How can we be sure that our health data is secure?

7 DECEMBER 2017 • 2:45PM

Rob Waugh

The open economy promises exciting opportunities for the healthcare sector, but health providers first need to ensure they are up to speed with cybersecurity

In May this year, the WannaCry cyber attack hit 47 NHS organisations across the country, with operations delayed as computers were infected by malware – itself built using leaked "cyberweapons".

Within 24 hours, 95pc of NHS services were up and running again, but the episode raised important questions about how secure patient data really is.

There are huge benefits to sharing health data – but health providers need to ensure patients can trust them with it. That's why, across the UK, NHS organisations are upgrading their technology while ensuring patient data remains safe, according to Ciaron Hoye, head of digital at NHS Birmingham and Solihull Clinical Commissioning Groups.

The group now uses "zero client" laptops with no hard drives, local operating systems or memory, meaning all data and applications are stored in the cloud. This means cybercriminals have less of an opportunity to get a foothold.

Mr Hoye says that switching to a cloud-based approach also pays dividends for patients: "In addition to the security implications, another key benefit of moving healthcare applications to the cloud is the ability to break down siloes between different departments."

He also says the switch allows doctors to access records faster, which means patients can get the right treatment more quickly. "This offers a far more joined-up service for patients," he explains, "as they will see a reduction in time spent in and between appointments, with diagnostic information more readily available.

Moving fast: it's crucial that NHS trusts prioritise security when upgrading technology CREDIT: GETTY

“Instead of waiting for records to be shared between practices, the information will follow the patient, enabling quicker and better-informed diagnosis.”

It’s key that NHS trusts take an approach that puts security first when upgrading their technology, according to Nick Wilson, managing director of public sector, health & care, at software company Advanced. “There’s no doubt technology will improve the quality of services for the public,” he says. “We have seen the Government launch a strategy that intends to make some of the most high-volume services ‘digital by default’.”

But Mr Wilson says that patient data is a special case when it comes to cybersecurity: “Fundamentally, the protection of patient data must be fail-proof. It’s bad enough if financial data gets leaked but it’s absolutely unacceptable if personal data is mishandled and gets out publicly.”

Putting privacy first

The huge amount of data held by the NHS could also offer a boost to medical research, says Andrew Rogoyski, vice president, cybersecurity, at global IT consultancy CGI, but it’s key that organisations stay abreast of privacy concerns.

With the EU’s General Data Protection Regulation (GDPR) coming into effect on 25 May next year, UK businesses will face strict rules over how personal data can be used.

As Mr Rogoyski points out: “Healthcare data covers a lot of ground, from appointment data and patient letters to clinical records, radiology images, test results and other forms of data. These are processed by a huge variety of different systems.”

So if the NHS were able to “share” data between different systems, it might offer useful insights for doctors and researchers. But trusts need to ensure they adhere to security guidelines. Mr Rogoyski says: “There are specific rules in GDPR about using pseudonyms when private sensitive data is shared: the original data subject should be impossible to identify.”

This holds promise for medical research, but there are security concerns, as it is often possible to combine data from different sources to identify the original subject – a so-called “jigsaw attack”.

The key is that healthcare providers need to be open about what steps they are taking to protect patient data, according to Dr Ben Silverstone of Arden University. He says: “Organisations like the NHS hold so much data about individuals – more than most people are
aware of – but how the data is used and why it is kept is never really discussed in an open and user-friendly way.

“Data security, especially in the case of the NHS, needs to be discussed openly to assuage the concerns of the public.”