Admin Policy

Data Protection & GDPR

DATE APPROVED:	28 Apr 18
APPROVED BY:	Andrew Thomas
SIGNATURE:	
IMPLEMENTATION DATE:	28 Apr 18
REVIEW DATE:	28 Apr 21
LEAD DIRECTOR:	Andrew Thomas

Policy Reference Number: ASOP 012

Change Control:

Document Number	ASOP 012
Document	**Data Protection**
Version	2.1
Owner	Andrew Thomas
Distribution list	All staff and relevant partners
Issue Date	28 Apr 18
Next Review Date	28 Apr 21
File Reference	ASOP 012
Author	Andrew Thomas

Change History:

Date	Change	Completed by
29 Nov 16	Draft Version	Andrew Thomas
29 Nov 16	Approved and issued	Andrew Thomas
25 Apr 18	Updated for GDPR Compliance	Andrew Thomas
28 Apr 18	Approved and issued	Andrew Thomas
30 Nov 20	Extended for review next year due to COVID 19	Andrew Thomas

Contents

EMPLOYEE DATA PROTECTION AND PRIVACY POLICY

1 INTRODUCTION AND SCOPE

1.1 This policy sets out information in relation to the processing of employee data and how employee privacy of data is protection. This policy does not confer any contractual rights.

1.2 CIPHER Medical is a "data controller" and needs to collect and hold data about you to enable us to administer day to day tasks related to your ongoing employment (e.g. we need to know your bank detail in order that we can pay you).

1.3 CIPHER Medical is permitted to hold and process data about you because you are an employee/worker and there is a contract between us (the main legal basis for processing your information).

2 THE COMPANY'S OBLIGATIONS IN RELATION TO THE PROCESSING OF PERSONAL DATA

2.1 CIPHER Medical is required to ensure that it complies with the following obligations when processing any of your personal data:

- that your data is used lawfully, fairly and in a transparent way
- that your data is collected only for valid purposes which have been clearly explained to you
- that the data collected is relevant to the purposes the Company has told you about and limited only to those purposes
- that the data is accurate and up to date
- that your data is kept in a format which allows for you to be identified for only as long as necessary
- that your data is kept securely

2.2 CIPHER Medical will only use your personal data for the stated purposes, unless there is a need to use it for another reason and that reason is compatible with the original purpose. If the Company consider that it is necessary to use your personal data for a different and unrelated purpose, this will be notified to you in writing with an explanation of the legal basis for doing so. There may be exceptional circumstances where the Company has to process your personal data without your knowledge or consent where this is required by law.

2.3 CIPHER Medical will only ask you to provide data which is necessary for the performance of the contractual employment relationship or any associated legal obligations. If you do not provide this data, the Company may not be able to meet its contractual obligations to you or may be unable to fulfil its legal obligations.

2.4 CIPHER Medical to meet the obligations of performing your contract or to meet legal obligations connected with your employment relationship it is necessary to share your personal information with certain third parties (e.g. payroll provider, pension provider, legal or professional advisers). The Company may also share your personal data with other third parties (e.g. where a possible sale or restructuring of the business may be being considered. The Company does not transfer personal data outside the EEA.

3 INDIVIDUAL RIGHTS AND OBLIGATIONS

3.1 Current data protection legislation provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

3.2 In order that we can ensure that the personal data we hold in relation to you is accurate, it is important that you keep us informed of any changes to your data.

4 HOW PERSONAL DATA IS COLLECTED

4.1 CIPHER Medical collects your personal data by a variety of means. At the recruitment stage the Company will already have collected data through the application process either directly from you or via any employment agency used, and references from current or former employers.

4.2 Where any additional personal data is required, the Company will ask you for this in writing, setting out the purpose for which is it required,

THE TYPE OF DATA THE COMPANY MAY PROCESS

5.1 The data processed includes, but is not limited to:

Type of data	Why we wish to hold it	How long it will be kept for
Recruitment data Previous employers, types of job held previously, skills and qualifications, CV, right to work information	This will allow us to make a decision on your suitability for employment/ engagement.	Data obtained during recruitment will be kept until an application has been declined, or if appointed, for the duration of employment and for 9 months afterwards.
Induction data Key personal data about you: e.g. name address, date of birth, next of kin, bank details, etc.	This will allow us to send you correspondence, contact next of kin in an emergency, pay wages into your bank, enrol you into benefits schemes etc.	This data will be kept for the duration of your employment and for 9 months afterwards.
Payroll data Salary and salary history, benefits, tax, NI and NI number, tax status, pension contributions, other deductions, student loans, CCJ's etc.	To allow us to pay you accurately and to fulfil out tax and reporting obligations with the HMRC.	The HMRC requires us to hold this information for 6 years after we have used it.
Time and attendance data Timesheets, shift rotas,	To allow us to ensure you are working the correct hours and that obligations	This data will be kept for the duration of your employment and for 9 months afterwards.

holiday forms etc.	under the Working Time Regulations are met.	
Health and medical data Data about your health, medical conditions, self-certificates, GP sick notes Your consent may also be sought to gain a report from your GP, consultant or occupational health specialist.	We may need to understand details about health/ medical conditions in relation to your work and ability to undertake your role, or alternative roles. We would only seek this information from you with your specific consent.	This data will be kept for the duration of your employment and for 9 months afterwards. If it relates to an accident at work, we would keep the data for 4 years after your employment has ended.
Ethnic monitoring data Data relating to your racial origin, religion, gender, sexual orientation, etc that are classed as protected characteristics under the Equality Act 2010	We use this data to understand the ethnic make- up of our workforce and it allows us to rebalance our workforce if we believe we do not have the correct diversity.	This data will be kept for the duration of your employment and for 9 months afterwards.
Disciplinary and grievance records	These will be kept on file as a reference for comparison purposes to ensure any requirements to improve your conduct or capability can be referenced.	This data will be kept for the duration of your employment and for 9 months afterwards. The warnings will be 'live' for the duration specified in them.
Other data Start date, location of workplace, driving licence details, training records, professional memberships, job performance details, appraisals, CCTV, photographs, use of IT/ communication systems etc.	We might need to calculate entitlements to benefits or rights arising from length of service, understand details about work performance, training needs, policy compliance etc., or making decisions about promotion or continued employment.	This data will be kept for the duration of your employment and for 9 months afterwards.
3rd parties who deal with our company benefits Pension, payroll providers etc.	If you enrol in a company benefit, we will need to share certain data with a 3rd party to allow them to process your benefits.	This data will be kept for the duration of your employment and for 9 months afterwards. The 3rd party may keep this data longer (e.g. pension provider holding your information).
Future reference data (after you have left the Company) Key data items: name, address, start and leave dates job history, last job title and summary of duties, salary	We would keep a small amount of basic data about you (after you had left) that would allow us to give a prospective employer a reference.	This data will be kept for the duration of your employment/engagement and for up to 5 years afterwards.

details, training courses attended etc.		

5 WHEN THE COMPANY WILL USE YOUR PERSONAL DATA

5.1Generally, CIPHER Medical will use your personal data for one of the following lawful reasons:

- to perform the contract we have entered into with you
- to comply with a legal obligation
- where it is necessary for legitimate interests (or those of a third party)

There are other rare occasions where your personal data or special category data will be used:

- where we need to protect your interests (or someone else's interests)
- where it is needed in the public interest, or where it has already been made public
- where the Company has to process this data for legal claims

6 SPECIAL CATEGORY DATA

6.1 Any personal data which identifies ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation is classed as special category data. The Company will only use this data:

- to comply with employment and other laws when processing and managing situations connected with absences arising in relation to your sickness or family/ dependant related leave etc.
- to ensure health and safety compliance
- to assess your capability to perform your role, monitor and manage your sickness absence, provide appropriate workplace adjustments etc.
- Where it is needed in the public interest, for example for equal opportunity monitoring and reporting

6.2 In limited circumstances, the Company may request your written consent to allow us to process special category data (e.g. for the purpose of gaining a medical report).

6.3 CIPHER Medical does envisage that it will hold data about criminal convictions. CIPHER Medical will only collect data about criminal convictions if it is appropriate to role and duties you will perform.

7 AUTOMATED DECISION MAKING

7.1 CIPHER Medical does not envisage that any decisions about your employment will be taken using automated means. If this position changes you will be notified in writing.

8 SUBJECT ACCESS REQUESTS

8.1 You are entitled to make a subject access request (SAR). Any request should be made in writing to HR/ Office Manager/a Director. If you make an SAR, the Company we may request specific information to confirm your identity to ensure that the data is released to the correct person.

8.2 The information will be provided in a commonly-used electronic form, unless otherwise requested by the individual.

8.3 CIPHER Medical will respond to an SAR within 30 calendar days, with a possibility to extend this period for particularly complex requests. The Company may withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others'.

8.4 CIPHER Medical will only charge you a fee for an SAR if your request is 'manifestly unfounded or excessive', or if further copies of data are requested.

9 THE CALDICOTT PRINCIPLES

9.1 The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Since then, when deciding whether they needed to use information that would identify an individual, an organisation should use the Principles as a test.

Principle 1 - Justify the purpose(s) for using confidential information
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

10 PERSON RESPONSIBLE

10.1 Andrew Thomas is the person responsible for Data Control.