Digital healthcare: mind the privacy gap

Healthcare

These are exciting times for digital healthcare. New business processes and business models are enabling individuals to understand more and quantify more about their health, their conditions, and their genome than ever before.

But this creates enormous security and privacy issues. "If people share their medical information with a technology company, who owns the data?" asks Caroline Rivett, head of KPMG's Information Protection team in Life Sciences and Healthcare. "How can or should the company share it? What implications does this have for the individual – and for their family members?"

The much-needed debate on privacy matters is starting in areas such as genome mapping for cancer research. But it will need to extend beyond that to other applications, in particular medical devices.

Medical monitors are becoming more widespread thanks to greater connectivity and the growth of the Internet of things. Their use raises a host of privacy concerns. "Who collects the data from the monitors, what do they do with it, how do they share it, and do they get appropriate consent? These are some of the questions consumers are beginning to ask," says Rivett.

The EU General Data Protection Regulation 2016 addresses these and other privacy issues. Organisations have a two-year grace period to comply with the new rules, meaning those affected will need to have appropriate procedures in place by May 2018.

A number of companies are starting to prepare for the new regulations and are in the early stages of carrying out privacy impact assessments. To date this has generally involved understanding how the data flows from a monitor into a collection device, such as a phone, and then into a database, often in the cloud. "They are seeing how the data flows, how it is protected – and what the impact would be on the individual concerned if the data were lost or its integrity compromised," Rivett says.

However, she thinks that many companies are being too superficial in their assessments. "Few are taking it to the next stage: thinking about who they share that data with, how they are going to use the data in the future, and what consent they need from their customers".

And sharing and consents is just the start. Organisations are often shocked to find there is not one, or two, but 35 different activities they need to consider in terms of personal and confidential data. "This is still an emerging area as companies work out what regulations apply to them, with some of these rules already in force and others still waiting to be implemented. But too many are leaving it to the last minute to get their heads around the full security and privacy implications of their business models," Rivett says.

What should companies be doing? After understanding data collection and data flow processes, they need to understand how the data is being protected and how it is being used. Organisations need to consider whether they have the appropriate resources and expertise to provide the necessary input to ensure privacy risk is managed to an appropriate level. Then they should assess their business practices to understand the wider control framework rather than specific issues in relation to a single product. They should also review the regulations in the countries in which they operate to make sure that they comply with these rules.

This matters, not just because of regulation, but because of individuals' views on use of their personal data. Commissioned by KPMG in the UK, a survey conducted by One Poll Limited looked into this. The research asked 1,000 adults questions about medical devices, data privacy, electronic health records and third-party involvement.

While nearly three-quarters of respondents said they would be happy to wear a medical device that monitors their health and reports back to their GP, the proportion willing to share information drops as the data is more widely shared.

Just under one-half of respondents would be happy to add their medical records to a single national NHS database that could be accessed by any medical practitioner in the UK.

And more than three out of five would not want aggregated data from a connected device to be shared with healthcare companies that might contact them about healthcare products.

"The message is clear," Rivett says – "Data privacy continues to be a sticking point for individuals. Societal expectations about the use of data from digital healthcare are not keeping pace with the rapid advances in technology driving new products. Device makers, data transmission and data storage companies must keep up with regulations. But they also need to think very carefully about individuals' expectations about third-party access to their personal health information."

Caroline Rivett

Manager
KPMG in the UK

Share your views and join the debate:

Visit us
kpmg.com/uk/healthcare

Email us
publicsectormarketing@kpmg.co.uk

Engage with us
Follow us on Twitter @
KPMGUK

CRT068831 | December 2016