MacIntyre
Providing support...your way

Confidentiality and Data Protection Policy Statement

Introduction

This Policy Statement describes MacIntyre's approach to confidentiality and to data security and protection.

MacIntyre is registered as a Data Controller on the Data Protection Register held by the Information Commissioners Office (ICO) - Registration Number: Z6791722.

MacIntyre's named representative for data security and protection purposes is Claire Toombs (Finance Director). Claire Toombs holds the role of Senior Information Risk Owner whose role is to take ownership of the organisation's information risk policy, act as an advocate for information risk and provide an annual statement to Trustees in regard to information risk.

Rowan Jackson, Head of Compliance and Safeguarding, holds the role of Caldicott Guardian. Her role is to protect the confidentiality of information about people we support and enable appropriate information-sharing, and to check that this Policy is implemented throughout the company.

Policy

MacIntyre recognises that it has a duty to protect the personal data of people receiving a service, staff and others, and recognises the importance of handling personal data legally, securely and appropriately.

MacIntyre will take all practical steps to ensure that the requirements of the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) are achieved and maintained throughout the organisation at all times; and will maintain records that demonstrate ongoing compliance with the Regulations.

MacIntyre will ensure that proportionate controls are consistently applied to all types of personal information. MacIntyre's processes for handling personal information will ensure that it is protected from the loss of confidentiality, integrity and availability while being managed in such a way that services can be provided efficiently and effectively:

- Confidentiality: Personal information is available only to authorised individuals
- Integrity: There are safeguards to ensure the accuracy and completeness of personal information and processing methods
- Availability: Authorised employees have access to relevant information when they need it

MacIntyre will implement additional controls on special category personal data and criminal convictions and offences data as required under the Data Protection Act 2018.

MacIntyre will:

- Issue privacy notices to all people on which it holds personal information, telling them the lawful basis for holding/processing their data and what we will do with that data
- Maintain internal records of information assets and processing activities (i.e. document what personal information we hold and for what purpose, our lawful basis for processing and whom we share it with), recording information defined in the UK GDPR
- Implement technical and organisational measures that evidence that we have considered and integrated data protection into our processing activities (called 'data protection by design and by default')
- Complete a Data Protection Impact Assessment (DPIA) when any new technology is being deployed
- Ensure and evidence that contracts with data processors comply with UK GDPR and cover off liabilities appropriately
- Ensure that systems for handling personal information are only available to authorised individuals and use appropriate security measures
- Record information security incidents and, where necessary, report personal data breaches to the ICO and (in defined circumstances) to the affected individuals

MacIntyre will help the people it supports and staff to understand the records that are kept about them, how the company respects their confidentiality and protects their personal information, their right to view information held about them and have inaccurate information corrected, and their right to have that information permanently erased (where that information is not required to be retained for set periods of time to fulfil our legal obligations).

MacIntyre will provide training in confidentiality and data protection to all its employees, tailored to the particular needs and responsibilities of their role; and will ensure that this training is updated when new systems, legislation or policies are introduced.

MacIntyre staff must not share personal information with anyone who is not under a duty to receive it, and must be conscientious in their handling of paper and computer records; any failure to do these may be considered under MacIntyre's disciplinary procedures.

Staff must not misuse IT equipment provided by MacIntyre, including accessing pornography, sending or posting derogatory comments or other such activities that might bring the company into disrepute.

Notwithstanding the above, MacIntyre fully endorses the Caldicott Principle that the duty to share information (with people's consent or in their best interests) can be as important as the duty to protect people's confidentiality; where there is regular data sharing with local partner organisations, MacIntyre will seek to conclude Information Sharing Agreements with those organisations.

All breaches of confidentiality and information security, actual or suspected, must be reported and investigated; failure to report a breach may be considered a disciplinary offence.

MacIntyre will provide clear guidance to its staff on the following areas:

- MacIntyre's governance arrangements for data protection
- Acceptable and safe use of computers, email and the internet; and the security arrangements for MacIntyre's IT networks
- Data quality and rectification, data protection by design and by default and how MacIntyre informs people about their rights
- MacIntyre's system for recording information assets and processing activities including the lawful basis on which personal information is held
- The sharing and transfer of personal information outside of MacIntyre, including with the families of people supported and in Information Sharing Agreements
- The engaging of external Data Processors (third party suppliers who will process personal information for or supplied by MacIntyre)
- The physical security of paper records, premises and equipment on which personal information is kept
- The creation, processing, retention, archiving, disposal and deletion of records containing personal information
- The handling of information security incidents
- The completion of Data Protection Impact Assessments and Legitimate Interests Assessments
- The handling of requests by people to view personal information held by MacIntyre about them (Subject Access Requests), and of the other rights for individuals under the UK GDPR
- The appropriate use of surveillance and remote monitoring systems
- MacIntyre's business continuity plan that sets out the procedures in the event of a security failure or disaster affecting computer/information systems.

If you have any queries or concerns about the way that MacIntyre handles personal data or wish to view further documentation on the implementation of this Policy Statement, please contact data.protection@macintyrecharity.org, ring us on 01908 230100 or write to Claire Toombs, MacIntyre, Seebeck House, 1 Seebeck Place, Knowlhill, Milton Keynes, MK5 8FR.

Good Practice Guidance

The associated guidance and materials to accompany this Policy contain a suite of documents to support implementation. These are reviewed and revised annually, or sooner as required.

The documents below are available to all MacIntyre staff through our Intranet (except for those marked 'locally stored' which can be obtained from the Data Protection Team). To view a copy of any non-confidential document, please email data.protection@macintyrecharity.org.

- DP0.1: List of Information Asset Owners
- DP0.2 Record of Processing Activities (locally stored)
- DP0.3 RoPA template
- DP0.4 Combined RoPA and IAR template
- DP0.5 Data Audit (Adult Services) – Excel (locally stored)

    - DP0.6 Data Audit (No Limits) – Excel (locally stored)
- DP1: Good Practice Guidance - Safe Use of Computers and the Internet
    - DP1.1: Guidance on Access to User Accounts
    - DP1.2: Audit of User Accounts Log (locally stored)
    - DP1.3 Unsupported Systems Risk Assessment (locally stored)
- DP2: Computer and Internet Safety Checklists
- DP3: Good Practice Guidance on Confidentiality, Data Protection, Data Sharing and Records.
    - DP3.1 Confidentiality, Data Protection, Data Sharing and Records – the basics (basic guidance - must be read before working unsupervised)
    - DP3.2 Guidance on local information sharing arrangements
    - DP3.3 Information Sharing Agreement template
    - DP3.4 Information Sharing Notice
    - DP3.5 Non-Disclosure and Confidentiality Agreement template
    - DP3.6 Record Retention and Archiving Workbook - Adult Services (Excel)
    - DP3.7 Example Information Sharing Agreement
    - DP3.8 Record retention and disposal schedule (Adult Services)
    - DP3.9 Archiving Procedure (Adult Services)
    - DP3.10 National Data Opt-Out
    - DP3.11 Guidance on transferring a service to a new provider
- DP4: Guidance on surveillance and remote monitoring
    - DP4.1: Privacy, Data Protection and Risk Assessment for surveillance or remote monitoring
- DP5: Guidance on Information Security Incidents
    - DP5.1: Information Security Incident Report Form
    - DP5.2: Information Security Incident Log (locally stored)
- DP6: Guidance on Data Protection Impact Assessments
    - DP6.1: Data Protection Impact Assessment form
    - DP6.2: Data Protection Impact Assessment example
    - DP6.3: Data Protection Impact Assessment Log (locally stored)
    - DPIA008 Data Protection Impact Assessment on Vaccination as a Condition of Employment
- Subject Access Requests
    - DP7.1: Subject Access & Other Individual Rights Requests (for all data subjects)
    - DP7.2: Subject Access & Other Individual Rights Requests from Staff, Volunteers and Job Applicants
    - DP7.3 Subject Access Requests from people we support
    - DP7.4: Subject Access and Individual Rights Requests Log (locally stored)
- DP8: Guidance on legitimate interests assessments
    - DP8.1: Legitimate Interests Assessment Form

    - DP8.2 example Legitimate Interests Assessment
    - DP8.3 Legitimate Interests Assessments Log (locally stored)
- Privacy Notices and data sharing consent forms (see Appendix 4 below):
    - DP9.1: Privacy Notice for adults we support ('How MacIntyre used information about people we support') - full wording
    - DP9.2: Privacy Notice for adults we support ('Looking after your personal information') - easy read
    - DP9.3: Data sharing consent form for adults we support ('Sharing my personal information form') - easy read
    - DP9.4: No Limits Privacy Notice for Learners - full wording
    - DP9.5: No Limits Privacy Notice for Learners ('Looking after your personal information') - easy read
    - DP9.6: Data sharing consent form for No Limits ('Sharing my personal information') - easy read
    - DP9.7: No Limits Privacy Notice for Parents/ Carers
    - DP9.8: MacIntyre School Privacy Notice for Parents/ Carers
    - DP9.9: Privacy Notice for Staff, Volunteers and Job Applicants
    - DP9.10: Privacy Notice for Supporters and Website Users – A Quick Guide
    - DP9.11: Privacy notice for families and circles of support
    - DP9.12: Privacy notice for people seeking support from MacIntyre
    - DP9.13: Privacy Notice for Supporters and Website Users – The Detail
    - DP9.14: Privacy Notice for Professionals Visiting our Care Homes
- Consent to data for publicity and training:
    - DP10.1: Consent Form for Staff
    - DP10.2: Easy-read Photos and Videos and Stories Form for people we support
    - DP10.3 Photos, Videos & Stories Consent Form for people we support (non-easy read)
- DP11: Guidance on data flows with third parties (this and other DP11 documents below are locally stored))
    - DP11.1: Data Processor Contract Checklist
    - DP11.2: Data Processor Contract Clauses
    - DP11.3: Data Processor Due Diligence Checklist
    - DP11.4: Third Party Data Flows Register (maintained by Data Protection, not on Intranet)

Appendix 1: MacIntyre's approach to data protection

MacIntyre recognises the importance of holding and protecting personal data to meeting its objectives. We have the following governance arrangements to oversee information governance and the implementation of the UK GDPR and the Data Protection Act 2018:

- We have a Lead Director/SIRO responsible for data protection.

- We have a Caldicott Guardian
- We have a Data Protection Manager
- In our Confidentiality and Data Protection Policy we have clearly defined the roles and responsibilities of each level of staff in relation to data protection. In particular the Policy sets out the responsibilities of the SIRO, Caldicott Guardian, and of MacIntyre's Information Asset Owners (heads of every business or operational function of MacIntyre that processes personal data) for the implementation of each of the UK GDPR's key requirements. The Policy is approved by MacIntyre's Directors.
- We have set up a Data Protection Team to
    - plan and coordinate the work of implementing data protection legislation and good practice across the whole of MacIntyre
    - review data protection and information governance risks
    - review information security incidents to improve data security

  The Team meets every 6 weeks.

Data Protection Officer (DPO)

Article 37 of the GDPR says that we must appoint a Data Protection Officer (DPO) if:

> a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
>
> b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and / or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
>
> c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

At the present time it is not clear what is meant (in the regulation quoted above) by:

- "core activities": The ICO states "Your core activities are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity. This is different to processing personal data for other secondary purposes, which may be something you do all the time (e.g. payroll or HR information), but which is not part of carrying out your primary objectives".
- "processing on a large scale of special categories of data": the GDPR does not define what is meant by large scale. We are aware that the Care Provider Alliance is liaising with the Information Governance Alliance and the Information Commissioner's Office to find an answer on this topic, but as yet there is no further advice.

With regard to 'core activities'**:** MacIntyre's core activity is to provide support to people with a learning disability. We consider that maintaining records to communicate and evidence this support is important but is not a core activity. However we will ensure that we keep abreast of any further guidance from the ICO on what constitutes a 'core activity' and will respond accordingly.

With regard to 'processing on a large scale of special categories of data'**:** An external consultancy that has provided advice and guidance to MacIntyre has advised that, based on the experience of its subscribers to date, the number of people on whom we hold special

category data (around 1300 people supported and 2200 staff) has not been the level at which organisations are likely to appoint a DPO. On the other hand we are aware that the Care Provider Alliance is of the view that larger social care providers may need to appoint a DPO. We will ensure that we keep abreast of any further guidance from the ICO on what constitutes 'large scale processing' and will respond accordingly.

Our decision therefore is that we are not currently required to appoint a DPO. MacIntyre will however keep this decision under regular review in the light of any further guidance or case law on the subject.

Authorised by Claire Toombs, MacIntyre's Finance Director and Senior Information Risk Owner 19/12/2018.

Appendix 7: National Data Opt-Out

What is the National Data Opt-Out?

The national data opt-out allows a person (aged 13 or over) to choose whether or not they want their confidential patient information to be used for purposes beyond their individual care and treatment – i.e. for research and planning. Those with parental responsibility, (parents and legal guardians) are able to set a national data opt-out on behalf of a child under the age of 13. The Opt-Out enables people using health or social care services (or people acting for them by) to have control over setting or changing their opt-out choice, and to change their mind at any time.

Section 251 of the NHS Act 2006 provides the statutory power for the NHS to use and share patient identifiable information to support essential NHS activity ***without the consent of patients***. The power can be used only to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice. The national data opt-out in England provides a partial opt-out from this data sharing. The opt-out was implemented by NHS Digital from 25 May 2018. All other health and social care organisations are required to apply the opt-out by March 2020.

The national data opt-out was recommended in the National Data Guardian's (NDG) Review of Data Security, Consent and Opt-Outs in July 2016. The Government accepted all the recommendations made by the NDG. The national data opt-out applies only to England. For information relating to Wales see Health in Wales's Privacy Notice.

The national data opt-out is based on the 8 principles set out in the NDG's report:

1. You are protected by the law
2. Information is essential to good quality care
3. Information is essential for other beneficial purposes
4. You have the right to opt out
5. The opt out will be respected by all organisations that use health and social care information
6. Explicit consent will still be possible
7. The opt-out will not apply to anonymised data (ICO code)
8. The opt out will not apply to exceptional circumstances

The national data opt-out applies to data that originates within the health and adult social care system in England; it is applied by health and care organisations that subsequently process this data for purposes beyond individual care. When the opt-out is applied, the entire record(s) associated with that individual must be fully removed from the data being disclosed. The NHS number is used as the identifier for the removal of the records. In broad terms the national data opt-out applies unless there is a mandatory legal requirement or an overriding public interest for the data to be shared. The opt-out does not apply when the individual has consented to the sharing of their data or where the data is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice on Anonymisation. The opt-out applies regardless of the format of the data and this includes structured and unstructured electronic data and paper records.

People opt out online, by phone or by post. Their preference will remain in place unless and until such a time that they decide to change their opt-out preference. A person's preference to opt-out will continue to be applied after their death. National data opt-outs are not applied retrospectively; this means that when a person sets their opt-out preference for their confidential patient information (CPI) not to be shared for uses beyond their individual care their records will be removed from any disclosure of CPI from that time onwards.

'Confidential patient information' (CPI) is defined in section 251 (11) of the National Health Service Act 2006. Broadly it is information that meets all of the following 3 requirements:

1. identifiable or likely identifiable (for example from other data likely to be in the possession of the data recipient); and
2. given in circumstances where the individual is owed an obligation of confidence; and
3. conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment.

Research and planning are broadly defined as follows:

- Research – finding ways to improve treatments and identify causes of and cures for illnesses.
- Planning – to improve and enable the efficient and safe provision of health and care services.

How does the National Data Opt-Out work?

National data opt-outs apply when an organisation such as a research body confirms they have obtained an approval from the Confidentiality Advisory Group (CAG) for the disclosure of CPI held by another organisation responsible for the data (the data provider) such as an NHS Trust or social care provider. A CAG approval is an approval made under section 251 of the NHS Act 2006 and its current regulations, the Health Service (Control of Patient Information) Regulations 2002, which enable the common law duty of confidentiality to be temporarily lifted so that CPI can be disclosed without the data provider being in breach of the common law duty of confidentiality. The data provider can then, if it wishes, disclose the information to the data applicant e.g. research body without being in breach of the common law duty of confidentiality.

When a person sets an opt-out choice, it is recorded against their NHS number on the 'Spine' (the network that links the NHS's IT systems). It will remain unless the person changes their mind, even after they have died. The Check for National Data Opt-outs service uses the 'messaging exchange for social care and health' (MESH) to enable organisations to submit lists of NHS numbers and receive lists back with the NHS numbers removed for those people that have opted out.

The following NHS resources are available from MacIntyre's Intranet under Confidentiality and Data Protection Policy:

- Leaflet 'Your Data Matters to the NHS'
- Easy read 'Your information matters to the NHS'

For more information see 'Understanding the national data opt-out'.
Information for the public about the national data opt-out can be found at https://www.nhs.uk/your-nhs-data-matters and downloadable resources are available at https://digital.nhs.uk/services/national-data-opt-out/supporting-patients-information-and-resources (including an easy read booklet).

What does MacIntyre do to comply with the national data opt-out?

- Our privacy notices for people we support (DP9.1 and DP9.2) tell people about the opt-out
- We have published this guidance and brought it to the attention of all staff
- We have included information about the opt-out in our data protection training which all staff are required to complete
- MacIntyre's Confidentiality and Data Protection Policy puts a responsibility on all employees and volunteers 'to be aware of the National Data Opt Out and to support people using the service to opt out if they wish to'
- The NHS leaflet 'Your Data Matters to the NHS' and the easy read booklet 'Your information matters to the NHS' are available to staff on MacIntyre's Intranet to assist in supporting people to understand the opt-out
- All managers must report any request to use MacIntyre's data about people it supports for planning or research purposes to the Senior Information Risk Owner/Finance Director, who will consider the request

- MacIntyre does not currently use or disclose confidential patient information for purposes beyond individual care. Any future request approved by the Confidentiality Advisory Group will be considered by MacIntyre's Directors
- Note that MacIntyre does not hold a central record of people it supports that have opted out. This is both because we have no right or legitimate interest in our knowing that people have opted out; and because people we support are free to opt out without informing us.

Scenario

Jim lives in supported living and is supported to do so by MacIntyre staff. One of his staff, Sue, talks to him about the national data opt out by going through the easy read document 'Your information matters to the NHS' with him, which she has downloaded from the Intranet.

Jim understands that his personal information will be shared by people in the NHS involved in his direct care and he is happy with this, but he doesn't want his information used by the NHS or social care for research and planning purposes. So he decides to opt out.

Jim decides to opt out online at www.nhs.uk/your-nhs-data-matters. He types in his name and date of birth but has a problem typing in his NHS number so he asks Sue to help him do so. He gets a 'passcode' from the NHS (because that's how he has told his GP he wants to be contacted) to type in, then clicks to opt out. He gets a text message from the NHS confirming his choice to opt out.

The following other Appendices are available on request:

Schedule of staff responsibilities under this Policy

Appendix 2: Data quality and rectification

Appendix 3: Data protection by design and by default

Appendix 4: How MacIntyre informs people about their rights

Appendix 5: MacIntyre's network security arrangements

Appendix 6: Information Asset Register and Record of Processing Activities