CODE OF CONFIDENTIALITY

There is updated GMC Guidance on confidentiality (May 2018).

Sandyford is committed to offering confidential sexual health advice, support and information either in person, by telephone or letter.

- Ensure staff are aware of and respect the confidentiality of clients
- Inform clients that services are confidential, within specific limitations

All personal information gained about a client during the course of duties, including acknowledgement of their attendance at the clinic, will be treated as confidential. This is irrespective of age. It includes health information and other personal information (relating to matters such as personal, family or social circumstances). This means that no information given in confidence will be divulged to any person outside Sandyford without permission of the client. **Exceptions are only under specific circumstances outlined later.** All disclosures and their extent should be documented in the client's case record.

Confidentiality resides within the clinical team setting, which includes doctors, nurses, health care workers and clerical staff. To provide clients with the best possible care and ensure that their specific needs are catered for, it is often essential to pass confidential information between team members. This would not be seen as a breach of confidentiality. However where a client has specifically requested that information should not be passed on within the team this should be respected, within the limits outlined below.

Data Protection Law

The processing of personal data must also satisfy the requirements of data protection law, which imposes various duties on data controllers. *The General Data Protection Regulation* (GDPR), supplemented by the *Data Protection Act 2018*, regulates the processing of personal data about living individuals in the UK. It sets out the responsibilities of data controllers when processing personal data as well as a number of rights for individuals, including rights of access to their information. The Information Commissioner's Office (ICO) is the authority responsible for upholding information rights in the UK. Detailed guidance on complying with data protection law is available on the ICO website: www.ico.org.uk.

The GDPR defines personal data as:
'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'

The first principle of the GDPR states that data must be processed lawfully and fairly. This means:

a. patients' information must not be processed in a way that breaches either statute or common law. For example, if disclosing information would be a breach of the

common law duty of confidentiality, it would also be unlawful under data protection law
b. patients' personal information must be handled in ways that are transparent and in ways they would reasonably expect.

One or more of the conditions for processing in Article 6 (for all personal data) and Article 9 (for 'special category data', which includes health data) to the GDPR must also be met for the processing to be fair and lawful.
In all cases where personal data is processed, at least one of the conditions set out in Article 6 must be met. The conditions most likely to be relevant in medical practice are that:

- the data subject has given consent
- the processing is necessary for the performance of a contract
- the processing is necessary because of a legal obligation that applies
- to the data controller (except an obligation imposed by a contract)
- the processing is necessary to protect the vital interests of the data
- subject
- the processing is necessary for the performance of a task carried out
- in the public interest or in the exercise of official authority
- the processing is necessary for the purposes of legitimate interests
- pursued by the data controller or a third party

Where special category data are being used, at least one of the conditions in Article 9 must also be met. Information on a patient's health record is likely to be special category data for the purposes of the GDPR. The conditions most likely to be relevant in medical practice are that:

- the data subject has given explicit consent
- the processing is necessary to protect the vital interests of the
- data subject or another person in a case where the data subject is
- physically or legally incapable of giving consent
- the processing is necessary for reasons of substantial public interest
- the processing is necessary for medical purposes where the
- processing is undertaken by a health professional or someone else
- who owes an equivalent duty of confidentiality
- the processing is necessary for reasons of public interest in the area
- of public health
- the processing is necessary for archiving purposes in the public
- interest, scientific or historical research purposes or statistical purposes

<u>Limits On Confidentiality</u>
Confidentiality will always be respected, whenever possible. In certain circumstances it may be necessary to disclose information without the client's consent. The most senior health professional(s) with overall clinical responsibility for the client should take this decision and every reasonable effort should be made to obtain the client's consent and to inform them of disclosure. The extent of disclosure should be the minimum required for the purpose of the disclosure. Disclosure without consent can raise very difficult moral, ethical and medical issues.

You may require to seek guidance from a line manager or professional body.

Where Disclosure Is Ordered By A Judge Or Presiding Officer Of The Court
You should disclose only as much as necessary to the proceedings. This should always involve a senior clinician.

Where Disclosure Is In The Client's Best Medical Interest
If the individual is deemed to be in a life-threatening situation because of the following:

- Victim of neglect, sexual or physical abuse and unable to give or withhold consent to disclosure.
- If there are indications of real danger of severe damage either physical, sexual or emotional or of death if the individual returns to an abusive situation.
- Threatening suicide or appears to have attempted suicide.

Where Disclosure Is Necessary To Prevent Serious Injury Or Damage To The Health Of A Third Party
It is necessary to assess the risks and seriousness of the potential injury or damage to the third party against the rights of the client to confidentiality.

Where Disclosure Is In The Wider Public Interest
This might include cases where disclosure would prevent a serious risk to the public health or assist in the prevention, detection or prosecution of serious crimes. In some cases the duty to disclose details lies with the client (e.g. HIV).

Where The Condition Of The Client Precludes Seeking Consent
Where judgement may be impaired by learning difficulty, serious psychiatric illness, dementia or brain injury or where the client has severe communication difficulties, disclosure without consent may be considered only if **all** of the following criteria are met:

- It is clinician's belief that disclosure be essential to the best medical interests of the client.
- The client does not have sufficient understanding to appreciate what the advice or treatment being sought may involve. Every attempt should be made to find treatment appropriate to their condition before such a judgement is made.
- The client cannot be persuaded to involve the appropriate person in the consultation.

Even when the doctor considers a person lacks capacity to consent to treatment, because of age or condition, confidentiality should still be respected unless there are very convincing reasons to the contrary.

Disclosure By Implied Consent

All clients are asked to complete a registration form on first attending the clinic. This asks for their permission for communication in the future with their general practitioner and to their given correspondence address. Clients may prohibit such contact and request no communication to their GP or in any way with themselves except at consultation. This must be respected unless any of the above circumstances hold.

Otherwise in completion of the registration form it may be assumed that an individual has consented to the disclosure of personal information where necessary:

- For operational management within the clinic and the health service
- Clients should be aware that since Sandyford services are throughout NHS Greater Glasgow and Clyde and information by clinicians is accessed via the National Sexual Health Database (NaSH).
- The investigation of complaints or other untoward incidents.

Communication Of Policy To Employees And Volunteers

All employees and volunteers should read the policy statement carefully. It is implicit that all employees of NHSGGC are required to adhere to Board policies. Ensure that national and local policy is adhered in the case of Sandyford employees and volunteers.

Communication Of Policy To Clients

Clients are informed regards data protection, confidentiality and the limitations where indicated via the information sheet that is handed to clients at registration, Your Personal Information: Your Choice. (2010).

SPECIFIC CONFIDENTIALITY ISSUES

Standard
All clients have the right to expect confidentiality at all times.

- All clients should be assured of confidentiality.
- Any breaches of the code will be subject to disciplinary procedures.

Consultation

- Verbal communication with the client is in a quiet and polite manner to maintain privacy and confidentiality.
- All other persons present at the consultation should be introduced by name and status and permission granted for their presence during the consultation. If there is a request for a student or observer to be present this request should be made prior to the student or observer being present.
- Agreement to correspondence to the GP of any prescription, procedure or test should be checked with the individual and their wishes respected.
- If any tests are performed then a means of correspondence should be established and recorded on the electronic record.

See specific tests for means of correspondence.

Telephone Enquiries:

Enquiries By The Client
Initial response should be without acknowledging that the individual is a client of the clinic. Telephone enquiries can only be responded to if the individual can identify themselves by name, NaSH number, address & DOB. If the client has forgotten their clinic number, the staff member must attempt to identify the client by other means.

Enquiries By Third Party
In exceptional circumstances there may be a recorded note of the means by which the third party will identify themselves and the client. The client's case record should be checked so that the record of whether the patient has given permission for telephone contact by another individual is clarified before any information is given.

Enquiries By GP Or Their Reception Staff
Initial response should be without acknowledging that the individual is a client of the clinic. The client's case record should be checked so that the record of whether the client has given permission for telephone contact by another individual is clarified before any information is given. If necessary take the surgery number, check & phone back.

Enquiries By Hospital Staff
Initial response should be without acknowledging that the individual is a client of the clinic. The case record should be checked to clarify that there is permission for disclosure by implied consent of the details requested.

Enquiries By Other Agencies
Initial response should be without acknowledging that the individual is a client of the clinic. Such enquiries e.g. social work should only be responded to with the permission of the client.

Storage of Records
Any Paper records should be kept secure so that no unauthorised persons can have access. No records should be left in public places.
All documentation identifiable to the particular client should be disposed of through confidential waste collection. Please check within your locality the system for this.

Computer Security & Confidentiality
Always ensure a password protected screensaver is activated or log off when leaving a PC;

Only view information that is relevant to the work that you are performing. Viewing information which is not pertinent to your work is a breach of several UK laws. (It is not permitted to view the records of a patient for
whose care you are not party to);

Never disclose your passwords – even to IT Support;

Never use somebody else's user ID and password; to do so is a breach of the Computer Misuse Act.

Email and confidentiality
1. NHS Greater Glasgow & Clyde's email systems may be used to send personal identifiable data (PID) within and between the following systems:

*@ggc.scot.nhs.uk; *@irh.scot.nhs.uk; *@glasgow.gov.uk; *@renver-pct.scot.nhs.uk; *@sw.glasgow.gov.uk; *@rah.scot.nhs.uk; *@no-smtp.glasgow.gov.uk; *@vol.scot.nhs.uk , @nhs.scot

PID via the above email systems is secure to any of these outside organisations:

*@gsi.gov.uk ; *@gse.gov.uk ; *@gsx.gov.uk; *@mod.uk ; *@pnn.police.uk ; *@scn.gov.uk; *@cjsm.net ; *@gcsx.gov.uk

2. NHSMail should not be used to send personal identifiable data to any addresses out with those listed above. This route is only secure if both sender and receiver have NHSmail accounts.

3. Clinical communication by email should be added to the patient's health record where appropriate

4. **Wherever possible** the email address (whether using NHSmail or an internal system) should be selected from a directory and not typed in to minimise the risk of errors.

5. The receipt facility must always be used for transfers of PID.

6. The subject line of the email must never contain PID.

7. If you receive an incorrectly addressed email containing PID, you must inform the sender so they can correct their records. You should then delete the email and confirm you have deleted the message.

References

General Medical Council Confidentiality (2017, updated 2018 to include GDPR) https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality [Accessed April 2022]

NHSGGC. Guidance on handling personal identifiable data. http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/eHealth/PoliciesandProcedures/Documents/Health%20Records%20Procedures/PROCEDURE%20FOR%20CONFIDENTIALITY%20SECURITY%20AND%20THE%20RELEASE%20AND%20MANAGEMENT%20OF%20INFORMATION%20(2).pdf (accessed April 2022)

Nursing and Midwifery Council. (2015). The Code: Standards of conduct, performance and ethics for nurses and midwives nmc-code.pdf [Accessed April 2022]

Information Commissioners Office: www.ico.org.uk. [Accessed April 2022]

FURTHER INFORMATION CAN BE ACCESSED VIA STAFF NET ON THE INFORMATION GOVERNANCE AND INFORMATION TECHNOLOGY SECURITY FRAMEWORK: http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/eHealth/InfoGovIndex/Pages/GDPR.aspx [Accessed April 2022]