| | KNOWLEDGE | | PRACTICE | | INFRASTRUCTURE |
|---|---|---|---|---|---|
| | Incremental improvement 1+ per month | | Store restricted data on servers only | | Enough UPS power to close out day |
| | Understand your obligations | | Ensure restricted data is password protected | | If cloud based, enough UPS to keep internet ON |
| | Build data sharing agreement clauses into contracts | | Personal username and password to EMR apps | | Dual power supplies to backbone items |
| | Understand where the data is at rest & where it flows | | DO NOT use admin privileges for routine work | | Create spreadsheet of all data locations |
| | Calculate your cash burn without collections & budget | | Anti-malware | | 3:One primary backup and two copies of your data |
| | Build continuity plans (data disruption, internet outage) | | Patch monthly | | 2: Save your backups to two different types of media |
| | Understand how much your data is worth | | Auto log-off from apps and computer | | 1: Keep at least one backup file offsite & offline |
| | User good firewalls at work and home; close ports | | NO outside devices plugged in | | 0: Zero errors with back-up testing |
| | Be paranoid about unknown url's | | Force logon to EMR network | | Server settings; especially with cloud assets |
| | Only download reputable apps | | Seperate network for restricted data | | Plan for costs of recovery |
| | Know the signs of phyishing emails | | MFA/2FA for remote access + VPN where possible | | Buy cyberinsurance |
| | Confirm any requests for money transfer | | UPDATE your firewall | | |
| | Use strong passwords / password keepers | | Strict internet use policy | | |
| | Keep IoT devices off of business networks | | Data policy | | |
| | If you build online forms, protect them | | ASSUME EVERY CONNECTION IS COMPROMISED | | |
| | Do not plug USB devices into work computers | | Extra cautious with access to cloud assets | | |
| | Update every 30 days (or less) | | | | |
| | EDUCATE everyone (font and back office) on risks | | | | |