WJ HEALTHCARE

DATA SECURITY POLICY DOCUMENT

7 The Precinct, Cheadle Hulme, Manchester, SK8 5BB
Tel: 0333 772 3242

WJ HEALTHCARE

CONTENTS

- Privacy statement
- Physical security measures
- Data collection and storage policies
- Data access policies
- Data monitoring, security threats & data breach policy
- Subcontracted appraisal software policies
- Additional computer data security measures for WJ Healthcare
- Addendum 1 – MyL2p data policies
- Addendum 2 – Clarity data policies

7 The Precinct, Cheadle Hulme, Manchester, SK8 5BB

Tel: 0333 772 3242

WJ HEALTHCARE

POLICY PURPOSE

WJ Healthcare are committed to ensuring the security of all personal data held by our practice, both in physical and electronic format. This objective is achieved by every member of the group and staff complying with this policy. The policy gives structured guidance on how physical and electronic safeguards are implemented and how specific security events are handled.

PRIVACY STATEMENT

WJ Healthcare is committed to safeguarding the privacy and security of individuals and their personal information. We take every reasonable measure to protect and secure the personal data we process. Our comprehensive information and data security policies and procedures are designed to prevent unauthorised access, alteration, disclosure, or destruction of personal information.

We recognise our obligation in updating and expanding this program to meet the requirements of GDPR.

A non-exhaustive but specific list of WJ Healthcare actions include:

- All staff employment contracts contain a confidentiality clause.
- Access to personal data is on a “need to know” basis only.
- Access to information is closely monitored, and any security breaches will not be tolerated. Such violations may result in staff dismissal.
- Procedures are in place to ensure that personal data is regularly reviewed, updated and deleted in a confidential and secure manner, when no longer required.

7 The Precinct, Cheadle Hulme, Manchester, SK8 5BB
Tel: 0333 772 3242

WJ HEALTHCARE

PHYSICAL SECURITY MEASURES

Personal data is only taken away from WJ Healthcare and its members premises in exceptional circumstances and when authorised by the data controller.

- If personal data is taken from the premises, it must never be left unattended in a car or in a public place.

- All records are kept in lockable, fireproof cabinets, or on computers which are password protected and never left unattended (including secure areas if out of hours providers like cleaners will be on the premises

- Efforts have been made to secure the group against theft, for example, the use of intruder alarms, lockable windows and doors.

- The practice has in place a business continuity plan in case of a disaster. This includes procedures set out for protecting and restoring personal data.

WJ HEALTHCARE

DATA COLLECTION AND STORAGE POLICY

WJ Healthcare collects and stores various data files for use in our process of providing key services such as appraisals, revalidations, guidance related to GMC governance, and other functions that a Designated Body is required to provide to its registered doctors. Various data sets are collected from connected doctors as well as our appraisers. The data collected can be split into two main sections:

- HR and personal data for admin use by WJ Healthcare
- Appraisal related information for use by appraisers and RO's

The first set of data collected and stored relates to the HR and personal data for admin use. This data is requested from each doctor, either initially when signing up to the services at WJ Healthcare, or later during HR file checks and controls. The data requested follows a standard process and includes the following:

- Annual declaration (completed on the WJ Healthcare website)
- Relevant certificates (CPD, additional courses etc)
- Copy of CV
- Copy of DBS file
- Equality and Diversity document (completed on the WJ Healthcare website)
- Copy of GMC registration documents
- Membership forms (completed on the WJ Healthcare website)
- Copy of Passport

The data collected as listed above is kept in a specific HR file for each doctor and is kept for the duration of their connection with WJ Healthcare. Once the connection is terminated the data is removed from our storage platform.

The second set of data collected and stored relates to the appraisal specific information. This data is compiled and uploaded by each individual doctor on the specific appraisal platform used for their organisation. Each platform has its own data and security policies, as well as its own Data Control Officer. The brief overview of these policies can be found in the attached addendums. For further in-depth guidance on the specific controls and policies, contact details can be provided for their respective officers.

WJ HEALTHCARE

DATA ACCESS POLICY

WJ Healthcare has strict policies in place to ensure that all data collected and stored are accessed by the correct and appropriate users within the WJ Healthcare structure. WJ Healthcare have the following levels of users in the organisational structure:

- Level 4 – Senior Management and Directors
- Level 3 – Responsible Officers
- Level 2 – Appraisers
- Level 1 – Connected Doctors

Depending on the specific level, certain access rights are assigned to each user. These levels are continuously monitored, and if changes need to be made to a specific employee level, this is done internally and records are updated accordingly.

The following access is provided to each specific level:

- **Level 4 –** Access and oversight over all HR files kept on record. Administrative Software platform privileges for appraisal software is also granted.

- **Level 3 –** Access and oversight given for all connected doctors for the specific Responsible Officer on the appraisal platform. HR files can be requested and will be provided for appraisal and revalidation purposes.

- **Level 2 –** Access and oversight given for all connected doctors for the specific appraiser on the appraisal platform. HR files can be requested and will be provided for appraisal and revalidation purposes.

- **Level 1 –** Doctors will have access to all of their submitted data on the appraisal platform.

Furthermore, access to HR files stored on our cloud software (iDrive) will be strictly controlled and access assigned as per the guidance above. The following safeguards are in place to ensure the integrity of our cloud access security.

- Data is stored on a secure central file system on iDrive which is supplied by Apple. The security protocols for iDrive are strict and comply with international cloud storage and data protection policies.

- Access to these data folders for WJ Healthcare is shared to the users as per the level system described above. Each user has their own login credentials and unique password. The system also uses two-factor identification for any new access on a device.

- Specific access policies for each appraisal platform used by WJ Healthcare can be found in the addendums attached to this document.

WJ HEALTHCARE

DATA MONITORING, SECURITY THREATS & DATA BREACH POLICY

Data monitoring is an important function within the Data Security Policy guidelines and is continuously reviewed and updated. All documents and data stored as per the guidelines above are subjected to monitoring and internal review to ensure the completeness of data stored, the integrity of documents, and the compliance with relevant laws and guidelines. Any new data that is added is checked and verified before being filed and stored into the correct storage areas within the cloud storage space.

Annual reviews and updates are conducted specifically for the following files stored for each associated doctor:

- Annual medical indemnity checks
- Annual invoice and financial documents
- Annual declaration and Equality documents

Another crucial part to our Data Policy is the identification and handling of various security threats. We have the following controls in place to handle a breach of security in terms of the integrity of our stored data:

- Cloud storage platform notifications of any new login attempts to data files.
- Cloud storage platform notifications of the location of any new login attempts
- Cloud storage platform notifications with two factor identification attempts for new login attempts.

7 The Precinct, Cheadle Hulme, Manchester, SK8 5BB
Tel: 0333 772 3242

WJ HEALTHCARE

If any of these notifications are received and its found that there was indeed a breach, the following actions are ready to be implemented in order to terminate the breached login and limit any data available to the breach:

- Cloud access to the device is immediately revoked.
- Cloud storage access is reviewed and controlled to ensure only the correct users are listed.
- Cloud access breach is investigated, and a report is filed.
- Once the breach has been handled and no further threat is found, access will be returned to the user on either a new device, or a newly secured device.
- The breached device will be required to change all login passwords and two factor identification protocols.

Data Breach Reporting closely follow the guidance outlined by the Information Commissioner's Office (ICO) guidance, and includes the following pathways.

- WJH has procedures in place to assess the severity of the risk to individuals as a result of a personal data breach.
- WJH has procedures in place to notify ICO within 72 hours of becoming aware of any breach.
- If the severity of the data breach is deemed not significant enough to report to the ICO, then reasons for this will be formerly documented.
- WJH has procedures in place to inform the affected individuals in simple, clear language and provide advice on how they can protect themselves

WJ HEALTHCARE

ADDITIONAL COMPUTER DATA SECURITY MEASURES FOR WJ HEALTHCARE

- Appropriate software controls are used to protect computerised records, e.g. the use of passwords and encryption. Passwords are strictly limited to individuals who require access to the information. They are regularly updated and never written down or stored near the computer, ensuring they remain secure and out of sight.

- Daily and weekly back-ups of computerised data are taken and stored in a fireproof container, cloud based, or kept off-site. Back-ups are also tested at prescribed intervals to ensure that the information being stored is usable should it be needed.

- Staff using practice computers will undertake computer training to avoid unintentional deletion or corruption of information.

- All WJ Healthcare computer systems have a full audit trail facility preventing the erasure or overwriting of data. The system records details of any amendments made to data, who made them, and when.

- Precautions are taken to avoid loss of data through the introduction of computer viruses

- Each staff member use their own unique log in.

- This statement has been issued to existing staff with access to personal data at the practice and will be given to new staff during their induction process. Should any staff have concerns about the security of personal data within the practice they should contact the WJH data controller.

WJ HEALTHCARE GROUP DATA CONTROLLER

Name: Mr Jacques Horn

Email: admin@wjhealthcare.co.uk