



palgrave▶pivot

# Responsible Innovation in Health

Concepts and Tools for  
Sustainable Impact

Pascale Lehoux  
Lysanne Rivard  
Hudson P. Silva

palgrave  
macmillan

**Box 5.3 The Mentallys App Project***Mitigating potential negative impacts on end users: The Mentallys app project*

Pathways to mental healthcare across different public, private, and frontline community services are long, labyrinthine, and discouraging. This compromises access to proper care for individuals with a mental health condition and their caregivers. Though difficulties in accessing mental healthcare have been documented for years, they are persistent.

The Mentallys project aims to improve, simplify, and unify access to mental healthcare via an app entirely codesigned with patients, families, caregivers, and clinicians. The Mentallys app will equip healthcare providers, patients, and family caregivers with a shared tool to navigate more easily and effectively care pathways.

While there is a lack of regulation and legislation for health apps in general, the development team knows that identifying and mitigating potential ELSIs is crucial to the success of the project. One key concern is the protection of users' privacy. Data generated through an app for mental health patients is highly sensitive and the commercial value of such data is a major concern (Torous et al., 2018).

Risks to data privacy include data leaks through security breaches or hacking as well as the disclosure of navigation information to third party data brokers (who mainly work for the advertisement industry). This generally occurs by accessing unencrypted metadata of communication exchanges taking place on the app and through tracking end users' activities via other apps installed on their smartphones.

To mitigate these negative impacts, the Mentallys app integrates a privacy by design approach as well as strict cybersecurity measures. In opposition to the current trend of digital phenotyping where passive data is collected in the background even if the user is not using the app (Benoit et al., 2020), the strategy is to reduce the quantity of data generated through the app. It will also be important to use sound privacy enhancing and/or data anonymization strategies to make data inaccessible or unusable if leaked or hacked.

Source: Stéphane Vial, PhD, Research Chair in Design for e-Mental Health, Associate Professor of Design, Université du Québec à Montréal (UQAM)