Jagvinder Singh Kang, partner and international & UK head of IT law at Mills & Reeve explains why 2022 could be an opportune time for healthcare organisations to re-examine their data protection compliance programmes

Key UK GDPR considerations

for healthcare organisations in 2022

As the burden of data processing intensifies, healthcare providers have been quick to adopt new technology such as Cloud Computing and AI. It's a trend which has been accelerated by the Covid-19 pandemic and subsequent move to digital and remote working as well as greater international collaboration.

However, adoption of new technology in healthcare comes with a very unique set of problems, from cyber criminals looking to leverage ransomware opportunities to disrupt critical medical healthcare provision to patients' legitimate expectations of privacy and transparency in the use of their health data. What is common to both is the importance of data protection law compliance.

But there is a mismatch in the way certain healthcare organisations approach cyber and data protection law compliance. They treat them as discrete and separate elements, when they are, in fact, symbiotic. Consequently, a truly holistic approach needs to be adopted by healthcare organisations.

Why UK GDPR is a good thing...if done correctly

The UK General Data Protection Regulation (GDPR) has received 'bad publicity'. It has been seen by certain organisations as bureaucratic and simply a 'tick-box exercise' to try to avoid the hefty potential fines (namely, the greater of £17.5m or 4% of global annual turnover). However, any organisation which approaches compliance in this narrow manner will be 'doomed to failure' when it comes to UK GDPR compliance and guarding against cyber risks. Such an approach also undermines the whole point of the UK GDPR.

> THERE IS A MISMATCH IN THE WAY CERTAIN HEALTHCARE ORGANISATIONS APPROACH CYBER AND DATA PROTECTION LAW COMPLIANCE

The UK GDPR has at its 'heart' seven key principles around the processing of personal data:

1. **Lawfulness, fairness and transparency** – having a valid legal ground for processing an individual's data. Furthermore, the processing must be in a manner which the individual is expecting.
2. **Purpose limitation** – the data must only be used for the purpose for which it was collected and which was notified to the individual
3. **Data minimisation** – only the minimum amount of information about an individual must be collected to fulfil the intended purpose
4. **Accuracy** – the accuracy of the data must be maintained
5. **Storage limitation** – the data must only be kept for the period necessary to fulfil the purpose for which it was collected
6. **Integrity and confidentiality (security)** – appropriate security measures need to be put in place to guard against data corruption, while also maintaining the confidentiality of the data
7. **Accountability** – the healthcare organisation must take responsibility for complying with the UK GDPR, while also being able to demonstrate how it achieves compliance.

If one considers the above, it is clear that the only way to achieve all of the above is to adopt a holistic approach which is embraced by healthcare organisations. Otherwise, what is achieved is a fragmented compliance model - opening up the healthcare organisation to risks.

This approach needs to extend to

data sharing, as well as to international personal data transfers – the latter is particularly topical in 2022. The position on international personal data transfers has become significantly more complex in the wake of the landmark Schrems II Court decision; Brexit, which has resulted in both an EU and a UK GDPR; and the new international data transfer agreements introduced by the Information Commissioner's Office in March 2022, which will require the healthcare sector to carefully plan and implement measures during the transition period up to the 21 September 2022 deadline.

Again, organisations that try to approach this under a misconceived view of it being a simple 'papering exercise' will be opening themselves up to considerable risks on both the cyber and data protection compliance fronts.

THE POSITION ON INTERNATIONAL PERSONAL DATA HAS BECOME SIGNIFICANTLY MORE COMPLEX IN THE WAKE OF BREXIT

Conclusion

It is an unfortunate fact that the lead up to the implementation of the GDPR in 2018 resulted in many organisations implementing and then building on 'weak foundations'. As is commonly said, the security of an organisation is only as strong as its weakest link. Likewise, a data protection compliance programme which has been built on a poor foundation cannot safeguard an organisation.

With the increasing focus on cyber threats, coupled with the recent changes in the data protection landscape, 2022 would be an opportune time for healthcare organisations to re-examine their UK GDPR compliance programmes with specialist data protection legal support. This would allow them to address any foundational issues and then build a strong compliance programme which tackles data protection compliance as well as cyber risk mitigation.