Data Privacy and Information Security

Help@hand powered by Square Health Limited

Help@hand is an app-based solution. The app enables users to manage their health and wellbeing more effectively by allowing fast and easy access to remote GPs, second opinions, mental health support and physiotherapy. Employees can choose to download the app to access the services.

Square Health Limited is an independent company providing services for Unum and is responsible for the Help@hand app. They are the Data Controller and collect, process and store all data provided by app users.

This information is designed to answer any questions you may have and to give you the assurance you require regarding your employee's data.

How do Square Health collect personal data?

The employer provides initial email contact details for their employees directly through the Square Health Employer Portal. Square Health collects personal data provided by the individual employee using the Help@hand app.

How does Square Health obtain consent from your employee?

It is at your employee's discretion if they choose to download the app and provide their personal information. A privacy notice is provided within the app and the user is asked to acknowledge this before proceeding.

Who is responsible for dealing with individual rights requests? (e.g., a person's right to access data, records and/or to be forgotten)

Square Health has a process in place for handling data subject rights. The individual rights are also noted in Square Health's privacy policy.

Where is the data stored?

Data is stored within the UK/EEA. No personal data is transferred outside of the UK/EEA.

Does Square Health have processes in place for their record keeping activities? (e.g., breach reporting, processing activities, updating records)

Square Health has an information security incident reporting and management policy and process. All incidents are logged on a register. Square Health is committed to ensuring they comply with their reporting obligations within the statutory timeframes.

Who is responsible for notifying employees of a data breach?

Square Health as the Data Controller is responsible for notifying any affected individuals and the relevant regulatory authority. This will be completed without undue delay but within 72 hours of the incident being identified.

What is Square Health's approach to record retention and data disposal?

Data is retained for 10 years. An automated process is in place to remove the data after 10 years.

Are Square Health's staff trained on compliance with UK GDPR?

All staff have undertaken information security and UK GDPR awareness training. This is carried out annually or when there is any change in the guidance.

How has Unum ensured that the Help@hand app meets our security requirements?

Unum conducts information security due diligence on our third parties and subcontractors where appropriate, including Square Health. We make sure this is an ongoing process and have robust contractual clauses in place.

What certifications does Square Health hold?

Square Health demonstrate commitment to keeping the data they hold safe and secure through successfully achieving ISO 27001 certification and Cyber Essentials Plus.

What security measures do Square Health have in place?

Square Health has multiple layers of technical and network security to provide robust protection from the changing landscape of cyber threats. These include:

- **Data Centres** – The infrastructure is hosted in data centres in the UK and Ireland. The centres are managed by industry leading datacentre providers and are purpose built with full UPS backup generators, airlocks, manned 24/7 security, access card readers, biometric security and a manned reception.

- **Access control** – Access to personal data is limited on a 'need to know' basis. System and Physical Access reviews are carried out on a quarterly basis.

- **Data Classification** - All client data is classified as client confidential and it is retained for a maximum of 10 years.

- **Access authentication** – Each user has been given a unique identifier to allow access to personal data. Square Health have a policy which is shared with staff to ensure they understand the need for complex passwords which are enforced on all unique identities.

- **Clear desk/screen policy** – A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is in place.

- **Anti-Malware controls** – Anti-malware software is installed on all Square Health employee's equipment.

- **Firewall** – All Square Health networks are protected by enterprise-class firewall devices which are configured into multiple zones and VLANS to increase security to personal data in live and test environments.

- **Software patching** – Patches are applied from a centralised software solution to ensure that vulnerabilities are not exposed.

- **Remote Access**
Remote access is enabled for remote workers using Square Health owned devices. All remote access requires MFA and is controlled by a number of additional security measures.

- **Portable Devices** – Laptops and smart phones have whole disk encryption implemented. In the case of smartphones, strong passwords are required at start-up and after several minutes of inactivity. If a device is reported as lost, then a remote wipe is promptly performed. Staff allocated with such devices are familiarised with the relevant procedures.

- **Logs and audit trails** – An auditing and logging solution helps technical staff to audit and review these logs from a central location. Restricted access has been given to users within IT to review and analyse certain events. The solution can identify the username that accessed a file and the time of the access. A log of alterations made, along with author/editor is created.

- **Backup systems** – Data is backed up regularly with near real-time site to site replication.

- **Disposal of equipment** – When disposing of obsolete or redundant equipment, all data stored on the devices is removed. A third-party contractor is used to ensure the correct standards are applied to removing data and provides certification once removed.

- **Physical security** – Square Health offices and data centres have audited and controlled external and internal access - with manned reception areas during office hours and security patrols overnight. Access and activities within data centres and other secure areas are strictly controlled.

  Visitor access is only authorised if there is a business justification and visitors are supervised at all times.

- **Third party penetration testing** – Annual security penetration tests are conducted by independent third parties at both the infrastructure and software layers.

Operational measures

- **Incident response plans** – The identification and response to all incidents or potential incidents is defined in formal policies and procedures.

- **Cyber Security Awareness Training** – Square Health invests time in raising awareness of security to staff. They have an induction programme which covers information security and data protection. All staff are required to sign the Information Security Policy. This is carried out annually or when there is any change in the guidance.

- **Certification** – Square Health follows the requirements for ISO9001 and is certified to ISO27001 and Cyber Essentials Plus.

- **Third parties** – Square Health conducts robust vetting and due diligence on all third parties prior to onboarding. This is undertaken in relation to suppliers and subcontractors as appropriate.

Square Health is registered with the Information Commissioner's Office and fully complies with the principles of good information handling practice contained in the Data Protection Act 2018 and the UK GDPR.