Patient Confidentiality Policy and Procedures

Author	Dr Angela Anderson
Policy Lead	Registered Manager
Version No.	1.0
Date of issue	Feb 2022
Date to be reviewed	Feb 2023
Not controlled once printed	

Introduction

All healthcare service providers have an ethical, legal and contractual duty to protect patient confidentiality. Information sharing can help to improve the quality of care and treatment, but it must be governed by the legal and ethical framework that protects the interests of patients.

Patients entrust the healthcare providers with their personal information and expect us to respect their privacy and handle their information appropriately. Everyone should seek to ensure that protection of patient confidentiality on collecting and sharing information is built into all healthcare to provide safe and effective care.

Policy Statement

This policy outlines the guiding principles for information sharing, based on legal and ethical requirements. It aims to provide a framework for the secure sharing of patient-identifiable information between partner organisations and also covers wider issues of disclosing information to third parties.

This policy sets out the standards and practice relating to confidentiality applicable to all staff who work for a healthcare service. This policy should be read in conjunction with all of Oxford Skincare Clinic's policies and procedures, but in particular the Information Governance Policy.

Scope

Staff, students, volunteers and contractors, must be aware of and respect a patient's right to confidentiality and must comply with this premise to protect patient confidentiality, which is built on best practice.

All staff members that share information are obliged to adhere to this policy and guidelines. Managers at all levels are responsible for ensuring that the staff for whom they are responsible are aware of, and adhere to, this policy. Oxford Skincare Clinic is also responsible for ensuring staff are updated in regard to any changes in this policy.

Definitions

Personal confidential data: information that relates to an identified or identifiable individual. This data should not be processed without a clear legal basis. Personal confidential data should only be disclosed with consent or under statute, and any disclosure must always be limited and accompanied by a contractual agreement that mitigates the risk of misuse and inappropriate disclosure. The contractual agreement needs to set out, as a minimum, the legal basis for the data flow, the purposes to which the data can be put, the safeguards that should be in place to protect data and how the public are informed about these.

Patient identifiable information: all personal health information is held under strict legal and ethical obligations of confidentiality. Information given in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. Patients should be involved in decisions about the use of their personal health information in most circumstances. Patient identifiable information includes:

- name
- address
- full post code
- date of birth
- NHS number
- National Insurance Number
- pictures, photographs, videos, audio-tapes or other images of the patient, as even a visual image (e.g., photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Non-person-identifiable information: can be classed as confidential, such as confidential business information (e.g., financial reports and commercially sensitive information, e.g., contracts, trade secrets and procurement information) which should also be treated with the same degree of care.

Special categories of personal information: previously known as 'sensitive' personal data, defined by the Data Protection Act 2018 as refers to personal information about:

- racial or ethnic origin

- political opinions
- religious or philosophical beliefs
- trade-union membership
- processing of genetic data
- biometric data (for the purpose of uniquely identifying a natural person)
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

Best Practice for Protecting Patient Confidentiality

It is your responsibility to make sure that you follow the measures set out below to protect the confidential information you have gained privileged access to because of your role. Your responsibility starts when you receive the information, it then continues when you use it, store it, share it with others and destroy it. This applies to both spoken and written information:

- keep accurate, relevant records
- record and use only the information necessary
- access only the information you need
- keep information and records physically and electronically secure and confidential (e.g., leave your desk tidy, take care not to be overheard when discussing cases and never discuss cases in public places)
- follow Oxford Skincare Clinic guidance when using removable devices, such as laptops, smart phones and memory sticks
- keep your usernames and passwords secret and change your passwords regularly
- follow Oxford Skincare Clinic guidance before sharing or releasing information (including checking who a person is and that they are allowed access to the information), and when sending, transporting or transferring confidential information
- make information anonymous where possible
- keep and destroy information in line with local policy and national guidelines
- always report actual and possible breaches of security or confidentiality as a matter of priority.

Best Practice for Keeping Patient Records Secure

For all types of records, staff working in offices where records may be seen must:

- shut/lock doors and cabinets as required
- wear building passes/ID if issued
- query the status of strangers
- know who to tell if anything suspicious or worrying is noted
- not tell unauthorised personnel how the security systems operate
- not breach security yourselves.

Manual records must be:

- formally booked out from the normal filing system
- tracked if transferred, with a note made or sent to the filing location of the transfer
- returned to the filing location as soon as possible after use
- stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently
- stored closed when not in use so that contents are not seen accidentally
- inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons
- held in secure storage with clear labelling. Protective 'wrappers' indicating sensitivity, though not indicating the reason for sensitivity, and permitted access, and the availability of secure means of destruction (e.g., shredding) are essential.

With electronic records, staff must:

- always log-out of any computer system or application when work on it is finished
- not leave a terminal unattended and logged-in
- not share logins with other people. If other staff have a need to access records, then appropriate access should be organised for them
- not reveal passwords to others
- change passwords at regular intervals to prevent anyone else using them
- avoid using short passwords or using names or words that are known to be associated with you (e.g., children's or pet's names or birthdays)
- always clear the screen of a previous patient's information before seeing another
- use a password-protected screensaver to prevent casual viewing of patient information by others.

Best Practice When Sharing Patient Information

Consent to share information must be sought from patients in a sensitive manner. At all times the rights, interests and dignity of the patient must be respected. Patients must have the opportunity to discuss any aspects of information sharing that are specific to their treatment and personal circumstances, for example:

- inform patients of how information will be used before they are asked to provide it. This includes informing patients of the kinds of purposes for which information about them is collected, and the types of people and agencies to which information may need to be passed, such as clinicians
- consent to share information must be recorded in the patient's clinical record and should be sought at the earliest opportunity
- once consent to share personal information has been obtained, it will be assumed to continue unless the patient withdraws consent but will be limited to the purposes for which consent was given
- a patient's case file or other personal record should always be checked for evidence of consent before personal information is shared with another agency
- consent may be verbal or written. Patients can change their choice about their consent at any time
- consent, whether implied (when a patient accepts a service) or explicit (when a patient indicates consent), must always follow the effective involvement of patients
- explicit consent is best practice and should become the norm as better-informed patients share in decisions about the uses of their information.

Caldicott Guardian

The Caldicott Guardian for Oxford Skincare Clinic is Megan Anderson. The Caldicott Guardian is the officer responsible for overseeing all aspects of confidentiality and security in relation to patient-identifiable information. The Caldicott Guardian must ensure that personal health information is kept confidential and that patients are informed and involved in decisions about the use of their information. The Guardian's responsibilities include:

- auditing current practice and procedures
- managing an improvement plan that is monitored through the clinical and corporate governance frameworks
- developing protocols for inter-agency information sharing at a local level

- making decisions about how the Company uses patient identifying information (e.g., provide advice in relation to research studies or disclosure in the public interest).

Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO) is Megan Anderson. She will also be utilised to seek advice on all aspects of data protection and confidentiality.

The Caldicott principles

Monitoring of patient confidentiality must be made by the professional responsible for the patient's assessment, care or treatment, or on the advice of a senior professional or clinical supervisor within the service, which may include the Caldicott Guardian. The principles to which you are expected to work in relation to patient confidentiality are:

- justify the purpose(s) for using confidential information (e.g., every proposed use or transfer of patient identifiable information within or from Oxford Skincare Clinic should be clearly defined and scrutinised, with continuing being uses regularly reviewed by an appointed guardian)
- only use it when absolutely necessary (e.g., patient identifiable information items should not be included unless it is essential for the specified purpose(s). The need for patient to be identified should be considered at each stage to satisfying the purpose(s))
- use the minimum that is required (e.g., where the use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred, or accessible, as is necessary for a given function to be carried out)
- access should be on a strict '**need to know'** basis (e.g., only those individuals who need access to patient identifiable information should have access to it and they should only have access to the information items that they need to see
- everyone must understand his or her responsibilities (e.g., action should be taken to ensure that those handling patient identifiable information, both clinical and non-clinical, are made fully aware of their responsibilities and obligations to respect patient confidentiality

- understand and comply with the law (e.g., every use of patient identifiable information must be lawful).

Legal Considerations

Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of a serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service.

Confidentiality must not be confused with secrecy. Consent to share information should be sought, but if this is not possible and others are at risk, it may be necessary to over-ride the requirement. It is inappropriate for staff/agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly those situations where other people may be at risk.

Sharing common law confidential information without consent for purposes other than direct care

There may be circumstances where it is not practicable to use de-identified information or to get consent and, in these cases, confidential information may be shared but only if there is a legal basis for the information sharing. Requirements for consent should be considered against each of the following criteria:

- **Legal Requirement**: the law requires clinicians to disclose information irrespective of the views of a patient (e.g., if patients contract certain notifiable diseases. The Data Protection Act requires that the patient be told about the disclosure).
- **To protect a patient's vital interests**: for example, where a healthcare professional is concerned that a child or adult may be at risk of death or serious harm. Professionals who have such concerns should draw the individual to the attention of the relevant authorities.
- **In the interest of the public**:
    - when there is a serious risk to public health

    - when there is a risk of serious physical/mental harm to the individual or those known to the individual
    - for the prevention, detection or prosecution of a serious crime
    - where disclosure is necessary to protect vital interests (i.e., where there is knowledge or belief of abuse or neglect of a child or adult at risk)
    - circumstances detailed in any Dangerous Persons Policy or guidance
    - where the disclosure is otherwise lawful (e.g., covered by section 60 of the Health and Social Care Act).
- **Children and adults who are unable to consent**: a patient is unable to give consent (e.g., some children, adults with incapacity and/or the critically ill). In many of these cases, particularly in the case of children, there will be someone (e.g., a parent) who is legally entitled to give consent on their behalf.

Both the Data Protection Act and professional standards specifically allow for information to be disclosed in this way.

The senior healthcare professional on duty must be prepared to balance the considerations for and against disclosure in the interests of the patient and any third party and also justify and record each decision to disclose or withhold. It will, therefore, be a matter for the healthcare professional's best judgement, as well as legal and professional guidance. Decisions should be taken on a case by case basis in the light of best available information, which may include advice from the Data Protection Officer (DPO) or Caldicott Guardian. Wherever possible, the patient should be informed what information has been disclosed and to whom.

Direct Care and Informing Patients Effectively

Sharing of information should, where possible, be with the consent of the patient. Patients should be informed of the purposes for which information about them may be recorded and shared. It is only with sufficient information that consent may be given. Patients should be given an opportunity to express their wishes as to how information should be used, and these wishes should be respected where possible.

Patients have a right to expect that information about them will be held in confidence and protected at all times against improper use and disclosure.

Under data protection law, you are responsible for patient data, for storing it securely and protecting it from unauthorised or unlawful processing. You must make sure any personal information about patients that you hold or control is effectively protected at all times against improper access, disclosure or loss. You must also make sure that identifiable patient data is not improperly disclosed in any circumstances. An inadvertent breach of patient confidentiality could result in disciplinary action or an investigation.

If in doubt, seek the advice of the local SIRO or Data Protection Officer. The following interactive guidance tool could help you to decide on any confidentiality decisions – https://www.gmc-uk.org/ethical-guidance/learning-materials/confidentiality-decision-tool

Registered and regulated professionals

Confidential information needs to be shared between registered and regulated health and social care professionals who have a legitimate relationship with the individual for the purposes of the individual's direct care. A registered and regulated health or social care professional has a legitimate relationship with the patient or service user when any or all of the following criteria are met:

- the individual presents themselves to the professional to receive care
- the individual agrees to a referral from one care professional to another
- the individual is invited by a professional to take part in a screening or immunisation programme for which they are eligible, and they accept
- the individual presents to a health or social care professional in an emergency situation where consent is not possible
- the relationship is part of a legal duty (e.g., contact tracing in public health)
- the individual is told of a proposed communication and does not object (e.g., the consultant in the ambulatory clinic says she will let the patient's social worker know of events in the clinic and the patient does not object).

Carers, family members and friends

Some friends and/or family have a special relationship with the patient, in that they act as a carer. Confidential information should be shared with the carer, when the patient

has given explicit, informed consent. In circumstances where the patient cannot give valid consent, confidential information should be shared with the carer subject to open dialogue with the patient, if possible. If it is not possible to engage in an open dialogue, information should be shared with the carer in the incapacitated person's best interests, when ALL of the following criteria are met:

- the patient lacks capacity
- the carer 'cares for' the patient
- there is no legal documentation in place to prevent sharing
- there are no contra-indications to sharing in the patient's record
- there are no safeguarding issues apparent.

Patient Consent Cannot be Obtained

In some circumstances it may not be possible to obtain consent because, in the opinion of the person responsible for the patient's care or well-being, the patient:

- is too ill
- does not have the capacity to consent as per the Mental Capacity Act
- the situation is urgent and the individual cannot be located to obtain consent.

In such cases, you should recognise that it may be necessary to share information with other agencies so that appropriate care and treatment can be provided to the patient, or in exceptional circumstances where disclosure would be in the public interest, for instance where disclosure of the information is necessary to prevent harm coming to another individual.

Refusal of consent

Patients have the right to object to the information they provide in confidence being disclosed to a third party in a form that identifies them, even if the third party is someone who might provide essential healthcare. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment. A number of issues to be considered if a patient refuses to consent to information sharing are as follows:

- the concerns of the individual must be clearly established, and attempts should be made to find out whether there is a technical or procedural way of satisfying these concerns without unduly compromising care
- the options for providing an alternative form of care or to provide care through alternative arrangements may need to be explored
- decisions about the options for alternative arrangements that might be offered to the patient have to balance the risks, staff time and other costs that may result against the risk to the individual of not providing assessment, care or treatment.

Careful documentation of the decision-making process and the choices made by the patient must be documented in the patient's records.

Anonymisation/Pseudonymisation

It is your responsibility to always consider making information anonymous, if possible, or allowing individuals to be distinguished in a data set by using a unique identifier, which does not reveal their 'real world' identity, in particular when information is being used for a purpose other than direct patient care. This includes information such as name, address, full postcode, date of birth and any other detail that might identify a patient being removed; the data about a patient being unidentifiable by the recipient of the information and the theoretical probability of the patient's identity being discovered being extremely small. Always consider anonymisation of data where possible. If data are anonymised, it is good practice to inform the patient, but consent is not needed.

Pseudonymisation may involve replacing names or other identifiers that are easily attributed to individuals with, for example, a reference number. Whilst you can tie that reference number back to the individual if you have access to the relevant information, you put technical and organisational measures in place to ensure that this additional information is held separately. Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations. The Oxford Skincare Clinic gives patients a unique identifying number which is used for pseudo anonymity when appropriate.

Patient's Rights of Access to their own Records

Patients (or their parents or legally appointed representative), subject to certain safeguards, have a right to access their own health records. You must comply with the requirements of the Data Protection Act 1998 in terms of requests to access personal identifiable information and should respect and help patients to exercise their legal rights to have access to, or copies of, their health records.

If an access request means disclosing information from or about a Third Party (someone other than the patient or staff involved in their care), the request may be refused unless Third Party information can be temporarily removed, the Third Party consents to disclosure or 'it is reasonable in all the circumstances' to comply with the request without the consent of the individual.

Information needs to be provided within 40 days of a request so staff must action requests promptly.

Training Requirements

All staff are required to complete annual mandatory Information Governance Training. Training on confidentiality is provided regularly to staff via induction training, mandatory refresher training and specific training opportunities developed to meet particular needs identified from training needs assessments and response to incidents.

All staff must be aware where to seek support, further information and training, and be able to demonstrate that they are making every reasonable effort to comply with the relevant standards. Failure to comply will result disciplinary action.

Personal information about patients should not be disclosed unless it is necessary. The following flowchart can help you decide whether personal information needs to be disclosed and, if so, what the justification is for doing so: https://www.gmc-uk.org/-/media/gmc-site-images/ethical-guidance/learning-materials/confidentiality_decision_tool.pdf

Monitoring

The effectiveness of this policy will be monitored through routine audit and investigation into any data breaches or breaches in the policies procedures by the leadership team.

Related Policies and Procedures

Information Governance Policy and Procedures

Safeguarding Policy and Procedures

Disciplinary Policy and Procedures

Incident Management Policy and Procedures

Legislation and Guidance

The Caldicott Principles

Common Law duty of Confidentiality

The General Data Protection Regulation (GDPR)

Data Protection Act 1998

Health and Social Care Act 2008

The Mental Capacity Act 2005

Human Rights Act 1998

Freedom of Information Act 2000

The GMC's guidance on confidentiality https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality

Confidentiality flowchart- https://www.gmc-uk.org/-/media/gmc-site-images/ethical-guidance/learning-materials/confidentiality_decision_tool.pdf

Guidance tool to decide confidentiality decision – https://www.gmc-uk.org/ethical-guidance/learning-materials/confidentiality-decision-tool

The UK Caldicott Guardian Council (UKCGC) Caldicott Principles https://www.ukcgc.uk/manual/principles

The Guidance on Confidentiality: NHS Code of Practice
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

ICO Anonymisation: Managing data protection risk code of practice
https://ico.org.uk/media/1061/anonymisation-code.pdf

Compliance

Safe	**S1:** How do systems, processes and practices keep people safe and safeguarded from abuse?
Effective	**E4:** How well do staff, teams and services work together within and across organisations to deliver effective care and treatment? **E6:** Is consent to care and treatment always sought in line with legislation and guidance?
Caring	**C3:** How is people's privacy and dignity respected and promoted?
Responsive	**R2:** Do services take account of the particular needs and choices of different people?
Well-led	**W4:** Are there clear responsibilities, roles and systems of accountability to support good governance and management? **W6:** Is appropriate and accurate information being effectively processed, challenged and acted on?