Ormeau Health Centre

Privacy Policy

Under the new GDPR regulations effective from 25th May 2018, Ormeau Health Centre as a 'data controller' must process person-identifiable or confidential data, fairly, lawfully and transparently.

Processing data encompasses holding, collecting, recording, obtaining or disclosing data or carrying out any operations on this data.

Ormeau Health Centre will process personal data on the following bases:

- Explicit Patient Consent
- Necessary for Provision of Healthcare Service
- Contract Fulfilment
- Legitimate Interest
- In the Vital Interest of the data subject
- Legal/Common Law

Data we hold will be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The purpose of this Privacy Policy is to lay down the principles of privacy which all staff in Ormeau Health Centre, who have access to person-identifiable or confidential information must adhere to. All staff must be aware of their responsibility for safeguarding the confidential personal data we hold.

- All employees both past and present are bound by a legal duty of confidence to protect personal information they may come into contact with. This is not only a contractual requirement but is a requirement under GDPR and common law. It is also a requirement under the NHS Code of Practice.

- Information will be stored on both paper and computer records. Digital records are kept in security protected PC's and paper records are kept in locked areas, with access only to authorised personnel. Laptops have multi-faceted security protection.

- This policy sets out the requirements placed on all staff in Ormeau Health Centre including independent contractors when sharing all person-identifiable data. Personal-identifiable data means information that contains a means of identifying a person:
- Name
- Address
- Post Code
- Date of Birth
- Health & Care Number

- National Insurance Number
- Email Address
- Hospital Number
- Payroll Number

All Staff (including independent contractors)

Confidentiality is an obligation for all staff and all are bound by the NHS code of practice and the confidentiality clause in their contract of employment at Ormeau Health Centre. Any breach of confidentiality regarding both patients and staff in the practice could be regarded as gross misconduct and may result in dismissal. They must be reported to the Data Protection Officer, Dr Claire Diamond.

The following principles must be adhered to:

- Person-identifiable or confidential information must be protected against improper disclosure when it is received, stored, transferred or disposed of.

- Access to person-identifiable data or confidential information is on a need to know basis.

- Disclosure of person-identifiable or confidential information must be limited to that purpose for which it is required.

- If the decision is taken to disclose information, that decision must be justified and documented and where appropriate consent must be obtained.

- Concerns regarding disclosure must be discussed with Data Protection Officer, the GP Partners and the Practice Manager.

See Ormeau Health Centre Patient Privacy Notice, Staff Privacy Notice and Children's Privacy Notice.

Ormeau Health Centre as the Data Controller is responsible for protecting the information it holds on both patients and staff.

Information is stored on both paper and computer records.

Data mapping is carried out in line with GDPR and for both staff and patients indicating what data we hold, where we got it from, why we have it, how we store it and who we share it with. Risk assessments will be carried out when new systems or software are implemented.

Ormeau Health Centre clinical research trial documentation is kept archived both on the premises, in a locked room and in off-site storage with an external company with which we have a contract. They will operate as processors of data under GDPR and their own strict controls.

Access to rooms where computers or person-identifiable data is found, must be controlled and away from the public. Doors must be locked with keys or keypads where confidential material is kept.

Desks must be cleared at the end of each day, in line with the clear desk policy at Ormeau Health Centre.

Computers locked every time a member of staff leaves the desk. All computers are password protected and users all have their own unique log-ins, which must not be shared.

Portable storage such as USB drives must be password encrypted.

All laptops are password protected and user specific. Staff must ensure that only a minimal amount of person-identifiable information is taken away from the premises and must be aware they are responsible for guarding this information.

Unwanted print-outs containing any person-identifiable material must be shredded, including discs and tapes.

Where a patient is no longer registered with the practice, we will transfer their paper and computer record, securely with the appropriate courier service engaged by the Business Services Organisation.

Where an employee has left their position at Ormeau Health Centre, we will dispose of their personnel file within 3 months' of their departure with the exception of pension and payroll information.

Sharing Personal/Confidential Information

Information will only be shared in appropriate circumstances, where there it falls under the afore mentioned bases. Consideration will be given to how much information is needed, ensuring only the minimal amount is disclosed.

Information can be shared:

- To fulfill a contract.
- In an anonymised form, in accordance with the ICO code of practice.
- Where there is a court order or a requirement by law. This must be discussed with the Caldicott Guardian using the Caldicott Principles – see Appendix 3
- In identifiable form, when required for a specific purpose with the subject's written consent.
- In child protection proceedings if it is in the child's or the public's interest.
- For the protection of the public and to prevent serious crime.

Disclosing a child's Personal Information

Children over the age of 12 years, deemed competent can give their own consent for the processing of their personal data. In the case of a child under the age of 12 years, consent must be obtained from whoever has parental responsibility unless the service being offered is a preventative or counselling service.

Care must be taken in transferring information to ensure that the method of transfer is as secure as it can be. Where appropriate, data processing agreements must be completed with the appropriate data processor.

All third party information must be redacted prior to transfer, after the appropriate consent has been obtained or where the request has a lawful basis.

Staff must ensure they follow the appropriate standards in respect of data sharing via telephone calls, faxes and emails:

- Three pieces of information must be verified before disclosure during telephone calls i.e. Name, DOB, address and if necessary a fourth piece will be obtained, such as last consultation.
- In the case of children, information will only be shared under one of the lawful bases. Consent will be sought from a child, gillick competent under the age if 16 years, before data will be shared with a parent or guardian.
- Faxed documents must have person-identifiable information removed before transmission.

- Emailed documents must have all person-identifiable information removed and where available, encrypted. Person-identifiable data must not be forwarded to personal email accounts unless a patient has made a specific request for emailed information.

Requests for Release of Personal or Special Category Data (Health Information)

From a patient or staff member for own personal information:

- A Subject Access Request (SAR) must be in writing to the Practice Manager, Claire Bateson and signed by the subject, their legal guardian or carer. The request will be processed and available within 28 days of receipt of the request or sooner if it is a request for print outs of test results or immunisations. The request will be coded and scanned into the subjects' record.

From a Third Party Source i.e. Solicitors, Government Agencies:

- Request must be in writing with a signed consent form from the subject, their guardian or carer. The request will be logged on the date it is received. The request will go to the GP with the full medical record for checking and redaction of any harmful third party information. The requested information will be ready for collection within 28 days of the date of the request. The request will be maintained in the medical record.

Removing data from the premises for Home Visits

Removal of patient data from the building usually in the form of a summary print out, by a GP partner, nurse, Locum GP is sometimes necessary to treat a patient during a home visit.

The information being taken from the premises must be kept to the minimal amount necessary to fulfill the healthcare needs of the patient on that day.

The person removing the data from the building for this purpose is solely responsible to ensure the data is kept safe, used and then disposed of by shredding.

Any loss of this data must be reported straight away and dealt with according to the GDPR guidance.

Ormeau Health Centre has a policy on the removal of data which can be referred to where required.

Carelessness

All members of staff have a legal and contractual duty to protect and keep confidential, any person-identifiable data. Any member of staff accidentally or purposely disclosing personal, confidential information may be held liable for a breach of confidence.

Staff must not:

- Talk about person-identifiable or confidential information in a public place or an area where this could be overheard i.e. on the reception desk.
- Leave any person-identifiable or confidential documents lying around unattended.
- Leave a computer terminal logged on to a system where person-identifiable or confidential data can be accessed.
- Knowingly browse, search for or look at any personal or confidential information relating to staff, patients or others, without a legitimate purpose.

Any breach or loss of this information must be reported immediately to the Practice Manager and the DPO. Serious breaches must be reported to the ICO within 72 hours. The data subject must be informed of the possible breach of their personal data.

Implementation

This privacy policy must be read and a log signed by all staff. Training up-dates will be annual. New staff must be made aware of the policy and ensure they follow the guidelines.

See
Patient Privacy Notice

Staff Privacy Notice

The Caldicott Principles:

- Justify the purpose for using patient-identifiable data
- Don't use patient identifiable data unless absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Everyone must understand and comply with the law