mentalwelfare commission for scotland

Policy Title: Data Protection Policy	**Policy Number:** 029
Issue Number: 11	**Date of First Issue:** June 2004
Date of Last Review August 2021	**Date of Next Review** August 2022
Lead Person: Information Governance Manager	**Approved by:** Commission Board

1. Introduction

The Mental Welfare Commission for Scotland needs to collect and use a variety of sensitive and personal information about people in order to fulfil its statutory functions and other operational duties. This information includes data on users of mental health, learning disability and social care services and their carers; current, past and prospective employees; suppliers; clients/customers; and others with whom it communicates. All such personal information shall be dealt with properly and securely no matter how it is collected, recorded and used.

The National Confidential Forum, (the NCF) was established as a Committee of the Commission in 2014 under the Victims and Witnesses (Scotland) Act 201 and came to an end on the 28 June 2021 under the terms of the Redress for Survivors (Historical Child Abuse in Care) (Scotland) Act 2021. During its lifespan, the NCF was a committee of the MWC and did not exist as a separate legal entity from the Commission. The NCF's core function was to receive and listen to testimony from those who were in institutional care as children. The Commission remains the data controller of the records produced by the NCF.

The UK General Data protection Regulation (UK GDPR) governs the processing of personal data of individuals by 'data controllers', such as the Commission. The Data Protection Act 2018 enshrine the regulation into UK legislation.

This policy applies to all Commission personnel. Failure to comply with this policy could result in disciplinary action. It is mandatory for all personnel to read and understand their responsibilities in accordance with the principles and practice set out in the NHS Code of Practice for Protecting Patient Confidentiality (updated 2012). Staff should also abide by the best practice guidance included in the Looking after Information: staff awareness leaflet published jointly by NHS Scotland and the Scottish Government in 2011.

In relation to GDPR/DPA, Board members are expected to abide by the Commission's policies and procedures about data protection, IT and information risk produced by the Commission and also to comply with the Board Code of Conduct.

2. The Data Protection Act Principles in UK GDPR

We must comply with the UK GDPR, which requires that data is collected and used fairly, stored safely and not processed unlawfully. In particular we will comply with the following GDPR principles while processing data subjects' data:

1. **Lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner;

2. **Purpose limitation.** Data shall only be obtained and processed for one or more specified, explicit and legitimate purposes;

3. **Data minimisation.** Data should be adequate, relevant and not excessive for those purposes;

4. **Accuracy.** Personal data shall be accurate and, where necessary, be kept up to date;

5. **Store limitation.** Data should not be kept for longer than is necessary for the original purpose for which it was obtained;

6. **Integrity and confidentiality.** Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7. **Accountability and governance**. The Commission must have in place appropriate technical and organisational measures able to demonstrate compliance with the UK GDPR.

Further Reading

Relevant provisions in the GDPR - see Article 5 and Recital 39

3. Statement

The Commission will comply with its obligations under UK GDPR and the UK Data Protection Act 2018 and any other relevant legislation. The Commission will ensure that it continues to treat personal information with due care and diligence.

4. Implementation

4.1. General

The Commission will:

- Establish and maintain an Information Asset Register with each identified asset having an owner who is accountable for safely managing assets in their domain.

- Ensure that there is an appropriately qualified Data Protection Officer (DPO) as required under GDPR.

- Fully observe conditions regarding the fair collection and use of information.

- Meet its legal obligations to specify the purposes for which information is used and establish the legal basis for the process in accordance with GDPR.

- Collect and process appropriate information, but only to the extent that it is needed to fulfil statutory responsibilities or operational needs.

- Ensure that information is of adequate quality.

- Control the length of time information is held in line with the Commission's, Records Management Policy (No. 39) and Business Classification Scheme with associated retention periods and in accordance with its approved Records Management Plan.

- Ensure that the rights of people about whom information is held can be fully exercised under GDPR. (website privacy policy). These include: the right to be informed that processing is being undertaken, the right of access to personal information, the right to prevent processing in certain circumstances and the right to rectify, block or erase information which is regarded by both parties as wrong information.

- Ensure that personal information is not transferred abroad without suitable safeguards.

- Take appropriate technical and organisational security measures to safeguard personal information.

- The Commission will elaborate Data Protection Impact assessment when introducing new IT/Communications system, when undertaking new projects or when reviewing existing ones.

- Ensure that the Commission only shares personal information with the relevant agents lawfully and securely by conducting risk assessment prior to sharing information further, following data sharing protocols and forms.

4.2. Organisational Issues

- The Commission will ensure that it complies with any directive from the ICO regarding the new registration process and pay the appropriate fee in accordance with guidance from the ICO.

- The Data Protection Officer for the Commission is the Information Governance Manager. Scrutiny for data protection at the Commission will be carried out by the Audit Risk and IG Committee. The Senior Information Risk Owner (SIRO) is the Head of Corporate Services who will delegate day-to-day responsibility for the operation of the Act/GDPR to the DPO/IG Manager.

- The Commission will observe the principles of the Caldicott Report and in particular will ensure that there is a nominated Caldicott Guardian. Guidance about the role and responsibilities of Caldicott Guardians is available from NHS Scotland Caldicott Guardians: principles into practice

  The Caldicott Guardian shall be the Chief Executive, except where the post-holder is not medically qualified, when the Executive Director (Medical) shall be nominated as Guardian.

- The Chief Executive is the accountable officer for data protection matters and is ultimately responsible for ensuring data protection practices are observed at the Commission

- The Chief Executive shall ensure that:

- Everyone managing and handling personal information understands their responsibilities and the need to follow good data protection practice and is appropriately trained to do so.

- Anyone wishing to make enquiries about handling personal information knows whom to approach.

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

- Methods of handling personal information are clearly described.

- The Commission will maintain a log of requests received for personal information (Subject Access Requests)

- The table below describes the required competency level for different staff.

Level of Competency	**Description of competency**	**Who covers that role at MWC**
Advanced knowledge and skills	Develops policy, procedures and practice in own organisation as it relates to information governance. Maintains own awareness of changes in legislation, case law, best practice, policy and guidance.	Information Governance Manager Caldicott Guardian
Intermediate level	Applies data protection principles and key legislation to own work role and work of others. Monitors compliance with policies/procedures	Practitioners Corporate Services Managers CWMs Executive
Foundation level	Understanding of data protection principles and awareness of key legislation and policy. Understanding of the need for secure and confidential information handling in relation to own work role. Awareness of sources of information, referral, advice and guidance (including local policies). Store, transport and transfer health records and other personal or other sensitive data securely and effectively.	All staff

4.3 Dealing with requests for personal information under the Act

Great caution should be exercised when processing Subject Access Requests (SARs) *(requests from individuals seeking access to the records we hold relating to them)*. Some best practice guidance is included at the end of this document and advice is available from the Information Governance Manager.

A living person (data subject) can apply for access to personal data processed by the Commission through a 'Subject Access Request'. Access to personal *health* information relating to deceased persons is governed by the Access to Health Records Act 1990. In certain circumstances, third parties can also apply for access to personal data about an individual, for example a solicitor acting for an individual or where a welfare guardian is empowered to do so under the terms of the guardianship.

See Annex for dealing with data subject access request.

Commission Policy & Procedures

Current versions of all relevant MWC policies and procedures can be found on the staff intranet or requested from the Information Governance and IT Manager

No 5 - IT Code of Conduct.

No 4 - IT Security Policy

No 17 - The Board Code of Conduct

No 39 - Records Management Policy

No 42 – Agile Working Guidance.

No 57 - Information Risk Management Policy

No 62 - Mobile Device Policy

No 66 - Data Breach Policy

The Commission has a privacy statement which explains more about data subject rights and how to make a request for personal information from the Commission (SAR form) (There is also a short film available from our website that explains some of the basic rights of data subjects under GDPR

External Guidance

1. Detailed advice on guidance on Records Management is available in the Records Management: NHS Code of Practice V2.1, published in January 2012 (this supersedes CEL 31).

http://www.scotland.gov.uk/Resource/Doc/366562/0124804.pdf

The Code is accompanied by a series of Guidance Notes, available at:

http://www.scotland.gov.uk/Publications/2010/04/NHS-record-management

2. The Commission's Records Management Plan, approved by the Keeper of National Records Scotland in 2014.

3. NHS Code of Practice on Protecting Patient Confidentiality is available at:

NHS Code of Practice for Protecting Patient Confidentiality

4. ICO Guidance on Access to information held in complaint files is available at:

https://ico.org.uk/media/1179/access_to_information_held_in_complaint_files.pdf

USEFUL WEBSITES

The UK Information Commissioner's Office: http://www.ico.gov.uk/

The British Medical Association: http://www.bma.org.uk

The General Medical Council: http://www.gmc-uk.org

NHS Inform – Includes links to useful leaflets about; consent, confidentiality and how to see health records. http://www.nhsinform.co.uk/rights/publications/leaflets/

Policy 29	Date	Summary of changes	Name
Issue 10	06/2020	Minor changes: Section 2 redrafted to make the principles easier to read. Obsolete hyperlinks updated	P.A
Issue 11	08/2021	Change GDPR to UK GDPR Update information about NCF Update link to SAR form available on the website (the form was reviewed in 2021 version) Update link to SAR letter templates reviewed in 2021.	P.A

ANNEX 1

HANDLING REQUESTS FOR PERSONAL DATA- general guidelines

The rights of data subjects are embedded in UK data protection legislation. The UK act is based on the provisions within GDPR. The new regulations strengthen data subject rights. Commission staff should always be aware of the strong rights of individuals to see the data we hold about them. This includes more formal documents as well as file notes and logs made of telephone calls or exchanges between professionals about the data subject.

We have **one month** to respond to a subject access request or SAR so time is of the essence. As soon as you receive a request for personal data, pass it to the appropriate Casework Manager or the Information Governance Manager.

As soon as Casework managers or the Information Governance Manager are aware of a request, they need to evaluate if it is a valid request.

Check list:

- Is there enough information to identify and ascertain the identity of the individual?
- Is there an appropriate proof of identity?
- Is there enough information to locate the information requested?
- Do we need to ask for a clarification?
- Is the signature of the data subject included, where request is being made by a representative?

Sending Subject Access Request Form

To ensure all the above, the best course of action is to send out the Commission Subject Access Request Form a Subject Access Form (SAR) and direct the data subject to the privacy statement and video on our website immediately. Send by e-mail where possible. Remember to add the Imps number as our reference.
[00 Initial letter.docx]

However, the form is not compulsory. If the written request has all the elements and the subject does not want to complete the form, we need to start processing the request.

Acknowledge the request and start processing it.

On receiving a complete SAR, the person handling the request should acknowledge it. The requester should be made aware of the timescales involved; we must respond within 1 month following receipt of a completed SAR and the appropriate proof of identity. If clarification of the request is required, until we have received any requested clarification.

[01 Acknowledge.docx]

Determine who will be handling the request. Information Governance Manager or Case Work Manager.

Log the request in IMP.

CWM to determine the level of administrative support needed.

Within 5 working days CWM with admin support must search for the requested information. Note that no information has been located; or make copies of the information requested; or note details of difficulties that have prevented progressing the request to either of the above two outcomes.

Serious harm test

Where required, we should send a letter to an appropriate professional[1], *(in the majority of cases this will be a medical person/psychiatrist- RMO)* to elicit opinion about any potential physical and/or mental harm that will be caused if the data concerned is shared with the data subject.

Prepare 'serious harm test' letter for RMO (medical person/psychiatrist) within 7 working days, where appropriate.

[03 Harm Test letter.docx]

Where the data on file is historical, MWC medically qualified people can be asked to undertake the harm test or it can be referred to a senior person at the NHS Board concerned and ask them to allocate it to an appropriate individual in their organisation.

You should prepare a table listing the documents to be assessed so that the person making the decision can record the rationale behind each decision. In most cases decisions which involve application of exemptions or redaction will be made by the IG Manager in consultation with an appropriate member of the Executive Team

On receipt of signed RMO response to serious harm test, make a record of date received (IMP).

Consider contacting the Ward Health Records department/manager if there are any issues in contacting the RMO.

Third Party

Where data contains references to 3rd parties you can either; seek to obtain explicit consent from the 3rd party or, where this is impractical, withhold the data or release it in a redacted format such that the 3rd party cannot be identified from the data released. Explicit consent means that the 3rd party has seen the data we intend to release and has indicated in writing that they are content with it being released.

[05 Third party consent.docx]

Remember permission is not necessary for any health professionals, or 'relevant persons'.
On receipt of signed third parties request, make a record of date received on IMPS.
In some instances, as a matter of courtesy, we should send a copy of the data/information we are considering for release to the author of the document(s). This could be a social worker,

[1] DPA 2018. Schedule 2. Part 2. Full text at the end of this document

doctor or other person. They must understand that we have a duty to release the data to the data subject unless there is a valid exemption and cannot withhold data only based on objections raised by them. We are alerting them to the fact that we will be releasing the data, subject to any valid, legal exemptions we feel apply.

When seeking consent to disclose third party information, only send the minimum necessary personal information relating to the data subject.

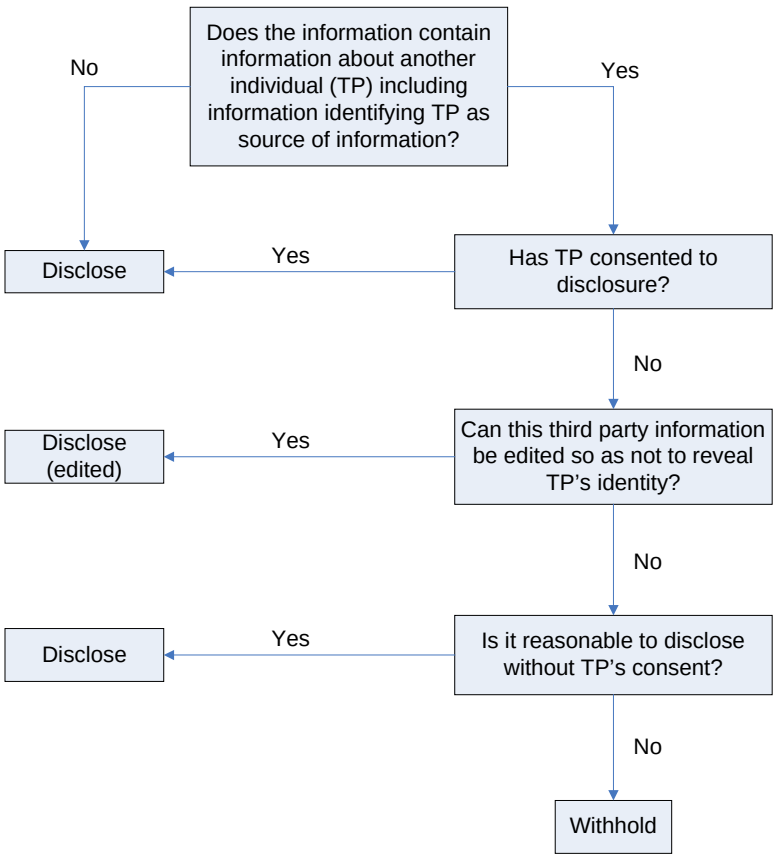
When asking for third party consent, remember to block out/remove the names of other non-health professionals in relation to health records (see definition), and non-relevant persons in relation to social work records (see definitions).

Reasonableness Test

In deciding whether it is reasonable to comply with the request without the consent of the third party the following must be considered:

- whether a duty of confidence is owed to the third party (e.g. health professional/patient, lawyer/client)
- what steps have been taken to get the third party's permission
- whether the third party is capable of giving consent
- whether the third party has expressly refused consent
- whether the information is of particular importance to the Data Subject*

*The European Court of Human Rights has ruled that in certain circumstances access to data including third party data is so important to the Data Subject that their rights over-ride the third party's right to confidentiality.



[04 Third party courtesy.docx]

Preparing the response

Always keep a list of what has been sent out to the requester. The list can destroyed after 3 months if there is no follow up to the SAR. If we are challenged on items we have, for example, redacted, we need to keep a record of redactions marking it clearly as a redacted version of an existing document.

Review the documents with the DPO. Check if any other exceptions apply.

When responding to the requestor, the letter sent should either state that all of the data we hold about them has been released and nothing has been withheld or redacted or we should give details of the exemptions we have applied where data has been withheld or redacted.

CWMs should seek advice from the Information Governance Manager if they are unclear about what action they need to take in relation to a request for personal information, especially if the request is a tricky or voluminous request or where there may be questions about whether a release of personal data is lawful.

[Template: 02 response.docx]

Sending the data

See Commission's Information Risk Policy (No 57) for guidance on sending personal, sensitive data. Data/information/files sent by post should be **double wrapped** and the internal package should state clearly that the contents are for the addressee only and should be returned to us if undelivered or if delivered and/or opened by anyone else apart from the addressee. Data should be sent by registered mail or courier depending on the sensitivity or time constraints involved.

Update the information to IMPS

It is the responsibility of the person who processed the SAR to keep a log of requests. There is an IMP form where details of requests can be recorded and used to report on SARs

DPA 2018. SCHEDULE 3.
EXEMPTIONS FROM THE GDPR: HEALTH, SOCIAL WORK EDUCATION AND CHILD ABUSE DATA

PART 2

Definitions
2(1)In this Part of this Schedule—
"the appropriate health professional", in relation to a question as to whether the serious harm test is met with respect to data concerning health, means—
(a)
the health professional who is currently or was most recently responsible for the diagnosis, care or treatment of the data subject in connection with the matters to which the data relates,
(b)

where there is more than one such health professional, the health professional who is the most suitable to provide an opinion on the question, or

(c)

a health professional who has the necessary experience and qualifications to provide an opinion on the question, where—

(i)

there is no health professional available falling within paragraph (a) or (b), or

(ii)

the controller is the Secretary of State and data is processed in connection with the exercise of the functions conferred on the Secretary of State by or under the Child Support Act 1991 and the Child Support Act 1995, or the Secretary of State's functions in relation to social security or war pensions, or

(iii)

the controller is the Department for Communities in Northern Ireland and data is processed in connection with the exercise of the functions conferred on the Department by or under the Child Support (Northern Ireland) Order 1991 (S.I. 1991/2628 (N.I. 23)) and the Child Support (Northern Ireland) Order 1995 (S.I. 1995/2702 (N.I. 13));

- "war pension" has the same meaning as in section 25 of the Social Security Act 1989 (establishment and functions of war pensions committees).

(2)For the purposes of this Part of this Schedule, the "serious harm test" is met with respect to data concerning health if the application of Article 15 of the GDPR to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

Exemption from Article 15 of the GDPR: serious harm

5(1)Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to data concerning health to the extent that the serious harm test is met with respect to the data.

(2)A controller who is not a health professional may not rely on sub-paragraph (1) to withhold data concerning health unless the controller has obtained an opinion from the person who appears to the controller to be the appropriate health professional to the effect that the serious harm test is met with respect to the data.

(3)An opinion does not count for the purposes of sub-paragraph (2) if—

(a)it was obtained before the beginning of the relevant period, or

(b)it was obtained during that period but it is reasonable in all the circumstances to re-consult the appropriate health professional.

(4)In this paragraph, "the relevant period" means the period of 6 months ending with the day on which the opinion would be relied on