The Health Alliance
141 Brigstock Road, Thornton Heath, CR7 7JN
07970 949346
07920 094663

Health Alliance @ Brigstock Medical Practice

Policy Statement

The purpose of this policy is to confirm that Health Alliance @ Brigstock Medical Practice is committed to processing and protecting personal data it holds about clients' employees, ex-employees, contractors or temporary workers and prospective employees.

By the nature of its work activities providing Occupational Health medical services, the Organisation is regularly entrusted with personal data (including health) and information by its Clients, and this policy aims to show how it can and will be processed, used, stored and safeguarded. All information provided to the Organisation by Clients is treated as highly confidential (each contractor or employee will be asked to sign the confidentiality statement). It will be used for normal business processing purposes only. This policy also acts as a Privacy Statement and is easily available to clients, employees in accordance with the regulations.

1. Scope

This policy covers the Organisation's standards and practises in respect of data which relates to personal (including health) and special categories of data which is held and processed on behalf of Clients.

All employees of Health Alliance @ Brigstock Medical Practice (and any contractors or associates who may work with us) are required to comply with the standards and rules detailed here. The Partners of the Organisation are responsible for complying with General Data Protection Regulation (GDPR) requirements, and the Organisation's nominated Data Controller.

2. Definitions

In this policy, the following definitions generally apply unless otherwise explained:

- **Company** Health Alliance @ Brigstock Medical Practice
- **Client/clients** are companies, Organisations or individuals who engage with and pay for the Organisation's services.
- **Data Controller** is the person who "owns" and decides what should be done with personal data held by the Organisation.
- **Data Processor** is the person who processes personal data on behalf of the data controller, but who has no long term interest in such data.
- **Data Subject** is the living individual(s) about whom personal data is being collected or processed.
- **Personal Data** is data which relates to a living individual who can be identified from that data or who can be identified by reference to an identifier such as name, NHS number, EMIS number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, culture or social identity of that person.
- **Prime Contacts** are the individual(s) defined in the Organisation's Service Agreement with its Clients, whose instructions are followed, and who may

authorise the Organisation to obtain and share data with other managers or directors in their respective organisations.

- **Special Categories of Personal Data** is personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, physical or mental health conditions, criminal offences, or data concerning a person's sex life or sexual orientation.

3. Consent

3.1. Consent will be obtained from Data Subjects to have, use, process and retain data where this is deemed necessary or is specifically required under the regulations.

3.2. Explicit consent will not be sought or required from Data Subjects in order to deal with day to day employment issues relating to the Company's employees, this will be covered by the client's policies and procedures.

3.3. Explicit consent from each Data Subject will not be sought in order to process ordinary personal data for legitimate business transactions, i.e. supporting and dealing with issues for a client where that client has provided the necessary data to the Company for that purpose.

3.4. Consent will not be sought from Data Subjects to share data with appropriate authorities or other organisations where there is a legal requirement to do so, and such data will be shared from time to time as appropriate.

3.5. For the purposes of recruitment on behalf of clients, a statement will be included in all cover emails to confirm the data subjects information will be shared with the associated client only.

4. Categories of Data

4.1. Personal and special categories of data about client's employees will be held and processed for the purposes of legitimate business.

4.2. The type and extent of personal data and special categories of data held and processed for Clients will depend on the types of services being provided at any particular time. Data will be held and processed by the Organisation for legitimate health purposes, and to comply with legal obligations and to advise Clients regarding compliance with legal obligations. This may therefore include a range of the following about individuals as is necessary to the work being undertaken:

- full name,
- home address,
- email address,
- home telephone number and/or mobile number,
- pay and remuneration information,
- date of birth,
- nationality/citizenship and passport/visa information,
- work performance and training history,
- CV with information about education (or information about planned college/educational courses in the case of apprentices),
- health information and medical certificates/information which relates to absence of workplace adaptations or medical conditions and disabilities recognised under the Equality Act,

- social media and other on-line public presence and contact points such as Twitter or blogs,
- family and data relating to family members, lifestyle or social circumstances where they may relate to application of workplace policies, or are relevant to specific investigations,
- any aspect of protected and personal characteristics or behaviours which may be relevant to investigation processes such as health records, race or ethnicity, trade union membership status,
- CCTV footage of individuals which may be seen and retained in electronic format as evidence as part of investigation processes.

This list is not exhaustive

5. Storage of Data

5.1. Data is stored electronically on the Organisation's server. Software used is primarily EMIS (clinical system), Docman (document scanning software integrated with our clinical system), Word and Excel, but data can also be held in photo format (e.g. certificates, photographs), pdf. This can be accessed through Practice computers (All of them have password protection unique to users, firewalls and anti-virus software protection systems are in place. Backups are kept on external tape in the premises in a secure cabinet. For referral letters a digital dictation is used which is integrated with our clinical system. Telephone calls (incoming and outgoing) are all recorded and stored on the computer hard drive, which is kept secured in a locked cupboard. Telephone recordings which is secured and password protected is shared for learning purposes, dealing with complaints, and can also be transcribed and shared with the relevant parties. Old telephone recordings are saved in secured external hard drive. This hard drive is kept in a locked cupboard, which is accessible to relevant members only.

5.2. The Organisation uses NHSmail, and access to this is met if they are either compliant with IGSoC or IGT which is based around ISO 27001. The NHS mail provider is ISO27001 compliant. The NHSmail service is certified for the use of patient identifiable data, which is independently verified by the ISO 27001 accreditor and the NHS Digital Security Team

5.3 Access to electronic data is strictly restricted to the Organisation employees and associates, and for the purposes of providing technical IT support only, to the IT support provider.

5.4. External data received by GP systems via electronically are required to provide functionality that allows GP staff to review the content of the external data. It is also a requirement on systems not to allow the filing of such reports into the record until they have been marked as viewed by member of the practice.

5.5 Paper files containing personal data are maintained in the form of notes and occasional copies of documentation. Client's documents that are posted are scanned and filed in their electronic records.

6. Sources of Data

6.1. Data may be obtained and collected from clients, who approach the Organisation directly or through the Organisation's specialist HR provider.

6.2. It is assumed that Clients who provide personal or special categories of data to the Organisation for legitimate business purposes have the appropriate consent (where necessary) from their respective employees and contractors to share that data with us as a provider of Occupational health services to the Client.

7. Recipients of Data

7.1. Data will be shared with Clients where it relates to their employees or contractors. It will be shared with prime contacts (as defined in the Organisation's contract with its Clients) or with approved contacts in a Client organisation, with the permission of the prime contact.

7.2. The Organisation will never share, sell, rent or trade any personal data or information to any third parties for marketing purposes.

8. Transfer of Data outside the EEA

8.1. Personal and special categories of data held by the Organisation on behalf of a Client will only be transferred to countries outside the European Economic Area (EEA) on that Client's direct instruction. This can happen in cases of merger and acquisition projects where another business involved in the project is located in a country outside of the EEA.

9. Length of Time Data will be retained

9.1. Data will normally be retained for as long as legitimate business interests warrant it. This includes keeping records and information for Clients while working with them, as business operations often require "old" information to be referenced and used.

9.2. At least once a year, paper and electronic files will be reviewed, and unnecessary data erased or destroyed.

9.3. In the case of information and reports produced or provided to the Organisation in connection with investigations, grievance and disciplinary cases, which may result in legal action or a need to provide information to clients to be used in evidence for legal actions sometime after the event, data will generally be kept for a period of 5 years.

9.4. Personal data will be erased without undue delay on request where:

- it is no longer necessary for it to be retained for the purposes collected or held;
- the Data Subject withdraws consent to it being held (if applicable);
- there is no overriding legitimate interest of reason for processing and the Data Subject objects;
- if the data was unlawfully processed, or must be erased in order to comply with a legal obligation; or
- where a Client requests that any data relating to their employees/contractors/ temporary workers or candidates in respect of recruitment projects undertaken for them is deleted at any time, in accordance with the Organisation's contract with the Client. Copies of all such data will be provided to the Client prior to deletion.

141 Brigstock Road, Thornton Heath, CR7 7JN
07970 949346
07920 094663

10. Suppliers & Sub Processors

10.1. Third party suppliers and Sub Processors who may process personal data held and provided to them by the Organisation, are required to provide assurances that data is held and processed in accordance with the regulations on appropriately secure systems, and with appropriately safe and secure recordkeeping and storage facilities in place.

10.2. The Organisation does not use any automated decision making software to process or evaluate data without human intervention.

11. Breaches & Complaints Procedure

11.1. Any personal data breaches or situations which compromise the security of personal or special categories of personal data will be reported by the Organisation to the ICO within 72 hours where feasible (or without undue delay). Data Subjects will also be notified IF the breach is likely to result in a risk to their rights and freedoms

11.2. Any complaints about the retention or processing of personal data should be addressed in the first instance to the Organisation's Data Controllers, and sent by email to Dipti Gandhi dgandhi@nhs.net

Employees and clients have the right and are also at liberty to contact the Information Commissioner, (www.ico.org.uk) who is the official who enforces data protection legislation in the UK, should they deem it necessary and appropriate to do so.