GP Hero Security Commitment

Data Security

We take security very seriously at GPHERO. Protecting your data is our mission. To that end we follow today's security best practices for clinics, including the following:

1. GPHERO's work from their own dedicated and password protected computer.
2. All passwords for GPHERO computers force secure passwords
3. Non-essential personnel are not allowed on the GPHERO workspace.
4. CD drives, flash drives, and bluetooth capabilities are removed from our computers.
5. There are no phones allowed on the GPHERO workspace.
6. All computers use up to date software programs and anti-virus software.
7. Third Party Authentication tools are required to remote access local computers.
8. 24 hr on-site security guards are present at the GPHERO offices.
9. There is 24 hr on-site CCTV setup at the GPHERO facility.
10. Internet access is controlled by firewall security and gated at a per-desk level
11. All computers are connected to the internet via cable and not WiFi.
12. Each GPHERO sub-office is locked to the 6-12 team members in that space.

To remain compliant with your insurance provider and accreditors, we also require you to:

1. Only share passwords using third party Password Security software (eg: Lastpass)
2. Set your software to force high security passwords for all your users.
3. Have your local IT provider review the computer setup to ensure it meets all required security standards and add this unit to your RACGP IT Security Documentation.

Power Backup

We have on-site backup power generators setup with automatic failover to provide the maximum fault tolerance for any power outages.

Internet Reliability

3 lines of high speed fiber internet lines run to the building from seperate local internet service providers to ensure maximum fault tolerance. Internet flow is controlled to each desk using firewall software which provides the ability to manage data allowance, IP address assignment, and security settings at a per desk level.

Incident Response

If we become a In case of a suspected or confirmed data breach we have a procedure that dictates how and when to make a timely and responsible disclosure to the affected parties with a first communication within 48 hours of us becoming aware of the incident.

Data Collection & Retention

GPHERO does not collect or retain any data that is not necessary to provide our service to you. We do not store any information about your clients or their health records. Your assigned GPHERO will access your general practice software via remote access only and will always use a Third Party Authentication tool.