PSC MEDIPROTECT
INSURANCE BROKERS

SHIELD YOUR DAY HOSPITAL FROM CYBER THREATS

6-Step Cyber Protection Checklist

Protect your data, operations, and patients in an increasingly digital world.

In today's healthcare landscape, day hospitals are increasingly reliant on digital systems to deliver care, manage patient information, and maintain operational efficiency. With this growing dependency comes heightened exposure to cyber risks, such as data breaches, ransomware attacks, and system failures. Cyber Liability Insurance is a critical tool in mitigating these risks, ensuring that your hospital remains protected from the financial and operational fallout of a cyber incident.

At PSC Mediprotect, we understand the unique challenges facing day hospitals, and we've developed this checklist to help you evaluate your cyber protection and ensure that your insurance coverage is aligned with the risks you face. By following this guide, you can safeguard your operations, maintain patient trust, and mitigate the potential damage from cyber threats.

Warm regards,

Your PSC Mediprotect Team

Disclaimer
Please note that the information provided in this guide is intended for general informational purposes only. It is not designed to be comprehensive nor to offer specific advice tailored to the unique circumstances of your business or individual situation. We strongly recommend consulting with a PSC Insurance Brokers professional to discuss your specific needs and to obtain advice that is tailored to your particular circumstances. The descriptions of insurance coverage are simplified and are subject to the terms, conditions, and exclusions of the actual policies. Always read your policy documentation carefully and discuss any questions or concerns with your insurance advisor.

PSC MEDIPROTECT INSURANCE BROKERS

Claims Examples

Real-World Cyber Incidents in Day Hospitals

Ransomware Attack Shuts Down Operations

A day hospital was hit by a ransomware attack that encrypted their patient records and locked them out of their booking and billing systems. Although the ransom demand was only $5,000, the hospital faced nearly $600,000 in costs to restore data, improve their cybersecurity infrastructure, and manage the financial losses from business interruption. The ransomware attack halted operations for three days, disrupting patient care and delaying critical appointments. Cyber Liability Insurance covered data recovery, forensic investigations, and business interruption costs.

Data Breach Exposes Patient Information

An administrative staff member at a day hospital inadvertently emailed a spreadsheet containing sensitive patient information to the wrong recipients. The email included patient names, medical conditions, and Medicare numbers. The hospital incurred significant costs to notify affected individuals, comply with regulatory reporting requirements, and provide credit monitoring services to patients at risk of identity theft. Cyber Liability Insurance covered the hospital's costs for patient notifications, compliance with privacy regulations, and legal fees associated with the breach.

Phishing Scam Leads to Financial Loss

A day hospital's finance department was targeted by a phishing email that appeared to be from a trusted supplier. After clicking on a link in the email, the finance manager unknowingly provided login credentials that allowed cybercriminals to access the hospital's accounts payable system. Over the next few weeks, fraudulent invoices were processed, leading to losses of over $150,000 before the breach was discovered. Cyber Liability Insurance covered the financial loss and the cost of implementing additional security measures to prevent future attacks.

IT System Failure After Cyber Attack

Following a cyberattack, a day hospital experienced a complete failure of its IT systems, affecting scheduling, imaging, and billing operations. The hospital had to revert to manual processes for patient care and documentation while the systems were restored. Cyber Liability Insurance covered the costs associated with data recovery, IT system repairs, and the additional staffing required during the downtime.

Cybersecurity is no longer optional in today's healthcare environment—it's essential. By following this checklist, you can ensure your day hospital is well-protected against cyber threats. At PSC Mediprotect, we are committed to working with you to assess your cyber risks and provide tailored insurance solutions that fit your needs. Whether you're updating your existing coverage or exploring new options, our team is here to guide you every step of the way.

PSC MEDIPROTECT INSURANCE BROKERS

Checklist

Protect your data, operations, and patients in an increasingly digital world.

1. Assess Your Exposure to Cyber Risks

- [ ] Identify all digital assets (e.g., patient databases, medical software, financial systems) that could be vulnerable to a cyberattack.
- [ ] Evaluate the security measures in place, such as firewalls, encryption, and antivirus programs.
- [ ] Consider the sensitivity of the data you store, particularly patient health information (PHI) and financial details.
- [ ] Understand the potential impact of a cyber breach, including operational downtime, patient care disruptions, and reputational damage.

2. Review Your Current Cyber Liability Coverage

- [ ] Ensure your policy includes coverage for common cyber threats such as data breaches, ransomware attacks, and denial-of-service attacks.
- [ ] Confirm that the policy covers the cost of notifying patients and authorities in the event of a data breach, including compliance with legal obligations.
- [ ] Verify if cyber extortion (ransomware) coverage is part of your policy, including negotiation and payment assistance.

3. Evaluate Incident Response Capabilities

- [ ] Ensure your policy includes access to a 24/7 incident response team that can guide you through immediate actions following a cyberattack.
- [ ] Confirm coverage for legal and forensic experts to investigate the breach and identify vulnerabilities.
- [ ] Check if the policy offers public relations support to manage any reputational damage following a data breach or cyber incident.

4. Understand Third-Party Liability

- [ ] Make sure your policy covers claims made by third parties, such as patients or vendors, who are affected by a data breach.
- [ ] Review the scope of coverage for regulatory fines and penalties, including those related to non-compliance with the Privacy Act or other relevant data protection regulations.
- [ ] Assess the adequacy of your coverage in case of lawsuits resulting from compromised patient data or financial loss caused by cyberattacks.

5. Consider Coverage for System Failures and Downtime

- [ ] Ensure that your cyber liability policy covers system failures that lead to significant downtime, disrupting patient care and hospital operations.
- [ ] Evaluate if your policy covers losses due to failed IT systems, including software crashes and hardware malfunctions, caused by cyber events.

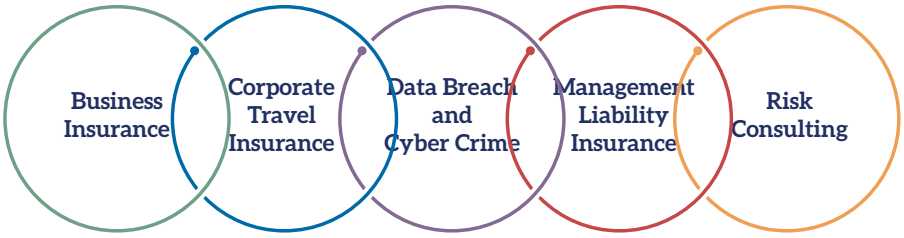
6. Explore Employee Negligence and Insider Threats

- [ ] Confirm that your cyber insurance policy covers incidents caused by employee negligence, such as accidental data leaks or improper handling of sensitive information..
- [ ] Assess coverage for insider threats, where employees or contractors intentionally compromise your systems for personal gain.

About PSC Mediprotect

For more than 20 years our team has been providing insurance broking and risk advisory services to small and medium sized primary and community health organisations across Australia. Combining our passion for the healthcare sector with our extensive insurance market knowledge, we strive to deliver a service acknowledged by our clients as valuable and personal.

As part of the multi-national PSC Insurance Group Limited, we have offices across Australia providing local support when needed. We have considerable buying power when negotiating with insurers and we use our collective knowledge to ensure your business is appropriately covered according to your needs and budget.



Our service offering includes:

- Accessing an extensive range of Australian and International Insurers to allow us to provide the most suitable solution for your needs.
- Insurance risk reviews that recognise every business is unique. This review helps ensure your insurance cover matches your risks.
- A dedicated in-house claims team that advocate on your behalf with insurers to optimise claim outcomes.
- Business interruption reviews to provide an assessment of the potential for loss of revenue and for increased costs following a claim.
- Education of directors, executives and advisory committee members.
- A national healthcare team focused on understanding every customer, every policy and every risk.

Servicing clients with branches across Australia

We help thousands of businesses every day

Our global reach provides additional risk solutions

Our skilled brokers make us your best partner

No matter how large, we always make it personal

Request a quote

For more information contact your dedicated PSC team:

Rachel Middendorp
Senior Account Manager
0448 225 908
rachel@mediprotect.com.au

Ashley Naylor
Managing Principal
0478 839 525
a.naylor@pscinsurance.com.au

PSC Mediprotect Insurance Brokers
ABN 74 088 790 327 | AFSL 234 421 A member of BrokersLink Global Alliance.
Please refer to our Financial Services Guide on our website for information on our products and services and how we are remunerated.

PSC MEDIPROTECT INSURANCE BROKERS