MEDICAL PRACTICE RESOURCE

Cyber Incident Response Checklist for Medical Practices

A calm first-response guide for suspected email compromise, malware, unauthorised access or loss of technology services.

REVIEWED	Ashley Tietze, Managing Director
UPDATED	3 August 2026
USE	Planning aid - not a compliance certification

How to use this resource

Work through each item with the people responsible for the process. Record evidence, an owner and a realistic due date for every gap. The online version provides related guidance and service links.

01 The first 15 minutes

1 Call the incident contact

Explain what was observed, when it began, who is affected and whether clinical work is disrupted.

Evidence / owner / due date: _____

2 Keep the affected device available

Disconnect only when directed. Do not wipe, reset or continue investigating it yourself.

Evidence / owner / due date: _____

3 Use a known-safe channel

If email may be compromised, coordinate by telephone or another approved channel.

Evidence / owner / due date: _____

4 Record decisions

Start a factual timeline of observations, calls, containment actions and decision makers.

Evidence / owner / due date: _____

02 Contain access and communication

1 Protect identity

Revoke suspicious sessions, reset affected credentials safely, enforce MFA and inspect forwarding rules.

Evidence / owner / due date: _____

2 Control remote access

Review VPN, Remote Desktop and support tools. Disable unexplained access while preserving evidence.

Evidence / owner / due date: _____

3 Brief staff

Tell reception, clinicians and administration what to stop, which channel to use and how to report symptoms.

Evidence / owner / due date: _____

4 Protect payments

Independently verify payment-detail changes and contact relevant banking personnel when fraud is possible.

Evidence / owner / due date: _____

03 Clinical systems and recovery

1 Engage vendors through known contacts

Confirm impacts to practice software, prescriptions, pathology, imaging and hosted services.

Evidence / owner / due date: _____

2 Activate approved downtime procedures

Protect patient safety without creating uncontrolled copies of sensitive information.

Evidence / owner / due date: _____

3 Validate before reconnecting

Confirm containment, secured accounts, clean restoration and active monitoring.

Evidence / owner / due date: _____

4 Hold a structured review

Document causes, impacts, notifications, improvements, owners and follow-up tests.

Evidence / owner / due date: _____

IMPORTANT CONTEXT

Do not place patient information, passwords or incident evidence into public websites or general-purpose AI services. Preserve evidence in approved systems and follow legal, insurer and regulatory advice.

Open the current online guide and related resources

Podium IT | (03) 8578 3077 | podiumit.com.au