Claire Smith Senior Associate
claire.smith@bristows.com
Bristows, London

Medication non-adherence

Patients who fail to take their medicines properly are having a staggering impact on healthcare budgets, as well as putting their own health at risk. Claire Smith of Bristows looks at a few of the innovative solutions that digital health companies are deploying to help to address such problems - including a digital pill - and some key legal issues that need to be considered when developing such solutions.

The impact of the problem

A huge number of medicines are dispensed every day, but, sadly, a significant proportion of these are never used. In 2013, a study[1] revealed the full extent of the problem of medication non-adherence, estimating that it was costing the UK National Health Service ('NHS') around £500 million a year.

It has been estimated that over 190,000 people in the EU die as a result of not following their medication regimes properly[2] - not to mention patients who suffer complications, the treatment for which may have been avoided had they stuck to their doctors' instructions.

Why does it happen?

A number of surveys have revealed that the main reasons for non-adherence include: simply forgetting to take medicines, having concerns about their side effects and/or failing to understand how they work. For instance, some patients who are prescribed blood pressure tablets may see no reason to take them because they do not feel ill, or feel no different when they are on the medication.

Most of these problems are largely preventable - for example, by providing better patient education and support (e.g. through initiatives such the UK's New Medicines Service). Digital health solutions can also help to alleviate them. The market for medication adherence technologies is growing, as the problem becomes increasingly important for ageing populations who, most likely, will have chronic health conditions in their later years.

What sorts of technologies are helping to combat the problem?

Some of the technologies that are emerging in this space include:

- Healthera's app (available in the NHS Apps Library), which lets users scan quick response (QR) codes from their medicine labels to create a pill-taking schedule. It reminds them when to take their medicines, and enables them to order repeat prescriptions via their own general practitioners ('GPs') and collect them from local pharmacies. It is coupled with an analytics portal that can give GPs access to their patients' medicine schedules and any information logged by patients about when they have taken their medication;
- Propeller Health has developed a digital sensor that attaches to asthma inhalers and synchs to an app on a smartphone. The system helps sufferers to understand their symptoms, and sends information automatically to their doctor every time the inhaler is used, giving the doctor adherence data to tailor their patient advice accordingly;
- Microchips Biotech has developed a microchip that can be implanted in the body, with as many as 400 doses of a hermetically sealed drug that are then released at precise times. The device can be controlled by the patient and/or a clinician via a wireless remote, or can be programmed to release the doses on a pre-determined schedule; and
- the first digital pill to be approved by the United States Food and Drug Administration ('FDA') - a combination of Otsuka's Abilify (an antipsychotic drug) and the Proteus Discover ingestible sensor in a single tablet - is used with a wearable patch and an app. It helps patients to keep track of whether, and when,

Image: Pina Messina / Unsplash.com

continued

they have ingested their medicines and (with patients' consent) sends this information to their doctors.

Some of the key legal issues

Digital health businesses face a number of legal challenges when bringing solutions like these to the market. It is key for them to understand, at an early stage, how their products will be regulated (including whether an app will be classified as a medical device) and how they will be impacted by privacy laws, so that they can develop, sell and operate them in a compliant manner. Product liability, consumer protection and advertising legislation are not covered here, but should also be at the forefront of people's minds as they apply to all digital health products, even if they are not classified as medical devices.

Medical device regulation

The EU Medical Devices Directive (Directive (EU) 93/42) (as amended) ('MDD') states that medical devices include (among other things) articles or software that are intended by the manufacturer to be used for the purpose of diagnosis, prevention, monitoring, treatment or alleviation of a disease, or the diagnosis, monitoring, treatment or alleviation of an injury or handicap. Manufacturers of medical devices must comply with the essential requirements and harmonised standards of the MDD (which include maintaining a technical file and implementing a documented quality management system) and must CE mark their devices before placing them on the market.

If software is incorporated into a medical device, it will be regulated automatically by the MDD. Even if it is not, software or an app may still be classified as an 'accessory' to a medical device (and therefore regulated in the same way) if the manufacturer specifically intends for it to be used together with the device, so as to enable the device to be used in accordance with its intended purpose.

However, many medication adherence apps are standalone software. These may also be regulated as medical devices if the manufacturer intends them to be used for a medical purpose (such as monitoring a disease), for the benefit of individual patients. If the manufacturer wishes to avoid an app coming under the MDD, care would need to be taken with its labelling, instructions for use and any associated marketing collateral (from which such intention will be drawn), as any claims that indicate that it may have a medical purpose could bring it within the MDD regime and, consequently, attract a heavier regulatory burden. The upside of having a CE mark, however, is that it helps to demonstrate the quality and credibility of the product.

The difficulty with some medical adherence solutions is that it can be hard to determine on which side of the line they fall. Apps that simply send patients reminders may well not be regulated as medical devices, but assessment becomes trickier when some form of monitoring is involved. Neither the MDD nor its associated European Medical Device Vigilance System guidance defines 'monitoring' precisely. Clearly, it involves direct monitoring of clinical signs such as blood pressure, but indirect forms of monitoring give rise to interesting borderline cases.

A relevant factor here is whether the information collected is made available to clinicians. If it is merely passed to a doctor for reference (e.g. in a digital format that simply replaces a patient's own written medication diary), to enable the doctor to form their own judgement, then the app is unlikely to be a medical device. However, if the information is passed to a doctor for the purpose of influencing the treatment of the individual patient, it is more likely to be a medical device. In particular, if an app carries out any analysis, calculations, enhancements or interpretations of patient data (e.g. symptom tracking or dosage calculations) then it will normally be considered a medical device.

App providers of decision support software, in particular, should note that the Medical Devices Regulation (Regulation (EU) 2017/745), which applies from May 2020, makes significant changes to the classification of medical devices) and generally imposes a much tougher regulatory regime. Many such tools that are currently classified as Class I (and subject to a self-certification process) will fall under Class II (requiring certification via an independent notified body).

Ultimately, products that monitor drug taking, rather than the disease or its symptoms, can present challenges to regulators. Some solutions do not sit easily within a country's established definitions of a medical device (such as Proteus's digital sensor, which was ultimately processed in a *de novo* category by the FDA before getting clearance in the United States). These types of products can have uncertain regulatory pathways and, particularly when further combined with a medicine, long regulatory timelines.

1. Aston Medication Adherence Study (AMAS), 2013.
2. Medi-Voice Project (FP6-017893), May 2008.

The difficulty with some medical adherence solutions is that it can be hard to determine on which side of the line they fall. Apps that simply send patients reminders may well not be regulated as medical devices, but assessment becomes trickier when some form of monitoring is involved.

Patient privacy

Under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), there are special categories of personal data (previously referred to as 'sensitive personal data') that include data concerning health. Health data is defined very broadly as 'any personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.'

This definition will capture much of the data that is normally collected by digital health products (including potentially lifestyle, fitness and wellbeing apps). The app provider will usually be 'processing' the data within the definition in the GDPR (and will therefore need to comply with its requirements), unless the data is only held locally on the smartphone or other user device and the provider has no access to it.

Special categories of personal data, such as health data, can be processed only in accordance with one of the lawful grounds set out in Article 9(2) of the GDPR - the first of which is where the individual has given their 'explicit consent.' This means that the consent must be affirmed by a clear statement from the individual - for example, by providing them with an active mechanism (e.g. the ability to tick an opt-in box) - it cannot be implied from their actions.

As before, consent must be specific, informed and freely given. However, the GDPR generally imposes a higher standard of consent than was previously required. Broadly worded and/or blanket privacy notices will not be sufficient. The different purposes for which the personal data may be used must be spelled out clearly, and data subjects should be given appropriate granularity of control over their data, with, for example, multiple opt-ins to consent (or withhold their consent) to the different uses of their data. They must also be provided with the ability to withdraw their consent at any time.

So, depending on its features, a medication reminder and prescription ordering app would normally need to have layers of consents - for example, allowing a user to decide separately whether to share their medicine regime with their carer, or to pass on their adherence statistics to their GP (in addition to the data that would be necessary to send to the GP in order to process their prescription requests).

If, for some reason, explicit consent cannot be obtained, the data controller must ensure that it can rely on an alternative ground for processing the health data under Article 9(2) of the GDPR. Other grounds include Article 9(2)(h), which, in very broad terms, allows processing for the purposes of providing medical care and applies to healthcare professionals who are subject to a duty of professional secrecy. However, these grounds would not normally be available to app providers, and so consent is usually the best, or only, option open to them.

Article 9(2)(j) of the GDPR allows further processing of personal data beyond the purpose for which the data was originally collected, if this is done for scientific or historical research purposes or statistical purposes, provided that certain safeguards are observed. This would allow app providers to carry out analysis on their user data - for example, to establish medicine adherence trends and statistics - provided that they ensure that appropriate technical and organisational measures are in place, in particular to minimise the amount and sensitivity of the personal data being used. The data should be anonymised for these purposes or, if this is not feasible, pseudonymised, to the extent that it is possible in order to conduct the research.

The Proteus pill sensor, in particular, raises an interesting issue around consent. Its patients can choose whether to send their doctors data that shows when their pills are ingested. However, patients may feel pressure to consent where their doctors have prescribed them medication in a form that allows them to be monitored - so whether their consent is freely given (and therefore valid) is questionable. Some patients may also be troubled by the 'Big Brother' aspects of these solutions.

Closing remarks

Ultimately, how widely a pioneering solution such as a digital pill will be used will come down to how much it actually improves adherence, and a number of other key factors, including how users feel about the privacy issues, the (in)convenience of the solution (for example, the need also to wear a patch), the product's price and the ability, in an increasingly tough health budgetary environment, to get adequate reimbursement. We wait with interest to see Otsuka's pricing strategy for its digital version of Abilify, a widely used drug that has recently come off patent and now competes with generic versions. Will the addition of a digital sensor give its sales the edge?