Safe and Secure: How Digital Technology is Revolutionising Patient Privacy

PEER REVIEWED

There is no doubt that the clinical trials arena is undergoing a seismic technological shift. Slowly, but now with gathering pace, the pharmaceutical industry is beginning to embrace technology. The days of paper diaries are numbered, as digital solutions become more prevalent for eCOA (electronic clinical outcome assessment) and ePRO (electronic patient-reported outcomes) capture. Now, it seems that digitalisation of healthcare is unstoppable, as it provides increased adherence, better health outcomes and – ultimately – billions of pounds saved worldwide.

However, one vital element remains a source of much debate: the need to protect patient data and provide the most secure environment possible during a clinical trial. The need to protect patients' data has never been more important. Due to multiple, complex and varying regulations across geographic territories, full compliance with HIPAA, Safe Harbor and EU Data Protection requirements is central to safeguarding data privacy in clinical and commercial health services.

This comprehensive approach provides confidence for patients that their data will be safe, which, most crucially, reduces a major barrier to enrolment in multi-country programmes. The advent of global clinical studies has meant that sponsors need to consider the legislation that vendors are expected to adhere to in order to provide the level of confidence to all stakeholders. Therefore, it is imperative sponsors ensure that the vendors they contract with abide by the respective legislation that governs their main place of business, for example Safe Harbor if contracting with a US legal entity and expecting to collect EU patient data, and EU Data Protection if the vendor is based within the EU member states and collecting EU member states' patient data.

The pharmaceutical companies should not just check for the explicit privacy and security regulations, but also subtle measures which affect privacy policies. To do this, they can undertake an audit to ascertain what the vendor does in its business day-to-day. The sponsor should not only check for the relevant certifications, but also establish a feel for how seriously the vendor takes data protection, and what status it is held at within an organisation, how important is it to that organisation and how willing it is to explain its privacy and data protection processes.

Of course, nothing is perfect. As for other industries, such as banking and insurance, there is no guarantee even with the most stringent checks in place that personal data – both at rest and in transit – is 100 per cent secure. However, with the correct foundations in place, providers can ensure maximum possible security and that the data isn't easily compromised. This should start with the highest standard of quality management system (QMS).

The QMS should dictate an adherence to privacy at every level. The environment which hosts data should be independently validated and include an intrusion detection system to protect against security threats. An audit trail of data changes is also crucial.

As a 'BYOD' (bring your own device) approach is becoming increasingly popular in carrying out clinical trials, complying with data privacy and security regulations becomes essential, whether it is being applied to eCOA data capture, or by programmes designed to engage patients in a clinical trial or health regimen.

The principal difference between a BYOD approach and a provisioned one is that BYOD is more cost-effective, alongside encouraging increased adherence from patients. This much has been proved. Controls have increased as the user of the device is being kept in contact without any qualification, and therefore it is important to place security at the heart of the technology to ensure that the highest standards of data security and safety are provided.

There has been some misinformation that provisioned devices are naturally more secure than use of personal devices. This isn't strictly true. Best practice is to understand data protection regulations and develop a platform that complies with regulation guidelines. Through ensuring separation of personally identifiable information (PII), the use of data encryption for locally stored data on the device, in transmission (i.e. over the internet), within study databases, and the inclusion of permissions for data handling in the ethics/IRB-approved consent process, it is possible to build security and protection controls into software, whether delivered through a provisioned device, or, in the case of a BYOD approach, the patient's own mobile device.

We have seen first-hand that more and more pharma companies are working with vendors who have taken these steps and incorporated them into the way they run their business. Ultimately, security in the mHealth arena cannot afford to be compromised, and neither does it have to be. With increased security comes timely engagement, an improved user experience, and – perhaps most important of all – better health outcomes.

Dale Jessop, Chief Technology Officer leads the technology group at Exco InTouch and is responsible for directing the technology strategy of the business. As a software engineer himself, Dale is passionate about software development and has been involved with architecting a variety of systems since the late 1990s.
Email: info@excointouch.com