Cyber security: risk management for care providers

The use of technology within the care sector has grown significantly over the last few years as care providers embrace "smart" in the way they provide care. An increasing number of operators are using technology such as electronic care management systems, mobile devices, listening devices, digital records and video consultations.

Whilst the benefits are significant, the move from paper to paperless comes with security challenges which need to be addressed and managed, particularly in terms of protecting personal data. In 2016, a nursing home in County Atrim was fined £15,000 after an unencrypted laptop taken home by a member of staff was stolen in a domestic burglary. The laptop contained personal data relating to 46 staff and 29 residents. A subsequent investigation by the ICO found widespread data protection failings across the home. The matter was widely reported in the national press, bringing bad publicity as well as financial consequences for that operator.

Since then the Data Protection Act 2018 has come into force, further tightening the data protection rules for businesses and increasing the level of fines that can be imposed for breaches.

Cyber security should be a high priority for care businesses, both in terms of taking practical steps to reduce the risk and ensuring adequate insurance is obtained to cover losses should a mistake (inevitable for humans!) be made. The following are useful safeguards that providers can put in place to protect their organisations:

- Ensure that data protection policies and procedures are GDPR compliant and regulate data sharing and contracts with third parties who may receive the organisation's data as part of services provided to it. It sounds basic but many operators have not put this in place yet, despite the legislation being 2 years old.

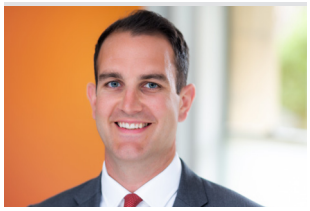
- Check that there are formal contracts in place with third parties with whom data is shared as part of the provision of IT services. These need to cover how the data can be used, whether it will be processed overseas and how it will be destroyed.

- Provide staff with basic practical cyber-security training at induction and at regular intervals including the use of strong password protection, locking devices, storing them safely, verifying bank account details when making and receiving payments and restricting the use of shared generic email accounts.

- Be aware of trends in cyber-fraud and update staff as and when necessary. The COVID-19 pandemic has brought new risks as cyber-fraudsters take advantage of the crisis to breach security systems. In the everyday of operating front-line care it can be easy for staff to click on am erroneous phishing link which can compromise security.

- Ensure that the identity of third parties who are in contact with the business, whether by phone or email, is verified before personal data is shared and that sensitive information shared by email is encrypted.
- Take out and scrutinise the small print of your cyber-liability insurance and check it offers you the protection that you need. These policies are by their nature detailed and drafted in a complex fashion so take professional advice if you are not sure.

Your key Social Care contacts



James Sage
Partner
T: 07508 297 597
james.sage@roydswithyking.com

Hazel Phillips
Partner
T: 07776 241 235
hazel.phillips@roydswithyking.com

Mei-Ling Huang
Partner
T: 07944 996 256
mei-ling.huang@roydswithyking.com

royds withy king
lawyers ahead of the curve