Virtual Group Consultations Cyber Insurance Overview

The key to successfully buying cyber insurance is time, research, and a thorough, transparent risk assessment. Anyone handling personally identifiable information, which is essentially any information that can be used to identify a specific person, you're required to comply with the General Data Protection Regulation (GDPR).

As important as this is, both accidental breach of privacy and malicious cyber-attacks put you at risk of huge unexpected expenditure. Violating GDPR could land you with a fine of up to €20 million, or up to 4% of your annual turnover for the preceding financial year, whichever is greater. And on top of this, there are legal and compensation payments to consider, for those whose data has been compromised.

Cyber/Data insurance normally includes cover for those regulatory penalty's insurable bylaw, your legal defence costs and compensation payments.

What is Cyber/Data Insurance?

Typically, a cyber/data insurance policy will cover losses and damages incurred by a breach or security event that includes the loss, exposure, improperly shared, or theft of patient data. Some coverage will also handle ransomware attacks, but health providers must ensure that the correct language is added to coverage when negotiating with an insurance agent.

However, unlike with traditional insurance policies, there's no standard format for underwriting these types of policies. Therefore, the burden falls to the purchasing team to research the differences in carriers, such as amounts and requirements of the holder. For example, coverage will be broken down into first-party or third-party.

The coverage will either be limited to the purchasing organisation itself or extend to the organisation's covered entities, in the event of cyber threat, breach, and other security incidents.Cyber insurance may also cover the costs of investigations following the breach, along with the cost to notify patients and the public. To start the purchasing process, an organisation will need to work with a cyber insurance agent to identify the different types of policies. Typically, the greater the coverage, the more the policy will cost.

What's included in your cyber cover?

Most cyber insurance policies cover (not exhaustive):

- Protects you for any GDPR non-compliance claims.
- Gets you back to business as usual, as quickly as possible where reputational damage is caused.
- Compensates for loss of income as a result of a data breach.
- Manages data breaches with forensic investigations, legal advice and notifies customers or regulators.
- Covers you for the costs of repair or replacement if you're hit by a cyber-attack that damages your equipment.

References

1. https://www.digitalrisks.co.uk/blog/4-reasons-to-consider-cyber-insurance/
2. https://healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations
3. https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance

Disclaimer: Due to the nature of the subject, the main sources of information are within the commercial sector. This cyber insurance is based on information taken from NHS England and NHS Improvement guidance, however by siting this information we/they are in no way recommending any of these commercial businesses and their respective products. Providers should make their own considerations based on their needs.