Health technology: digital therapy by prescription

The healthtech sector has been on the rise for years, changing the traditional ways for patients to interact with healthcare.

04 June 2019

The healthtech sector has been on the rise for years, changing the traditional ways for patients to interact with healthcare. Paper prescriptions are rapidly giving way to the electronic authorisation of medication and apps allow you to book GP appointments and seek medical advice in a few taps of the finger. There are now dozens of companies that provide 24-hour access to GPs via audio or video chat; some even store recordings of your online appointment for you to replay at any time.

'Prescription Digital Therapeutics' (PDT) is said to be the next piece of cutting-edge technology set to revolutionise the provision of healthcare. PDT is entering the healthcare mainstream, mostly in the US at present. It has been coined 'revolutionary' due to its movement from traditional prescription medication to the usage of specialised apps combining behavioural and lifestyle changes with medication to treat illnesses such as substance abuse, dementia and the management of some chronic illnesses.

Some forms of PDT are apps which aid the management of chronic illnesses by reminding a patient when to take medication; others use sensory stimuli to manage insomnia and depression, replacing drugs completely. The main difference between PDT and other health and wellness apps is that PDT products mostly seek to secure approval from the Food and Drug Administration (FDA). In the US, if a product is labelled, promoted or used in a manner that meets the definition of a medical device within the meaning of the Federal Food Drug and Cosmetic Act, it will be subject to FDA regulatory controls.

The Medicines and Healthcare products Regulatory Agency (MHRA) is the UK equivalent of the FDA. In the UK, medical devices must register with the MHRA and must be CE marked in line with the EU medical device directives. The CE mark confirms that the medical device meets certain 'essential requirements' and is fit and safe for the intended purpose.

An example of the first form of FDA-approved PDT is 're-SET-O', a program designed to treat opioid addiction. The Re-SET-O app can be downloaded directly to a patient's phone after they receive a prescription from their doctor. Patients participate in a 12 week program of behavioural and skill-building therapy through text, audio and videos, teamed with traditional drug therapy. Doctors can review their patient's progress by checking a dashboard on their reciprocal app.

There has been some criticism amongst health technology professionals that the apps promote themselves as a new medical therapy but are simply rebranding existing treatments. Others claim that the high price of developing, testing and releasing the products compared with the relatively small number of people who can benefit is problematic.

As yet, the security of the data contained within PDT has received relatively little criticism, although it is early days for this technology, but concerns about information security and health technology have been increasing.

Following the May 2017 cyber-attack on several NHS trusts, the vulnerability of data has been high on the list of concerns for public and private bodies offering healthcare services. Health data in particular is a valuable prize for hackers. A recent BMJ study showed that, of 24 health apps in a recent study, 19 shared user data with companies, including Facebook, Google and Amazon; data which could be passed on to credit agencies or used to target advertising.

The risk of cyber-attacks increases as more interfaces become available and the quantity and detail of health data available is on the increase. Patients can now access their health records and details of historical prescriptions on the NHS App, information that was largely paper-based only a few years ago. Sensitive data in the wrong hands could have far-reaching and devastating implications. It is not just healthtech apps that present data security risks. Cybersecurity researchers in Israel have also demonstrated how malware can access a

hospital's network and infiltrate AI screening tools such as those used by radiologists to identify cancer. The research showed how a malicious attacker could theoretically insert or remove lung cancer from a patient's CT scan and demonstrates how developments in health technologies must include parallel developments security.

Data security aside, critics also question the diagnostic ability of some online GP services. Whilst remote GP access is not yet available through any of the NHS apps, there is a question mark over the diagnostic support software currently used in some private health apps, the fear being that the software may potentially miss symptoms.

The benefits of health technology like digital therapeutics and the NHS App have the potential to be significant. From the diagnosis and treatment of depression to the management of diabetes, there are numerous advantages to the digitalisation of health services. However, the focus on safeguarding sensitive data and addressing technical vulnerabilities must remain a priority.

Contact

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000

Related expertise

Commercial and outsourcing for health

Health law

Medical treatment decisions and disputes