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 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.

Square Health is under separate, but related ownership with the Doctors Chambers Group and any processes or accreditation relating to DCG within this document, by association, will also apply to Square Health.

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 email contact details for their employees directly to 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 own choice if they decide 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 on the privacy notice displayed in the app.

Where is the data stored?

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

Do 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 also 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 application in place automatically removes the data/information after 10 years.

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

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

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

We have completed our thorough security due diligence process which is applied to all relevant third parties and subcontractors. We also make sure this is an ongoing process and robust contractual clauses are in place.

What certifications do Square Health hold?

They demonstrate commitment to keeping the data they hold safe and secure through successfully achieving ISO 27001.

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 Ireland data centres. 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 until instructed to be deleted.
- **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.
- **Automatic Screen Savers** – All desktops have been configured with an automatic screen saver. Users are also trained to ensure desktops are locked when workstations are left unattended. Inactivity on a computer requires the user to re-establish access.
- **Anti-virus software** – Anti-virus software is installed through the DCG network.
- **Firewall** – All DCG 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** – DCG only allow remote access to a limited number of staff. Remote access is controlled via firewall VPN rules.
- **Wireless Networks** – DCG have identified that wi-fi access is a risk to personal data, so wireless technology is not enabled on their private network.
- **Portable Devices** – Laptops and smart phones are vulnerable to theft and accidental loss, so DCG consider it essential to ensure whole disk encryption is used. In the case of smartphones, strong passwords are required at start-up and after several minutes of inactivity. If a device is lost, steps are taken immediately to ensure that the remote memory wipe facility is activated. Staff allocated such devices are made familiar 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 previously 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 have alarmed and monitored premises, 24/7 . Square Health also has swipe card access to all offices and a log is retained of all staff movements. In addition, there are high security locks to doors to the critical areas of our offices. Access to these areas is restricted.

  Physical access to the buildings, computer installation environment and equipment processing information is restricted to authorised personnel by the following methods:

  + **Installed locks activated by keypads and swipe cards**
  + **Locking doors/windows when the environment is vacated**
  + **Fitting intruder alarms**
  + **All individuals wear visible methods of identification**
  + **Permanently staffed reception desk during office hours**
  + **Employed security guards at all other times**

  Visitor access is only authorised if it is thought to be justified 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.
- **The human factor** – DCG 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.
- **Audits** - Internal audits are carried out for ISO 9001 and ISO 27001.
- **Certification** – Doctors Chambers Group is certified with ISO27001:2013 standard.
- **Third parties** - DCG undertakes a robust vetting and due diligence of all third parties. This is undertaken by the Group in relation to suppliers and sub-contractors as appropriate.

Information Security Policy for Medical Examiners is also sent to all suppliers carrying out examinations and Square Health have a robust audit process in place which is reviewed by the Care Quality Commission (CQC) when they audit.

Doctors Chambers Group 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 GDPR.