Liaison Agreement between the Mental Welfare Commission for Scotland and the Health and Safety Executive

March 2022

Liaison agreement between the Mental Welfare Commission for Scotland (MWC) and the Health and Safety Executive (HSE) in relation to the sharing of information

1 Purpose of this agreement

1.1 This agreement is intended to promote an effective working relationship and information sharing protocol between the Mental Welfare Commission for Scotland (MWC) and the Health and Safety Executive (HSE) in Scotland on areas of mutual interest.

2 Responsibilities

2.1 MWC has duties set out under the Mental Health (Care and Treatment) (Scotland) Act 2003 and the Adults with Incapacity Act (Scotland) 2000. It acts to promote the welfare of individuals with mental illness, learning disability or related conditions. It investigates cases where it appears that there may be ill treatment, deficiency in care and treatment or improper detention of any such person. Following investigations, MWC can make and follow up on recommendations made and this can include recommendations for statutory authorities.

2.2 HSE and local authorities are responsible for enforcing the Health and Safety at Work etc Act 1974 (HSWA) and associated legislation throughout Great Britain. As a GB-wide regulator, HSE aims to reduce death, injury and ill-health by securing the health, safety and welfare of workers and protecting others, such as patients or service users, who may be affected by work activities. Whilst HSE leads on the health and safety of employees, it may also consider investigation of patient or service user deaths or serious injuries, where there is an indication that a breach of health and safety law was a probable cause or a significant contributory factor. However, where other regulators[1] have more specific legislation they will consider when they are better placed to secure justice or necessary improvements in standards.

2.3 Where appropriate, HSE may issue a notification of contravention of the law, a notice of improvement or prohibition, and report the outcomes of its investigations to the Crown Office and Procurator Fiscal Service (COPFS), who decide whether or not to initiate criminal proceedings and who to prosecute. When HSE investigates work-related deaths, it works closely with the police, in accordance with the Scottish Work-related Deaths Protocol, as agreed by COPFS, who investigate all deaths in Scotland.

3 Co-operation to support statutory investigations

3.1 HSE agrees to consult MWC to obtain advice and guidance in areas of MWC's expertise on such matters that may support its investigations under HSWA, for example, of deaths by suicide.

3.2 MWC agrees to provide HSE with specialist advice on mental health and incapacity legislation and standards for the care and treatment of people with mental illness, learning disability and related conditions that may be relevant to HSE's investigations under HSWA.

3.3 MWC advice will be provided on the basis of specialist evidence (e.g. a statement or report) intended to assist HSE to carry out its functions. MWC will not provide legal advice or replace HSE seeking independent expert advice where that may be necessary. Where

[1] *E.g. the Care Inspectorate, the General Medical Council, the Nursing and Midwifery Council, etc.*

there is the potential for a conflict of interest to arise e.g. where MWC has prior involvement in a case, HSE may seek advice from COPFS.

3.4 For more serious or complex investigations, consideration should be given to holding an early meeting involving all interested parties (e.g. the police, COPFS, HSE, MWC)

4 Information Sharing

(i) Additional Information

4.1 HSE may seek information held by MWC on individual cases brought to its attention[2]. The majority of cases will be in connection with deceased individuals (deaths mainly due to suicide). However, on rare occasions, the information requested may relate to a living individual HSE will need to submit its request for information in writing by completing the data sharing form [Addendum] and will be considered by MWC under the General Data Protection Regulations the Data Protection Act, on a case by case basis.

4.2 MWC may seek information on the outcomes of HSE investigations once legal proceedings have been concluded. HSE will provide this information under the terms of, the Data Protection Act and the General Data Protection Regulations. HSE would prefer these requests in writing, where possible. From time to time, HSE will provide MWC with anonymised information on cases that fall within MWC's areas of interest.

4.3 Disclosure of information by MWC to HSE or vice versa must always follow the established laws and procedures. Annex 1 sets out the data controller declaration for both organisations. Annex 2 sets out the preferred form for requesting data from MWC.

4.4 The following links provide the relevant privacy statement for each organisation:

MWC - About your personal information | Mental Welfare Commission for Scotland & https://www.mwcscot.org.uk/sites/default/files/2021-09/privacy_statement_September2021_v2.pdf

HSE – Information Sharing Privacy Statement - http://www.hse.gov.uk/privacy.htm & https://www.hsl.gov.uk/privacy-notice

(ii) Matters of Concern

4.5 MWC may, on occasion, identify concerns about health and safety standards for patients, service users and/or employees within the services it visits. Where these might indicate systemic health and safety management failings, MWC should report the matter to the nominated HSE contact for HSE to consider appropriate action.

5 Communication

---

[2] *HSE is often informed of patient service user deaths, potentially caused by work, by COPFS. It receives information on work related injuries to patients/service users from RIDDOR, from complaints received or from other agencies, etc.*

5.1 There will be nominated points of contact in each organisation as follows:

Redacted from published version under the following exemptions:
FOI Act Section 40 / FOI (Scotland) Act Section 28 (personal information)

HSE	MWC
Health and Safety Executive Queen Elizabeth House 1 Sibbald Walk Edinburgh EH8 8FT	**Mental Welfare Commission for Scotland** Thistle House, 91 Haymarket Terrace Edinburgh EH12 5HE

6 Dispute Resolution

6.1 Where a dispute occurs, the staff from the respective organisations who have been involved should attempt to resolve the matter, involving line management as necessary. For ongoing disputes, the 'nominated contacts' will work together to affect a resolution.

7 Review

7.1 MWC and HSE will endeavour to ensure that the relevant staff in each organisation are made aware of this agreement and the working arrangements. The agreement will be reviewed every 3 years to ensure it remains relevant.

7.2 In addition every year MWC and HSE will discuss matters of mutual interest arising from their respective responsibilities and arrange face to face meetings if deemed appropriate.

Signed for MWC

Julie Paterson, Chief Executive, Mental Welfare Commission
Date: 28 March 2022

Signed for HSE

Iain Brodie, HSE Director for Scotland / Deputy Director, Field Operations Division
Date: 24 March 2022

Annex 1: Data Controller Declaration

Purpose

1. The purpose of this annex is to explain the respective roles that the Mental Welfare Commission (MWC) and HSE will play in managing the processing of personal data associated with the effective operation of this Liaison Agreement. MWC and HSE are considered independent controllers of the data collected, as both parties separately determine the means and purpose of processing personal data as part of the functions defined in the broader Liaison Agreement.

Data Protection

2. MWC and HSE will comply with all relevant provisions of the Data Protection Act 2018 (and the General Data Protection Regulation). MWC and HSE will act as independent data controllers, in respect of any personal data pursuant to this Liaison Agreement; they will only process such personal data to the extent defined in the relevant regulatory framework.
3. Both parties have functions prescribed by law and written in statute which are likely to provide a lawful basis for sharing personal, sensitive data - where sharing is necessary for the exercise of those functions, proportionate, and carried out in accordance with the rights of the data subjects (GDPR article 6.1 (e) and 9.2.g. DPA 2018 DPA Section 8 and Schedule 1. Part 2. 6 for the purpose of exercising a function conferred on a person by enactment or rule of law.

4. Neither MWC nor HSE will transfer any personal data it is processing outside of the European Economic Area, unless appropriate legal safeguards are in place, such as an adequacy decision or Model Contract Clauses.

5. MWC and HSE will ensure that they have appropriate technical and organisational procedures in place to protect any personal data they are processing. This includes any unauthorised or unlawful processing, and against any accidental disclosure, loss, destruction or damage. MWC will promptly inform HSE, and vice versa, of any unauthorised or unlawful processing, accidental disclosure, loss, destruction or damage to any such personal data. Both parties will also take reasonable steps to ensure the suitability of their staff having access to such personal data.

<u>Specific MWC responsibilities</u>

6. MWC has the following specific responsibilities:

    i. Carrying out any required Data Protection Impact Assessment for any element of business or process change.

    ii. Following MWC Data Security Guidance to ensure that the necessary measures are taken to protect personal data.

    iii. Ensuring MWC staff are appropriately trained in how to use and look after personal data and follow approved processes for data handling.

    iv. Ensuring MWC staff have appropriate security clearance to handle personal information collected as part of this process.

    v. Secure transfer of personal data to HSE as necessary for fulfilment of HSE's regulatory functions.

    vi. Responding to Data Subject Access Requests when and where required.

    vii. Reporting any data breaches within MWC to their Data Protection Officer and the ICO (where appropriate).

    viii. Maintaining any Article 30 processing records for data held on MWC systems

<u>Specific HSE Responsibilities</u>

7. HSE has the following specific responsibilities:

    i. Carrying out any required Data Protection Impact Assessment for any element of business or process change

    ii. Following HSE Data Security Guidance to ensure that the necessary measures are taken to protect personal data.

    iii. Ensuring HSE staff are appropriately trained in how to use and look after personal data and follow approved processes for data handling.

    iv. Ensuring HSE staff have appropriate security clearance to handle personal information collected as part of this process.

    v. Secure transfer of personal data to MWC as necessary for fulfilment of MWC's regulatory functions

    vi. Responding to Data Subject Access Requests when and where required in relation to personal data being processed as part of the regulatory function

vii. Reporting any data breaches to their Data Protection Officer and the ICO (where appropriate)

viii. Maintaining any Article 30 processing records for data held on HSE systems

Individual Rights

8. GDPR specifies new rights for individuals over the processing of their data. These rights, and the process an individual should follow when making a request, are listed in both MWC and HSE's privacy notice. Both parties should ensure they consult and comply fully with their respective privacy policies in the event of a Data Subject exercising any of their rights under data protection legislation.

9. In response to any subject access request, MWC or HSE will undertake a proportionate and reasonable search and respond within one month of the original request.

Data breach

10. MWC is responsible for reporting any breach occurring within their authority to their Data Protection Officer and the Scottish ICO (where appropriate). MWC will also inform HSE of the breach if there is any direct impact on their staff or wider interest.

11. HSE are responsible for reporting any data breaches within their Authority to their Data Protection Officer and ICO (where appropriate), as well as to MWC if there is any direct impact on their staff or wider interests.

12. Any personal data breach as defined by GDPR Article 4 (12) that meets the relevant threshold criteria will be reported to the relevant Information Commissioners' Office (ICO) within 72 hours of notification. This will include informing the affected data subject should the circumstances warrant it. The appropriate Data Protection Officer (see below) will be responsible for making the report, following consultation their Chief Executive Officer (CEO).

Data retention

13. MWC and HSE will retain personal data associated with the effective operation of this Liaison Agreement in accordance with their respective organisational disposal policies. Each party is responsible for ensuring appropriate technical and procedural functions are in place to ensure the secure and timely destruction of personal data.

Information Disclosure

14. Either party to this Liaison Agreement may receive a request for information from a member of the public or any other person under the various pieces of information disclosure legislation, i.e. UK General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (DPA), Environmental Information Regulations 2004 (EIRs), the Freedom of Information (Scotland) Act 2002 (FIOSA), and the Freedom of Information Act 2000 (FOIA).

15. The recipient party to any request for information is ultimately responsible for making the final decision on disclosure. All requests for information will be considered on case-by-case basis, and all resulting disclosures must be lawful. The default position for both parties is to disclose unless one or more absolute exemptions (as defined by the appropriate legislation) apply to a specific request. Where the recipient party wishes to apply a qualified exemption (as defined by the appropriate legislation) to all or part of a request, they must ensure this is validated by a documented public interest test.

16. If a party receives a request for information that has been supplied by the other party ("the information supplier"), the party that has received the request for information will consult the information supplier as early as possible and before any information is disclosed in response to the request to enable sufficient time for the views of the information supplier, including any objections to disclosure, to be taken into account when determining whether the information is to be disclosed or withheld.

17. If a party receives a request for information that it holds and knows or believes the information is held by the other party, the party that received the request will consult the other party as early as possible and before any information is disclosed in response to the request. The purpose of this consultation is to ensure that the party that received the request is able to share any concerns about information that might be disclosed to the requester, that the party holding the information is able to take those concerns fully into account in its decision-making, and that the parties can co-ordinate their handling of requests.

Data Protection Officers

The contact details of the Data Protection Officers are:

Mental Welfare Commission for Scotland	HSE
Data Protection Officer Mental Welfare Commission for Scotland Thistle House 91 Haymarket Terrace Edinburgh EH12 5HE email, to mwc.enquiries@nhs.scot	Data Protection Officer Health and Safety Executive 1.3 Redgrave Court Merton Road, Bootle Liverpool L20 7HS Email: Data.Protection@hse.gov.uk

Annex 2

Data sharing and the Mental Welfare Commission for Scotland (MWC)

Form to request personal data from MWC

In order for us to consider your request for the Commission (the data controller) to share personal, sensitive data with your organisation, we need you to complete this form. No data will be released until the completed form has been returned. Thank you.

<table>
<tr>
<td>A. Details about your organisation and the person who is requesting the data. (Principle 4)</td>
<td>Contact person for this request: name, address and title;

Senior person within your organisation who has specific responsibility for information governance: name, address and title;</td>
</tr>
<tr>
<td>B. Description of the data requested

(Principles 2 and 3)</td>
<td>Which identifiable data items are required? Please detail why these are required.
<table>
<tr><th>PID Required</th><th></th><th>Justification</th></tr>
<tr><td>CHI Number</td><td></td><td></td></tr>
<tr><td>Forename</td><td></td><td></td></tr>
<tr><td>Surname</td><td></td><td></td></tr>
<tr><td>DOB</td><td></td><td></td></tr>
<tr><td>Age</td><td></td><td></td></tr>
<tr><td>Gender</td><td></td><td></td></tr>
<tr><td>Address</td><td></td><td></td></tr>
<tr><td>Post code (full)</td><td></td><td></td></tr>
<tr><td>Post code (partial)</td><td></td><td></td></tr>
</table>
</td>
</tr>
</table>

	Clinical data - please specify		
	Mental Health Act (MHA) data- please specify		
	Criminal Procedures Act (CPA) data- please specify		
	Adults With Incapacity Act (AWI) data- please specify		
	Other - please specify		
C. Outline of the purpose for which the data will be used. (e.g. a specific project, monitoring - give details) (Principle 1)	Audit □ Research □ Service Improvement □ Other □ If other, please provide further details:		
D. A rationale for why anonymised data would not be sufficient to fulfil the purpose stipulated above. (Principle 2)			
E. Please provide a statement to confirm that the data supplied by us to you will not be further shared with			

anyone out with your organisation or used for any purpose beyond that stipulated on this form. (Principle 6)	
F. How would you envisage data being transferred between MWC and your organisation (this could be via encrypted e-mail nhs.net or.gsi accounts if this were a viable option) (Principle 5)	
G. Please give a statement of how data will be stored following disclosure. (e.g. provide assurances that data will be stored on a suitably encrypted device with adequate password protection and not be held on an unencrypted device and will not be transferred/stored in an unprotected format) (Principle 5)	
H. Please provide details of staff within your organisation who will have access to this data and indicate how your organisation ensures that staff accessing personal/sensitive	

data understand their responsibilities in relation to this data. (this could include details of staff training/induction as well as internal policies and/or published procedures) (Principle 4)	
I. Subject Access Rights under Data Protection. Please describe how you would deal with enquiries from Data Subjects about accessing data we had supplied to you (Principle 6)	
J. Please provide details of how individuals will be informed about how and why their confidential information will be used, for example, links to privacy notices or other types of engagement. (principle 8)	

RULES ON CONFIDENTIALITY, SECURITY AND RELEASE OF INFORMATION FOR USERS OF PERSONAL DATA FROM THE COMMISSION

1. Personal data held by The Mental Welfare Commission for Scotland have been notified to the UK Information Commissioner as required under the GDPR Data Protection Act 2018. Our registration number is: **Z9097121**

2. If the data received from the Commission are to be held on computer, the person who signs this form should have an appropriate notification with the Office of the Information Commissioner. Your data protection registration number should be entered below prior to the signature section. Whether stored on computer or otherwise, the signatory should be aware that the Data Protection Act 2018 requires that all personal data is processed fairly and lawfully and in accordance with the Data Protection Principals.

3. Data received from the Commission should not be divulged to any person whose name is not specified as a user of data as stipulated on this form. All users and co-users must understand their responsibilities in protecting data provided.

4. Proper safeguards should be applied in keeping the data secure and destroying it on completion of the work/project. Any misuse, loss or theft of the data should be notified immediately to the Commission. It should be marked for the attention of the Information Manager and sent to mwc.enquiries@nhs.scot Confidential data should not be sent via this e-mail account.

5. Statistics or results of research based on data received from the Commission should not be made available in a form which directly identifies individual data subjects or creates a risk of indirect identification. If you feel such a risk exists, you should contact the Information Manager at the Commission to discuss the risks prior to publication.

6. The information provided to you is derived from systems used by the Commission in carrying out its functions. Although there are robust quality assurance processes in place, the data may contain undetected inaccuracies.

Data Protection Public Register – The UK Information Commissioner's Office
Please give your registration number:

I/we the undersigned have read and understood the rules on confidentiality, security and release of information for users of personal data from the Commission.

Contact person for this request:
PRINT NAME
Signature: Date:

Senior person within your organisation who has specific responsibility for information governance:

PRINT NAME
Signature: Date:

All applications in the first instance should be made to:

Information Governance Manager
MWC, Thistle House, Edinburgh EH12 5HE

Caldicott Guardian for Mental Welfare Commission is:
Medical Director, MWC, Thistle House, Edinburgh EH12 5HE

The release of data as described above is:

approved/not approved

Caldicott Guardian ……Date …….

Appendix A
Caldicott Principles

Principle 1 – Justify the purpose(s)
Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 – Don't use patient-identifiable information unless it is absolutely necessary
Patient-identifiable information items should not be used unless there is no alternative.

Principle 3 – Use the minimum necessary patient-identifiable information
Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

Principle 4 – Access to patient-identifiable information should be on a strict need-to-know basis
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.

Principle 5 – Everyone should be aware of their responsibilities
Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Understand and comply with the law
Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

Principle 8- Inform patients and service users about how their confidential information is used.
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this.