Cymorth Llywodraethu Gwybodaeth ar gyfer Gofal Sylfaenol
Information Governance Support for Primary Care
IGDC • DHCW

IG Guidance for Primary Care Services

Cyber Insurance

Introduction

As independent contractors, it is the practice's responsibility to consider the most appropriate insurance cover to put in place based on the practice's risk appetite and perceived risk of a cyber event occurring. This guidance aims to support practices when deciding whether cyber insurance is a suitable product for them.

A cyberattack can impact a practice in many ways, for example:

- loss or damage to electronic information – health and corporate records;
- additional expenses – extra costs incurred in keeping the practice operating;
- network security and privacy lawsuits – individuals sue you for failure to protect their information;
- notification costs – expenses incurred when notifying individuals of attack/breach;
- reputation – potential damage to the reputation of the practice;
- fines and penalties – issued under Data Protection Act 2018 by the ICO, up to 4% of annual turnover or £17.5 million, whichever is higher.

When deciding if cyber security is a high risk for the practice, you should consider the implications of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), as well as other risks in everything the practice does and make necessary changes to protect your information and systems.

When IT systems are secure, cyber attackers see people as the weak link. Therefore, it's imperative that all staff have relevant training to help them spot a scam and to understand the importance of being vigilant.

Documented information/cyber security policies and procedures will help reinforce the message with staff to stay vigilant and keeps data protection and system security forefront of minds. Back-up plans in your Business Continuity Plans are essential for continuing to run the practice if a breach is suffered.

What is Cyber Insurance?

Cyber insurance can have several terms, for example, cyber risk insurance or cyber liability insurance coverage. Like any other type of insurance, it is an insurance policy that helps to mitigate risk exposure due to a cyber security breach or event. It will normally cover your practice liability for a data breach.

These policies can vary in their coverage, therefore it's important to check if they meet the requirements of the practice.

What is a Cyber Event?

As more and more processes and transactions occur online, the number of cyber events has increased, and risks being exposed in all businesses. Cyber events can be anything from a specific attack or cybercrime, for example, malware, ransomware, phishing. Or cyber events could be distributed denial-of-service-attack which are because of hacking or insider threat; both malicious and non-malicious.

Is Cyber Insurance compulsory?

Cyber insurance is not compulsory.

However as with any type of insurance, the practice will need to decide its level of risk and if it requires insurance to offset any costs due to a cyber event occurring.

What is covered by Cyber Insurance?

Cyber insurance can be costly, and you should carefully consider what you are insuring against. Policies under the heading of "Cyber Insurance" can cover a number of things. The following details the most common coverage however, each policy will be different, and you should always check the details carefully, including cover provided and any mitigations you need to have in place.

Investigation

Policies will sometimes cover what is called forensic investigation. This is specialist investigation that takes place to determine how the cyber-attack has occurred, repair damage to network of infrastructures and remediate/fix the problem so it cannot happen again.

Note: Practice networks and infrastructures are fully managed by Digital Health and Care Wales (DHCW), this means that any significant event will be managed and co-ordinated by DHCW and therefore this type of insurance is likely to cover a very small element of practice business processes. DHCW will not allow third parties to complete remediation on its network or to its hardware. In most cases this type of policy will not be relevant to practices.

Business Losses

Some cyber policies may cover the practice for losses experienced by network down time or business interruption, they can also cover additional costs for managing a significant event.

Note: Practices will not be covered by the Health Board or DHCW for their business losses. In some cases, practices may already have cover for business loss or interruption as part of other insurance policies. You will need to check the cover carefully and decide if this is required or meets your needs.

Privacy and Notification

Some policies will cover notifying and managing incidents on your behalf, along with providing additional services like access to credit reference checking for all individuals whose data has been subject to the breach.

Note: If you are a subscriber of DHCW's enhanced Information Governance and DPO Support Service, the service will assist you in reporting your incident to the ICO and responding to incidents, when required. Additional services such as access to credit monitoring will not be covered by the DPO Support Service, therefore practices will need to check this cover and carefully decide if this is required to meet your needs.

Legal Claims and Expenses

Such policies may provide cover to support with legal expenses, for example loss of confidential information, and cyber extortion.

Note: Practices should contact General Medical Practice Indemnity (GMPI) and current Medical Defence Union (MDU) cover to check provisions available to them for legal support.

GMPI in most cases only covers clinical negligence and will not cover practices for claims or legal expenses relating to Data Protection Breaches. Practices will need to check what cover is already in place and if the additional cover offered meets the needs. These are the most common types of cover however this area is evolving, and cyber risks change frequently, so it's important to review and check the cover.

Is this cover not included under my general liability policy?

General liability policies cover injury and property damage, cyber events are often excluded from general liability policies.

What should be considered when comparing policies?

When comparing policies or looking for cyber insurance you should consider the following:

- Does the insurer offer different types of cyber insurance policies?
- What is the cover being offered? Can you customise this?
- Consider what insurance you already have in place, are you already covered elsewhere?
- What are the limits of the cover?
- What 'parties' does the policy cover? Policies will often refer to the first party (i.e. the practice investigation and support) and third party (i.e. patients or suppliers claiming against you or legally defending a claim)
- What will the practice have to do or prove for a claim to be paid out? i.e. do you have to do regular security checks or gain certain assurance, watch out for clauses.

• Does the policy cover any type of attack or just certain ones? i.e. does it cover social engineering as well as network attacks?

• Does the policy cover non-malicious actions taken by an employee?

• What are the timeframes for cover and reporting? For example, attacks can take place over time which can be detected months or even years after the attack has occurred, what are the time limitations of the policy?

• What is the excess amount?