CYBERSECURITY AND DATA SECURITY ESSENTIALS

CYBERSECURITY ESSENTIALS

UPDATE PROMPTLY
- Install updates for OS and applications
- Update clinic systems (CMS/EMR)
- Prioritise security patches

PROTECT DEVICES
- Install Anti Malware
- Enable automatic signature update and scanning
- Report suspicious activity

CONNECT SAFELY
- Use firewalls to block unauthorised traffic
- Avoid public networks and use trusted networks
- Use applications only from trusted sources

CONTROL ACCESS
- Unique accounts for all users
- Remove inactive/shared accounts
- Use strong passwords (≥12 mixed characters)
- Enable 2FA for admin/ remote access

ENSURE BACKUPS
- Regular backup of critical and essential data
- Align backups with recovery needs
- Store backups separately

MANAGE ACCESS
- Maintain hardware & software inventory
- Replace unsupported assets
- Authorise new IT assets

DATA SECURITY ESSENTIALS

STORE SECURELY

- Store records in secure, access-controlled locations
- Lock devices storing health info
- Apply confidentiality clauses for staff and vendors

CONTROL ACCESS

- Personnel should only access health info of patients under their care
- Personnel should acknowledge their data protection and security obligations before given access to health info
- Use screen-locks and privacy filters

TRANSFER SECURELY

- Password-protect files containing health info before sending by email
- Send the passwords through a different channel
- Check recipients' email addresses before sending.

COPY SECURELY

- Copies of health info should only be made by authorised personnel, and where necessary for work purposes
- Maintain possession of all copies of health info made at all times

COMMON CYBERSECURITY & DATA SECURITY ESSENTIALS

MANAGE THIRD PARTIES

- Understand the security services that IT service providers will provide, and ask for regular updates on security issues
- Understand the remaining steps that you need to take (e.g. configurations)
- Check service providers' certifications and safeguards

REVIEW SECURITY

- Review CS/DS measures periodically
- Review compliance with security measures
- Act promptly upon lapses

TRAIN PERSONNEL

- Ideally attend annual cybersecurity and data security training
- Develop basic cybersecurity and data security hygiene practices for personnel to adopt

SECURE DISPOSAL

- Shred physical records when no longer required
- Encrypt or overwrite electronic records

BUSINESS CONTINUITY

- Prepare for disruptions (e.g. when IT systems are compromised)
- Establish a continuity plan to ensure resilience

INCIDENT RESPONSE

- Set out clear roles and responsibilities for key personnel
- Detect, respond and recover from incidents
- Communicate with affected persons and regulators