Your patients' attitudes towards cyber security

The currency of cyber trust

Cyber security is now a core public service responsibility – and critical to the evolution of modern healthcare services.

Cyber security in the UK today

As cyber crime rises and public services are increasingly digitalised, public opinions on cyber security are changing. People are becoming increasingly careful about how they share their information and more aware of organisations who might fail to protect it. To find out more, we surveyed over 3,000 UK citizens to explore how and why attitudes and behaviours around cyber security are evolving and what this might mean for healthcare organisations.

With healthcare organisations working hard to meet complex demands, digital technologies and electronic data are increasingly part of everyday services. UK citizens' lifestyles and expectations are also changing. They want more access to information and services via our smartphones, tablets and wearable devices. Whether it's ordering a prescription or getting care and advice for a long-term condition, digital access to healthcare will continue to grow.

All this places cyber security firmly on healthcare organisations' agenda. Unsurprisingly, as our survey found, medical information is among some of people's most precious data.

Changing awareness

There have been recent wake-up calls to the consequences of a data breach. The consequences of failing to meet public expectations of cyber security can be severe – including impacts on services, on patient experience and on reputation. It makes sense that public awareness of cyber security risks is growing. 73% of respondents say they are aware of global cyber attacks, with 66% believing that the chances of organisations suffering a cyber attack have increased over the last 12 months.

Not surprisingly, changing awareness has eroded public trust. Only 13% of our survey respondents say their trust in organisations has increased over the last two years and 38% say they do not trust organisations to store their data. Just 12% believe healthcare organisations are most able to protect themselves from a cyber attack.

36% of people say that their medical details are the personal information they value the most

12% of people believe healthcare organisations are most able to protect themselves from a cyber attack

1 in 10 people say that healthcare is the area they consider most at risk of cyber attack

Your report into cyber security in the UK today and the data behind our Digital Vision for Cyber Security

atos.net/cyber-research-uk

Atos

It's important to note that healthcare organisations are perceived as more capable of protecting themselves than other sectors, after government, defence and financial services. Yet healthcare needs to stay ahead of the curve – not least because medical data is so critical and because of the unique relationship between providers and service users.

Enabling digital access to healthcare

So, what does all this mean for healthcare organisations as digital access to healthcare increases? We asked people where responsibility for cyber security lies between organisations and individuals. We found a mixed picture and some serious gaps in understanding. While 87% say individuals need to take responsibility for keeping their information safe online, 40% don't take any active steps at all to protect themselves and over half (52%) say this is because don't know how.

Perceptions and knowledge about personal responsibility and cyber security will be crucial as digital transformation continues. Cultural change to encourage and empower citizens increasingly to 'own' their own data needs to be supported by public awareness of how to keep that data safe. Ultimately, as our survey explores, cyber security should be a partnership between healthcare organisations and citizens.

Building wider trust

To underpin public trust, our survey points to the benefits of raising public awareness not only of what citizens should do, but also of the measures that healthcare organisations themselves are taking.

Our findings also show that the public recognises the importance of using advances in technology to protect their data, with expectations of healthcare organisations being relatively high in comparison with sectors such as retail and utilities.

While these technologies are all part of the picture, 58% of respondents also want cyber security defences to be managed by a combination of human insight and automated technology. Threat monitoring is critical and as cyber threats evolve, so must health organisations' capabilities.

To get a copy of the full report, download **The currency of cyber trust.**
atos.net/cyber-research-uk

Conclusion

New generations of citizens expect far more personalised interactions and digital engagement; and at the macro level, digital transformation is essential to make healthcare services more efficient and to drive down costs. That means cyber security must be integral both to the digital patient experience and to ongoing digital transformation.

Clearly there are challenges to stay cyber secure within budgetary constraints; success depends on implementing a comprehensive, proportionate, risk-based end-to-end cyber security strategy. But there are also opportunities to underpin essential service transformation and to underscore the public's wider trust in healthcare provision.

37% of people expect healthcare organisations to have password/PIN managers

26% of people expect healthcare organisations to have multi-factor authentication

Over half of people expect healthcare organisations to have data encryption

"Just as in every other part of our lives, health services are being transacted in an ever more digital, paperless way and this is essential to the evolution of healthcare. Citizens expect a more digital patient experience – and as guardians of patients' data, organisations have a duty to protect it.

This starts with education and making sure the essential infrastructure is in place. Then it's about continuously adapting to stay ahead of the threat. The responsibility is clearly with healthcare organisations and their partners to safeguard people, systems and data along every care pathway – innovating today to protect for tomorrow."

Pooven Maduramuthu
Vice President, Health Sales,
Atos UK & Ireland

atos.net/cyber-research-uk