# CYBER SECURITY CHECKLIST FOR PHYSIOTHERAPISTS & SMALL HEALTH PRACTICES

BLACK SWAN
CYBER SECURITY SOLUTIONS

Protect your patient records. Maintain confidentiality. Support compliance.

You handle highly personal information - medical histories, treatment notes, exercise plans and referral letters. If this data is lost or accessed unlawfully, it can breach GDPR and the NHS Data Security & Protection Toolkit (DSPT) requirements (where relevant).

Use this checklist to make sure your practice keeps patient data safe and trust intact.

## 1 Access & Authentication

- [ ] Enable Multi-Factor Authentication (MFA) on all systems — especially email, booking and clinical record platforms.
- [ ] Give each team member their own unique login.
- [ ] Store passwords securely in a password manager (e.g. Keeper).
- [ ] Ensure passwords are strong (at least 12 characters or three random words).
- [ ] Do not reuse passwords across systems.
- [ ] Remove access promptly when staff or locums leave.
- [ ] Limit administrator rights to essential users only.
- [ ] Use account lockout after several failed login attempts.
- [ ] Follow a secure password reset process that verifies identity.

## 2 Email & Communication Security

- [ ] Use advanced phishing protection.
- [ ] Enable MFA on all staff email accounts.
- [ ] Use encryption for patient reports, referrals and invoices.
- [ ] Transfer sensitive attachments using secure messaging or file transfer tools.
- [ ] Display external email warnings to highlight potential risks.
- [ ] Train staff to identify and report phishing or suspicious messages.
- [ ] Configure DMARC, SPF and DKIM on your email domain to stop spoofing.

## 3 Data Protection & Backup

- [ ] Back up patient data and booking systems daily.
- [ ] Use immutable cloud backups and test restores regularly.
- [ ] Store backups in the UK or another GDPR-compliant region.
- [ ] Encrypt devices that store patient data (BitLocker / FileVault).
- [ ] Restrict access to treatment notes by job role.
- [ ] Ensure cloud systems comply with NHS DSPT or equivalent standards.

## 4 Device & Endpoint Protection

- [ ] Install Next-Gen Antivirus / Managed EDR on all computers.
- [ ] Enable automatic patch management for software and operating systems.
- [ ] Lock and encrypt mobile phones and tablets; ensure they can be wiped remotely.
- [ ] Encrypt and secure practice laptops when not in use.
- [ ] Regularly check that updates and security software are current.
- [ ] Keep a centralised asset inventory.

## 5 Network & Wi-Fi Security

- [ ] Protect Wi-Fi with WPA3 encryption and a strong password.
- [ ] Separate patient/guest Wi-Fi from clinical systems.
- [ ] Enable DNS filtering and web protection.
- [ ] Keep firewalls configured and updated.
- [ ] Change router admin passwords from defaults.
- [ ] Disable remote access to routers unless necessary and secured.

## 6 Staff Awareness & Training

- [ ] All team members complete annual data protection and cyber awareness training.
- [ ] Provide basic cyber hygiene induction for new starters.
- [ ] Run phishing simulations or short awareness campaigns regularly.
- [ ] Foster a no-blame culture for reporting mistakes or incidents.
- [ ] Set clear policies for personal device use when accessing patient data.
- [ ] Keep training records to evidence compliance.

## 7 Governance, GDPR & DSPT

- [ ] Maintain ICO registration and annual fee.
- [ ] Complete or work towards the NHS DSPT self-assessment if applicable.
- [ ] Keep an Information Security Policy and Data Protection Policy.
- [ ] Maintain Records of Processing Activities (who, what, why, how long).
- [ ] Appoint a Data Protection Lead or Caldicott Guardian where relevant.

## 8 Incident Response & Monitoring

- [ ] Have a clear process for responding to data breaches and cyber incidents.
- [ ] Retain logs for at least 12 months on key systems.
- [ ] Review Microsoft 365 or cloud audit logs for unusual activity.
- [ ] Use Managed Detection & Response (MDR) or 24/7 alerting.
- [ ] Review cyber insurance and confirm it meets DSPT and insurer control requirements.
- [ ] Test your incident response and recovery plan annually.

## Who this checklist is for

This checklist applies to:

- Physiotherapists
- Chiropractors
- Osteopaths
- Podiatrists
- Acupuncturists
- Private GP clinics and small medical practices
- Independent rehabilitation or sports injury clinics

BLACK SWAN
CYBER SECURITY SOLUTIONS

# Need Support?

If you'd like reassurance that your practice meets DSPT and GDPR expectations, we can help.

**Black Swan Cyber Security Solutions** - affordable protection for independent healthcare providers.


blackswancyber.co.uk

hello@blackswancyber.co.uk

01246 927142