Data Protection and Confidentiality Policy

1.0 Policy aim

1.1 The aim of this Data Protection and Confidentiality Policy is to ensure compliance with data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK. The policy will lay down the principles that must be observed by all who work for Heath and Her and have access to person-identifiable information or confidential information.

2.0 Policy statement

2.1 Health & Her need to collect and process personal data about people with whom it deals to carry out its business and provide its services. Such people include but are not limited to clients, suppliers and employees (present, past and prospective). It is important that Health & Her protect and safeguard person-identifiable and confidential business information that it gathers, creates processes and discloses. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information will be processed lawfully and correctly.

3.0 Scope

3.1 This policy applies to all Health & Her staff, including those engaged to provide services on our behalf.

4.0 Guiding principles

4.1 All staff need to be aware of their responsibilities for safeguarding, confidentiality and preserving information security. All employees are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

4.2 Health & Her is considered a data 'controller' as it determines the purpose and means of the processing its data.

4.3 Health & Her fully supports and must be able to demonstrate compliance with the six principles of the Data Protection Act which are summarised below:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or company measures.

4.4 Confidential information is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including client level health information, employee records, occupational health records, etc. It also includes Health & Her confidential business information. Information can relate to clients and staff (including temporary staff and those engaged to provide services on our behalf), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

4.5 The Managing Director has overall responsibility for strategic and operational management, including ensuring that policies comply with all legal, statutory and good practice guidance requirements.

4.6 Confidentiality is an obligation for all staff.

4.7 Section 170 (1) of the Data Protection Act (2018): Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

(a) to obtain or disclose personal data without the consent of the controller

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

Any breach of confidentiality, inappropriate use of health data, staff records or business sensitive/confidential information, or abuse of computer systems

is a disciplinary offence, which could result in dismissal or termination of employment contract.

4.8 All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.

4.9 Person-identifiable information, wherever appropriate, in line with the data protection principles stated in the Data Protection Policy, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the ICO's Anonymization Code of Practice.

4.10 Access to rooms and offices where terminals are present, or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties. All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

4.11 Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

5.0 Information covered by data protection legislation

5.1 The GDPR (2016) definition of "personal data" covers any information relating to an identified or identifiable natural person – i.e. living individuals. Pseudonymised personal data is covered, however anonymised or aggregated data is not regulated by the GDPR (2016) or DPA (2018), providing the anonymization or aggregation has not been done in a reversible way. Individuals can be identified by various means including their name and address, telephone number or Email address, NHS Number, NI Number.

5.2 The GDPR (2016) defines special categories of personal data (previously referred to as sensitive personal information) as information related to:

- Race or ethnic origin.
- Political opinions.

- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Health data.
- Sexual history and/or sexual orientation.
- Criminal data.

6.0 Information collected by Health & Her

6.1 The data collected by Health & Her may include identifiers such as:

- Name.
- Address.
- Email address.
- Date of birth.
- NHS Number.
- National Insurance Number.
- GP Name and Surgery address.

6.2 Health & Her may also include private and confidential information, and special categories of personal data.

6.3 In order to comply with The General Data Protection Regulation, Health & Her has a Privacy Statement on our website.

7.0 Employer responsibilities

7.1 Health & Her will:

- Provide training for all staff members who handle personal information and ensure access to further guidance and support.
- Carry out regular checks to monitor and assess new processing of personal data and to ensure the notification to the Information Commissioner is updated to take account of any changes in processing of personal data.
- Develop and maintain procedures to ensure compliance with data protection legislation.
- Maintain a record of processing activities.
- Ensure the company complies with its transparency and fair processing obligations in relation to data subjects' personal data.

8.0 Employee responsibilities

8.1 All employees will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
- Understand fully the purposes for which Health & Her uses personal information.

- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by Health & Her to meet its service needs or legal requirements.
- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.
- On receipt of a request by or on behalf of an individual for information held about them, or any other data subject's rights in relation to their personal data, staff will abide by the Procedure for managing personal data requests.
- Understand that breaches of this policy may result in disciplinary action, up to and including dismissal.

9.0 Disclosing personal/confidential information

9.1 Health & Her's Clinic clients will be asked for consent to provide to share the notes from the consultation with their own GP.

9.2 To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed. Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioner's Office Anonymization Code of Practice (https://ico.org.uk/).
- When the information is required by law or under a court order.

9.3 Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime.

9.4 Care must be taken in transferring information to ensure that the method used is as secure as it can be. When transferring client information or other confidential information by email, encryption must be used.

9.5 It is not permitted to include confidential or sensitive information in the body of an email. When e-mailing to addresses other than the secure domains described above the information must be sent as an encrypted attachment with a strong password communicated through a different channel or agreed in advance. When communicating via the secure domains, to protect against the risk of accidentally sending to an incorrect recipient, the data should be sent in a password protected attachment, again with the password communicated through a different channel or agreed in advance.

9.6 Sending information via email to clients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent, or the information is not person-identifiable or confidential information.

10.0 Working away from the office environment

10.1 There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

10.2 Taking home/removing paper documents that contain person-identifiable or confidential information from Health & Her's premises is discouraged. To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location.

10.3 Confidential information must be safeguarded at all times and kept in lockable locations. Any electronic removable media must be encrypted. Staff must minimise the amount of person-identifiable information that is taken away from Health & Her premises. If staff need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of Health & Her buildings.
- Confidential information is kept out of sight whilst being transported.
- If staff need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car.

10.4 Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately-owned computer or device.

11.0 Carelessness

11.1 All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.

11.2 Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on

computers. Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal. This could also constitute an offence under the Computer Misuse Act 1990.

12.0 Abuse of privilege

12.1 It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose, unless through established self-service mechanisms where such access is permitted. Under no circumstances should employees access records about their own family, friends or other persons without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018.

13.0 Personal data breech

13.1 The GDPR introduces a duty on all companies to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

13.2 The Information Commissioner's Office (ICO) describes a personal data breach as,

a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

13.3 Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

14.0 Recording and reporting a data breech

14.1 The ICO advises

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you

don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.