Central London Healthcare CIC (CLH) Privacy Notice

Author	Joe Brazil
Responsible Director	Operations Director
Publication Date	May 2018
Review Date	May 2019
Version	1.0

Contents

Central London Healthcare CIC (CLH) Privacy Notice 1
What is the purpose of this Privacy Notice? 3
Definitions 3
How is Personal Data collected? 4
For what purposes is Personal Data used? 4
What safeguards are in place? 4
What rights and obligations do Employees have? 5
Duty to inform us of changes 5
Rights in connection with Personal Data 5
What we may need to comply with a Data Subject Access Request 6
Charges 6
Right to withdraw consent 6
Our Data Protection Officer 6
Making a complaint 6
Amending this Privacy Notice 6
Appendix One 7
Appendix Two – Our safeguarding measures 8
Appendix Three – Our nominated Data Protection Officer 9

Amendment History

Version	Status	Date	Reason for change	Authorised
1.0		May 2018		

What is the purpose of this Privacy Notice?

We need to collect and process Personal Data that relates to employees in connection with their employment. This Notice is to explain how we use and safeguard that Personal Data.

Definitions

The definitions below are enshrined in EU law. We have included examples to make things clear.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Simply, this can be summarised as information that we hold about an individual employee from which they can be identified.

It may include but may not be limited to the following:-

- Personal contact information such as name, title, address, telephone number(s) and personal and/ or company email addresses.
- Date of birth.
- Gender.
- Marital status and details of next of kin or dependents.
- Employment records (including job titles, start date, work history, working hours, training records and professional memberships).
- Workplace location.
- Salary and benefit details and history including payroll records and tax records/information.
- Holiday and absence records.
- Copy documents such as passport or driving license or other identification document provided to us as part of our legal obligation to check an employee's right to work in the UK.
- Recruitment information (including references and other information included in a CV or cover letter or as part of the job application process).
- Information relating to qualifications and performance including appraisal records.
- Disciplinary and grievance information.
- CCTV footage, photographs and other information obtained through electronic means such as swipe card records, time and attendance data and/or data from vehicle tracking software.
- Information about an employee's use of our information and communications systems.
- Telephone conversation recordings and activity related to making and receiving telephone calls.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction such as collection, recording, organization, storage, adaptation or alternation,

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Sensitive Personal Data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"Sensitive Personal Data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

How is Personal Data collected?

Typically an employee will have provided Personal Data or we have recorded Personal Data about the employee in connection with or in the course of their employment.
Occasionally we are passed Personal Data by a third party such as our payroll provider, HR advisers or training providers.

For what purposes is Personal Data used?

We will only use Personal Data when the law allows us to which can be summarized under the following headings:

(a) Consent: an individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law.

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party.

Details of the Personal Data that we are most likely to process are set out in Appendix One.

What safeguards are in place?

We will comply with the eight data protection principles in the Data Protection Act which states that Personal Data must be:

- processed fairly and lawfully ;
- obtained only for one or more specified and lawful purposes and not be further processed in any manner incompatible with that purpose or those purposes;
- be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- be accurate and, where necessary, kept up to date;
  shall not be kept for longer than is necessary for lawful purposes;
- shall be processed in accordance with the rights of data subjects under the Data Protection Act;
- protected by having appropriate technical and organisational measures in place to safeguard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, the Personal Data;
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Details of the key safeguarding measures that we adopt are set out in Appendix Two.

What rights and obligations do Employees have?

Duty to inform us of changes

It is important that Personal Data is kept accurate and up to date. Employees should please advise us if their personal information changes whilst they are employed by us.

Rights in connection with Personal Data

Under certain circumstances, individuals have the right to:

- Request a copy of their Personal Data (commonly known as a "data subject access request"). This enables them to receive a copy of the personal information we hold about them and to check that we are lawfully processing it.

- Request correction of the Personal Data that we hold about them.

- Request the erasure of Personal Data. An individual may ask us to delete or remove Personal Data where there is no good reason for us continuing to process it. An individual may also request that we stop processing Personal Data where we are relying on a legitimate interest and there is something about their particular situation which permits an object to processing on this ground.

- Request the restriction of processing of Personal Data for example until its accuracy or the reason for processing it is more clearly established.

- Request the transfer of Personal Data to another party.

Individuals who wish to review, verify, correct or request erasure of Personal Data, object to the processing of Personal Data, or request that we transfer a copy of Personal Data to another party, please contact our nominated Data Controller.

What we may need to comply with a Data Subject Access Request

We may need to request specific information to help us confirm a lawful right to access the information (or to exercise any other rights). This is another appropriate security measure to ensure that Personal Data is not disclosed to any person who has no right to access it.

Charges

No fee is usually required to access Personal Data (or to exercise any of the other rights). However, we may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Right to withdraw consent

In certain circumstances consent may be required to the processing of Personal Data. Where an employee provides such consent to the processing of Personal Data for a specific purpose, that employee has the right to withdraw consent for that specific processing at any time. To withdraw consent, please contact the nominated Data Controller. Once notification is received that consent has been withdrawn, we will no longer process Personal Data for the said specific purpose, unless we have another lawful basis to do so.

Our Data Protection Officer

We will have in place a Data Protection Officer at all times so far as is possible. At the date of issue of this Privacy Notice we have appointed the person named in Appendix 3 as our Data Protection Officer. The Data Protection Officer will oversee compliance with this Privacy Notice. For any questions about this Privacy Notice or how we handle Personal Data, please contact the Data Protection Officer using the contact details included in Appendix 3.

Making a complaint

Individuals have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection matters.

Amending this Privacy Notice

We may update this Privacy Notice from time to time and we will issue a new privacy notice when we make any material changes including when we the identity of the Data Protection Officer changes.

Appendix One – Data Processing

The situations in which we are most likely to process Personal Data are in connection with the following processes set out below:

- Dealing with recruitment or appointment and termination matters including the assessment of experience, qualifications and overall suitability for a particular role.
- Determining an individual's employment terms and the subsequent administration of matters connected with the employment relationship.
- Checking upon an individual's legal entitlement to work in the UK.
- Checking upon an individual's unspent convictions through the completion of a basic Disclosure and Barring Service check.
- Checking upon an individual's spent/unspent convictions through the completion of a standard Disclosure and Barring Service check but only limited to those individual who carry out regulated activities with patients.
- Payroll and benefit provision.
- Managing our business including accounting, forecasting, planning, scheduling and auditing.
- Conducting appraisals, managing performance and determining performance requirements.
- Dealing with grievance and disciplinary matters.
- Dealing with training and development requirements and related issues.
- Dealing with conflicts and disputes involving employees.
- To monitor use of our information and communication systems to ensure compliance with our IT policies.
- Managing absence including assessing fitness to work.
- Health and safety matters including compliance.
- To prevent fraud.
- Equal opportunities monitoring and advice.

We believe that we have a legitimate interest in processing the above Personal Data in the context of the overall employment relationship. Some of the above grounds for processing may overlap and there may be several grounds which justify our use of Personal Data.

Appendix Two – Our safeguarding measures

Please note that we do not transfer any Personal Data to countries or territories that do not have adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

We do not use any Personal Data for automated decision making or other form of profiling.

We aim to keep Personal Data accurate and up to date. Data that is out of date or inaccurate will be amended when we are made aware of that. Employees should notify us if they become aware of any inaccuracies in their Personal Data held by us.

We will not keep Personal Data for longer than is permitted. This means that data will be destroyed or erased from our systems when it is no longer lawfully required. For regulatory purposes we are required to keep certain Personal Data for a six year period after which it is securely destroyed.

We have in place procedures and solutions to maintain the security of all personal data from the point of collection to the point of destruction and have taken appropriate measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data. For example, we take the following steps to protect data:

- Staff are trained in relation to the importance of privacy and data security.
- Laptops are protected by encryption.
- Electronic files can only be accessed via password logins

We will only pass Personal Data to third parties where we are lawfully obliged to do so. For example, an employee may ask us to provide their salary details to a building society when they apply for a mortgage or we may lawfully pass data to our payroll adviser in order to ensure that employees are paid.
We will not disclose Personal Data to a third party without consent unless we are satisfied that they are legally entitled to the data. Where we do disclose Personal Data to a third party without consent, we will only do so where that third party has confirmed that it has in place adequate measures to protect Personal Data.

Appendix Three – Our nominated Data Protection Officer

Mr Tom James

02075358309
07703466472

Email: tomjames@nhs.net