Confidentiality and Data Protection Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	08.02.2024	Carolina Guariniello	Paul Flynn	formatted to fit in the new the Policies template.
1.1	08.02.2025	Carolina Guariniello	Paul Flynn	Added the first paragraph to Policy statement. Changed from patient identifiable information to personal confidential data Removed mention about DVD, CDs and USB. Added Janine McNab, COO, as the date protection lead Added points 2.4, 2.5, 2.6, 2.7 and 2.8
			,	
			,	
				,

Policy Statement

This policy explains and enforces the obligations of confidentiality and non-disclosure among the employees of this organisation. This applies to information generated, held and processed by the organisation. Furthermore, it outlines the principles that are to be adhered to by all staff at this organisation to understand the requirement for effective controls of personal confidential data (formerly patient identifiable information).

The Harbor independent healthcare service is fully committed to complying with the Data Protection Act 1998 which came into force on 1 March 2000 and the General Data Protections Regulation (GDPR) that came in to force on 25th May 2018.

It is important that Harbor protects and safeguards personal confidential data and confidential business information that it gathers, creates, processes and discloses, in order to comply with the law, and to provide assurance to patients who use the healthcare services on offer.

All employees of Harbor are bound by a legal duty of confidentiality to protect personal information that they may come into contact during their work.

This policy sets out the principles that must be observed by all staff who work within Harbor and have access to personal confidential data or confidential information.

All members of staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

Respect for confidentiality is an essential requirement for Harbor as an independent healthcare provider.

1 General Principles

2.1 Data protection

The ease with which personal information can be passed within Harbor - often electronically - is a benefit for patients and for those involved in their care and treatment. However, all staff need to be aware of their legal responsibilities under the Data Protection Act and GDPR to protect the confidentiality of patient information, and other information relating to the business activities of Harbor.

Personal information on staff is also protected by the Data Protection Act. and GDPR legislation. The Act affords members of staff the same rights of protection for, and of access to, their personal information held by Harbor.

The term **'personal confidential data'** refers to information relating to any identifiable individual, and it is important to be aware that healthcare information is considered in the Data Protection Act to be 'sensitive information' requiring the highest levels of care and protection.

Harbor fully supports and complies with the principles of the Data Protection Act and GDPR legislation. In summary, this means personal information must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant, and sufficient for the purpose
- Accurate and up to date
- Kept for as long as is necessary and no longer
- Processed in line with individuals' rights
- Secure and protected against unlawful access, loss or damage, and
- Only transferred to others that have suitable data protection controls

Everyone working for Harbor who records, handles, stores or otherwise comes across information, has a statutory duty under the Data Protection Act, along with a duty of confidentiality in common law, to patients and to Harbor as an employer.

These duties apply equally to staff who are permanent or temporary, full or part-time, agency or bank staff, staff who have been granted practising privileges, students or trainees, volunteers, or to staff on temporary placements.

Harbor will follow procedures to ensure that all employees, contractors, agents, consultants and other relevant parties who have access to any personal information held by, or on behalf of Harbor, are fully aware of and abide by their duties and responsibilities under the Act.

2 Personal Confidential Data

Personal confidential data is anything that contains the means to identify a person, e.g. an individual name, address, postcode, date of birth, email address, telephone number, or unique identifiable reference number.

Confidential information within Harbor is not restricted to a person's health information. It also includes private information that an individual would not expect to be shared such as staff employee records, occupational health records, and business information about Harbor.

The data that falls under the General Data Protections Regulation is:

- Name
- Photo
- Email address.
- Social media posts

- Personal medical information
- IP addresses
- Bank details.

Information can relate to Harbor patients and staff (including temporary staff), however stored. Information may be held in:

- Paper format
- Desktop computers
- Laptops
- Tablet devices
- Mobile phones
- Digital cameras

This list is not exhaustive.

2.1 Disclosure of personal information

Strict conditions apply to the disclosure of personal information within Harbor. Harbor will not disclose personal information to any third party unless it is believed to be lawful to do so.

Information relating to identifiable patients must not be divulged to anyone other than an authorised person, for example medical, nursing or other healthcare professional staff, as appropriate, who are concerned directly with the care, diagnosis and/or treatment of the patient.

Maintaining confidentiality is an important duty but there are circumstances when it may be appropriate to disclose confidential patient information. These are:

- when the patient has given consent
- when the law says it must be disclosed, or
- when it is in the public interest to do so.

An example of such circumstances would be child protection where the overriding principle is to secure the best interests of the child.

Harbor will also seek the consent of staff for the passing on of identifiable personal information for any purpose other than those outlined to staff on appointment. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- Harbor has the statutory power or is required by law to do so, or
- the information is clearly not intrusive in nature, or
- the member of staff has consented to the disclosure, or
- the information is in a form that does not identify individual employees.

If staff have any concerns about disclosing information, they must discuss this with their line manager.

2.2 Caldicott principles

The following eight Caldicott principles will be adhered to by Harbor in all cases where the appropriate use of person identifiable health information is considered.

Principle 1: Justify the Purpose(s) for Using Confidential Information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Examples of justifiable purposes include:

- Delivering personal care and treatment
- Assuring and improving the quality of care and treatment
- Monitoring and protecting public health
- Managing and planning healthcare services
- Risk management
- Investigating complaints and potential legal claims
- Teaching purposes
- Statistical analysis, and
- Medical or health services research

Principle 2: Use Confidential Information Only When It Is Necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals

should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the Minimum Necessary Confidential Information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to Confidential Information Should Be On a Strict Need-To-Know Basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone With Access to Confidential Information Should Be Aware of Their Responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with The Law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The Duty to Share Information for Individual Care Is as Important as the Duty to Protect Patient Confidentiality

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

Principle 8: Inform Patients and Service Users About How Their Confidential Information Is Used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

The above principles do not and cannot provide definitive answers for every situation as much depends on the context of each individual case. If in doubt, staff working at Harbor must seek appropriate advice from the Data Protection Lead, Janine McNab, before releasing personally identifiable information.

2.3 Handling of personal information

Harbor will handle all person-identifiable information securely and in keeping with the requirements of the Data Protection Act.

All staff, through appropriate training and responsible management, will be expected to:

- fully observe conditions regarding the collection and use of personal information
- meet legal obligations to specify the purposes for which personal information is gathered and used.
- collect and process appropriate personal information only to the extent that it is needed to fulfil Harbor's operational needs or to comply with any legal requirements.
- apply strict checks to determine the length of time personal information is held, and
- take appropriate technical and organisational security measures to safeguard personal information.

Harbor will take disciplinary action against any member of staff found to have breached patient confidentiality and ensure that all staff are aware that they risk personal prosecution for breaches of the Data Protection Act.

2.4 Non-disclosure of information

All employees must adhere to the clauses outlined in their individual contract of employment in relation to confidentiality, data protection and intellectual property.

2.5 Third-party requests for information

Any employee approached by a third party, including any media source, and asked to make comments or provide information relating to the organisation and its affairs (or the affairs of its patients, partners, employees, contractors or any business associate) must not, under any circumstances, respond without having sought permission and guidance from the CEO, Paul Flynn.

2.5 Whistleblowing or protected disclosures

In respect of any malpractice or unlawful conduct, any employee is entitled to submit a protected disclosure under the Whistleblowing Policy.

2.6 Disclosing information

The GMC offers guidance in the document titled Disclosing patients' personal information: a framework. Supporting information can also be found in the organisation's Consent Guidance.

2.7 Protecting information under the Gender Recognition Act

Section 22 of the Gender Recognition Act 2004 states that it is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.

This is classified as *protected information* and is defined in Section 22(2) as information relating to a person who has applied for a Gender Recognition Certificate (GRC) under the Act, and which concerns that application (or a subsequent application by them) or their gender prior to being granted a full GRC.

While Section 22 is a privacy measure that prevents officials from disclosing that a person has a trans history, there are exemptions for medical professionals as detailed within Statutory Instrument 2005 No.635 (Section 5) provided all the following circumstances apply:

- The disclosure is made to a health professional
- The disclosure is made for medical purposes; and
- The person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent

As a precautionary measure, it is good practice to apply the Section 5 criteria to all disclosures of information about the trans status of a patient. Furthermore, patients should never be asked to produce a GRC to 'prove' their trans status.

2.8 Confidentiality and non-disclosure agreement

All persons engaged to work for and on behalf of the organisation will be required to sign the confidentiality and non-disclosure agreement. A signed copy will be held on the individual's personnel file. Visitors to the organisation will also be expected to sign the organisation's third-party confidentiality agreement.

3 Compliance

Harbor will ensure that:

- There is always someone with specific responsibility for Data Protection in Harbor
- Patients are pro-actively informed of the uses to which their information is put.
- Staff are informed, on appointment, of the uses to which their personal information is put, e.g. equal opportunity monitoring.
- Consent is sought before passing personal identifiable information on for any reason other than to fulfil justifiable purposes.

- Staff are reminded of their obligations under the Data Protection Act

- Everyone managing and handling personal information understands that they are directly and personally responsible for following good Data Protection practice.

- Only staff who need access to personal information as part of their duties are authorised to do so. Unauthorised access to personal information, either in paper or electronic format, is considered to be a breach of the Data Protection Act and this Harbor policy.

- Everyone managing and handling personal information is appropriately trained to do so.

- Everyone managing and handling personal information is appropriately supervised, where necessary

- Anyone wishing to make enquiries about handling personal information knows what to do.

- Queries about handling personal information are dealt with promptly and courteously.

- Methods of handling personal information are clearly described, and

- The way personal information is managed and handled will be regularly reviewed and evaluated.

4 Breaches of Confidentiality

Breaches of confidentiality are often unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or by poor computer security. However, the consequences could be equally serious for all concerned.

Obligations to maintaining confidentiality and preventing breaches include:

- Not gossiping

- Taking care not to be overheard when discussing a patient's circumstances in a public area

- Closing and locking doors/cabinets/drawers when not in use

- Not leaving a computer unattended and logged-in

- Always logging out of a computer when work is finished

- Making sure computer screens are never visible to the public.
- Querying the status of visitors to Harbor, and
- Knowing who to tell if anything is suspicious or worrying

The simple rule of thumb is that personal confidential data must always be held securely and, when used, treated with respect.

This rule applies regardless of whether the information is stored on paper, saved on a computer, or retained in a staff member's memory.

5 Policy Awareness

All new members of staff at Harbor will be made aware of this policy through their induction programme.

Existing staff will be reminded of the policy which will be readily accessible within Harbor.

All staff and relevant third parties must be familiar with and always comply with this policy.

6 Responsibilities

Data Protection Lead
Janine McNab, COO, has overall responsibility for maintaining confidentiality within Harbor and ensuring that this policy is complied with by all staff.

All Members of Staff
All staff have a responsibility to protect the personal information held by Harbor.

Each member of staff will be expected to take steps to ensure that personal data is always kept secure and protected against unauthorised, unlawful or accidental loss, damage or disclosure. This applies to all personal identifiable information held in all formats, whether is it in patients' healthcare records or staff employee files, or in any other format such as diaries, message books, notebooks, appointment books, emails and other notes held about individuals.

Staff must ensure that:

- They are appropriately trained and knowledgeable in the handling of personal information.
- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.

- Where they are required to take personal information away from a Harbor healthcare environment as part of their work, including information held in all formats, this should be held securely at all times and everything possible done to safeguard against unauthorised access or accidental loss or damage.

- Personal information is always transferred securely, whether it is being sent electronically or by surface post.

- Personal data held on computers and computer systems is protected using secure passwords, and

- All relevant policies are adhered to when processing personal data to ensure adequate levels of protection are maintained.

Where staff, as part of their Harbor responsibilities, collect, hold and process information about other people, they must comply with this policy. No- one should disclose personal information outside this policy or use personal data held about others for their own purposes.

All healthcare professionals practising within Harbor have professional and ethical duties of confidentiality within their respective codes of conduct which they are expected to follow.

Signature:	Carolina Guariniello
Date:	18 Feb 2025
Name and role:	Carolina Guariniello - CQC Registered Manager

Signable

Issuer	Harbor London Ltd
Document generated	Tue, 18th Feb 2025 15:45:38 GMT
Document fingerprint	81c8714f5a0cd288f8dd986872465700

Parties involved with this document

Document processed	Party + Fingerprint
Tue, 18th Feb 2025 15:51:56 GMT	Carolina Guariniello - Signer (82724d97c0dba90008ddda2c69b81328)

Audit history log

Date	Action
Tue, 18th Feb 2025 15:45:38 GMT	Envelope generated by Carolina Guariniello188.39.80.130
Tue, 18th Feb 2025 15:45:50 GMT	Document generated with fingerprint 5ead582ff358b87fc317c1914e05b447188.39.80.130
Tue, 18th Feb 2025 15:46:02 GMT	Document generated with fingerprint 378b01469157794e6e907aaf322f8a5a188.39.80.130
Tue, 18th Feb 2025 15:46:14 GMT	Document generated with fingerprint 13b7b4133d0cd58d2d473e5aeb03d850188.39.80.130
Tue, 18th Feb 2025 15:46:26 GMT	Document generated with fingerprint 16a8707860f953dddc2a862548c3cc50188.39.80.130
Tue, 18th Feb 2025 15:46:38 GMT	Document generated with fingerprint 0c053b5d419394322a2f18149f2a8a35188.39.80.130
Tue, 18th Feb 2025 15:46:51 GMT	Document generated with fingerprint 4e6c7ee32104754d16619634cbf33b1d188.39.80.130
Tue, 18th Feb 2025 15:47:03 GMT	Document generated with fingerprint e408d5ddc4111253bf01f413f1e34df3188.39.80.130
Tue, 18th Feb 2025 15:47:11 GMT	Document generated with fingerprint 81c8714f5a0cd288f8dd986872465700188.39.80.130
Tue, 18th Feb 2025 15:47:19 GMT	Document generated with fingerprint f9494d01f1ad672f041e9bfc97d2bc70188.39.80.130
Tue, 18th Feb 2025 15:47:27 GMT	Document generated with fingerprint a9f610b841f68b2a21b8dcf9da6e9692188.39.80.130
Tue, 18th Feb 2025 15:47:34 GMT	Document generated with fingerprint 4788017cf1e83df729bec5a1f8f63a14188.39.80.130

Tue, 18th Feb 2025 15:51:27 GMT	Sent the envelope to Carolina Guariniello (carolina@harborlondon.com) for signing188.39.80.130
Tue, 18th Feb 2025 15:51:27 GMT	Document emailed to carolina@harborlondon.com13.40.100.148
Tue, 18th Feb 2025 15:51:31 GMT	Carolina Guariniello viewed the envelope188.39.80.130
Tue, 18th Feb 2025 15:51:56 GMT	Carolina Guariniello signed the envelope188.39.80.130
Tue, 18th Feb 2025 15:51:56 GMT	This envelope has been signed by all parties188.39.80.130
Tue, 18th Feb 2025 15:51:57 GMT	Carolina Guariniello viewed the envelope188.39.80.130