms and risks to patients

Samuel Wairimu

Disruptive technologies in the form of e-Health or electronic healthcare (the use of information technology in health) have the ability to provide positive implications to both patients and healthcare professionals. Recently, public health agencies deployed contact tracing apps with the aim of curbing the spread of COVID-19, by aiding manual contact tracing, and lifting restrictions. Despite this, their ubiquitous nature in the sector has opened doors to new threats in the area of information security and privacy, where these apps, for instance, contain security and privacy risks such as violation of the principle of least privilege, which when exploited can cause privacy harms, for example, re-identification of users.

In general, information security and privacy in the healthcare sector is essential due to the nature of the data they process, and the need to keep the patient safe. While this is so, the general security posture of the sector, which is poor due to its under-financing in IT security among other reasons such as the use of legacy systems, makes it vulnerable to cyber-attacks that end up with exfiltration of personal health data, among other data, for instance, relevant research data. Such data can be misused incurring privacy harm to patients that have been affected by the breach.

The research shows that with the poor state of the healthcare sector in terms of its cybersecurity, the privacy and security of health data, and in particular personal health data that could be exploited to cause privacy harm is at risk from not only opportunistic or hacktivist attackers but also state-sponsored attackers, for example, Fancy Bear in the case of World Anti-Doping Agency in 2016. The research follows an experimental approach to assess the privacy and security risks of m-Health apps, with the selected case study of these m-Health apps, that is, COVID-19 contact tracing apps. In addition, it also contributes with a theoretical approach to assessing impacts and consequences in the healthcare sector, including what harms patients could face in the event of a state-sponsored cyber-attack. Fundamentally, the research shows the critical and significant nature of the sector, and the impact a cyber-attack would have on individuals and the sector itself.