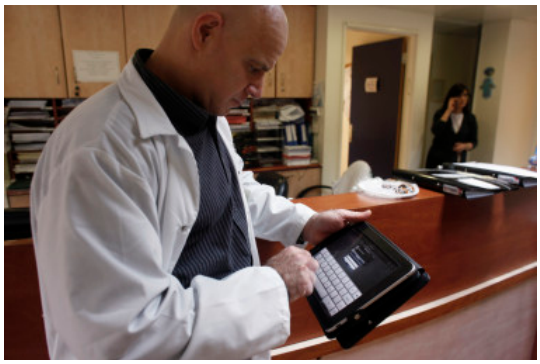
Health apps for mobile devices provoke privacy concerns

European Commission consultation leads to calls for greater security for those using mobile health applications.

by **Peter O'Donnell** on 13.01.2015 / 13:44 CET



The boom in mobile apps is raising public concerns over privacy – particularly in relation to personal health. The need for stronger security came out at the top of the list of issues identified in a European Commission consultation on m-health, according to a report published today (13 January).

As the European Public Health Alliance (EPHA) said in its response to the consultation: "The variety of health apps available is mindboggling – they do everything from counting calories and detecting allergies to measuring blood glucose levels, sending medication reminders, and providing nutrition information." But for applications that depend on collecting personal health data, the principles of the current EU rules on data protection and e-privacy must apply, insists EPHA, "and the responsibility of securing data should rest with the developers". In addition, networks used in healthcare settings that transfer m-health data must be secured so that no data interception can occur when interacting with users' personal mobile devices.

"Patients need to be assured that sufficient measures are taken to avoid data being retrieved by third parties not involved in their medical treatment, included but not limited to health insurers", said the European Heart Foundation. The European Blind Union emphasised the need for robust personal data protection to build trust in m-health solutions, and advocated the use of security safeguards such as the encryption of patient data and patient authentication mechanisms.

Similar anxieties are reflected in the dozens of individuals' responses to the consultation. Jordi Jané Cardo of Spain urged mandatory use of biometric permissions, such as fingerprint unlocking features, on mobile devices to secure access to data. Manuella Dautan of France said it was necessary for the end-user to have clear understanding of which jurisdication their data are stored in, and users must be able to request – and receive proof of – total erasure of their data. And Frederik Feys of Belgium insisted that clear contractual agreements should allow users to be able to decide whether they want to share their data with third parties.

Many of the concerns over privacy are shared by industry. According to the European Federation of Pharmaceutical Industries and Associations, "the data security of m-health solutions will be an important element in driving widespread use in healthcare systems. Clarity over the 'intended uses' of the solution are key elements in determining what safety features are needed. 'Encrypted data transmission' decreases the risk of leakage and unintended use by third parties, and should be specifically considered in the case of patient remote monitoring and guidance

are key elements in determining what safety features are needed. 'Encrypted data transmission' decreases the risk of leakage and unintended use by third parties, and should be specifically considered in the case of patient remote monitoring and guidance by healthcare professionals."

Although market predictions suggest that Europe will become the world's largest market for m-health by 2018, the European Commission recognised in its consultation that 77% of Europeans have still not used their mobile phones for m-health. Respondents to the consultation pointed out that this confirms the continuing public concern that data security is not yet taken seriously enough. The Commission's own summary of the responses notes the widespread support for data encryption and authentication mechanisms, with encryption for data both in transit and when stored.

Other frequent comments among the responses to the consultation included calls for improved interoperability and wider promotion of standards, a clearer legal framework – including relating to app developers' liability, and certification of m-health applications to ensure patient safety. The Commission intends to discuss options for further policy actions – legislation, self- or co-regulation, guidelines – over the coming year. Several m-health deployment projects are already foreseen under Horizon 2020, and m-health will be one of the key topics on the agenda of e-health week in Riga in May.