MyPatients

CYBERSECURITY AWARENESS FOR MEDICAL PROFESSIONALS

PROTECTING YOUR PATIENTS, PRACTICE AND PROFESSIONAL REPUTATION

AS A MEDICAL PROFESSIONAL, CYBERSECURITY VIGILANCE IS CRUCIAL TO ENSURE THAT PATIENT CONFIDENTIALITY IS PROTECTED AND TRUST IS MAINTAINED.

WHY CYBERSECURITY MATTERS IN HEALTHCARE

Healthcare is one of the most targeted industries for cyberattacks due to the sensitive nature of patient data and medical records. A breach can lead to:

- Patient data theft
- Medical identity fraud
- Financial and reputational damage
- Legal and regulatory penalties (POPIA)

TOP 8 CYBERSECURITY PRACTICES FOR MEDICAL PROFESSIONALS

1. Use strong, unique passwords

ELEMENT	BEST PRACTICE
Length	Minimum 10-12 characters
Characters	Mix of upper case, lower case, numbers and symbols
Avoid	Personal information (name, birthdate, etc.)
Unique	Never reuse the same password across multiple platforms
Security	Use multi-factor authentication (MFA) wherever possible
Storage	Use a password manager (such as 1Password) for secure password storage

2. Watch out for phishing attempts

- Phishing is a scam where attackers attempt to deceive individuals into providing sensitive information, such as passwords, credit card numbers or personal details, by impersonating a trusted person or organisation, typically through email, SMS or fraudulent websites
- Do not click suspicious links in emails, SMSs or WhatsApp messages, even if they appear to come from medical boards or hospitals.
- Watch out for spelling errors, unusual links and messages that encourage urgent action.
- Be very alert for suspicious links that prompt you to enter your credentials.
- Keep your work-related and personal email addresses separate.

3. Secure your devices

- Lock your phone, tablet and PC when unattended – enable automatic locking.
- Use disk encryption to secure your files.

4. Protect patient records

- Never email patient records without encryption.
- Avoid storing sensitive data on USB drives or unsecured devices.

5. Update software regularly

- Ensure your operating systems, antivirus and apps are always up to date.
- Security patches fix known vulnerabilities exploited by attackers.

6. Be cautious when using WiFi in unsecured settings

Avoid accessing patient data or logging into systems via shared WiFi.

7. Report incidents immediately

- If you suspect a breach or malware infection or your device has been lost, notify the Mediclinic Service Desk on 0860 122 123 to have your Mediclinic account disabled or reset accordingly.
- In addition, reach out to your local IT provider to assist with containment and remediation.
- An early response can prevent further damage.

8. Know your legal obligations

- Familiarise yourself with POPIA regulations in South Africa and the importance of reporting certain data breaches to the regulator (inforegulator.org.za).
- Maintain documentation for patient data access, use and storage.

COMMON THREATS IN HEALTHCARE

THREAT TYPE	WHAT COULD IT LOOK LIKE?	HOW TO PREVENT IT
Phishing email	Fake lab results, invoice attachments, urgent login requests	Verify the sender email address
Ransomware	Files locked and encrypted – attackers demanding payment to restore access	Ensure your systems are backed up securely Ensure your systems are updated regularly
Data leak	Accidental sharing of personal files over WhatsApp/email	Use secure sharing platforms and verify the recipient
Stolen device	Unlocked phone Stolen laptop/device	Encrypt and lock all devices with strong passwords and multi-factor authentication

EXPERTISE YOU CAN TRUST.

www.mediclinic.co.za

1516IDWRW