Confidentiality and Data Protection Policy

Version	11.0
Ratified By	Jill Best
Originator/Author	Catherine Wakeling
Date Issued	January 2020
Review Date	March 2023
Target	Hartlepool and East Durham Mind Employees and Volunteers

Document History

Version	Owner	Author	Change Summary	Document Date
1.0	Information Governance	Catherine Wakeling	Draft to final	2009
2.0.	Information Governance	Catherine Wakeling	None	2010
3.0	Information Governance	Catherine Wakeling	None	2011
4.0	Information Governance	Catherine Wakeling	None	2012
5.0	Information Governance	Catherine Wakeling	None	2013
6.0	Information Governance	Catherine Wakeling	None	2014
7.0	Information Governance	Catherine Wakeling	None	2015
8.0	Information Governance	Catherine Wakeling	None	2016
9.0	Information Governance	Catherine Wakeling	None	2017
10.0	Information Govenance	Catherine Wakeling	IG information added	March 2018
11.0	Information Governance	Catherine Wakeling	Data Processing and Data Protection Information	January 2020

1. Definition

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within Hartlepool and East Durham Mind and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in Hartlepool and East Durham Mind and delivering NHS and Social Care contracts 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 the Data Protection Act 1998. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information

2. Roles and Responsibilities

The Chief Executive
The Chief Executive has overall responsibility for strategic and operational management, including ensuring that Hartlepool and East Durham Mind's policies comply with all legal, statutory and good practice guidance requirements.

The Caldicott Guardian
The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information.

The Information Governance Working Group An Information Governance Working Group oversees the development and implementation of Information Governance compliance, policy and procedure.

The Data Protection Officer are responsible is overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements**.**

All employees working at Hartlepool and East Durham Mind are bound by a legal duty of confidentiality. This means that they are obliged to keep any personal and confidential information, commercially sensitive and business in confidence details they become party to as part of their employment strictly confidential. Information should only be disclosed with the consent of the individual concerned, written consent from senior management or with the approval of the Caldicott Guardian.

No employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to defeat any of Hartlepool and East Durham Mind's security systems or controls in order to do so. Legal obligations in relation to confidentiality derive from:

Data Protection Act (2018)

Computer Misuse Act (1990)

Human Rights Act (1998)

Common Law Duty of Confidentiality

Calicott Principles

General Data Protection Regulations (2018)

Under the Common Law Duty of Confidentiality any employee (permanent, contracted or agent) may be personally liable in a court of law for unauthorised disclosure of personal data. This code has been produced to protect staff, by making them aware of the correct procedures for making disclosures and dealing with personal information.

Confidentiality is an important principle that enables people to feel safe in sharing their concerns and to ask for help. However, the right to confidentiality is not absolute. Sharing relevant information with the right people at the right time is vital to good safeguarding practice.

All staff and volunteers should be familiar with internal safeguarding procedures for raising concerns. They can also contact either the police or the local authority safeguarding lead for advice, without necessarily giving an individual's personal details, if they are unsure whether a safeguarding referral would be appropriate.

Some basic principles:

- Don't give assurances about absolute confidentiality.
- Try to gain consent to share information as necessary.
- Consider the person's mental capacity to consent to information being shared and seek assistance if you are uncertain.
- Make sure that others are not put at risk by information being kept confidential:
- Does the public interest served by disclosure of personal information outweigh the public interest served by protecting confidentiality?
- Could your action prevent a serious crime?
- Don't put management or organisational interests before safety.

- Share information on a ‘need-to-know’ basis and do not share more information than necessary.
- Record decisions and reasoning about information that is shared.
- Carefully consider the risks of sharing information in relation to domestic violence or hate crime.

The sharing of information in health and social care is guided by the Caldicott principles. These principles are reflected in the Data Protection Act and the General Data Protection Regulations:

- Justify the purpose(s).
- Don’t use personal confidential data unless it is absolutely necessary.
- Use the minimum personal confidential data necessary for purpose.
- Access to personal confidential data should be on a strict need-to-know basis.
- Everyone with access to personal confidential data should be aware of their responsibilities.
- Comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

3. Legal Basis for Processing Confidential Information

The organisation must demonstrate a legal basis for the processing of and the sharing of confidential information. The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the ‘conditions for processing’ under the Data Protection Act 1998 (the 1998 Act). However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing. The GDPR also brings in new accountability and transparency requirements. The organisation should make sure it has clearly documented the lawful basis so that it can demonstrate compliance in line with Articles 5(2) and 24. Legal basis for processing information can be found on the organisations privacy notices.

4. Confidentiality Guidance

4.1 Exceptions to confidentiality (Clients)

If the receiver of information has good reason to believe that the client is involved in the following, the relevant bodies should be notified:

- Risk to public or staff safety
- Vulnerability or safeguarding concerns
- Terrorism (The Prevention of Terrorism Act)
- Committing a serious crime
- Serious physical harm to others
- Abuse of a child

- Serious harm to yourself

4.2 Verbal information

Information received from clients or workers should be treated in confidence and not discussed with others without consent (subject to exceptions).
For supervision; clients must not be identified only by the problems/issues that need to be discussed.
For case studies; there should not be any identifying information given, only context of the person's life situation.

4.3 Access to client information

Staff and volunteers will be permitted access to client information on a need to know basis only. Access to client information will be monitored and any staff member accessing information without a legitimate reason for doing so will be subject to disciplinary action.

External Agencies requesting access to client information will be subject to the Subject Access Request policy. Justification for releasing information must be identified and logged, along with client consent for information to be released. In addition to justification for releasing information, a log will be kept of the external agency requesting the information, the purpose of the request, the date the request was received, what information was released and who released it.

If the client has not provided explicit consent to liaise with family, friends or external agencies, this must be respected, and no information should be disclosed. This includes confirmation of the person accessing the service or attendance at appointments.

If information is requested by a referrer prior to the initial appointment being carried out, the service can confirm that the referral has been received and an appointment has been booked. This information should not be imparted without first confirming the identity of the person requesting the information and confirming that they are the referrer as outlined in the 'Admin guide to requests for client information'. During the initial appointment, the client should be informed of the information request and be asked for consent to provide any further details. If they refuse consent at this point, no further information should be disclosed unless it relates to the exceptions of confidentiality outlined above.

If the organisation receives a call of an urgent nature from the police, crisis team or GP and the information is conducive to client care then it may be necessary to disclose information. Prior to any information disclosure, advice should be sought from the Information Governance Lead or Caldicott Guardian in the first instance. Callers must always be informed that they will be called back whilst the nature of the information request is reviewed, and a decision is made.

If there is any doubt as to whether information should be disclosed, the decision must be passed to the Caldicott Guardian for approval.

4.4 Confidentiality of Information

All employees and volunteers are responsible for maintaining the confidentiality of any information gained as a result of their employment by Hartlepool and East Durham Mind.

4.5 Types of Information

- **Personal Confidential Information** – this term describes personal information or data about identified or identifiable individuals, which should be kept private or secret. For the purposes of this notice 'personal' includes the Data Protection Act and General Data Protection Regulations definition of personal data, but it is adapted to include deceased as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive', as defined in the Data Protection Act and General Data Protection Regulations. Confidential information can be anything that relates to clients (e.g. complaints, serious untoward incidents), staff or any other person, held either on paper, disc, computer file or printout, video, photograph or even heard by word of mouth. It includes information stored on portable devices such as laptops and palmtops. It can take many forms including patient details, audits, employee records, occupational health records etc.
- **Pseudonymised** – this is data that has undergone a technical process that replaces your identifiable information such as NHS number, postcode, date of birth with a unique identifier, which obscures the 'real world' identity of the individual patient to those working with the data
- **Anonymised** – this is data about individuals but with identifying details removed so that there is little, or no risk of the individual being re-identified
- **Aggregated** – Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data such as age ranges.

4.6 Requests for Information by the police and Media

Any requests for information from the media (newspapers, TV companies etc.) should always be referred to the service manager and must be discussed with the Caldicott Guardian. The request may constitute a Freedom of Information request and must follow the guidance outlined in the Information Sharing Framework.

4.7 Data Protection

Anyone who obtains personal information ("data") about other individuals is a 'data controller' and is thus regulated by the General Data Protection Regulations (GDPR) (2018). The regulations control what can lawfully be done with information and gives individuals certain rights to control how information about them is obtained, used, stored and distributed. These rights include the right to find out what information a data controller has about them and ask for copies of it.

4.8 The principles for processing personal and confidential data are as follows:

Processed lawfully, fairly and in a transparent manner

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

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 may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

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 organisational measures

5. Data Retention Period

Client data will be retained as necessary for up to 8 years. Data will only be retained for a period of longer than 8 years if it is material to legal proceedings or should otherwise be retained in our interests after that period. We will process data in accordance with rights under the Act. Data will be kept in a secure system whether manual or computerised to the best of our ability at all times.

Please refer to Employee Data Protection Policy for employee data retention schedules.

5.1 Data Security

An encrypted Dreytek vigor 2820n router stops any unauthorised users from accessing our network and Avira anti-virus software is installed on all laptops and desktops.

5.2 Storage of Confidential Data/Information

Hartlepool and East Durham Mind store client information on an information management system called IAPTus, which is provided by Mayden. Their system security is of the same standard used by the Ministry of Defence and the NHS. Each member of staff has a username and password for the system. There is a 2-point security process that needs to be completed before the staff member can get access to the system. Access to records is monitored and restricted to those staff members who have a legitimate purpose for accessing it. This includes the administration team, data team, management team and allocated clinician. All access to records must be justified. The data team monitor access and report on this to the Information Governance Manager on a regular basis.

Hartlepool and East Durham Mind also utilise Pragmatic Tracker for use in its smaller projects. This is hosted on a secure network and only non-identifiable information is stored on the system.

Hartlepool and East Durham Mind also store minimal paper records which are used as a backup if the electronic system is not accessible. These are stored in a locked filing cabinet whilst the client is active within the service. The filing cabinet is in a locked room with a keypad lock; the code for which is changed monthly. We have a secure storage unit for archived paper records at an offsite storage facility. The unit is only accessible via a keypad lock and limited staff members have the code.

Please refer to Employee Data Protection Policy for detail on how employee records are stored.

5.3 Disposal of Confidential Information

When disposing of paper-based person-identifiable or confidential information the confidential waste bins must always be used. The organisation has a contract with Shred Centre who ensure that all confidential information is disposed of in line with data protection legislation.

5.4 Confidentiality of Passwords

Personal passwords issued to or created by employees should be regarded as

confidential and those passwords must not be communicated to anyone. Passwords should not be written down. Passwords should not relate to the employee or the system being accessed (e.g. do not use your name as a password). Passwords should contain a combination of upper and lowercase letters, numbers and symbols to comply with IT standards and DH guidance. Passwords should be routinely changed and should differ from passwords used previously.

5.5 Password Security

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately recorded on an incident reporting form and reported to the HR manager. This could also result in a breach of the Computer Misuse Act 1990 that could lead to civil or criminal action.

5.6 E-Mailing Confidential Information

The transmission of personal identifiable information externally over the internet e-mail (e.g. Outlook, Webmail) is prohibited. Personal information should not be emailed to and from organisation email accounts. However, if client confidential must be transmitted via email, the Information Governance Lead has access to an encrypted NHS email account.

5.7 Commercially Sensitive Information

Any form of information that could adversely prejudice the commercial interests/activities of Hartlepool and East Durham Mind, any other organisation or individual should be considered as confidential and must not be used or disclosed to third parties unless required by exception.

6. Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the Information Governance Group. The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

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; and
- loss of availability of personal data.

7. Data processing on behalf of other data controllers

In addition to the above-mentioned aspects of this policy, any processing carried out on behalf of other organisations must have a data processing agreement in place. The data controller remains responsible for their data, it is the responsibility of HEDM as the data processor to comply with all clauses contained within the agreement. It is expected that all information and data obtained as part of this agreement will be held to the same high standard of data protection and confidentiality that its own data is.